

**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ  
ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ  
КАФЕДРА КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ**

**МАТЕРІАЛИ  
Всеукраїнської  
науково-практичної конференції**

# **КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ**



**21 жовтня 2016 року  
м. Одеса**

*Одеський державний університет внутрішніх справ  
«Кібербезпека в Україні: правові та організаційні питання»*

**Міністерство внутрішніх справ України**

**Одеський державний університет внутрішніх справ**

# **КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ**

**Матеріали**

**Всеукраїнської науково-практичної конференції**

**21 жовтня 2016 року**

Одеса  
ОДУВС  
2016

**УДК 343.9:004.7(477)**  
**ББК 67.51+67.408.135(4Ук)**  
**К 38**

Рекомендовано до друку рішенням кафедри кібербезпеки та інформаційного забезпечення  
Одеського державного університету внутрішніх справ  
(протокол № 4 від 03 листопада 2016 року)

**Всі матеріали надані в авторській редакції та виражають  
персональну позицію учасника конференції**

**Кібербезпека в Україні: правові та організаційні питання : матеріали всеукр. наук.-практ.  
К38 конф., м. Одеса, 21 жовтня 2016 р. – Одеса : ОДУВС, 2016. – 233 с.  
ISBN 678-717-7020**

У збірнику представлено стислий виклад доповідей і повідомлень, поданих на всеукраїнську науково-практичну конференцію «Кібербезпека в Україні: правові та організаційні питання», яка відбулася на базі кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ 21 жовтня 2016 року.

У матеріалах конференції приділено увагу актуальним теоретичним та практичним проблемам забезпечення інформаційної безпеки в Україні. Висвітлюється широкий спектр питань, пов'язаних з удосконаленням правового регулювання та адміністративно-правового забезпечення кібербезпеки в Україні. Розглянуто використання інформаційних систем та технологій в боротьбі з кіберзлочинністю та надано обґрунтовані рекомендації щодо вдосконалення підготовки персоналу для боротьби з кіберзлочинністю в Україні.

Матеріали всеукраїнської науково-практичної конференції адресовано вченим, працівникам правоохоронних органів, аспірантам (ад'юнктам), слухачам магістратури, студентам та курсантам вищих навчальних закладів.

**УДК 343.9:004.7(477)**  
**ББК 67.51+67.408.135(4Ук)**

ISBN 678-717-7020



Вступне слово  
ректора Одеського державного університету внутрішніх справ  
доктора юридичних наук, доцента  
**Катеринчука Івана Петровича**  
під час відкриття всеукраїнської науково-практичної конференції  
«Кібербезпека в Україні: правові та організаційні питання»  
21 жовтня 2016 року, м. Одеса

### **Шановні учасники конференції!**

*Я радий вітати Вас у стінах нашого навчального закладу. Сьогодні ми зібралися для обговорення досить важливої теми: «Кібербезпека в Україні: правові та організаційні питання», хоча Ви знаєте що це проблема не тільки України.*

*До цієї конференції ми готувалися відповідально, намагалися запросити науковців із навчальних закладів та наукових установ, що розташовані у різних куточках нашої держави, представників різних наукових шкіл і, напевно, різних наукових поглядів, підходів з тим, щоб найбільш комплексно відбувся діалог з організаційних та правових питань забезпечення кібербезпеки в Україні.*

*Сучасний світ майже не можливо уявити без інформаційно-телекомунікаційних технологій, які впливають на усі сфери життєдіяльності суспільства. Але, на жаль, інформаційно-телекомунікаційні технології використовуються і для вчинення злочинів, які є найбільш суспільно небезпечними.*

*Сьогодні в Україні з проявами кіберзлочинності стикаються у банківській, кредитно-фінансовій, соціальній, культурній, духовній та інших сферах суспільного життя. За різними оцінками фахівців, кіберзлочинність посідає п'яте місце після торгівлі зброєю, наркотиками, злочинами у банківській сфері та економіки.*

*Проблема боротьби з кіберзлочинністю сьогодні розглядається як одна з глобальних проблем сучасності, і потребує вирішення на міжнародному рівні.*

*На вітчизняному просторі, в системі Національної поліції створенні підрозділи по боротьбі з кіберзлочинністю, які, поки що, можна сказати знаходяться на стадії становлення та розвитку і потребують правового, організаційного, кадрового, матеріально-технічного та іншого забезпечення.*

*Ці та інші проблеми й визначили тему нашої конференції.*

*Упевнений, що за результатами роботи конференції нами будуть сформульовані слушні пропозиції по запобіганню і протидії кіберзлочинності в Україні.*

*Обговорювані на сьогоднішній конференції ідеї та рекомендації сприятимуть подальшому розвитку кібербезпеки в Україні, удосконаленню механізму використання інформаційних систем та технологій в боротьбі з кіберзлочинністю.*

*Шановні учасники конференції, бажаю усім творчого натхнення, жвавих та цікавих дискусій, плідної роботи.*

## **ПЛЕНАРНЕ ЗАСІДАННЯ**

### **Правоохоронні органи в боротьбі з кіберзлочинністю**

**Катеринчук Іван Петрович**

доктор юридичних наук, доцент  
ректор Одеського державного університету внутрішніх справ

Сучасний світ майже не можливо уявити без інформаційно-телекомунікаційних технологій, які впливають на усі сфери життєдіяльності суспільства як позитивному, так і негативному сенсі. На сьогодні злочини з використанням інформаційних технологій є однією з найдинамічніших груп суспільно небезпечних посягань.

Особливу занепокоєність викликає можливість розробки, застосування та розповсюдження інформаційної зброї, виникнення у зв'язку з цим інформаційних війн та кібертероризму, чий негативні наслідки майже не передбачувані. На сьогодні, в Україні з проявами кіберзлочинності стикаються, в першу чергу, у банківській, кредитно-фінансовій та інших сферах. За даними проведених досліджень, кіберзлочинність – це п'ятий за розмірами вид економічної злочинності в Україні після незаконного привласнення майна, корупції та хабарництва, недобросовісної конкуренції та маніпуляції з фінансовою звітністю.

Організація протидії цьому виду злочинності в Україні складалася тривалий час не досить ефективно що, в першу чергу, пов'язувалось з відсутністю необхідної законодавчої бази. Тому можна констатувати той факт, що раніше зазвичай не приділялося достатньої уваги цьому виду суспільно небезпечних злочинних діянь. І лише після того, коли, наприклад, матеріальні збитки від вищевказаних діянь досягли таких розмірів, що стали різко виділятися на загальному рівні збитків від загально кримінальної злочинності, прийшов час, коли на цьому новому злочинному явищі зосереджено увагу, зроблено акцент.

Діяльність правоохоронних органів, які ведуть боротьбу з кіберзлочинністю, характеризується специфічними завданнями, реалізація яких повинна забезпечити всебічність та об'єктивність їхніх висновків та рішень. До них, зокрема, належать:

- початок діяльності правоохоронних органів у кожному випадку повинен мати підстави – повідомлення про вчинення злочинів у сфері використання комп'ютерних технологій та комп'ютерної інформації, або іншого правопорушення, необхідність їхнього попередження чи розкриття;

- правоохоронну діяльність по боротьбі з кіберзлочинністю можуть здійснювати тільки особи, які перебувають на службі в правоохоронних органах, мають спеціальну, переважно юридичну, технічну або економічну освіту;

- рішення правоохоронних органів в усіх випадках реалізуються через заходи юридичного впливу, які базуються на законі і є такими, що відповідають обставинам вчинення дії (або бездіяльності), якими мотивується втручання цих органів. Порушення даної вимоги тягне за собою скасування прийнятого рішення, а іноді й відповідальності особи, яка його прийняла;

- правоохоронні органи здійснюють свою діяльність по боротьбі з кіберзлочинами тільки на основі закону у встановленій процесуальній формі. Будь-які довільні дії не припустимі, а порушення вимог закону, допущені у процесі правоохоронної діяльності, можуть кваліфікуватись як самостійне правопорушення, що тягне за собою дисциплінарну, адміністративну або кримінальну відповідальність;

- законні й обґрунтовані рішення, які приймаються правоохоронними органами, підлягають виконанню усіма посадовими особами та громадянами.

У науковій літературі боротьба зі злочинністю розглядається як першочергове загальнодержавне завдання, яке є складовою частиною діяльності органів державної влади і, насамперед, Національної поліції. Особливе місце в боротьбі зі злочинами, пов'язаними з протиправним використанням комп'ютерної інформації та комп'ютерних технологій, необхідно надати правоохоронним органам України і, особливо, Національній поліції.

Але розглянемо історію створення спецпідрозділів по боротьбі з кіберзлочинами спочатку. Правоохоронні органи технологічно розвинутих країн досить швидко усвідомили, наскільки

серйозними наслідками може обернутися для інформаційного світу комп'ютерна злочинність у разі відсутності відповідного реагування на неї. І тому у структурі поліцій світу почали з'являться спеціальні підрозділи по боротьбі з цим видом злочинності. З 1991 року при Генеральному секретаріаті Інтерполу діє Робоча Група з проблем комп'ютерної злочинності, яка приділяє особливу увагу питанням міжнародного співробітництва при розслідуванні кіберзлочинів. Також в багатьох країнах для боротьби з цим видом злочинності створені спеціалізовані підрозділи, які займаються виявленням, розслідуванням комп'ютерних злочинів та збором іншої інформації з цього питання на національному рівні. Саме такі спеціалізовані поліцейські підрозділи утворюють головне ядро сил протидії міжнародній комп'ютерній злочинності. Для взаємодії цих підрозділів, обміну оперативною інформацією між країнами 18 європейських країн, членів ООН, створили національні центральні пункти з проблем комп'ютерної злочинності.

В Україні на базі НЦБ Інтерполу створено Національний центральний консультативний пункт по проблемам комп'ютерної злочинності. Це надало можливості накопичити матеріал про законодавче регулювання та організаційний досвід боротьби з кіберзлочинністю в різних країнах, підготувати ряд аналітичних оглядів та публікацій з цих питань, ознайомити співробітників МВС, прокуратури, суду з цим новим для України видом злочинів, внести конкретні пропозиції по удосконаленню кримінального законодавства України [1, с. 286].

У Службі безпеки України функціонує Департамент спеціальних телекомунікаційних систем та захисту інформації. Нормативні акти СБУ потребують вмикання спеціальних ділянок захисту інформації у складі її підрозділів, органів та установ. Вони повинні захищати інформацію, яка обробляється відомчими автоматизованими системами від злочинних посягань. В ряді оперативних підрозділів СБУ утворено групи, які протидіють окремим видам кіберзлочинів.

В структурі ДСБЕЗ при МВС України в 2001 році були створені підрозділи по боротьбі з правопорушеннями у сфері інтелектуальної власності та високих технологій, одним із завдань котрих є боротьба із злочинами у галузі комп'ютерної інформації, електронних рахунків і телекомунікації.

5 листопада 2015 року була створена нова Кіберполіція, як структурний підрозділ Національної поліції. Як вказує Міністр МВС Арсен Аваков: «Кіберполіція – ваш захист у віртуальному просторі і не лише!» Відтепер, користуючись Інтернетом та його можливостями, ви зможете отримувати поліцейську допомогу в режимі реального часу [2].

Так, основна мета створення кіберполіції це - реформування та розвиток підрозділів МВС України, що забезпечить підготовку та функціонування висококваліфікованих фахівців в експертних, оперативних та слідчих підрозділах поліції, задіяних у протидії кіберзлочинності, та здатних застосовувати на високому професійному рівні новітні технології в оперативно-службовій діяльності.

Поетапне перетворення теперішньої моделі до новітнього органу правозахисного призначення, який за своїми технічними та професійними можливостями матиме змогу миттєвого реагування на кіберзлочини та кіберзагрози, а також, у відповідності до кращих світових стандартів проводитиме міжнародну співпрацю по знешкодженню транснаціональних злочинних угруповань у даній сфері.

До основних завдань кіберполіції відносять:

1. Реалізація державної політики у сфері протидії кіберзлочинності.
2. Протидія кіберзлочинам:

У сфері використання платіжних систем:

- скімінг (шимінг) – незаконне копіювання вмісту треків магнітної смуги (чіпів) банківських карток;

- кеш-трепінг – викрадення готівки з банкомату шляхом встановлення на шатер банкомату спеціальної утримуючої накладки;

- кардінг – незаконні фінансові операції з використанням платіжної картки або її реквізитів, що не ініційовані або не підтверджені її держателем;

- несанкціоноване списання коштів з банківських рахунків за допомогою систем дистанційного банківського обслуговування.

У сфері електронної комерції та господарської діяльності:

- фішинг – виманювання у користувачів Інтернету їх логінів та паролів до електронних гаманців, сервісів онлайн аукціонів, переказування або обміну валюти, тощо;

- онлайн шахрайство – заволодіння коштами громадян через інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку;

У сфері інтелектуальної власності:

- піратство – незаконне розповсюдження інтелектуальної власності в Інтернеті;

- кардшарінг – надання незаконного доступу до перегляду супутникового та кабельного TV;

У сфері інформаційної безпеки:

- соціальна інженерія – технологія управління людьми в Інтернет просторі;
  - мальваре – створення та розповсюдження вірусів і шкідливого програмного забезпечення;
  - протиправний контент – контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості і насильства;
  - рефайлінг – незаконна підміна телефонного трафіку.
3. Завчасне інформування населення про появу новітніх кіберзлочинів.
4. Впровадження програмних засобів для систематизації та аналізу інформації про кіберінциденти, кіберзагрози та кіберзлочини.
5. Реагування на запити закордонних партнерів, що надходять каналами Національної цілодобової мережі контактних пунктів.
6. Участь у підвищенні кваліфікації працівників поліції щодо застосування комп'ютерних технологій у протидії злочинності.
7. Участь у міжнародних операціях та співпраця в режимі реального часу. Забезпечення діяльності мережі контактних пунктів між 90 країнами світу.

Станом на 10 лютого 2016 року Міністр внутрішніх справ Арсен Аваков заявив, що реформа кіберполіції на даний час «пробуксовує». Він повідомив, що Управління кіберполіції знаходиться на завершальній стадії становлення [2].

Розглянувши основні засади протидії кіберзлочинності слід визначитися з напрямками та методами боротьби. Але визначити всі напрямки боротьби з даним видом злочинністю досить складно, що пов'язано з багатогранністю цього суспільно-небезпечного явища. Відзначимо лише два основні напрямки цієї боротьби.

До першого напрямку слід віднести запобігання кіберзлочинам, що передбачає: створення, сертифікацію, ліцензування і впровадження необхідних засобів технічного і програмного захисту інформації; створення спеціалізованих організаційних структур адміністрацій і служб комп'ютерної безпеки, завданням яких є забезпечення надійного функціонування засобів захисту, генерації ключів і паролів, їхньої роздачі, контролю використання, заміни і знищення; підготовку кваліфікованих кадрів для правоохоронних органів.

Другий напрямок боротьби з кіберзлочинністю включає виявлення і припинення кіберзлочинів. У стадії вирішення перебуває проблема організації ефективної взаємодії всіх суб'єктів протидії кіберзлочинності.

Множинність суб'єктів боротьби з кіберзлочинністю передбачає багаторівневу координацію їхньої діяльності. Фахівці вказують, що необхідний диференційний підхід до визначення задач, напрямків та оцінки результативності діяльності органів, які входять до загальної і спеціалізованої підсистеми боротьби зі злочинністю [3, с. 219]. При цьому важливе значення має їхня скоординована, узгоджена діяльність як між собою, так і всередині підсистем, наприклад між органами влади та управління, різними службами поліції.

Узагальнюючи вищезазначене, можна зробити висновок, що протидія кіберзлочинності складається з трьох напрямків діяльності: попередження кіберзлочинів, загальна організація боротьби з кіберзлочинністю та правоохоронна діяльність, спрямована саме на виявлення, припинення та розкриття кіберзлочинів, застосування заходів кримінальної відповідальності і покарання стосовно осіб, які вчинили кіберзлочин. Попереджувальна діяльність, як одна із форм боротьби зі злочинністю, передбачає як загальнодержавні заходи економічного, ідеологічного, правового і виховного характеру, так і спеціальні - організаційні, технічні, програмні та криптографічні заходи.

### **Література:**

1. Бандурка О.М. Інтерпол: Міжнародна організація кримінальної поліції: науково-практичний посібник. – Х.: Основа, 2003. - 324 с.
2. Кіберполіція (крок реформ) // Арсен Аваков. – Назва з екрана: <http://blogs.pravda.com.ua/authors/avakov/561a92c183c27/>
3. Курс кримінології: Загальна частина: Підручник / О.М. Джужа, П.П. Михайленко, О.Г. Кулик та ін.; За заг. ред. О.М. Джужи. – К.: Юрінком Інтер, 2001. – 352 с.

**Албул Сергій Володимирович**  
кандидат юридичних наук, доцент,

перший проректор Одеського державного університету внутрішніх справ

Україна сьогодні зіткнулася з невідомою досі агресією з боку РФ, яка отримала назву гібридно-месіанської війни [2, с. 16]. Ключову роль в цій війні Росія відводить телевізійним формам подачі інформації. Інформаційна кампанія є невід'ємною складовою агресії РФ в Україні. Тобто первинною є мета керівництва Росії ослабити Україну та залишити її у сфері свого безпосереднього впливу. Для цього використовується увесь наявний арсенал інструментів впливу: економічних, інформаційних, дипломатичних, військових, політичних тощо.

Інформаційні впливи на масову свідомість існували завжди. Як технологію його використовували ще шамани і жерці, коли вони намагалися «конструювати майбутнє» в тому чи іншому напрямку.

Інформаційна війна – це комунікативна технологія по впливу на інформацію та інформаційні системи супротивника з метою досягнення інформаційної переваги в інтересах національної стратегії, при одночасному захисті власної інформації і своїх інформаційних систем [4, с. 116]. Інформаційна чи комунікаційна компонента є однією з найважливіших складових загальної стратегії та не існує відокремлено від інших компонент [1, с. 4; 3, с. 237]. Це важливо для розуміння неможливості відокремлено «виграти інформаційну війну». Комунікації, інформаційна компонента є складовою політики, але вони не можуть замінити собою політику. На сьогоднішній день супротивник використовує широке коло комунікаційних та інформаційних методів та технологій, сповідуючи принцип «мета виправдовує засоби». Важливо, що російські спецслужби швидко адаптують для своїх цілей будь-який інструментарій: маркетингові (рекламні) ходи; соціальні мережі та чутки; вигадані постановочні сюжети тощо. Крім цього, чітко сегментується й аудиторія впливу: власні громадяни; громадяни України на окупованому Сході; громадяни неокупованої території України; іноземна аудиторія (яка, за можливості, також сегментується географічно) тощо.

Для дестабілізації ситуації РФ використовує усі доступні канали комунікації: телебачення, Інтернет, радіо, пресу, чутки, дипломатію, експертне середовище. Слід, на наш погляд, виділити сильні сторони такої кампанії, з тим, щоб враховувати їх у заходах протидії. До таких, сильних сторін можна віднести: глобальність та системність задуму; чітку централізовану виконавчу вертикаль; залучення значних матеріальних та людських ресурсів; високий рівень медіавиробництва; високий технологічний рівень; чудові навички маніпуляції емоціями та почуттями (психологічне супроводження).

Російська інформаційна війна проти України продемонструвала, що пропаганда може бути різновидом зброї «масового ураження», яка атакує людську психіку, позбавляючи мільйони здатності до об'єктивного і критичного мислення.

Засоби, що їх використовують в інформаційній війні, швидко прогресують. Сьогодні дослідники вже говорять про перехід від першого до другого покоління моделей інформаційної боротьби. При цьому засоби інформаційної боротьби першого покоління – це:

- у воєнний час або за умов «гібридної війни» – збройне придушення тих чи тих елементів інфраструктури державного та військового управління;

- одержання розвідувальної інформації через перехоплення інформаційних потоків, які сьогодні є вельми різноманітними;

- несанкціонований доступ до інформаційних ресурсів, їх фальсифікація чи викрадення;

- масове подання в інформаційних каналах та глобальних мережах дезінформації для впливу як на осіб, які приймають рішення, так і на населення з метою викликати паніку.

Інформаційна боротьба другого покоління включає більш глибинні процеси:

- створення атмосфери бездуховності й аморальності, негативного ставлення до культурної спадщини противника;

- маніпулювання свідомістю соціальних груп населення з метою створення політичної напруженості та хаосу;

- дестабілізація відносин між партіями й рухами для провокації конфліктів, недовіри, репресій проти опозиції;

- погіршення стану інформаційного забезпечення органів влади, провокування помилкових управлінських рішень;

- дезінформація населення про роботу державних органів, їх дискредитація;

- підрив міжнародного авторитету держави в очах урядів та населення інших країн;



• спотворення інформації про життєво важливі інтереси держави в політичній, економічній, оборонній та інших сферах.

Головним об'єктом ураження залишається людина, прихований вплив на яку здійснюється через її нервову систему та психіку, здебільшого на підсвідомому рівні. При цьому використовується подвійна психобіологічна природа інформації. Так, «комфортна» на рівні психобіологічного сприйняття інформація може спричинити шкоду на психосоціальному рівні чи навпаки, «цікава» - призвести до неусвідомлюваних психобіологічних негараздів, стимулюючи девіантну поведінку особи та руйнувати позитивні соціальні тенденції в суспільстві.

Цілеспрямований інформаційний вплив на населення передбачає пануюче становище суб'єкта інформаційної війни у всіх сферах життєдіяльності іншої держави: економічній, політичній, психологічній, релігійній, науково-технічній, мистецькій, а також міжнаціональних і міжнародних зв'язків. Зростання ефективності заходів безпосереднього підризу, зокрема інформаційної війни, досягається за рахунок встановлення контролю над інформаційним простором іноземної країни, точності та цілеспрямованості таких акцій з урахуванням необхідного обсягу та рівня достовірності інформації, що доводиться, ступеня диференціації населення за системами матеріальних і духовних цінностей, здатності адекватно сприймати відомості та реагувати на них, а також політичної, економічної, етнорелігійної та іншої ситуації в державі й регіоні.

На наш погляд, система контрзаходів передбачає, що одну глобальну задачу із протидії інформаційним загрозам слід поділити на менші підзадачі, виконання яких є абсолютно реалістичним. Такими під задачами виступають:

1) Правоохоронна діяльність із захисту демократичних засад держави. Сюди належить контррозвідувальна, оперативно-розшукова та процесуальна робота спрямована на фіксацію та руйнування системи поширення різноманітних закликів (незаконне захоплення влади, дії, направлені на зміну територіальної цілісності, міжнаціональна ворожнеча тощо). В умовах загострення загроз особливо важлива роль тут належить РНБО як органу, що координує діяльність правоохоронного та безпекового сектору держави та знаходиться під контролем Глави держави [4, с. 114]. Саме цей орган має усі потрібні організаційні важелі для об'єднання розрізнених зусиль відомств (Прокуратура, СБУ, МВС, фінансові органи) з протидії єдиній ворожій системі пропаганди.

2) Робота з контентом, тобто зі змістом інформації, яка формує картину світу для людини. Передбачає впровадження стимулюючих заходів для створення власного інформаційного продукту, зробленого на власному історичному досвіді, з урахуванням власних цінностей та характеристик.

3) Постійний розвиток власної інформаційної інфраструктури. Окремо необхідно підкреслити важливість зменшення залежності українського інформаційного простору від російського сегменту Інтернет: виведення України з під юрисдикції московських офісів Гугл, Фейсбук, тощо.

4) Реалізація «стратегічних комунікацій» системи влади. Фактично, це прямий обов'язок з інформування громадськості та форма звітності перед замовником-громадянином. Стратегічні комунікації передбачають чітко сформульовану мету та постійний пакет інформації на тему того, як ми досягаємо поставленої мети. Наразі за цим напрямом немає проблем у різних консультантах, а існують лише «підводні камені» в процесі узгодження позицій різних політичних сил.

Підсумовуючи викладене, слід зазначити, що протидія інформаційним загрозам в умовах антитерористичної операції має базуватися на наступному:

1. Протидію інформаційній агресії Росії організаційно доцільно здійснювати через інструментарій РНБО під єдиним керівництвом Глави держави.

2. Система включає як заходи з протидії протиправній діяльності, так і заходи зі стимулювання розвитку відповідних вітчизняних галузей. Протидія спрацьовує через притягнення до відповідальності та регуляторні заходи, стимулювання розвитку – через економічні та організаційні заходи.

3. Уся система повинна охоплюватись єдиним задумом, бути керованою та пов'язаною з громадянським суспільством за допомогою мережі стратегічних комунікацій.

### **Література:**

1. Албул С.В. Кримінальна розвідка як функція оперативно-розшукової діяльності: Європейський досвід та Українські перспективи // *EuropeanReformsBulletin: internationalscientificpeer-reviewedjournal: GrandDuchyofLuxembourg*. – 2015. – № 2. – Р. 2-6.

2. Березовець Т.В. Анексія: острів Крим. Хроніки «гібридної війни» / Т.В. Березовець. – Брайт Букс, 2015. – 584 с.

3. Захаров В.П. Інформаційна розвідка як перспективний напрям розвитку правоохоронної діяльності у боротьбі зі злочинністю / В.П. Захаров // *Вісник Львів. держ. ун-ту внутр. справ (юридична серія)*. – 2006. – № 2 – С. 236-242.

4. Словник ключових понять та аббревіатур сектору безпеки: англо-українсько-російський (на матеріалах інтернет-джерел) / Л.Ф. Компанцева, О.В. Акульшин, Н.Т. Акульшина, Т.О. Дедушкіна, Г.Ю. Зінченко, О.В. Завадська, І.О. Хома; за заг. ред. І.І. Мусієнка. – Х.: «Оберіг», 2014. – 428 с.

### **Адміністративно-правові заходи боротьби з кіберзлочинністю в Україні**

**Грохольський В.Л.**

доктор юридичних наук, професор,  
професор кафедри кібербезпеки  
та інформаційного забезпечення

Одеського державного університету внутрішніх справ

Інтеграція України до Європейського співтовариства, а ще краще до світового товариства, передбачає входження нашої держави до інформаційного суспільства, яке характеризується широким використанням переваг нових інформаційних технологій у всіх сферах виробництва, науки, культури, безпеки тощо.

В Україні, як і в інших державах світу, невпинно розвиваються якісно нові галузі економіки, що базуються передусім на використанні сучасних інформаційних технологій, локальних та глобальних комп'ютерних мереж, зокрема мережі Інтернет.

Наслідком розбудови інформаційного суспільства є те, що пропорційно розвитку інформаційних ресурсів зростає й кількість правопорушень з використанням комп'ютерних технологій. Наразі кіберзлочинність є однією з найбільш серйозних проблем багатьох держав, щорічні збитки від якої становлять мільярди доларів США.

Аналіз сучасних тенденцій розвитку нашої держави свідчить про те, що з'явилися нові загрози національній безпеці України – комп'ютерна злочинність та комп'ютерний тероризм.

Проблеми кіберзлочинності в контексті інформаційної безпеки як складової національної безпеки неодноразово розглядалися Верховною Радою України, Президентом України та Радою національної безпеки і оборони України, однак чітких і дієвих заходів протидії цим видам злочинів поки що не визначено.

Враховуючи вище викладене та інші обставини кіберзлочинності в Україні, вбачається за необхідне здійснити наступні кроки:

1. Криміногенна ситуація у сфері використання інформаційних технологій вимагає комплексного підходу як із боку правоохоронних органів, так і з боку інших зацікавлених відомств (органів). Але, сьогодні, на жаль, відсутня взаємодія між суб'єктами, які причетні до розробки комп'ютерних технологій і правоохоронними органами (підрозділами), які здійснюють боротьбу з кіберзлочинністю. На законодавчому рівні ще не створено умов, які б дозволяли ефективно взаємодіяти заради протидії кіберзлочинності.

2. Протидія злочинам у сфері використання інформаційних технологій вимагає якісного кадрового забезпечення. Адже зрозуміло, що не кожний працівник, наприклад, органів (підрозділів) Національної поліції у змозі виявляти і протидіяти особам, які вчиняють такі злочини. У зв'язку з цим, виникає проблема підбору і підготовки фахівців для протидії кіберзлочинності. На наш погляд, таких фахівців у навчальних закладах системи МВС України готувати досить складно, з різних причин, і це окрема тема. Але цю проблему необхідно вирішувати уже сьогодні. Тому вбачається за доцільне здійснювати відбір кадрів для боротьби з кіберзлочинністю, по-перше, - серед студентів-випускників вищих навчальних закладів, які готують фахівців для роботи у сфері інформаційних технологій, по-друге, - серед працівників, які уже працюють у сфері інформаційних технологій. Звичайно, слід враховувати, що висококваліфіковані фахівці такого напрямку не будуть працювати за 4-5 тис. грн. Тому, необхідно приваблювати таких фахівців як достойною зарплатою, так і соціальними пакетами, які у нашій державі ще не розроблені і не використовуються, наприклад, – пільгові кредити для придбання житла, автомобіля, меблів тощо, право виходу на пенсію за вислугою років і т. ін.

3. Основна проблема боротьби з кіберзлочинністю сьогодні полягає у тому, що розвиток законодавчої бази і реагування на всі проблеми боротьби з кіберзлочинністю поки що відстає від розвитку інформаційних технологій. А відтак, відсутності дієві правові механізми контролю, необхідні для правозастосування.

4. Слід звернути увагу на те, що, сьогодні, майже увесь світ обговорює проблему боротьби з кіберзлочинністю, і Україна визнала, що кіберзлочинність загрожує національній безпеці, але Стратегії

боротьби з цим явищем не вироблено. Тому, ми вважаємо за необхідне на державному рівні розробити і прийняти Програму боротьби з кіберзлочинністю в Україні.

5. Ефективна боротьба з кіберзлочинністю вимагає проведення низки досліджень з цих проблем. Враховуючи актуальність проблеми, доцільно було б такі дослідження здійснювати за участю і під егідою НАН України.

6. Потребують чіткого визначення завдання та функції підрозділів Національної поліції по боротьбі з кіберзлочинністю. Аналіз положень наказу Національної поліції України від 10.11.2015 р. № 85 «Про затвердження Положення про Департамент кіберполіції Національної поліції України» дає підстави говорити про те, що сьогодні на рівні центрального апарату Національної поліції не має чіткого бачення щодо шляхів боротьби з кіберзлочинністю. Тому, багато визначених функцій цих підрозділів носять поверховий і загальний характер, наприклад:

- в межах компетенції розробляє рекомендації для підвищення професійного рівня і поінформованості органів Національної поліції України, а також, громадськості про результати діяльності кіберполіції;

- відповідно до чинного законодавства створює та забезпечує функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні злочинів, пов'язаних з комп'ютерними системами та даними, переслідуванні осіб, що обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі;

- відповідно до чинного законодавства збирає, узагальнює, систематизує та аналізує інформацію про криміногенні процеси та стан боротьби зі злочинністю за напрямом діяльності Департаменту на загальнодержавному та регіональному рівнях, оцінює результати за окремими показниками службової діяльності, надає, відповідно до законодавства України, звіти про результати роботи та відповідну інформацію керівництву Національної поліції України, МВС, органів державної влади з питань попередження та протидії кіберзлочинам;

- забезпечує своєчасний розгляд звернень та запитів громадян, підприємств, установ, організацій з питань, віднесених до компетенції кіберполіції, контроль за належним дотриманням порядку їх прийняття, реєстрації, обліку і розгляду;

- сприяє правильному підбору, розстановці, навчанню та вихованню кадрів Департаменту та підпорядкованих йому підрозділів;

- здійснює інші повноваження відповідно до вимог чинного законодавства [1].

Що стосується останнього, то ми бачимо, що розробники Положення не досить чітко відділяють функції від повноважень. Хоча тут можна погодитись з тим, що функції визначаються виходячи з повноважень. Але головне, можливо і не в цьому. Саме головне, на мій погляд, полягає в тому, що в нормативно-правових актах, які регламентують діяльність цих підрозділів, не має чіткого визначення: що таке кіберзлочинність; її способи вчинення (з використанням високих інформаційних технологій – це не спосіб, а інструмент); в яких основних напрямках необхідно працювати (тому, що охопити усе не можливо, а зводити основну роботу до виявлення торгівлі піратськими дисками, то це могли б робити й дільничні інспектори) та інше.

### **Література:**

1. Про затвердження Положення про Департамент кіберполіції Національної поліції України : наказ Національної поліції України від 10.11.2015 р. № 85.

### **«Киберпреступление» или преступление в сфере использования информационных технологий?**

**Карчевский Н.В.**

доктор юридических наук, профессор  
проректор Луганского государственного  
университета внутренних дел имени Э.А. Дидоренко

Аннотация: предпринимается попытка определить понятие «преступление в сфере использования информационных технологий», рассмотреть его в контексте предложенных в науке уголовного права понятий «компьютерное преступление», «киберпреступление».

Ключевые слова: информатизация, преступление в сфере использования информационных технологий, компьютерное преступление, киберпреступление.

Количественный и качественный рост киберпреступности прямо пропорционален успехам компьютерных технологий и расширению сферы их применения. Первые упоминания о компьютерной технике в контексте нарушений уголовного законодательства относятся к 60-м годам прошлого столетия [8, с. 18]. В то время количество ЭВМ в мире исчислялось десятками тысяч (первая ЭВМ была построена в 1946 году). Преимущественно речь шла о физическом повреждении чрезвычайно дорогостоящих в то время электронно-вычислительных машин [5], а также совершении работниками крупных компаний (только такие могли позволить себе использование ЭВМ) хищений с помощью компьютеров [1, с. 10]. На территории бывшего СССР компьютерное преступление было впервые зарегистрировано в 1979 году в Вильнюсе. Оператор почтовой связи путем мошенничества с использованием автоматизированного программно-технического комплекса в течение двух лет совершала хищения денежных средств, направляемых соответствующими государственными органами гражданам в качестве пенсий и пособий по старости. Несовершенство программного обеспечения и наличие двойной бухгалтерии, ведущейся на различных (по форме представления информации) материальных носителях, позволили преступнице длительное время создавать излишки подотчетных денежных средств, изымать их из кассы и присваивать, а также уходить от ответственности [21]. Качественное изменение компьютерной преступности связано с развитием сетевых компьютерных технологий. К 1990 году большинство профессиональных пользователей компьютеров в США имели доступ к интернету, количество компьютеров, включённых в сеть, начало стремительно возрастать [2, с. 267]. Сегодня доступ к интернету имеет 34,3 % населения планеты [9], суммарные продажи персональных компьютеров и смартфонов в год оцениваются более чем в 2 миллиарда штук [3]. В таких условиях компьютерная преступность уже обосновано рассматривается как существенная угроза не только национального, но и международного уровня [11]. По мнению экспертов Организации по Безопасности и Сотрудничеству в Европе (ОБСЕ), преступность, связанная с использованием компьютерных систем и сетей, способна создать не меньший хаос, чем экономический кризис. Если в 2008 году вред, который ежегодно причиняет киберпреступность в мире, оценивался примерно в 100 млрд. долларов США [19], то по оценкам 2013 года этот показатель приблизился к одному триллиону [7].

Сказанное свидетельствует об актуальности проблем уголовно-правового регулирования в сфере информатизации. Одним из ключевых вопросов здесь является определение понятий «преступление в сфере использования информационных технологий», «компьютерное преступление», «киберпреступление» и т.д. Попытка ответить на данный вопрос и является целью данной статьи.

Прежде всего уточним содержание понятия «преступление в сфере использования информационных технологий». Обеспечение уголовно-правового стимулирования положительных и минимизации негативных социальных последствий информатизации, предполагает определение в качестве самостоятельного объекта уголовно-правовой охраны системы общественных отношений, обеспечивающих реализацию информационной потребности. Для обозначения этой системы предлагается использовать термин «информационная безопасность», ее структуру составляют отношения в сфере формирования информационного ресурса, обеспечения доступа к информации, а также отношения в сфере использования информационных технологий. При этом социальная значимость отношений информационной безопасности, а следовательно и целесообразность их уголовно-правовой охраны, определяются значимостью тех отношений, в пределах которых возникает информационная потребность [18]. В свою очередь, информационная технология представляет собой организованную совокупность информационных процессов с использованием средств вычислительной техники, которые обеспечивают высокую скорость обработки данных, быстрый поиск информации, передачу данных, доступ к источникам информации независимо от места их расположения [18]. Таким образом, преступления в сфере использования информационных технологий, являясь одним из видов преступлений в сфере информационной безопасности, представляют собой предусмотренные законодательством об уголовной ответственности, общественно опасные, виновные, совершенные субъектом преступления деяния, причиняющие вред обеспеченным средствами вычислительной техники отношениям в сфере реализации информационной потребности. Анализ действующего УК позволяет прийти к выводу, что к таким преступлениям следует относить посягательства, предусмотренные ст. ст. 361, 361-1, 361-2, 362, 363, 363-1, 376-1 УК.

Наряду с предлагаемым понятием («преступление в сфере использования информационных технологий») в уголовно-правовом дискурсе достаточно активно используются следующие: «компьютерное преступление», «киберпреступление», «интернет-преступление» и т.д. Объем данных понятий определяется по-разному. Тем не менее, наиболее распространенным является отнесение к компьютерным преступлениям всех общественно опасных посягательств, при совершении которых

компьютеры используются как технические средства [12, с. 11; 17, с. 14; 22, с. 243; 15, с. 35-40; 10, с. 72; 13, с. 65; 20, с. 87; 27, с. 55-57].

Появление термина «киберпреступление» связывают с расширением технической базы информатизации. В частности отмечается, что вследствие широкого распространения так называемых «коммуникаторов» и «смартфонов», сочетающих в себе свойства мобильных телефонов и компьютеров, термин «компьютерное» преступление в буквальном понимании, перестал охватывать весь спектр общественно опасных деяний в сфере применения информационных технологий. Это, по мнению некоторых исследователей, свидетельствует о необходимости введения в научный оборот термина «киберпреступление» [28, с. 32-33]. В частности, Т.Л. Тропина предлагает определять киберпреступление как «виновно совершенное общественно опасное уголовно наказуемое вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные противоправные общественно опасные деяния, совершенные с помощью или посредством компьютеров, компьютерных сетей и программ, а также с помощью или посредством иных устройств доступа к моделируемому с помощью компьютера информационному пространству» [28, с. 38]. Здесь следует обратить внимание на то, что нормативные определения вычислительной машины и электронно-вычислительной машины не позволяют толковать понятие «компьютер» настолько ограничительно [26; 25]. Понятием ЭВМ полностью охватываются как современные устройства мобильной связи так и любые другие устройства, представляющие собой «совокупность технических средств, создающую возможность проведения обработки информации и получение результата в необходимой форме, основные функциональные устройства которой выполнены на электронных компонентах» [26]. Таким образом, понятия «компьютерное преступление» и «киберпреступление»<sup>1</sup> можно рассматривать как тождественные.

Данный вывод подтверждается и анализом зарубежных источников. Так, на Десятом конгрессе Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями (Вена, апрель 2000 года) киберпреступления рассматривались как любые преступления, которые могут совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети. При этом отмечалось, что существуют две категории киберпреступлений:

а) киберпреступление в узком смысле ("компьютерное преступление"): любое противоправное деяние, осуществляемое посредством электронных операций, целью которого является преодоление защиты компьютерных систем и обрабатываемых ими данных;

б) киберпреступление в широком смысле ("преступление, связанное с использованием компьютеров"): любое противоправное деяние, совершаемое посредством или в связи с компьютерной системой или сетью, включая такие преступления, как незаконное хранение, предложение или распространение информации посредством компьютерной системы или сети [23].

Изложенный подход используется и на уровне научных исследований [6]. Yvonne Jewkes определяет киберпреступления (cybercrimes) как противоправные деяния совершенные с использованием или посредством компьютеров, компьютерных сетей, Интернет, сетевых информационных или коммуникационных технологий [4]. Susann W. Brenner рассматривает три категории киберпреступлений: преступления, в которых компьютер является целью преступления, преступления в которых компьютер используется в качестве средства совершения преступления, а также преступления, в которых компьютер играет незначительную роль в совершении преступления (crimes in which a computer plays an incidental role in the commission of the offense). В качестве примера преступлений третьей группы автор приводит преступление, совершенное Melanie McGuire. В 2007 году последняя была осуждена за убийство мужа. По данным прокуратуры, обвиняемая использовала сильнодействующее снотворное чтобы усыпить потерпевшего, несколько раз выстрелила в него, расчленила труп и скрыла останки в водоеме. После обнаружения останков, работники полиции обнаружили в компьютере обвиняемой следы, свидетельствующие об осуществлении поиска в интернет по темам «совершение убийства», «незаконное приобретение оружия», «яды». Также была

---

<sup>1</sup>Необходимо отметить, что в науке также высказывались предложения понимать под киберпреступлениями преступления, совершаемых в так называемом «киберпространстве». Следует отметить, что применение категории «киберпространство» в уголовно-правовом контексте, тем более на уровне определений, нам представляется нецелесообразным. Очевидно, что определяемая им информационная среда не может рассматриваться как вид некоего пространства, территории в классическом юридическом смысле. Поэтому, попытка описывать при помощи данного термина новый вид преступлений или особенности юрисдикции скорее всего не будет результативной, создаст путаницу, лишние терминологические и концептуальные сложности.



обнаружена электронная переписка («romantic e-mails») обвиняемой и ее начальника. В ходе судебного рассмотрения дела прокуроры использовали «компьютерные доказательства» для обоснования того, что у обвиняемой был мотив для убийства мужа, и ею исследовались методы совершения убийства, в том числе методы, использованные при совершении преступления [1].

В целом, приведенное определение киберпреступлений является практически общепризнанным в зарубежной научной литературе, а также достаточно широко представлено в отечественной. Тут необходимо отметить, что зарубежный опыт несомненно должен изучаться и быть использованным. В тоже время, безоглядный перенос западных стандартов регулирования политических, экономических и социальных процессов без учета исторических и национальных особенностей далеко не всегда приводит к положительным результатам. Представляется, что в случае с определением компьютерных преступлений и использованием данного понятия в отечественном уголовно-правовом дискурсе имеет место как раз такая ситуация.

При описанном понимании, любое преступление, совершенное с использованием компьютерной техники (мошенничество, шпионаж, незаконное распространение наркотических средств и т.д.), должно считаться компьютерным. Хотя абсолютно очевидно, что вышеперечисленные общественно опасные деяния не являются преступлениями нового вида. Такие действия, несмотря на использование для их совершения компьютерной техники, остаются государственной изменой, шпионажем, кражей, мошенничеством, незаконным сбором сведений, которые составляют коммерческую тайну и т.д. Средство не меняет сути преступления. Недостатком данного подхода является его несоответствие основному принципу структурирования национального законодательства об уголовной ответственности – систематизации уголовных законов на основе классификации посягательств по объекту. Определение новой группы преступлений всегда должно производиться на основе признаков, характеризующих объект посягательства. Именно поэтому в пределах национального уголовно-правового дискурса необоснованным следует считать определение группы преступлений на основе признаков, характеризующих способ, орудие или средство посягательства. Об этом достаточно красноречиво свидетельствует приведенный ранее пример отнесения к числу киберпреступлений конкретного умышленного убийства на том основании, что получение доказательств осуществлялось путем исследования компьютера обвиняемой.

Уместным будет и следующий пример. Как известно, изготовление поддельных денежных купюр с помощью современных печатающих устройств, несмотря на повышение общественной опасности, не изменило квалификации этих действий: виновные привлекались и продолжают привлекаться к уголовной ответственности по статьям о фальшивомонетничестве, так же как и те, кто использовал для подделки фототехнику или обычные карандаши, краски и лезвие бритвы. Компьютерная техника позволяет до совершенства довести процесс изготовления поддельных документов: перенесенные с оригинала печати, подписи, другие реквизиты практически идентичны. Для установления подделки будет необходимо проведение высококвалифицированной криминалистической экспертизы, но это не означает, что такого рода подделки документов требуют особой, отличной от существующей квалификации. Вывод может быть только один: модификация орудий и средств совершения преступления, использование с этой целью достижений научно-технического прогресса не меняет тех отношений, на которые оно посягает, не свидетельствует о появлении преступлений нового вида.

Сказанное вовсе не означает, что расширение сферы применения компьютерных технологий не привело к появлению преступлений нового вида, как, например, считает Ю. Батурин. По его мнению, компьютерных преступлений как особой группы преступлений в юридическом смысле не существует. Несомненная модификация традиционных преступлений позволяет говорить лишь о компьютерных аспектах преступлений, не выделяя их в обособленную группу [12]. С такой позицией трудно согласиться, далеко не всегда общественно опасное посягательство, совершенное с использованием компьютерной техники, можно рассматривать как традиционное преступление, усложненное применением новых средств. Как быть, например, с квалификацией распределенной атаки отказа от обслуживания, совершенной с использованием бот-сети? В терминах какого из традиционных преступлений можно описать незаконные множественные рассылки электронных сообщений (спам)?

Вместе с тем, следует признать, что определение компьютерных преступлений как группы посягательств, характеризующейся общими признаками способа, орудия или средства, может быть востребовано. Речь идет об установлении особенностей методики раскрытия или расследования преступлений, специфики фиксации следов и т.д. Можно частично согласиться с В.В. Веховым, который предлагает давать различные определения компьютерных преступлений с точки зрения уголовно-правовой охраны и с точки зрения криминалистической. Очевидно, что именно последнюю группу можно определять как деяния, в которых компьютер является предметом, орудием или

средством совершения преступления. Такая группа безусловно имеет значение для криминалистики. Однако применять такой же термин, но с другим определением в уголовном праве представляется ошибочным. Использование термина, имеющего скорее криминалистическое значение, в пределах уголовно-правового дискурса приведет к путанице и неопределенности. Данный подход обусловит сложности в четком определении предметов соответствующих научных исследований.

Кроме того, одной из очевидных тенденций современной преступности является рост числа традиционных преступлений, совершаемых с использованием компьютерной техники. Так, например, исследование, проведенное в Великобритании, показало, что четыре из пяти ограблений совершаются при помощи Twitter и Facebook [29]. В таких условиях, использование критикуемого подхода приведет к искажению и утрате информативности данных официальной статистики. Группа «компьютерные преступления» будет разрастаться, складываться из самых разнообразных посягательств (от блокирования сайтов организаций до торговли оружием и наркотиками). В конце концов, подобные статистические данные потеряют актуальность для решения задач противодействия преступности.

Таким образом, уместное в пределах зарубежного уголовно-правового дискурса определение компьютерных преступлений имеет весьма ограниченную ценность для национальной науки уголовного права. Как известно, в зарубежной уголовно-правовой доктрине материально-правовые проблемы рассматриваются в неразрывной связи с процессуальными. В таких условиях критикуемый подход к определению компьютерных преступлений имеет смысл и несомненно оправдан. В свою очередь, попытка исследования проблем национального уголовно-правового отражения тенденций информатизации на основе такого же подхода, как представляется, не имеет перспективы.

Понятия «компьютерное преступление» и «киберпреступление», в общепризнанном понимании, могут быть эффективно использованы при проведении криминологических, уголовно-процессуальных, криминалистических<sup>2</sup> исследований. Что же касается национального уголовно-правового дискурса, то здесь их применение следует ограничить, и использовать предложенное понятие «преступление в сфере использования информационных технологий».

#### **Литература:**

1. Brenner S. Cybercrime : criminal threats from cyberspace / Susan W. Brenner. – Praeger, 2006.–281 p.
2. Campbell-Kelly M., Aspray W. Computer: A History Of The Information Machine [Second Edition] / Martin Campbell-Kelly, William Aspray. - Westview Press : 2004. – 325 p.
3. Gartner: Планшеты и смартфоны продолжают вытеснять настольные компьютеры [Электронный ресурс] // Новости сайта «Открытые системы». - 25.06.2013. – Режим доступа : <http://www.osp.ru/news/2013/0625/13019543/>
4. Jewkes Y. Cybercrimes / Yvonne Jewkes // The Sage Dictionary of Criminology. Compiled and edited by Eugene McLaughlin, John Muncie. Third Edition. - Sage Publications, 2013. – 536 p.
5. Kabay M. E. A Brief History of Computer Crime: An Introduction for Students [Electronic resource] / M. E. Kabay // Personal Site of M. E. Kabay, PhD— Mode of access: [www.mekabay.com/overviews/history.pdf](http://www.mekabay.com/overviews/history.pdf)
6. Leukfeldt R., Veenstra S., Stol W. High Volume Cyber Crime and the Organization of the Police: The results of two empirical studies in the Netherlands [Electronic resource]/ Rutger Leukfeldt, Sander Veenstra, Wouter Stol // International Journal of Cyber Criminology. Vol. 7 Issue 1 January - June 2013. – Mode of access: <http://www.cybercrimejournal.com/Leukfeldtetal2013janijcc.pdf>
7. Lewis A., Baker S. The Economic Impact of Cybercrime and Cyber Espionage. Report, July 2013 [Electronic resource] / James Andrew Lewis, Stewart Baker // Center for Strategic and International Studies (CSIS). – Mode of access: <http://csis.org/publication/economic-impact-cybercrime-and-cyber-espionage>
8. Sieber U. Legal Aspects of Computer-Related Crime in the Information Society / Ulrich Sieber. - Brussels, Belgium : European Commission, 1998. – 239 p.

---

<sup>2</sup>Примечательно, что в отечественной юридической науке термин «компьютерные преступления» первоначально применялся именно в криминалистическом контексте. В марте 1993 года в НИИ проблем укрепления законности и правопорядка при Генеральной прокуратуре РФ на заседании межведомственного семинара на тему «Криминалистика и компьютерная преступность» было отмечено, что термин компьютерная преступность, уже воспринятый как отечественной, так и зарубежной литературой, имеет право на существование. Компьютерными преступлениями предлагалось именовать те предусмотренные уголовным законом общественно опасные деяния, в которых машинная информация является либо средством, либо объектом преступного посягательства [24, с.37; приводится по: 14, с. 167].

9. World Internet Users and Population Stats [Electronic resource] // Internet World Stats. – Mode of access : <http://www.internetworldstats.com/stats.htm>
10. Азаров Д. С. Порухення роботи автоматизованих систем – злочини у сфері комп'ютерної інформації / Д. С. Азаров // Право України. – 2000. – № 12. – С. 69–73.
11. Антонов С. Компьютерные преступления в банковской сфере / С. Антонов // Юридическая практика. – 1997. – № 8. – С. 7.
12. Батурин Ю. М. Компьютерная преступность и компьютерная безопасность / Ю. М. Батурин, А. М. Жодзишский. – М. : Юридическая литература, 1991. – 157 с.
13. Біленчук П. Д. Комп'ютерна злочинність : навчальний посібник / Петро Дмитрович Біленчук, Володимир Васильович Бут, Владислав Данилович Гавловський, Михайло Васильович Гуцалюк, Руслан Леонідович Колпак. – К. : Атіка, 2002. – 240 с.
14. Геллер А.В. Уголовно-правовые и криминологические аспекты обеспечения защиты электронной информации и Интернета : Дис. ... канд. юрид. наук : 12.00.08. Москва, 2006. – 219 с.
15. Голубев В. О. Правові проблеми захисту інформаційних технологій / В. О. Голубев // Вісник Запорізького юридичного інституту. – 1997. – № 2. – С. 35–40.
16. Закон України «Про національну програму інформатизації» від 04.02.1998 р. [Електронний ресурс] // Управління комп'ютеризованих систем Апарату Верховної Ради України. – Режим доступу: <http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=74%2F98-%E2%F0>.
17. Калюжный Р. А. Теоретические и практические проблемы использования вычислительной техники в системе органов внутренних дел (организационно-правовой аспект) : автореф. дис. ... доктора юрид. наук: 12.00.02 / Ростислав Андрійович Калюжный. – К., 1992. – 47 с.
18. Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України : монографія / М. В. Карчевський ; МВС України, Луганський державний університет внутрішніх справ імені Е. О. Дідоренка. – Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. – 528 с.
19. Киберпреступность страшнее финансового кризиса [Электронный ресурс] // Новости сайта Центра исследования компьютерной преступности. – 03.12.2008. – Режим доступа : <http://www.crime-research.ru/news/03.12.2008/5056/>.
20. Лісовий В. «Комп'ютерні» злочини: питання кваліфікації / В. Лісовий // Право України. – 2002. – № 2. – С. 86–88.
21. Манифест и история [Электронный ресурс] // Отдел «К» при ГУВД Воронежской области. – Режим доступа : <http://k-vrn.ru/pages/about>
22. Правовая информатика и кибернетика : учебник / Г. А. Атанесян, О. А. Гаврилов, П. Дёри, А. Г. Каблуков, А. К. Караханьян, И. Ковачич, К. Ковачичне, В. В. Крылов, А. Малиновский, М. Г. Мальковский, Г. О. Матюшкин, Я. Петцель, Н. С. Полевой, Л. Д. Самыгин, Д. Д. Хан-Магомедов, И. Ханец, С. И. Цветков, Н. П. Яблоков ; [под ред. Н. С. Полевого]. – М. : Юридическая литература, 1993. – 528 с.
23. Преступления, связанные с использованием компьютерной сети. Справочный документ для семинара-практикума. Десятый конгресс Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями. Вена, 10-17 апреля 2000 года [Электронный ресурс] // United Nations Crime and Justice Information Network. – Режим доступа: <http://www.uncjin.org/Documents/congr10/10r.pdf>
24. Селиванов Н. Проблемы борьбы с компьютерной преступностью // Законность. – 1993. – № 8. – С.37.
25. Системи оброблення інформації. Основні положення. Терміни та визначення : ДСТУ 2938-94. – [Чинний від 1996-01-01]. – К. : Держспоживстандарт України, 1996. – 20 с.
26. Системы обработки информации. Термины и определения. - ГОСТ 15971-90. - Дата введения 01.01.92
27. Супруненко А.М. Кіберзлочинність як особливий вид протиправної діяльності / А.М. Супруненко, М.С. Гожий // Боротьба з інтернет-злочинністю : матеріали міжнародної науково-практичної конференції (м. Донецьк, 12-13 червня 2013 р.). – Донецьк : ДЮІ МВС України, 2013. – С. 55–57.
28. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы : Дис. ... канд. юрид. наук : 12.00.08. Владивосток, 2005. – 235 с.
29. Чирков Д.К., Саркисян А.Ж. Преступность в сфере высоких технологий: тенденции и перспективы // NB: Национальная безопасность. — 2013. - № 2. - С.160-181. DOI: 10.7256/2306-0417.2013.2.608. URL: [http://e-notabene.ru/nb/article\\_608.html](http://e-notabene.ru/nb/article_608.html)

**Інформаційна та кібернетична безпека: роль та місце в умовах гібридної війни**

**Гришук Р.В.**

доктор технічних наук, старший науковий співробітник  
начальник науково-дослідного відділу інформаційної та кібернетичної безпеки  
наукового центру Житомирського військового інституту імені С. П. Корольова

Кардинальна зміна форм та способів збройного протистояння внаслідок повсюдного поширення надбань високих технологій, суттєво вплинула на виконання завдань за призначенням силовими та спеціальними структурами будь-якої розвиненої держави світу [1, с. 555]. При цьому Україна прагне увійти до кола держав з розвинутою економікою, а тому активно впроваджує в усіх сферах технологічні інновації, які окрім усіх інших позитивних аспектів створюють передумови для виникнення нових й нетипових до сьогодні для силових та спеціальних структур держави викликів й загроз безпеці. Наприклад, комп'ютеризація економічної, військової, соціальної та інших сфер породжує такі нові виклики та загрози для силових та спеціальних структур держави: для Служби безпеки України – проблему боротьби з кібертероризмом; для Міністерства внутрішніх справ України – проблему боротьби з кіберзлочинністю; для Міністерства оборони України – проблему забезпечення кібероборони держави; для Державної служби спеціального зв'язку та захисту інформації України – проблему кіберзахисту державних інформаційних ресурсів тощо.

Таким чином, кожна силова або спеціальна структура держави постала перед фактом: противник (кібертерорист, кіберзлочинець тощо) застосовує нові гібридні форми для досягнення своїх цілей, при цьому для досягнення максимального ефекту, вкладає в них новий зміст – діє асиметрично. Отже, проблема забезпечення кібербезпеки держави на сьогодні є актуальною. Особливо її значення зростає, коли проявляються елементи гібридизації – не нові за сутністю але унікальні за узгодженістю цілей, динамічністю їх досягнення, зростанням ролі інформаційної та кібернетичної складової на усіх рівнях.

На сьогодні, як відомо [2, с. 1], в державі відбувається становлення національної системи кібербезпеки. Але суттєвим стримуючим чинником на шляху її практичного впровадження є розрізненість не тільки суто технічних підходів та технологічних прийомів, а й в першу чергу непорозуміння обумовлене дефініційною невизначеністю. Відбувається розмиття та взаємопідміна таких понять як кібербезпека, інформаційна безпека, безпека інформації та технічний захист інформації.

Якщо виходити з того, що інформаційна безпека – це стан захищеності людини, суспільства та держави від зовнішніх та внутрішніх деструктивних інформаційних (інформаційно-психологічних) впливів, а кібербезпека (у вузькому сенсі цього слова) – це стан захищеності процесів управління в кіберпросторі від явних та потенційних кіберзагроз, за якого забезпечується сталий розвиток суспільства, держави та особистості, то в умовах гібридної війни, незалежно від сфери її ведення, під інформаційними та кібернетичними діями слід розуміти наступне [3, с. 133]. Інформаційні дії – це дії, які спрямовані на зміну масової та індивідуальної свідомості суб'єкта впливу (соціуму) з метою стимулювання у нього заданого типу поведінки. Кібернетичні дії – це дії, які спрямовані на об'єкти та суб'єкти кіберпростору (соціум, технічні та соціотехнічні системи), у вигляді різноманітних деструктивних впливів, наприклад кібератак, реалізація яких призводить до контрольованого управління згаданими об'єктами та суб'єктами.

У доповіді подано приклади [4, с. 9], що підтверджують справедливості наведених вище тез. Зокрема, розкрито технологію першого в сучасній світовій історії потужного кібернападу на Естонію 2007 року, який паралізував практично всі її критичні кібернетичні інфраструктури й супроводжувався інтенсивною підтримкою інформаційних дій. Також яскравим прикладом протистояння в кіберпросторі, який наведений в доповіді є інформаційні та кібернетичні дії, що здійснювалися під час Російсько-грузинської війни в 2008 році. Типовим актом несилового протистояння в кіберпросторі є й кібернапад на іранські ядерні об'єкти за допомогою мережевого хробака «Stuxnet» у рамках американської програми під кодовою назвою «Олімпійські ігри» 2010 року. Окремо показано роль та місце інформаційних та кібернетичних дій під час організації та проведення «кольорових революцій» та заворушень на близькому сході у 2010 р. під час «Арабської весни».

Основні акценти в доповіді розставлено на ролі та місці інформаційної та кібернетичної безпеки під час гібридної війни в Україні [5, с. 84]. Показано поетапність нарощення сил та засобів протидією стороною, розкрито технологію здійснення інформаційних та кібернетичних дій, приведено можливі сценарії розвитку подій. Крім того, подано результати практичних дій з питань забезпечення інформаційної та кібернетичної безпеки [6, с. 11]. Розкрито сутність та зміст

синергетичного підходу – як основи для прогнозування можливих подій унаслідок інформаційної та кібернетичної взаємодії [7, с. 66].

### **Література:**

1. Гришук Р.В. Основи кібернетичної безпеки : Монографія / Ю.Г. Даник, Р.В. Гришук ; за заг. ред. проф. Ю.Г. Даника. – Житомир : ЖНАЕУ, 2016. – 636 с.
2. Указ Президента України №96/2016 Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “Про Стратегію кібербезпеки України” [Електронний ресурс]. – Режим доступу : <http://www.president.gov.ua/documents/962016-19836> . – Назва з екрану.
3. Гришук Р.В. Синергія інформаційних та кібернетичних дій / Р. В. Гришук, Ю. Г. Даник // Труді університету. – К. : НУОУ, 2014. – № 6 (127). – С. 132–143.
4. Гришук Р.В. Кіберінциденти: передумови скоєння та наслідки / Р. В. Гришук // Перша міжнар. наук.-практ. конф. ["Проблеми науково-технічного та правового забезпечення кібербезпеки у сучасному світі"] (Харків, 30 бер. – 1 квітн.). – Харків : ХТУ “ХПІ”, 2016 р. – С. 9–10.
5. Гришук Р.В. Технологічні аспекти інформаційного протистояння на сучасному етапі / Р.В. Гришук, І.О. Канкін, В.В. Охрімчук // Захист інформації. – 2015. – Том 17. – № 1 – С. 80–86.
6. Гришук Р.В. Синергетика безпекових кластерів: теорія та практика / 5 міжнар. наук.-техн. конф. ["Захист інформації і безпека інформаційних систем"] (Львів, 02– 03 черв. 2016 р.). – Л. : НУ ЛПІ, 2016. – С. 10–11.
7. Hryshchuk R. The Synergetic Approach for Providing Bank Information Security: The Problem Formulation / Ruslan Hryshchuk, Sergii Yevseiev // Безпека інформації. – 2016. – Том 22. – № 1 – С. 64–74.

### **Місце кібертероризму у структурі кіберзлочинності та напрями боротьби з ним**

**Пядишев В.Г.**

кандидат технічних наук, доцент,  
доцент кафедри кібербезпеки та інформаційного забезпечення  
Одеського державного університету внутрішніх справ

На думку науковців наразі найбільшу загрозу для всієї міжнародної спільноти становить саме кібер-тероризм. Це жакливе явище має два крила: кіберзлочинність та тероризм.

Кіберзлочинність доцільно розглядати як дві сфери: 1) низка старих відомих злочинів, які значно “вдосконалилися” через підтримку останніх комп’ютерних технологій; 2) нові злочини, які були б принципово неможливі без досягнень в інформаційно-телекомунікаційній галузі. Причому вже наразі кіберзлочинність по прибутковості посідає одне з перших місць серед всіх видів злочинності. Як і всі види над-прибуткової злочинності, вона впевнено переростає в організовану та транснаціональну.

Одночасне все більш зловісні ознаки і розміри розпочала проявляти сукупність відомих зі стародавньої історії таких злочинів, як тероризм, структура якого з кожним роком ускладнюється.

Саме наразі спостерігається драматичне зрощування зазначених явищ — кіберзлочинності та тероризму: тероризм набуває нових сучасних можливостей свого втілення.

Зауважимо, що в зонах локальних збройних конфліктів, тобто в умовах послаблення правоохоронного контролю, спостерігається значне зростання рівню і різноманіття всіх видів злочинності. Це торгівля наркотиками, зброєю, природними ресурсами, награваними виступами мистецтва, людьми, людськими органами... Вся ця злочинність набуває індустріальної організованості та транснаціонального розмаху. Також розвивається і тероризм. Саме тут він набуває поширення аж до рівню домінування у державі. Більш того, він стає транснаціональним, тобто таким, що його агенти скоординовано працюють у багатьох державах світу.

Транснаціональний тероризм такого легко підкорює всі види організованої злочинності: з одного боку він надає їй захист, з іншого він її експлуатує.

Ми вважаємо, що транснаціональний тероризм характеризується наступними ознаками.- компонентами:

- звичайною практикою його є геноцид;
- методом досягнення цілей є насильницький екстремізм;
- здійснюється вербування, професійна підготовка і впровадження своїх агентів до всіх страт суспільства;



- економічним джерелом є використання організованої злочинності, якій при цьому надається захист від правоохоронних органів;

- активна діяльність транснаціонального тероризму пов'язує собою велику множину держав, незалежно від рівню їх економічного, і політичного розвитку, а також стану безпеки.

Пояснимо останнє. В зонах збройних конфліктів терористи загартовують кадри. В відсталих та економічно ослаблених країнах вони вербують додаткові кадри. До розвинених країн серед потоків чисельних біженців вони спрямовують свої кадри для подальшого впровадження на усіх рівнях. Нагадуємо, що корпус терористів-смертників формують майже виключно люди з вищою освітою.

Таким чином, сучасний транснаціональний тероризм характеризується крайньою жорстокістю, підпорядковує собі, розвиває і захищає організовану злочинність, намагається пов'язати у своїй діяльності значну кількість країн, а також підкорити собі владу в одній чи більше країнах. Серед іншого, він починає у своєму арсеналі використовувати кібер-тероризм.

Сьогодні існує більш ста визначень поняття “тероризм”. Більш того, видатні науковці вважають, що через низку причин, зокрема, міжнародних протиріч, взагалі неможливо створити універсальне визначення цього поняття [2, с.6], [3].

Все це, безумовно, не сприяє здійсненню визначення поняття “кібер-тероризм”. Але це явище існує. І саме транснаціональний кібер-тероризм сьогодні створює найбільшу небезпеку для суспільств.

Це є великим викликом всім державам. Найбільш розвинуті держави світу розпочали створювати всеосяжні програми протидії цьому небезпечному явищу.

У вересні 2014 року у своїй “Заяві перед Комітетом Сенату з питань національної безпеки і справ уряду” Р. Андерсон, виконувач обов'язків помічника директора ФБР, виклав комплексний підхід до здійснення кібербезпеки у США [4].

Отже, вважається, що кібер-загрози для держави виходять від “хакерів, які проплачені іншими державами”, від “хакерів-найманців”, від глобальних “кібер-синдикатів” та терористів. Вважається, що зазначені суб'єкти намагаються розкрити “державні секрети, торгові секрети, технології та ідеї”. Вважається також, що вони намагаються вразити інфраструктуру та пошкодити економіку держави.

Агентства федерального рівню через масштаби кібер-загроз надають вищий пріоритет кібербезпеці. Отже заходи загальнодержавного масштабу по боротьбі з кібер-загрозами зроблено ФБР, їхніми партнерами в Департаменті внутрішньої безпеки, Агентствами національної безпеки, Розвідувальним спів-товариством США та правоохоронними органами. ФБР приділяє головної уваги “втручанням високого рівня”, які здійснюються найнебезпечнішими, найбільшими ботнетами, також хакерами, які проплачені іншими державами, а також глобальними кібер-синдикатами.

Значна увага приділяється роботі з партнерами. Причому тут головне — своєчасне прогнозування атак, а також запобігання їм.

Отже у боротьбі беруть участь агенти ФБР, аналітики та комп'ютерні науковці. Використовується всі сукупність технічних можливостей та традиційних методів одержання інформації: всілякі джерела, спостереження, прослуховування телефонних розмов, криміналістичні дослідження.

Робота здійснюється сумісно на всіх рівнях: федеральному, рівні штатів та місцевому. На місцевий рівень 56 територіальних офісів ФБР забезпечують зв'язок з місцевими партнерами з кібернетичних сил спеціального призначення. Працює Національний Кібернетичний Слідчий Об'єднаний Відділ спеціального призначення (NCIJTF).

Працює також Цілодобовий командний центр кібер-спостереження (CyWatch), який у випадку значних кібер-атак об'єднає ресурси ФБР і NCIJTF. Це дозволяє забезпечувати зв'язок юридичних аташе на місцях і приватного сектора з федеральними кібер-центрами, урядовими установами та офісами ФБР.

Партнерські зв'язки, такі як Рада Альянсу внутрішньої безпеки, ІнфраГард та Спілка Національної кібер-криміналістики та навчання (NCFTA), забезпечують обмін інформацією про кібер-загрози з приватним сектором. Спілку Кібер-Шит на [www.leo.gov](http://www.leo.gov) започатковано для партнерів в державних і місцевих правоохоронних органах. Вона забезпечує з одного боку — можливість повідомляти ФБР про кібер-інциденти, з іншого — доступ до можливостей кібернетичного навчання та інформації.

Уряд США усвідомлює, що успіх в боротьбі з кіберзлочинністю значною мірою залежить від повноцінної роботи з персоналом: набору, розвитку і утримування його в системі. Для цього розроблено значну кількість програм з підготовки кадрів, яка в певному ступені залежить від партнерства з приватними підприємствами.

Значна праця здійснюється за кордоном. Там юридичні відділення ФБР забезпечують координацію кібер-розслідувань та усунення юрисдикційних перешкод. Одночасно продовжується виявлення нових місць за кордоном, де необхідно розташувати кібер-персонал США. До того ж, з моменту створення центрів по боротьбі з злочинністю в Інтерпол та Європол, розпочато роботу з ними.

Безумовно, робота по боротьбі з кіберзлочинністю, зокрема з кібер-тероризмом ведеться і в інших країнах. Наприклад у “Стратегії кібер-безпеки у Німеччині” звертається увага, що злочинці, терористи і шпигуни використовують кіберпростір як місце для своєї діяльності і не зупиняються на державних кордонах. При цьому позаду таких нападів також можуть бути і військові операції [5, с. 3].

#### **Література:**

1. Конвенція про кіберзлочинність. Міжнародний документ від 23.11.2001. Конвенцію ратифіковано із застереженнями і заявами Законом N 2824-IV ( 2824-15 ) від 07.09.2005, // ВВР. – 2006. – N 5-6. ст.71.
2. Jeffrey Record J. Bounding the Global War on Terrorism / Jeffrey Record. – New York: Oxford University Press, – 1999. – p. 312.
3. Martyn A. The Right of Self-Defence under International Law-the Response to the Terrorist Attacks of 11 September [Електронний ресурс] / Angus Martyn // Australian Law and Bills Digest Group, Parliament of Australia Web Site, – February 12, 2002. – Режим доступу: [http://www.aph.gov.au/About\\_Parliament/Parliamentary\\_Departments/Parliamentary\\_Library/Publications\\_Archive/CIB/cib0102/02CIB08](http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/Publications_Archive/CIB/cib0102/02CIB08)
4. Anderson R. Jr. Statement Before the Senate Committee on Homeland Security and Governmental Affairs [Електронний ресурс] / Robert Anderson, Jr. // the Federal Bureau of Investigation. – September 10, 2014. – Режим доступу: <https://www.fbi.gov/news/testimony/cyber-security-terrorism-and-beyond-addressing-evolving-threats-to-the-homeland>
5. Cyber Security Strategy for Germany/ – Berlin: Federal Ministry of the Interior, – 2011. – p. 18.

#### **Нормативно-правові засади використання високотехнологічних і програмних інструментів у боротьбі з кіберзлочинністю**

**Лефтеров Л.В.**

старший інспектор Департаменту Кіберполіції НП України,  
ад'юнкт кафедри кримінального права та кримінології ОДУВС

**Бабенко А.М.**

доктор юридичних наук, доцент  
професор кафедри кримінального права і кримінології  
Одеського державного університету внутрішніх справ

Темпи інноваційного розвитку при сьогоденному змаганні технологій дуже високі. Кожен день розробляється більше 100 тисяч нових зразків шкідливого програмного забезпечення. За деякі шкідливі програмні модулі сплачуються суми, які перевищують мільйон доларів. За оцінкою Центра стратегічних і міжнародних досліджень (Center for Strategic and International Studies) збиток від кіберзлочинності для світової економіки становить понад 445 мільярдів доларів на рік[3].

Згідно з висновками звіту організації, які хочуть проявляти пильність, повинні бути готові виявити будь-яку атаку. Швидка мобілізація включає в себе раннє визначення напряду дії загрози і причини атаки. Також швидкі дії, кваліфіційні навички та вміння використовувати у своїй діяльності високотехнологічні і програмні інструменти повинні бути присутніми у працівника підрозділів боротьби з кіберзлочинністю.

Розділ II Конституції України з метою захисту прав і свобод громадян, забезпечує таємницю листування, недоторканність особистих даних, заборону збирання особистих даних [1, ст. 21-29]. Однак вказані права – виключають можливість швидкого реагування за тяжкими кіберзлочинами та особливо тяжкими злочинами загального характеру в яких використовуються електронно обчислювальні мережі.

Основними принципами якісного та результативного реагування у зазначених вище випадках, є виявлення «гарячих слідів», що були залишені зловмисником. Основним фактором отримання електронної інформації є порядок повноцінного аналізу і упорядкування відомостей наданих потерпілою стороною. З інцидентами у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж, відповідальність за які передбачена Розділом 16 Кримінального кодексу України, одним з основних доказових чинників є результати запису інформації про події з об'єктами (в рамках комп'ютерної мережі, або з автоматизованою системою). Цей процес також називається аудитом, дані про який вкладаються системою у файл с записами про події у хронологічному порядку (файл реєстрації, протокол, журнал або лог-файл).

Лог-файли можуть містити вичерпну інформацію про:

- загальні дані про дії з ядром системи (контроль доступу програм в мережу);
- завантаження системи (зберігає основні системні події, журнал операційної системи);
- дані про звернення до сервера, інформацію щодо помилок веб-сервера (логи веб-сервера);
- запити до баз даних, помилки сервера (логи сервера баз даних);
- спроби входу в панель, поновлення ліцензії та панелі, статистики використання ресурсів сервера (логи хостингової панелі);
- дані щодо всіх відправлених і доставлених повідомленнях, помилки поштового сервера (логи поштового сервера);
- дані щодо виявлення шкідливого програмного забезпечення у системі (журнал антивірусної програми).

З нормативно-правової точки зору, аналізування наданих протоколів, не є порушенням процесуального законодавства, а навпаки на етапі первинної перевірки факту, надає змогу визначити безпосередню кваліфікацію кримінального правопорушення [4, ст. 16].

Використання програмних та високотехнологічних інструментів для аналізування лог-файлів є невід'ємною частиною якісного розкриття кіберзлочинів. Насамперед, слід зазначити, що технічні характеристики файлів журналу мають формат тексту або таблиць, що дозволяє у своїй діяльності використовувати комп'ютерні текстові редактори та пакети офісних додатків, з функцією сортування і пошуку даних.

Отриману в ході аналізу електрону інформацію слід використовувати для подальшого збору доказів в рамках кримінального провадження. Частіше за все при пошуку осіб використовуються інформація про IP-адреси.

IP-адреса це ідентифікатор (унікальний числовий номер) мережевого рівня, який використовується для адресації комп'ютерів чи пристроїв у мережах [5, ст. 113]. Аналізування IP-адрес або доменних імен Веб-сайтів здійснюється за допомогою вільних сервісів які працюють за Інтернет протоколами «WHOIS». Сервіси WHOIS використовується для запитів до бази даних, щодо визначення власника доменної зони, отримання відомостей про IP-адресу, або автономного системного номера в Інтернеті. Згідно вимог ICANN (Internet Corporation for Assigned Names and Numbers - міжнародна некомерційна організація, щодо регулювання питань, пов'язаних з доменними іменами, IP-адресами і іншими аспектами функціонування Інтернету) та «Угоди про акредитацію реєстраторів» від червня 2013 року, в рамках реєстрації доменних імен та IP-адрес в WHOIS, реєстратор повинен представити, або розмістити в базі даних реєстру наступні елементи даних:

- Ім'я реєстратора;
- найменування оператора або провайдера (щодо належності IP-адрес);
- контактні дані реєстратора або оператора (провайдера);
- первісна дата створення реєстраційної записи;
- дата закінчення терміну реєстрації;
- найменування та поштову адресу власника зареєстрованого імені;
- ім'я, поштову адресу, адресу електронної пошти, номер телефону, а також (за наявності) номер факсу контактної особи з технічних питань для зареєстрованого імені;
- ім'я, поштову адресу, адресу електронної пошти, номер телефону, а також (за наявності) номер факсу контактної особи з адміністративних питань для зареєстрованого імені [6].

Слід зазначити, що до конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження. Не допускаються збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини [2, ст. 21]. Аналіз та збирання цифрової інформації у вигляді IP-адрес не є конфіденційними даними про фізичну особу. Також інформація не є конфіденційною, якщо особа самостійно надала згоду на її опублікування та обробку. У цьому випадку якісним програмними інструментами виступають самостійно сформовані бази даних загально доступних соціальних мереж.

Подібних масиви даних, також можуть нести в собі помилкову або неправдиву інформацію, тому важливо використання у своїй діяльності все більших сервісів та програмних інструментів що можуть допомогти у боротьбі з кіберзлочинністю. Високотехнологічні і програмні інструменти можуть застосовуватись на всіх етапах кримінального процесу та використовуватись у якості доказової бази. Неодмінним фактором долучення отриманих відомостей у якості доказів до кримінального провадження є їх допустимість. Саме в цьому випадку підготовка усіх даних повинна проводитись згідно чинного законодавства.

**Література:**

1. Конституція України / Відомості Верховної Ради України від 23.07.1996 — 1996 р.;
2. Закон України «Про інформацію» ( Відомості Верховної Ради України (ВВР), 1992, N 48);
3. Report: Cybercrime and espionage costs \$445 billion annually [Електронний ресурс] // Washingtonpost. – 2014. – Режим доступу до ресурсу: [https://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a\\_story.html](https://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html);
4. Юрасов А.В. Основы электронной коммерции / А. В. Юрасов., 2008. – 480 с. – (Телеком);
5. Комп'ютерні мережі / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. – Львів: Магнолія 2006, 2013. – 256 с.;
6. Соглашение об аккредитации регистраторов [Електронний ресурс] // icann. – 2013. – Режим доступу до ресурсу: <https://www.icann.org/resources/unthemed-pages/approved-with-specs-2013-10-31-ru>

**Особливості забезпечення кібернетичної безпеки України в сучасних умовах розвитку кіберпростору**

**Мусасва С.С.**

слухач 2-го курсу магістратури факультету № 1  
Одеського державного університету внутрішніх справ

**Ісмайлов К.Ю.**

кандидат юридичних наук,  
завідувач кафедри кібербезпеки інформаційного забезпечення  
Одеського державного університету внутрішніх справ

На сьогодні, сучасні процеси формування та розвитку інформаційного суспільства, факт створення якого офіційно було визнано ще в липні 2000 року представниками держав Великої вісімки в ході Окінавської зустрічі, базуються на синтезі двох технологій - комп'ютерної та телекомунікаційної. Із входженням комп'ютерних технологій практично у кожен сферу людської діяльності, досить актуальним є питання захисту суб'єктів та процесів, заснованих на використанні даних технологій.

З огляду на це, поряд із такими важливими сферами безпеки життєдіяльності людства, як військова, економічна чи інформаційна, повстає ще одна – кібернетична безпека.

Національна безпека України, її економічне та соціальне процвітання залежать від доступності, цілісності та конфіденційності інформаційних ресурсів, які в свою чергу забезпечуються інформаційними та комунікаційними технологіями, або в більш широкому розумінні - кіберпростором. Термін «кіберпростір» (cyberspace) вперше застосували письменники-фантасти В. Гіббсон, Б. Стерлінг, Дж. Барлоу. Сьогодні без цього терміну вже складно уявити як міжнародно-правові акти, так і національні джерела права, переважно англо-американської правової сім'ї, а також в доктринальних працях зарубіжних та вітчизняних науковців. Кіберпростір згідно Проекту Закону України «Про основні засади забезпечення кібербезпеки України» - це середовище, яке виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних (автоматизованих), телекомунікаційних та інформаційно-телекомунікаційних систем [1].

Водночас, зростання залежності від інформаційно-комунікаційних технологій робить наше суспільство ще більш уразливим перед можливими негативними наслідками протиправного використання кіберпростору.

Термінологічні дослідження з проблем кібербезпеки знайшли належне відображення у працях Дж. Ліпмана, Д. Фахренкурґа, Ф. Крамера, Л. Вентца. Віддали належне цій тематиці й вітчизняні дослідники з нормативно-правової проблематики кібербезпеки, серед яких: О. Порфимович, А. Марченко, М. Погорецький, О. Манжай та інші.

На сьогодні, усе більш зростає загроза використання проти інтересів України кібернетичних засобів як з середини держави, так і за її межами. Серед основних джерел кібернетичних загроз слід виокремити міжнародні злочинні групи хакерів, окремі підготовлені у сфері інформаційних технологій злочинці; іноземні державні органи; терористичні та екстремістські угруповання; транснаціональні корпорації та фінансово-промислові групи [2].

Наприклад, в сусідній державі - Російській Федерації, діють наукові групи інформаційно-правового спрямування, кафедри інформаційного права та інститути права і інформації, діяльність яких приводить до активної інформаційної пропагандистської політики у світовому масштабі, здатної

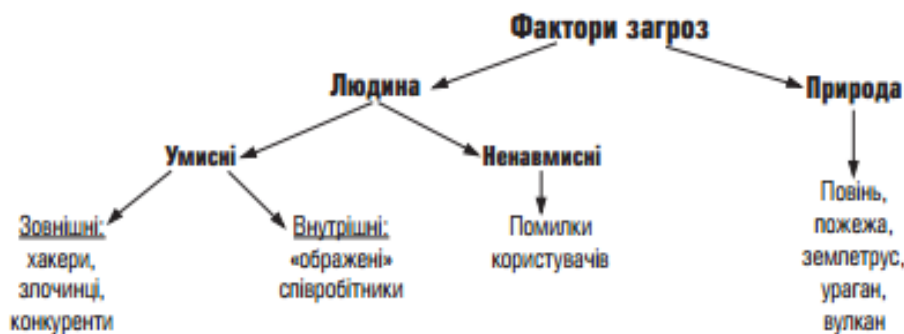
проводити інформаційну експансію у всьому світі по дискредитації сусідніх держав та нав'язуванні світовій спільноті «новітніх стандартів «Руського миру». І хоча в даному випадку йдеться про негативний приклад використання інформаційної зброї, однак, це, водночас і показник того, що ця держава володіє цілою армією навчених фахівців[3, с. 216]. А де такий «людський арсенал» в Україні? Тільки із створенням Департаменту кіберполіції Національної поліції України, який на сьогодні проходить свій шлях становлення із штатною чисельністю у 170 поліцейських на всю країну, запроваджує та реалізовує державну програму з протидії кіберзлочинам, а чисельність співробітників даного структурного органу в подальшому планується збільшити до 410, з яких 39 співробітників будуть спецагентами [4].

В цих умовах головним завданням держави є вжиття заходів, що дозволять принципово зменшити негативні наслідки від кібератак та забезпечити належний рівень безпеки в інформаційній та комунікаційній сфері.

Дуже важливим з точки зору кібербезпеки був минулий 2015 рік, оскільки в ньому були започатковані події і процеси, які мають тенденцію до продовження як в 2016 року, так і протягом наступних років. В якості найбільш вагомих можна назвати появу все більш складних методів протидії кібератакам, більш активне залучення державного сектору до діяльності в кіберпросторі, збільшення інтенсивності його використання в контексті гібридних конфліктів, підвищення моніторингу за соціальними мережами в Інтернеті, посилення нормативної та регулятивної діяльності з метою підвищення контролю над використанням кіберпростору на міжнародному рівні, а також на сьогодні керівництво МВС України ініціює підготовку на базі вищих навчальних закладів системи МВС України фахівців з протидії кіберзлочинності [5].

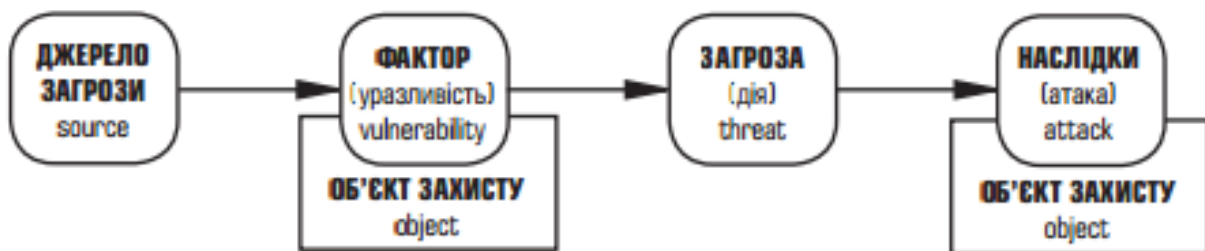
Одними з прикладів останніх кібератак в Україні були події 05 жовтня 2016 року в м. Києві, в якому відбулось відключення системи електронного декларування, що напряму зв'язують із хакерською атакою [6] та 06 жовтня 2016 року, де хакерами було зламано офіційну сторінку прес-центру АТО в соціальній мережі Facebook, розмістив на неї проросійську риторику [7].

Слід виокремити чотири категорії, що охоплюють вилучені (можливо, віддалені) кібератаки, а остання стосується локальних кібератак (вони реалізуються на вузлі, що зазнає атаки). При цьому всі кібератаки можуть бути як автоматизованими, так і неавтоматизованими (мал. 1).



Мал. 1. Механізм формування кібератаки.

Що ж до об'єктів впливу кібератак, то це можуть бути системи і канали зв'язку, канали передачі даних, тобто системи, що взаємодіють з інформаційним середовищем. Суб'єктами кібератак можуть виступати джерела несанкціонованих дій, спрямованих на той чи інший об'єкт (мал. 2).



Мал. 2. Джерела несанкціонованих дій.



Що стосується перспектив розвитку ситуації в кіберпросторі, протягом 2016 року в Україні було прийнято ряд нормативно-правових актів, регулюючих процедуру здійснення та стан захисту об'єктів від кібератак. Так, з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави, Указом Президента України від 15 березня 2016 року № 96/2016 було затверджено Стратегію кібербезпеки України, яка передбачає розбудову національної системи забезпечення захисту кіберпростору, координацію, взаємодію і розподіл повноважень та відповідальності органів сектора безпеки й оборони України в питаннях кібербезпеки, кіберзахисту та протидії кібертероризму й кіберзлочинності, своєчасне виявлення та нейтралізацію кіберзагроз, а також запобігання їм з урахуванням практики провідних держав-членів НАТО та ЄС застосування заходів, спрямованих на захист життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі [8].

Прийнятий Указ Президента України від 07 червня 2016 року № 42/2016 «Про Національний координаційний центр кібербезпеки», виокремлює основні завдання даного центру є здійснення аналізу щодо стану кібербезпеки, щодо:

- результатів проведення огляду національної системи кібербезпеки;
- стану готовності суб'єктів забезпечення кібербезпеки до виконання завдань з питань протидії кіберзагрозам, здійснення заходів щодо профілактики і боротьби з кіберзлочинністю;
- стану фінансового та організаційного забезпечення програм та заходів із реалізації державної політики у сфері забезпечення кібербезпеки України;
- стану виконання вимог законодавства щодо кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також критичної інформаційної інфраструктури та ін. [9].

Проведення виваженої державної політики відповідно до прийнятих в установленому порядку концепцій, стратегій та програм щодо забезпечення кібербезпеки в Україні призвело до створення Проекту Закону України «Про основні засади забезпечення кібербезпеки України» згідно Постанови Верховної Ради України «Про прийняття за основу проекту Закону України про основні засади забезпечення кібербезпеки України» від 20 вересня 2016 року [10]. Новостворений Проект закону визначає правові та організаційні засади державної політики, спрямованої на захист життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, основні принципи та напрями забезпечення кібербезпеки України.

Таким чином, на сьогодні не існує жодної держави в світі, яка б не зазнала кібератак. В Україні, з метою захисту інформаційних та комунікаційних мереж, а також боротьбою із кіберзлочинністю функціонує новостворений Департамент кібербезпеки України, структурні підрозділи якого проходять сумісне навчання з іноземними спецпідрозділами з метою отримання передового зарубіжного досвіду у протидії кіберзлочинам. Однак, для повноцінної реалізації повноважень, покладених на підрозділи боротьби з кіберзлочинністю повинна здійснюватись належна організація та планування необхідних заходів з протидії кіберзагрозам.

### **Література:**

1. Проект Закону про основні засади забезпечення кібербезпеки України // [Електронний ресурс]. - Режим доступу: [http://w1.c1.rada.gov.ua/pls/zweb2/webproc4\\_1?pf3511=55657](http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657)
2. В тенетах світової павутини: тенденції розвитку кібербезпеки у 2016 році // [Електронний ресурс]. - Режим доступу: <http://defence-ua.com/index.php/statti/>
3. Ісмаїлов К.Ю. Прорахунки в інформаційно-правовій підготовці фахівців / К.Ю. Ісмаїлов // Роль та місце правоохоронних органів у розбудові демократичної правової: Матеріали VIII Міжнародної науково-практичної конференції (м. Одеса, 25 березня 2016 р.). – Одеса: Одеський державний університет внутрішніх справ, 2016. – С. 216.
4. Керівник кіберполіції Сергій Демедюк: Про нас багато міфів і казок // [Електронний ресурс]. – Режим доступу: <http://asn.in.ua/ua/news/interview/36361-rukovoditel-kiberpolicii-sergejj-demedjuk-o-nas-mn.html>.
5. «Система підготовки правоохоронних кадрів потребує вдосконалення» – Олексій Тахтай // [Електронний ресурс]. - Режим доступу: <http://oduvs.sem-dev.co.ua/news/sistema-pidgotovki-pravoohoronnih-kadriv-potrebuye-vdoskonalennya-oleksij-tahtaj/>
6. Соболев сообщил о хакерской атаке на систему е-декларирования // [Електронний ресурс]. - Режим доступу: <https://news.mail.ru/politics/27352330/?frommail=1>
7. Страницу пресс-центра штаба АТО в Facebook взломали // [Електронний ресурс]. - Режим доступу: <http://ubr.ua/ukraine-and-world/technology/stranicu-press-centra-shtaba-ato-v-facebook-vzlomali-438823>

8. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію [...]": Указ Президента України від 15.03.2016 № 96/2016 // [Електронний ресурс]. - Режим доступу: <http://zakon2.rada.gov.ua/laws/show/96/2016>

9. Про Національний координаційний центр кібербезпеки: Указ Президента України від 07.06.2016 № 242/2016 // [Електронний ресурс]. - Режим доступу: <http://zakon3.rada.gov.ua/laws/show/242/2016>

10. Про прийняття за основу проекту Закону України про основні засади забезпечення кібербезпеки України: Постанова Верховної Ради України від 20.09.2016 № 1524-VIII // [Електронний ресурс]. - Режим доступу: <http://zakon3.rada.gov.ua/laws/show/1524-19>

## **СЕКЦІЯ 1 ПРАВОВЕ РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ**

### **Вплив на людську свідомість в медіапросторі як інформаційна загроза сучасності**

**Головко О.М.**

аспірант Науково-дослідного  
інституту інформатики і права  
Національної академії правових наук України

**Савінова Н.А.**

д.ю.н., с.н.с. Науково-дослідного  
інституту інформатики і права  
Національної академії правових наук України

Згідно з положеннями п. 8 Окінавської хартії Глобального Інформаційного суспільства (далі – ІС), зусилля міжнародного співтовариства, спрямовані на розвиток глобального ІС, повинні супроводжуватися узгодженими діями по створенню безпечного і вільного від злочинності кіберпростору [1, с. 51]. Не тільки національними, але й міжнародними пріоритетами ІС майбутнього є збереження стану захищеності кіберпростору.

Перш за все, з'ясуємо підходи деяких науковців до кіберпростору як якісно нової субстанції сучасного суспільного буття. Зокрема, в проекті Концепції інформаційної безпеки України при МПІ України його визначають як середовище, яке виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних (автоматизованих), телекомунікаційних та інформаційно-телекомунікаційних систем [2]. Важливо, що в цьому визначенні робиться акцент не тільки на комп'ютерних мережах як таких, але й на телекомунікаційних та інформаційно-телекомунікаційних системах, котрі також можуть бути полем активних кібератак зловмисників.

Перш ніж перейти до питання впливу на людську свідомість пропонуємо розглянути підхід науковців Національного інституту стратегічних досліджень при Президенті України щодо кібератак. Отже, це цілеспрямовані дії, які реалізуються в кіберпросторі та призводять до досягнення несанкціонованих цілей (порушення конфіденційності, авторства, доступності інформації, деструктивних інформаційно-психологічних впливів на свідомість, психологічний та психічний стан громадян) [3].

Характерним для цього визначення, котре вважаємо найбільш раціональним з точки зору підходу до об'єктів посягання особами, що вчиняють кібератаки, є наявність в переліку деструктивних інформаційно-психологічних впливів, тобто впливів на свідомість осіб із застосуванням технічних засобів в поєднанні з психологічними прийомами сугестивного характеру. Одразу зазначимо, що на протигагу концепту убезпечення свідомості населення від негативного інформаційно-психологічного впливу із опосередкуванням ІКТ вирують дискусії щодо вкрай хиткого стану свободи слова та похідних від неї прав та свобод, що ставляться у глухий кут при тотальному контролі за тим контентом, що з'являтиметься в інформаційному просторі. Ці крайні нині позиції стають на терезах рівноваги між свободою слова та безпекою в інформаційному просторі.

Виходячи з цього звернемося до позицій провідних лідерів сучасності. Зокрема, як зазначила 8 грудня 2011 року у своїй промові Державний секретар Гіллари Клінтон на конференції про свободу в

інтернеті: «проблема підтримки безпеки та боротьби із кіберзлочинами, такими, як крадіжка інтелектуальної власності, є реальною» [4]. В цьому аспекті варто звернути увагу на загрозу інтелектуальній власності у кіберпросторі та загрозу свідомості людини у медіапросторі. Звичайно, ці категорії не можна вважати тотожними по своїй суті, однак їх можна зіставляти за ступенем тієї суспільної небезпечності, яку вони можуть становити в майбутньому, а в деяких випадках реалізуються вже сьогодні. Тобто, за своєю суттю дані правовідносини є різними, але за ступенем небезпечності діянь, вчинених щодо своїх чітко відокремлених об'єктів вони потребують від світової спільноти акумулювання всіх можливих засобів задля протидії посяганням на інтелектуальну власність та інформаційно-психологічну безпеку людини.

Звернувшись до міжнародного становища у сучасному світі з точки зору його трансконтинентального сприйняття стає зрозумілим, що нині простір віртуальний стає не менш важливим для охорони та врегулювання, аніж більш зрозумілий людству фізичний простір. В умовах, коли цивілізовані держави досягли відносної стабільності у суспільних відносинах в повітряному, водному, земельному та навіть космічному просторі, вони ж виявилися неспроможними протидіяти загрозам віртуальним. І хоча зараз в цьому аспекті більше уваги приділяють кіберпростору та захисті електронних продуктів та ресурсів від кібератак, майже незайманим залишається питання інформаційно-психологічного тиску на усталені соціальні інститути, а як наслідок й на індивідуум. У цьому аспекті людина потребує від держави захисту своєї свідомості від ймовірного насильства. Відтак, медіапростір як значна частина інформаційного простору, що доступний звичайному громадянину має бути чітко визначеним національним та міжнародним законодавством.

Складність аналізу сфери медіадосліджень («media studies») полягає у тому, що вона є міждисциплінарним полем, а тому потребує особливо ретельного підходу з точок зору різних наук, у тому числі соціології. Для того, щоб врегулювати певні процеси у суспільстві, необхідно спочатку пізнати їх характер та першопричину. Зокрема, для аналізу розвитку кіберсоціуму необхідно застосовувати вже не стільки технологічні категорії, скільки соціологічні і соціально-філософські [5, с. 93]. Сьогодні специфіка медіадосліджень та безпеки в цій сфері полягають саме у просторовій невизначеності даного поняття.

З появою нових можливостей завжди з'являються і нові ризики, заходи превенції яких мають розроблятися поряд із новітніми тенденціями сучасних технологій. Проблема безпеки в цій сфері зводиться до здійснення адекватності кіберкомунікації потребам соціальної комунікації локального співтовариства, спантеличеного проблемою забезпечення самовідтворювання [5, с. 132]. Існуюча соціальна модель дає людям можливість уявної безпеки, але при цьому перетворює їх на безлику масу [6, с. 37]. Саме тому сьогодні здатність відрізнити точне знання від аналізу фактів від емоційної спекуляції є базовою навичкою для членів ІС.

Сьогодні містифікація в медіапросторі створює дестабілізуючий, часто деструктивний стан психіки людини, руйнуючи існуюче світосприйняття. З цього приводу Маркузе Г. зазначає, що сьогодні містифікуючі елементи, своєні і поставлені на службу виробничій рекламі, пропаганді та політиці [7, с. 250]. Все інформація з вище переліченого є відображенням контенту, що продукується через медіа джерела. Відсутність або недостатність фактажу та спекулятивний характер медіа контенту виникає у зв'язку зі специфічною роллю, яка надається мас-медіа – роллю посередника між людиною та державою та постачальника соціально важливої інформації. Причина цих негативних явищ, також, криється у низькій інформаційній культурі соціуму, яка нездатна відокремити раціональне від ірраціонального. Саме такими поняттями оперує Маркузе Г., говорячи про містифікацію в дійсності. Містифікована суть реальних фактів та оманлива гармонізація чи, навпаки, антагонізм соціальних протиріч становлять собою засіб ефективного маніпулювання людською свідомістю, змушуючи людину йти у необхідному для маніпулятора напрямку.

При цьому, зараз спотворення інформації варто розуміти не тільки як втручання в бази даних, але й як застосування методів та технологій сугестивного характеру, котрі прямо чи опосередковано впливають на свідомість людини, тим самим спотворюючи її розуміння та адекватне сприйняття реальності.

Розглядаючи явище новацій у праві Матвєєва Л.Г. зазначає: «неминучою є юридизація електронних соціальних відносин, навіть ширше – поведінки в кіберпросторі або віртуальної правової поведінки» [8, с. 29]. З точки зору державного управління механізм реалізації державної політики повинен бути спрямованим на досягнення конкретних цілей (розв'язання соціальних суперечностей) шляхом впливу на конкретні фактори (елементи управління та їхні зв'язки) [9].

Отже, задля правового регулювання убезпечення свідомості населення від деструктивних інформаційних та інформаційно-психологічних впливів є, перш за все, надати людині інструменти для самостійного виявлення дезінформації та маніпуляцій, що можна реалізувати через впровадження

медіаосвіти. А також, розробити чіткі стандарти якості медіа контенту, які дадуть змогу покращити національний медіа продукт, при цьому не звужуючи спектру дії свободи слова.

### **Література:**

1. Окинавская Хартия глобального информационного общества від 22 липня 2000 р. № 998-163 / [Okinawa Charter on Global Information Society] // Дипломатический вестник. – 2000. – № 8. – С. 51–56.
2. Проект Концепції інформаційної безпеки України / [Електронний ресурс]. – Режим доступу : [http://mip.gov.ua/done\\_img/d/30-project\\_08\\_06\\_15.pdf](http://mip.gov.ua/done_img/d/30-project_08_06_15.pdf).
3. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування : аналітична записка Нац. ін-ту стратегічних досліджень при Президенті України / [Електронний ресурс]. – Режим доступу : <http://www.niss.gov.ua/articles/454/>.
4. Промова Державного секретаря Гіллари Клінтон на конференції про свободу в інтернеті / [Електронний ресурс]. – Режим доступу : <http://ukrainian.ukraine.usembassy.gov/uk/clinton-intfreedom2011.html>.
5. Дзьобань О.П., Пилипчук В.Г. Інформаційне насильство та безпека: світоглядно-правові аспекти: Монографія / За заг. ред. проф. В.Г. Пилипчука. – Харків: Майдан, 2011. – 244 с.
6. Уваров Е.А. Жизненная усталость как ведущая девиация эпохи социальных перемен. / [Електронний ресурс]. – Режим доступу : <http://cyberleninka.ru/article/n/zhiznennaya-ustalost-kak-veduschaya-deviatsiya-epohi-sotsialnyh-peremen>.
7. Маркузе Г. Одномерный человек. Исследование идеологии Развитого Индустриального Общества. Пер. с англ. – М., 1994. – 368 с.
8. Матвєєва Л.Г. Новація як вияв транзитивності у праві. Науковий вісник Херсонського державного університету. - Випуск 1. Том 1. 2015 – с. 27-30
9. Ільченко Н. М. Деякі аспекти формування механізму реалізації державної політики України в галузі засобів масової інформації / Н. М. Ільченко // Державне будівництво [Електронний ресурс]. – 2007. – № 2. – Режим доступу до журн. : [www.kbuara.kharkov.ua/e-book](http://www.kbuara.kharkov.ua/e-book).

### **Співвідношення публічного та приватного інтересу у межах протидії кіберзлочинності**

**Бабенко Т.С.**

курсант 3-го курсу факультету № 3  
Одеського державного університету внутрішніх справ

**Маковій В.П.**

кандидат юридичних наук, доцент  
завідувач кафедри цивільно-правових дисциплін  
Одеського державного університету внутрішніх справ

В останні десятиліття у світовій правовій теорії та юридичній практиці з'явився термін «кіберзлочин». Відповідно до Конвенції Ради Європи про кіберзлочинність, кіберзлочини у широкому розумінні – це ті ж злочини, але які пов'язані саме з комп'ютерними системами, тобто це протиправні, іноді суспільно небезпечні дії, які вчиняються суб'єктами кіберпростору. Також, деякі вчені, наприклад Т. Тропіна визначає кіберзлочин як – винно вчинене суспільно каране втручання в роботу комп'ютерів, комп'ютерних програм, комп'ютерних мереж, несанкціонована модифікація комп'ютерних даних [1, с 30].

Уряди багатьох держав світу вже усвідомили загрози для національної безпеки кожної країни, що породжуються існуванням і поширенням комп'ютерної злочинності та комп'ютерного тероризму. Не є виключенням і наша держава, за законодавством якої комп'ютерна злочинність і комп'ютерний тероризм належить до найбільш серйозних загроз національній безпеці й національним інтересам в інформаційній сфері [2, с.43]. Безумовно, як ніколи, в цій сфері суспільних відносин виникає питання співвідношення приватного та публічного інтересу в частині гармонійного поєднання відповідного правового механізму їх врегулювання.

Україна, в особі органів державної влади вже робить значні кроки щодо протидії та запобігання злочинам у сфері інформаційних технологій. Це проявляється насамперед прийняттям низки законів, нормативно-правових актів, в яких чільне місце посідає Указ Президента України №96/2016 “Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “Про Стратегію кібербезпеки України””. В Указі регламентовано становлення національної системи кібербезпеки,

досягнення відповідності до стандартів ЄС та НАТО, створення вітчизняної нормативно-правової та термінологічної бази у цій сфері, розвиток та удосконалення системи державного контролю за станом захисту інформації, а також проведення навчань щодо надзвичайних ситуацій та інцидентів в кіберпросторі. Указ Президента України також передбачає посилену діяльність та взаємодію низки державних органів в цій сфері, серед яких: Державна служба захисту спеціального зв'язку та захисту інформації; Служба безпеки України; Національна поліція України; Національний банк України; Розвідувальні органи України [3].

Тобто, відповідно до наведеного Указу Президента України запобігання, протидія, усунення кіберзлочинів загалом можливе лише за умови ефективної та раціональної взаємодії та координації органів державної влади та спеціально уповноважених органів.

Безумовно, при аналізі вищезазначеного нормативно-правового акту щодо захисту прав людини та держави від злочинних посягань в сфері інформаційних технологій, не можна оминати також Закон України «Про захист персональних даних», який тісно взаємопов'язаний з іншими нормативно-правовими актами. Останній передбачає здійснення заходів, які пов'язані з захистом та обробкою персональних даних. В Законі та Указі вказуються положення про те, що органи державної влади, органи місцевого самоврядування, а також інші суб'єкти, які здійснюють обробку даних, створюють структурний підрозділ чи призначають відповідального щодо захисту персональних даних. Для захисту персональних даних та запобігання, ліквідації кіберзлочинів усі суб'єкти обробки даних, володілці, користувачі повинні діяти лише в межах чинного законодавства, зокрема наведених нормативних актів [4].

Ефективна боротьба з кіберзлочинністю неможлива без розробки цілісної концепції основ кримінологічного та статистичного вивчення злочинності, що включає в себе основи дослідження кіберзлочинності. Як наголошується, в 2014 році управління по боротьбі з кіберзлочинністю МВС зареєструвало 4800 злочинів у сфері ІТ, в 2015 році - 6025 [5], не говорячи про високий коефіцієнт латентності у цьому спектрі злочинності.

Викликає зацікавленість питання розробки «Закону більшого брата» у Російській Федерації, сутністю якого є встановлення посиленої відповідальності за міжнародний тероризм, певні прояви радикалізму і зобов'язання операторів зв'язку, месенджерів та соціальних мереж зберігати всі розмови і листування користувачів, а також фото- та відео- матеріали протягом тривалого часу. Як зазначає стаття 3 Конституції України – людина, її права та свободи являються найвищою цінністю, також стаття 27, яка каже, що кожна людина має невід'ємне право на життя. Згідно статті 14 Закону України «Про захист персональних даних» конфіденційна інформація може поширюватися за бажанням відповідної особи у визначеному нею порядку відповідно до передбачених нею умов. У наведених нормах закладені підвалини до гармонійного поєднання правової регламентації публічного та приватного інтересу у цій сфері. Тобто «Закон більшого брата» неможливо співвідносити у призмі законодавства більшості країн, адже згідно конституційних засад будь-якої цивілізованої країни наявне домінування гуманістичних положень, де права та свободи людини визнаються найвищою цінністю. Визнаючи пріоритет приватно-правових інтересів у чинному національному законодавстві необхідно вживати певних заходів щодо соціальної відповідальності окремих осіб. Прийняття наведеного закону визвало неоднозначні коментарі з боку деяких знавців. Американський спеціаліст з інформаційних технологій та розвідки – Едвард Сноуден зазначив, що ці заходи не спроможні забезпечити безпеку будь-якої країни, а також звернув увагу саме на непрактичність усіх дій, спрямованих на забезпечення безпеки держави, людини та суспільства у такій формі [6].

Зазначені нормативні акти, як національні так і міжнародні дають змогу зробити висновок про те, що злочини у сфері інформаційних технологій є надзвичайно небезпечними, тому задля їх нейтралізації потрібна не тільки увага органів державної влади у вигляді видання централізованих актів, а також і увага суспільства щодо сконцентрованості на цій проблемі як глобальній шкоді людства.

Боротьба з кіберзлочинністю вимагає всебічного підходу. Якщо проаналізувати іноземний досвід, то наприклад у Китаї існують певні обмеження на користування мережею Facebook, у КНДР взагалі навіть Google використовувати заборонено. У США, прийнято законодавство щодо здійснення контролю в Інтернеті, виділяються кошти на прослуховування в Інтернеті та слідкування за людьми. Крім того, в останні роки у різних регіонах світу було застосовано низку своїх підходів для боротьби з кіберзлочинністю. Так, у 2002 році Співдружністю націй був розроблений типовий закон про комп'ютерні та пов'язані з комп'ютерами злочини, метою якого є удосконалення законодавчих норм держав-членів Співдружності в галузі боротьби з кіберзлочинністю і поглиблення міжнародної співпраці.

Враховуючи все вищезазначене, законодавець визначив пріоритет публічного інтересу, зважаючи на його особливий характер. Водночас слід наголосити, що особливий характер публічних інтересів не

може бути основою для його необмеженого домінування в правовому регулюванні суспільних відносин. Сьогодні кіберзлочинність більш масштабна, професійна, організована та технічнооснащена. Сучасний стан злочинів у сфері високих інформаційних технологій характеризується тим, що спостерігається її постійне зростання та розширення існуючих меж. Цілком очевидно, що гостро та проблему цій сфері боротьби стає потенційною небезпекою для держави та вимагає прийняття неординарних рішень, кардинальних змін стереотипних підходів до її вирішення, розроблення нових форм боротьби зі кіберзлочинністю, але з врахуванням при цьому пріоритетності інтересів людини й громадянина. Заходи щодо захисту даних у сфері інформаційних технологій є комплексними та систематичними, але необхідно і дуже важливо звертати увагу на взаємодію приватного та публічного інтересу, що встановлює свій відбиток на протидії різним проявам кіберзлочинності.

### **Література:**

1. Погорецький М. Правове забезпечення боротьби з кіберзлочинами в Україні / М. Погорецький // Вісник прокуратури. – 2011. – Вип. 8. – С. 30-38
2. Мельник Д.С. Створення Національного контактного пункту формату»24/7» як необхідна передумова протидії транснаціональній компютерній злочинності та компютерному тероризму /Д.С. Мельник // Південноукраїнський правничий часопис. – 2009. – Вип. 4. – С. 43-45
3. Указ Президента України №96/2016 Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" [Електронний ресурс]: Режим доступу - <http://www.president.gov.ua/documents/962016-19836>
4. Про захист персональних даних : Закон від 01.06.2010 № 2297-VI
5. В Україні збільшується кількість кіберзлочинів: [Електронний ресурс]: режим доступу - <http://imi.org.ua/news/52857-v-ukrajini-zbilshuetsya-kilkist-kiberzlochiv.html>
6. Сноуден раскритиковал пакет Законов Яровой: [Електронний ресурс]: режим доступу - <https://lenta.ru/news/2016/06/25/snowden/>

### **Захист інформаційної діяльності органів публічного адміністрування в Україні**

**Делія Ю.В.**

кандидат юридичних наук, доцент,  
доцент кафедри загально-правових дисциплін  
Донецького юридичного інституту МВС України

В Україні серед актуальних завдань у побудові правової держави пріоритетним є розвиток публічного адміністрування, зокрема, його історичні, політичні, економічні та соціальні складові. У світлі реалізації даних завдань вимагають подальшого дослідження питання відносно методів і форм інформаційного забезпечення. На продовження демократичного курсу спрямована загальнодержавна програма «Стратегія реформ – 2020», яка включає реформування державних інституцій у тому числі і тих, які відповідають за подальше впровадження публічного адміністрування та наближення українського суспільства до європейських стандартів.

Деякі аспекти означеної проблематики досліджували у своїх працях російські та українські вчені різних часів, серед них: В.Б. Авер'янов, О.Ф. Андрійко, М.О. Баймуратов, О.В. Батанов, Т.А. Костецька, В.Ф. Погорілко, О.Ф. Фрицький, В.Л. Федоренко та інші автори.

Розвиток національної держави і правотворчості ставить перед сучасною юридичною наукою складні завдання, від ефективності та оперативності вирішення яких залежить майбутнє людини, суспільства і держави в цілому. Сенс завдань полягає насамперед у своєчасному теоретико-методологічному забезпеченні конституційних, адміністративних, правотворчих, правозастосовних процесів та інформованості суспільства.

Одним з основоположних принципів управління є принцип взаємної відповідальності держави і людини, який означає, що державу і особу пов'язано взаємодіючими правами та обов'язками. Забезпечувати виконання даного принципу покладено на публічне управління. У наукових розробках вітчизняних і зарубіжних вчених під терміном «публічна адміністрація», розуміють будь-яку установу публічного права (включаючи державу, регіональні та місцеві органи державної влади, органи місцевого самоврядування, незалежні публічні підприємства та будь-яких фізичних осіб при виконанні ними повноважень офіційних органів).

Політичні, економічні та соціальні процеси останнього часу дають привід з упевненістю говорити, що саме в інституті публічного адміністрування закладено резерви для розвитку держави і суспільства

в цілому. Для того щоб у майбутньому запобігти політичній нестабільності, проблемам конституційної побудови держави потрібно протиставити реформи, наблизити до участі в управлінні членів територіальної громади та надати їм більше можливостей для вирішення місцевих питань на рівні громади.

Право, за допомогою якого будуються суспільні відносини, настільки універсальне і одночасно складне явище, що і на сьогодні науковий інтерес до питання публічного управління не зменшується. Бажання упорядкування соціального буття, творення нового, зменшення кількості непізнаного – властивість людського розуму, яке має своє втілення в постійному процесі вироблення конструктивних реформаторських ідей. Таку сталість, на думку академіка В.Я. Тація, «обумовлено не тільки складністю людського буття, але і тим, що ще нікому і ніколи не вдавалося в процесі пізнання, дослідження різних сторін буття побачити його в заключному виді, дійти до абсолютних висновків і результатів» [1, с. 9]. Саме тому українській державі і суспільству слід будувати власну модель громадського управління, а не брати готові моделі, навіть незважаючи на те, що вони ефективно працюють у розвинених європейських та світових державах. Головна мета творців суверенної України – гуманізація національного законодавства, упровадження в юридичну науку і практику людиноцентристської ідеології, коли моральний розвиток і відповідальність, не тільки за долю держави, але і за майбутнє всієї планети, мають стати пріоритетними соціальними цінностями. У даному контексті доцільно процитувати професора М.О. Баймуратова, який зазначає, що «феномен місцевого самоврядування повинен бути врахований у процесі створення національної моделі місцевого самоврядування за допомогою вибору оптимальних форм самоорганізації і самоврядування населення» [2, с. 8].

У функціонуванні системи публічного управління на сучасному етапі розвитку суспільства все більшу роль відіграє інформація. Розглядаючи правові проблеми та розкриваючи сутність інформаційного забезпечення органів публічного адміністрування, перш за все, слід сформулювати визначення терміна «інформаційне забезпечення», у спеціальній літературі це – сукупність єдиної системи класифікації та кодування інформації уніфікованих систем документації, систем інформаційних потоків, що циркулюють в організації, а також методологія побудови бази даних; створення інформаційних умов функціонування системи, забезпечення необхідною інформацією, включення в систему засобів пошуку, отримання, зберігання, накопичення, передачі, обробки інформації та створення баз даних.

У вирішенні зазначених питань особливого сенсу набувають проблеми ефективності інформаційного забезпечення діяльності органів публічного управління. На сьогодні інформаційне забезпечення публічного управління все більше набуває атрибуту самостійності – зі специфічними відносинами, суб'єктами (об'єктами) цих відносин, їх правами і обов'язками, найбільш значні елементи якого вже знайшли правову регламентацію. Закон України «Про інформацію», зокрема, визначає інформацію державних органів та органів місцевого самоврядування як основні об'єкти інформаційних відносин у суспільстві та державі (ст. 21), а обов'язок цих органів інформувати про свою діяльність та прийняті рішення як гарантію права на інформацію (ст. 10). Для інформаційного забезпечення публічного адміністрування слід визначити основну його мету – створення умов для вирішення питань місцевого значення, налагодження ефективного управління територією. Виходячи з пріоритетних завдань, організаційні зусилля органів публічного адміністрування повинні спрямовуватися на: централізацію інформації, створення фонду відомостей (банку даних), що підлягають доведенню до відома громадян, визначення їх оптимального обсягу для кожного виду інформаційних зв'язків, визначення оптимального режиму використання форм і методів обробки самої інформації; встановлення відповідної інформаційної системи в рамках організаційних структур ради; розроблення та запровадження механізму обговорення населенням проектів рішень, процедури обліку висловлених при цьому зауважень і пропозицій (ухвалюються відповідним органом або її головою, мають відбивати інтереси як певних соціальних груп, так і всієї територіальної громади) і відповідно визначати зміст напрямків інформаційних потоків та їх структуру.

Наявні інформаційні зв'язки різноманітні, громіздкі й вимагають свого впорядкування. Рівень упорядкування конкретної системи залежить від інформаційного різноманіття; від інформаційного забезпечення також залежить швидкість перетворень, які відбуваються в системі. Вдало обрана структура інформаційних зв'язків набуває важливого значення не лише для проведення конкретних заходів, а також для функціонування всієї системи публічного управління. Об'єктом аналізу в нашому дослідженні візьмемо рішення ради як базового рівня публічного адміністрування. Саме ради регіонального рівня виступають центром у системі місцевого самоврядування в Україні.

Охоплюючи систему інформаційних взаємин, слід виділити деякі аспекти. Що стосується інформаційних зв'язків, у забезпеченні системи самоврядування, то їх наявність пояснюється різноманітністю факторів. А саме, реалізація принципу гласності в діяльності органів публічного



управління опосередковує інформаційні відносини з державними органами, підприємствами, установами, організаціями, органами самоорганізації громадян і населення.

Інформаційна захищеність органів публічного адміністрування, на сьогодні, постає досить гостро та потребує державної підтримки. Адже, захиститися самотужки органам публічного адміністрування від комп'ютерної злочинності, або кіберзлочинності, без необхідних сил та засобів непросто. В Конвенції Ради Європи про кіберзлочинність [3] вказується на серйозність даної проблематики та створення на рівні Європейського Союзу існує проект CleanIT, метою якого є боротьба з цим явищем.

Таким чином, правові основи інформаційного забезпечення у функціонуванні органів публічного адміністрування мають важливе значення, по-перше, відкритість і публічність функціонування органів публічного адміністрування досягається за допомогою засобів інформації, по-друге, суспільство має більш широкі можливості інформаційного забезпечення у прийнятті рішень щодо питань місцевого значення, по-третє, саме інформаційне забезпечення є резервом для залучення широких верств населення щодо вирішення питань місцевого значення, по-четверте, захист інформаційного забезпечення має бути під державним ґрунтовним забезпеченням. При якісному інформаційному забезпеченні започатковані реформи проводитимуться на багато швидше і будуть сприйняті громадськістю.

### **Література:**

1. Селіванов В.М. Право і влада суверенної України: методологічні аспекти: [Монографія] / В.М. Селіванов - К.: Видавничий Дім «Ін Юре», 2002. – 724 с.
2. Баймуратов М.О. Місцеве самоврядування в Україні: до питання формування національної моделі / М.О. Баймуратов // Конституційні засади формування правової системи: Матер. міжнарод. наук-практ. конф. (Одеса, 20 квітня 2012 р.) / Укладачі. З.В. Кузнецова, А.В. Левенець. – Одеса, 2012. – С. 8.
3. Конвенція про кіберзлочинність // Конвенція Ради Європи від 23.11.2001 [Електронний ресурс]. – Режим доступу: [http://zakon2.rada.gov.ua/laws/show/994\\_575](http://zakon2.rada.gov.ua/laws/show/994_575)

### **Вплив Інтернету як фактор вчинення неповнолітніми злочинів проти життя та здоров'я особи у регіонах України**

**Бібік І.С.**

аспірант заочної форми навчання  
докторантури та аспірантури

Одеського державного університету внутрішніх справ

**Бабенко А.М.**

доктор юридичних наук, доцент

завідувач кафедри теорії та історії держави і права

Одеського державного університету внутрішніх справ

Стрімкий розвиток науково-технічного прогресу суспільства у сфері інформаційних технологій дає підстави стверджувати, що ХХІ ст. є століттям «процвітання» кібернетичних технологій. Розвиток сучасних інформаційних технологій значно прискорює процес обігу інформації та розширює можливості її надання безпосереднім споживачам. Насамперед це стосується мережі Інтернет, як найбільш об'ємної інформаційної складової розвитку суспільства. При цьому використання можливостей мережі Інтернет для правового виховання неповнолітніх є актуальною проблемою в сучасних умовах проведення профілактики їх протиправної поведінки шляхом ознайомлення з відповідною правовою інформацією.

Протягом останніх десятиріч в Україні простежуються загальносвітові тенденції кардинальних змін соціального середовища, які пов'язані з впровадженням нових технологій. На сьогоднішній день спостерігається формування по суті нового типу соціальної парадигми – інформаційного суспільства. Невід'ємним елементом сучасного інформаційного середовища стала всесвітня комп'ютерна мережа Інтернет, яка дала суспільству безмежні можливості з оперативної передачі, отримання, обліку та обміну будь-якою інформацією. Нові можливості, які з'явилися в результаті розвитку інформаційних технологій стали широко використовуватися представниками кримінального світу. І, як наслідок, кіберзлочинність перетворилась на чинник, який став здійснювати вагомий тиск на суспільні

відносини. Це почало негативним чином впливати на криміногенну ситуацію в країні і окремих її частинах – в регіонах [1, с.122].

Метою нашого дослідження є визначення впливу Інтернет-технологій на вчинення неповнолітніми злочинів проти життя та здоров'я особи у регіонах України та розробка відповідних рекомендацій по її запобіганню.

Варто зауважити, що проблему впливу Інтернету на протиправну поведінку неповнолітньої особи відображені у працях таких зарубіжних та вітчизняних вчених, як: А.М. Бабенко, Р. Берон, І.О. Бугера, В.В. Голина, І.М. Даньшин, А. І. Долгова, О. Ю. Дроздов, В.В. Куницький, Д. Майерс, Д. Річардсон, І.К. Туркевич, В.І. Шакун та ін.

Як загальновідомо, сучасний Інтернет-простір містить велику кількість позитивної та корисної, швидко доступної інформації, що, безумовно, відіграє важливу роль у житті суспільства. Поряд з цим, мережі Інтернет характеризуються перенасиченістю і різного роду негативною інформацією – порнографією, пропагандою наркотиків, інструкціями з виготовлення зброї, вибухівки, та психотропних речовин. В Інтернеті також можна легко знайти інформацію про послідовність вчинення протиправних дій, поради стосовно скоєння різних злочинів та уникнення відповідальності. Мережі Інтернет переповнені іграми, що пропагують насильство та масові вбивства і т.д. Нерідко через мережі Інтернет вчиняються й самі злочини – торгівля людьми, шахрайства, замовлення на вбивство, продаж зброї та наркотиків. Враховуючи велику латентність Інтернет-злочинності, в цілому така ситуація негативно впливає на криміногенну ситуацію у країні [2, с. 65].

Зараз у мережі Інтернет набувають розвитку такі молодіжні рухи як «Ліголайз», «Гроверство», «Ентеогени» та інші, які пропагують культуру споживання різного роду психотропів та галюциногенів, вироблених з наркотиковмісних та психотроповмісних рослин та грибів. Представники цих рухів (клубів) обмінюються досвідом культивування вказаних рослин у природних та у штучно створених умовах; отримання з них одурманюючих речовин; обговорюють антинаркотичне законодавство, способи ухилення від кримінальної та адміністративної відповідальності [3].

Так, за даними компанії BIGMIR-Internet найвищого поширення користувачів в мережі Інтернет набули у східних областях України. Географія Інтернет-користувачів у нашій країні має такий вигляд: м. Київ – 55%, області: Донецька – 6,98%; Харківська – 6,16%; Одеська – 5,00%; Дніпропетровська – 4,32%; АР Крим – 2,55%; Луганська – 2,14%; Запорізька – 1,30%. Для порівняння, західні області України характеризуються низьким розповсюдженням Інтернету і такими показниками щодо його користувачів: Закарпатська – 0,65%; Тернопільська - 0,57%; Вінницька – 0,61%; Чернівецька – 0,31%; Івано-Франківська – 0,15% і т.д. Така географія майже повністю співпадає з географією поширеності злочинності серед регіонів України. Причому не лише Інтернет-злочинністю, а й загальною та окремими видами злочинності [ 4, с.116-123; 5, с. 151-159].

Відомо, що естетичні смаки та моральні якості молоді на сучасному етапі формуються переважно під впливом стихійних факторів суспільного оточення. Адже інформація, яка містить елементи насильства, жорстокості, агресії, формує відповідні моральні якості, естетичні смаки, що моделюють поведінку підростаючого покоління.

Встановлено, що існує наслідково-причинний зв'язок між «розважальним медіа-насильством» і проявами агресії серед молоді. Дослідники стверджують, що негативна інформація впливає на ціннісні орієнтації особистості і молоді люди, у яких ще недостатньо сформована психіка, вважають, що насильство – прийнятний шлях вирішення соціальних конфліктів. Ці висновки підтверджує і той факт, що досить часто неповнолітні правопорушники серед причин, які штовхнули їх на скоєння злочину, називають перегляд відповідних відеоматеріалів. Крім телебачення, комп'ютерних ігор на поведінку молоді людини також негативно впливає використання інтернет-технологій.

Сучасний світ неможливо уявити без досягнень інформаційних технологій. Безперечно Інтернет - технології також мають певні переваги і зокрема щодо можливості доступу до значних масивів інформації, швидкості її опрацювання та ін. Разом з тим, виникає проблема щодо уникнення негативного впливу Інтернету, йдеться передусім про інформації з елементами насильства, жорстокості та порнографії, на неповнолітніх.

Необхідно зазначити, що останнім часом в Інтернеті все частіше з'являються відеоролики з проявами жорстокості з боку підлітків. При цьому самі неповнолітні є їх авторами. Тобто, все частіше вільний доступ до Інтернету використовується неповнолітніми, як можливість похизуватися своєю фізичною силою та жорстокістю. При цьому наявність значного масиву негативної Інтернет-інформації спонукає їх до копіювання «героїчних» вчинків таких персонажів.

Тексти, відео та фото, на які підліток може натрапити у всесвітній мережі, є більш руйнівними, ніж найбрутальніший ТВ-контент. У мережі немає заборон і табу. Немає обмежень. І якщо дорослий може

обмежувати себе сам, то дитина навряд чи. В більшості цивілізованих країн уже давно працює кіберполіція, яка має дуже широкі повноваження [6].

На думку О.А. Присяжнюк всесвітня комп'ютерна мережа Інтернет на початку ХХІ сторіччя поступово перетворилася з суто технологічного явища в суспільно-політичне, таке що визначає розвиток сучасних схем державного управління. Вперше за всю історію розвитку людства, межі державного втручання у суспільні відносини обумовлені об'єктивними технічними законами та закономірностями розвитку комп'ютерних комунікацій та інформаційних технологій. Також пропонується створити відповідну державну установу, правовий статус якої дозволяв би фіксувати та підтверджувати відповідним правозастосовним органам фактів інформаційної діяльності у мережі Інтернет [7, с. 15].

На думку В. Малахова, головного наукового співробітника Інституту філософії імені Г. Сковороди НАН України, сучасна молодь живе за нав'язаними рекламою стереотипами, уявленнями, які не є результатом внутрішньої роботи. Вона краще поінформована, але не має власних суджень. Більше налаштована на те, що підкажуть Інтернет, ЗМІ, а сама втрачає здатність до самостійного відповідального мислення [8, с. 4].

Отже, необхідним є вдосконалення правового регулювання доступу молоді до інформації негативного характеру, яку вони можуть отримати через Інтернет. Зокрема, доцільним є прийняття окремого законодавчого акту, правові норми якого, докладно б регламентували ці питання. Необхідно також проведення відповідної виховної роботи на рівні сім'ї та школи щодо правил користування інформаційними Інтернет-ресурсами для неповнолітніх.

Національна експертна комісія України з питань захисту суспільної моралі на своєму сайті оприлюднила попередній перелік 50 безпечних сайтів для дітей віком від трьох років. До каталогу «білих сайтів» увійшли безпечні Інтернет-ресурси, які рекомендовані для перегляду дітьми. На думку експертів, створення «білого списку» буде більш дієвим, ніж постійне поповнення «чорного списку» небезпечних сайтів, які з'являються в мережі щохвилини. Цей проект став першою соціальною програмою в Україні, метою якої є протидія поширенню через Інтернет-мережу шкідливої інформації для дітей та підлітків [9, с. 7].

Крім того, останнім часом серед учнів та студентів стало популярним

розповсюдження відео-та фотозображень за допомогою мобільного зв'язку із насильницьким та аморальним змістом: побиття однолітків, статеві акти, різноманітні форми приниження, так званого булінгу (англ. bullying, від bully

– хуліган, забіяка, грубіян, гвалтівник). Це поняття означає залякування, фізичний або психологічний терор стосовно особистості з боку групи дітей, молоді, спрямований на те, щоб викликати в неї страх і тим самим підкорити її собі. Використання мобільних телефонів, чатів, інтернет-сайтів як інструментів булінгу отримало назву «кібербулінг» [10].

Так, відповідно до ст. 5 Закону України «Про захист суспільної моралі», змістом державної політики у сфері захисту суспільної моралі є створення необхідних правових, економічних та організаційних умов, які сприяють реалізації права на інформаційний простір, вільний від матеріалів, що становлять загрозу фізичному, інтелектуальному, морально-психологічному стану населення [11].

Отже, за результатами нашого дослідження, можна зробити такі висновки. По-перше, Інтернет у сучасному суспільстві здійснює неабиякий вплив на свідомість особи неповнолітнього. Але, на теперішній час, можна стверджувати, що Інтернет справляє більше негативного впливу на неформовану особистість неповнолітнього, ніж слугує фактором превентивності його неправомірної поведінки. Варто зауважити, що розширення мережі Інтернет тягне за собою не лише позитивні зміни, а на фоні не контрольованості з боку громадськості та правоохоронних органів створює значні криміногенні загрози. По-друге, Інтернет є сприятливим віртуальним середовищем для формування злочинного світогляду та злочинної культури у неповнолітнього. Правове інформування підростаючого покоління через Інтернет є важливим напрямом формування їхньої правової культури. Для посилення їх впливу на даний процес необхідно активізувати популяризацію правових знань різноманітними каналами ЗМІ та Інтернет.

### **Література:**

1. Бабенко А.М. Кіберзлочинність як чинник негативного впливу на криміногенну ситуацію у регіонах / А.М. Бабенко / Безпека інформації. – 2013. – Том 19 (2). – С.122-117.
2. Бабенко А. М. Мережі Інтернет як об'єкт регіонального дослідження в контексті профілактики злочинності / А. М. Бабенко // Боротьба з Інтернет-злочинністю : матеріали міжнародної наук.-практ. конф. (м. Донецьк, 12-13 червня 2013 р.). – Донецьк: ДЮІ МВС України, 2013. – С. 65–68.

3. Энтеогены и гроверство [Электронный ресурс]. – Режим доступа: <http://okor.org/1post.php>. – Название с экрана.
4. Бабенко А.М. Кримінологічна класифікація регіонів України та її значення для протидії злочинності / А.М. Бабенко // Бюлетень Міністерства юстиції України. – 2013. - № 3 (137). – С. 116-123.
5. Бабенко А.М. Регіональний підхід в кримінології як метод вивчення злочинності/А.М. Бабенко// Проблеми правознавства та правоохоронної діяльності. – 2013. - №1 (52). – С.151-159.
6. Бугера О.І. Інтернет та неповнолітні – кримінологічний аспект / О.І. Бугера[Електронний ресурс]. — Режим доступу: <http://nauka.kushnir.mk.ua/?p=63537> — Назва з екрану.
7. Присяжнюк О.А. Основи концепції правового регулювання інтернет-відносин в Україні (загальнотеоретичні аспекти): автореф. дис. на здобуття наук. ступеня канд. юрид. наук: спец. 12.00.01 «Теорія та історія держави і права; історія політичних і правових учень» / О.А. Присяжнюк; Харк. нац. ун-т внутр. справ. – Х., 2007. – С. 15-16.
8. Опанасенко Л. Правила життя для підростаючого покоління / Л. Опанасенко // Голос України.- 2010. – № 206.- С. 4.
9. Нацкомісія з моралі створила перелік дозволених сайтів // Урядовий кур'єр.- 5 листопада 2010.- № 207.- С. 7.
10. Куницький В.В. Захист неповнолітніх в інформаційному просторі як об'єкт гуманітарної експертизи: український та зарубіжний досвід / В.В. Куницький [Електронний ресурс]. — Режим доступу: <http://www.academy.gov.ua/ej/ej14/txts/Kunitskiy.pdf> — Назва з екрану.
11. Закон України про захист суспільної моралі: за станом на 15 жовтня 2016 р. // Відомості Верховної Ради України. — 2004. — № 14. — С. 192.

### **Деякі питання кримінально-правової характеристики DDOS-атаки**

**Сверба Ю.І.**

студент 6-го курсу Інституту кримінальної юстиції  
Національного університету «Одеська юридична академія»

**Березовська Н.Л.**

кандидат юридичних наук  
доцент кафедри кримінального права  
Національного університету «Одеська юридична академія»

Масштабний розвиток інформаційних технологій, і не менш розвинутий інструментарій для вчинення злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку змушують не тільки практиків, а й теоретиків розробляти надійні механізми протидії, в тому числі кримінально-правовими засобами.

Також, суспільна небезпечність злочинів в сфері використання комп'ютерної техніки головним чином визначається соціальною значущістю тієї діяльності, для інтенсифікації якої використовуються інформаційні технології. Знищення або перекручення інформації призводить до порушення певної діяльності, для здійснення якої вона необхідна. Саме це і визначає суспільну небезпечність конкретного посягання в сфері використання інформаційних технологій [3, с. 70].

Одним з найрозповсюдженіших в Україні з так званих «кіберзлочинів» є несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку за допомогою DDoS-атаки (Distributed Denial-of-service attack – анг.) [2, с. 415-416]. Про поширеність такої злочинної практики свідчать офіційні повідомлення органів державної влади про масові DDoS-атаки на інформаційні сервіси відомств. Так, спроби закриття в лютому 2012 року файлообмінного сервісу «ex.ua» спричинили хвилю протестів, що переросли в масовані DDoS-атаки на ресурси органів державної влади, зокрема на сайт Президента України, Кабінету Міністрів України, Верховної Ради України, Служби безпеки України, Національного банку України та інші.

Крім того, кожен бажаючий в мережі Інтернет може замовити за відносно помірну ціну (15-100 доларів США) DDoS-атаку веб-сайту. Як стверджують самі виконавці таких послуг, вищевказані атаки спрямовані на усунення конкурентів в інформаційному полі, шантаж, тестування програмного забезпечення чи громадський протест. Перелічені цілі злочинців є лише додатковим об'єктом вчинення злочину, оскільки родовий об'єкт – це безпосередньо нормальне та безперебійне функціонування

електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Не акцентуючи увагу на організаційно-технічних засобах вчинення такого злочину, пропонуємо розглянути інші питання кримінально-правової характеристики.

Першочерговою проблемою при кваліфікації DDoS-атаки є відсутність легальної дефініції. Таким чином, теоретично можливо припустити, що будь-які дії, які призвели до блокування процесу обробки інформації на сайті можуть кваліфікуватися за ст. 361 КК України.

На сьогодні, КК України не містить спеціальної норми, яка передбачала б кримінальну відповідальність виключно за DDoS-атаку, хоча в парламенті реєструвалися законопроекти щодо встановлення відповідальності за несанкціоноване втручання в роботу державних електронних інформаційних ресурсів, що призвело до блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації.

Слід зазначити, що сучасна судова практика виходить з того, що особу, яка вчинила DDoS-атаку, слід притягувати до кримінальної відповідальності за ч. 1 ст. 361 КК України, тобто несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації [1]. Однак, перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку є самостійним складом злочину, що передбачений ст. 363-1 КК України.

Проблемним питанням також є і встановлення суб'єкта злочину. Дуже часто DDoS-атаки проводяться з незаконним «залученням» електронно-обчислювальних машин (комп'ютерів) інших користувачів, шляхом, заздалегідь поширених, шкідливих програмних чи технічних засобів, які утворюють так звану «бот-мережу». В результаті, тисячі користувачів можуть і не підозрювати, що регулярно беруть участь в DDoS-атаках [4, с. 38].

Зрозуміло, що такі особи не будуть притягнуті до кримінальної відповідальності в силу відсутності будь-якого умислу, проте, це кардинально ускладнить процес розслідування, а також максимально розширить коло підозрюваних. Крім того, створення «бот-мережі» із застосування шкідливих програмних чи технічних засобів не може розглядатися, як підготовчі дії до вчинення злочину, передбаченого ст. 361 КК України, а повинно кваліфікуватися як самостійний склад злочину, передбачений ст. 361-1 КК України, а саме: створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Виходячи зі змісту ст. 361 КК України, даний злочин з матеріальним складом, тому обов'язковою умовою є настання передбачених наслідків. Як правило, DDoS-атаки спрямовані на неправомірне блокування певних сайтів, яке виникає внаслідок перевантаження серверу. Тому, наслідок у вигляді блокування інформації буде мати місце тоді, коли власник чи уповноважені особи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку не матимуть доступу до інформації, не отримуватимуть її і не матимуть можливості користування нею внаслідок несанкціонованого втручання в роботу.

Підсумовуючи вищевказане та ґрунтуючись на міжнародному досвіді боротьби з DDoS-атаками, можливо констатувати, що в чинному КК України необхідно окремо закріпити відповідальність за вчинення таких дій. До того ж, позитивним буде надання легального визначення DDoS-атаки в спеціалізованих нормативно-правових актах. Це дасть змогу не тільки посилити кібербезпеку державних порталів, які регулярно піддаються таким атакам, а й дозволить призначати покарання за вчинення DDoS-атаки на основі принципу винної відповідальності.

### **Література:**

1. Кримінальний кодекс України: Верховна Рада України; Закон від 05.04.2001 № 2341-III (Редакція станом на 08.10.2016 р.). [Електронний ресурс] – Режим доступу: <http://zakon4.rada.gov.ua/laws/show/2341-14>
2. Бельський Ю. Щодо визначення поняття кіберзлочину / Ю. Бельський// Юридичний вісник: щоквартальний журнал. – 2014. – № 6. – 414-418 с.
3. Карчевський М.В. Питання оптимізації зобов'язань, зумовлених ратифікацією Конвенції про кіберзлочинність / М.В. Карчевський// Бюлетень Міністерства юстиції України. – 2012. – № 3. – 70-74 с.
4. Самошина З.Г. DdoS-атаки как способ совершения преступлений / З.Г. Самошина, Е.Ю. Фурсова // Вестник криминалистики. – 2007. – № 2. – 34-41 с.

**Мукоїда Р.В.**

кандидат юридичних наук, доцент  
професор кафедри ОРД ОДУВС

**Шелехов А.О.**

кандидат юридичних наук, доцент  
завідувач кафедри АД ОВС та  
економічної безпеки факультету № 2 ОДУВС

Величезний технічний потенціал і безмежні можливості Інтернет все частіше в сучасних умовах можуть бути використані в злочинних цілях. Дії кіберзлочинців стають все більш майстерними, що становить реальну проблему для суспільства. Це загострює необхідність боротися зі злочинами такого виду, створення комп'ютерних систем і технологій з підвищеним рівнем безпеки в мережі Інтернет, а також законодавчої бази, що дозволяє карати злочинців належним чином.

Кіберзлочинність - це злочинність в так званому «віртуальному просторі». Віртуальний простір (або кіберпростір) можна визначити як модельований за допомогою комп'ютера інформаційний простір, в якому знаходяться відомості про осіб, предмети, факти, події, явища і процеси, представлені в математичному, символічному або будь-якому іншому вигляді і що знаходяться в процесі руху по локальних і глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального пристрою, а також іншого носія, спеціально призначеного для їх зберігання, обробки і передачі.

Питанням криміналізації суспільно небезпечних діянь у сфері комп'ютерної інформації присвятили наукові праці П.П. Андрушко, С.В. Албул, М.В. Карчевський, В.В. Кузнецов, А.А. Музика, С.О. Орлов, Н.А. Розенфельд та ін. На початку 2003 р. Д. С. Азаров запропонував невідкладно гармонізувати чинне кримінальне законодавство України з положеннями щойно укладеної Міжнародної конвенції про кіберзлочинність [1, с. 13].

Поняття «комп'ютерна злочинність» вперше з'явилося в американський, а потім і в іншій іноземній літературі, на початку шістдесятих років минулого століття і застосовувалось для визначення злочинів, де комп'ютер (чи інший електронно-обчислювальний прилад) є предметом злочину, а інформаційна безпека – об'єкт злочину.

У червні 2001 р. Європейським комітетом з проблем злочинності був розроблений проект Конвенції про кіберзлочинність. У листопаді того самого року Конвенція була затверджена комітетом міністрів Ради Європи і підписана 35 державами, які взяли на себе зобов'язання здійснювати погоджену політику боротьби зі злочинністю у цій сфері. До Конвенції приєдналася і Україна, ратифікувавши її у 2005 році. Проте, навіть через 10 років після ратифікації Конвенції українське законодавство в інформаційно-комунікаційній сфері та у сфері боротьби із кіберзлочинністю у повній мірі не відповідає світовим стандартам та вимогам часу.

За останні 10-15 років поняття «комп'ютерна злочинність» трансформувалось у термін «кіберзлочинність» – поняття, яке охоплює власне комп'ютерну злочинність та інші протиправні діяння, де комп'ютер є знаряддям або способом вчинення злочину проти власності, авторських прав, громадської безпеки, моралі тощо. Відтак, кіберзлочин – це будь-який злочин, який може вчинятися за допомогою комп'ютерної системи або мережі, в рамках комп'ютерної системи або мережі чи проти інформації в комп'ютерній системі або мережі. В принципі, воно охоплює будь-яке злочин, який може бути скоєно в електронному середовищі [2].

Отже, загальноприйнятого визначення комп'ютерної злочинності не існує. Ці злочини тісно пов'язані з ІКТ. Вони часто містять в собі цілий ряд незаконних дій, вчинених за допомогою системи обробки даних або проти неї. Термін охоплює комп'ютер, допоміжне обладнання, програмне забезпечення, засоби зв'язку та телекомунікацій, інформаційні мережі та бази даних, комп'ютерну інформацію тощо [3].

Злочини у сфері ІКТ дуже часто є міжнародними, тобто злочинці діють в одній державі, а їхні жертви перебувають в іншій. Тому для боротьби з такими злочинами особливе значення має міжнародне співробітництво.

У 2001 р. було розроблено Конвенцію Ради Європи «Про кіберзлочинність» [4], що є на сьогодні базовим міжнародним нормативно-правовим актом у сфері боротьби з комп'ютерною злочинністю. Конвенція про кіберзлочинність відкрита для підписання як державами-членами Ради Європи, так і державами, що не є членами Ради, які брали участь у її розробці. Зокрема, Конвенцію підписали США і Японія [5].

Україна у 2005 році ратифікувала Конвенцію про кіберзлочинність, проте нормативно-правова основа боротьби зі злочинами у сфері ІКТ й дотепер залишається недосконалою. Зокрема в законодавстві досі залишаються невизначеними такі терміни як кіберзлочин, кіберзлочинність, кібератака, комп'ютерний тероризм. Таким чином, можна стверджувати, що здебільшого вітчизняне нормативно-правове поле у сфері кібербезпеки оперує термінами та поняттями, визначень яких фактично немає, або вони не узгоджені між різними нормативно-правовими актами.

Отже, Конвенція передбачає чотири групи злочинів, пов'язаних з використанням комп'ютерних технологій як інструменту їх учинення. До першої групи віднесено злочини проти конфіденційності, цілісності й доступності комп'ютерних даних і систем (протизаконний доступ, протизаконне перехоплення, вплив на дані, вплив на функціонування системи, а також протизаконне використання пристроїв і комп'ютерних програм). До другої групи – злочини, пов'язані з використанням комп'ютерних засобів (підроблення, шахрайство). До третьої групи віднесено злочини, пов'язані зі змістом даних (дитяча порнографія). До четвертої – злочини, пов'язані з порушенням авторського права та суміжних прав. Держави, що приєдналися до Конвенції, взяли зобов'язання переглянути своє законодавство, з метою приведення його у відповідність з рекомендаціями, викладеними в цьому міжнародному документі. Аналіз чинного законодавства України свідчить, що за більшість злочинів, зазначених у Конвенції, у нашій країні передбачено кримінальну відповідальність. Так, розділ XVI Особливої частини КК України містить низку статей, що передбачають кримінальну відповідальність за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: ст. 361 (несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку); ст. 3611 (створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут); ст. 3612 (несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації); ст. 362 (несанкціоновані дії з інформацією, яку опрацьовують в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігають на носіях такої інформації, вчинені особою, яка має право доступу до неї); ст. 363 (порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яку в них опрацьовують); ст. 3631 (перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку) [6]. На виконання вимог Конвенції до розділу XVI Особливої частини КК України Законом України від 5 червня 2003 р. № 908-IV внесено відповідні зміни.

Орлов Ю.Ю. зазначає, що перелік кіберзлочинів не вичерпується діями, визначеними в розділі XVI Особливої частини КК України. Певні злочини, що існували задовго до створення комп'ютерів, також можуть бути вчинені із застосуванням інформаційних технологій. Використання комп'ютерів спрощує вчинення злочину або уможливорює його вчинення в нових формах. Отже, ці злочини можна розглядати як такі, що підпадають під дію Конвенції. Зокрема, ідеться про такі злочинні дії: різні види підроблення: грошей, цінних паперів, платіжних карток, знаків поштової оплати, марок акцизного збору, контрольних марок, номерів вузлів та агрегатів транспортних засобів, документів на отримання наркотиків, інших документів тощо (ст. 199, 200, 215, 216, 224, 290, 318, 358, 366 КК України); шахрайство з різними предметами (ст. 190, 192, 222, 262, 308, 312, 313, 357, 410 КК України); увезення, виготовлення, збут і розповсюдження порнографічних предметів (ст. 301 КК України); порушення авторського права й суміжних прав (ст. 176 КК України). [7]

Це говорить про те, що процес гармонізації українського та міжнародного законодавства ще не завершений та вітчизняна нормативно-правова база має бути вдосконалена. Насамперед, потрібно усунути прогалини та певні протиріччя в законодавстві України, чого можна досягти шляхом кодифікації законодавства у сфері боротьби з кіберзлочинністю.

#### **Література:**

1. Азаров Д.С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.08 / Д. С. Азаров. – К. : Ін-т держави і права НАН України, 2003. – 18 с.
2. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М.: ООО Издательство «Юрлитинформ», 2002. – 86 с.



3. Логінова Н.І., Дробожур Р.Р. Правовий захист інформації: Навчальний посібник. – Одеса: Фенікс, – 2015. – 208 с.
4. Конвенція про кіберзлочинність // Офіційний вісник України від 10.09.2007 р.–№ 65.– 2535 с.
5. Malyshev M. Convention on cybercrime: the main objectives and legal aspects // Науково-практична Інтернет-конференція «Інформаційно-комунікаційні технології в сучасному світі: стан, проблеми, перспективи розвитку» (2013 р.): [Електронний ресурс]. – Режим доступу: <http://conf.inf.od.ua/arkhiv/doklady-konferentsii-2013/42-statya-28>.
6. Кримінальний кодекс України : Закон України від 5 квіт. 2001 р. № 2341-III [Електронний ресурс]. – Режим доступу : <http://www.liga.net>.
7. Актуальні напрями державної політики України у сфері боротьби з кіберзлочинністю / О. В. Орлов, Ю. М. Онищенко // Теорія та практика державного управління. - 2013. - Вип. 3. - С. 3-9. - Режим доступу: [http://nbuv.gov.ua/j-pdf/Tpdu\\_2013\\_3\\_3.pdf](http://nbuv.gov.ua/j-pdf/Tpdu_2013_3_3.pdf)

### **Кібербезпека як об'єкт кримінально-правової охорони**

**Березовська Н. Л.**

кандидат юридичних наук, доцент,  
доцент кафедри кримінального права Національного університету  
«Одеська юридична академія»

Д.В. Дубов та М.А. Ожеван зазначають, що на сьогоднішній день більшість потужних держав світу (США, Росія, ЄС, Китай, Індія та інші) перебувають у процесі трансформації власних військових підрозділів з огляду на можливості використання мережі Інтернет. За даними керівника компанії McAfee, оприлюдненими на Всесвітньому економічному форумі в Давосі у 2010 р., у 2009-2010 рр. уже понад 20 країн планували або здійснили різноманітні інформаційні операції. Формуються спецпідрозділи, що мають на меті: ведення розвідувальної роботи в мережах, захист власних мереж, блокування і “обвал” структур супротивника із використанням можливостей кіберпростору. Згідно з офіційними заявами такі підрозділи створено у США (U.S. Cyber Command), Великобританії (урядовий Cyber Security Operations Centre), Німеччині (Internet Crime Unit та Federal Office for Information Security), Австралії (The Cyber security operations centre), Індії та інших державах. Активну позицію щодо протидії кіберзагрозам посідає провідна міжнародна безпекова організація – НАТО (Cooperative Cyber Defence Centre of Excellence). Таким чином, провідні держави світу все більше уваги приділяють розвитку та захисту власних інформаційних ресурсів, а також можливості впливати на інформаційні ресурси інших країн, що в цілому вигляді описується проблемою забезпечення кібербезпеки держави [1, с.4].

Хан Н. вказує на важливість кібербезпеки, що поступово зростає в сучасному світі. У той час як набуває поширення використання інформаційних та комунікаційних технологій (ІКТ), зростають можливості їхнього застосування та їхня важливість. У результаті залежність громадських та приватних організацій безпосередньо пов'язана з їхньою вразливістю перед зовнішнім втручанням. Очікується, що кіберзалежність та вразливість ІКТ буде зростати в майбутньому. Більше того, дедалі більша кількість ключових елементів національної інфраструктури ставатиме головною метою кібератак. Водночас покращення в сфері кібербезпеки будуть спричинені підвищенням рівня обізнаності в безпечних питаннях приватних і громадських акторів, що дозволить їм захищатися від цих атак. Однак, якби не були здійснені заходи в сфері кібербезпеки, дедалі більша залежність від ІКТ неминуче призводитиме до зростання числа успішних кібератак. Сторона, що прицілюється, завжди буде трохи попереду від сторони, що є ціллю, через ефект неочікуваності і впровадження новітніх технологій [2, с.1].

Політика країн Заходу у сфері внутрішнього інформаційного (кіберпростору) дедалі частіше набуває окремих рис політики тих країн, що традиційно відносять до авторитарних, щоправда у цих процесах мають місце суттєві відмінності. Якщо в країнах авторитарного типу передусім здійснюється політика прямого обмеження доступу, то країни Заходу нарощують кількість даних про користувачів, здійснюють моніторинг національного інтернет-трафіку та створюють можливості цільового відключення окремих елементів мережі або її користувачів. Такий акцент на «моніторинговому дискурсі» обумовлений, зокрема, зростанням кількості телекомунікаційних послуг та мереж, контроль за якими є складним для державних правоохоронних служб. Це стосується, наприклад, контролю за розмовами власників смартфонів та VoIP-системи. Зокрема смартфони Blackberry підтримують систему шифрування даних, що передаються, а сервери цих

компаній розташовані у США та Великобританії, що унеможливило контроль за спілкуванням користувачів Blackberry та потенційно робить доступним листування власників смартфонів для американських і британських спецслужб. Саме це стало причиною введення обмежень (особливо в державному секторі) на використання цих засобів зв'язку у Франції, Німеччині, Індії, Об'єднаних Арабських Еміратах та Російській Федерації. Крім того, співробітникам керівних структур ЄС також заборонено користуватись смартфонами зазначеної фірми. Щодо VoIP-телефонії, то основні претензії висуваються до програмного продукту Skype, оскільки він забезпечує ефективний криптографічний захист розмов абонентів, що практично унеможливляє перехоплення їх з боку спецслужб. Це стало однією з причин конфлікту між авторами програми та спецслужбами деяких країн (Італія, Російська Федерація, Індія, Німеччина, Великобританія). Крім того, в 2010 році уряд США додатково виділив для ФБР 234 млн. дол. для спеціального проекту з «прослуховування Інтернету» (Advanced Electronic Surveillance –Going Dark), спрямованого передусім на можливість прослуховування Інтернет-комунікаторів (наприклад, того ж Skype) [1, с.7].

Актуальність розгляду захисту кібербезпеки останнім часом набуває розголосу не лише в міжнародних чи зарубіжних джерелах. Баранов О.А. зазначає: «Кібербезпека – це деякий стан систем, за якого нейтралізуються загрози доступності, цілісності або конфіденційності даних, що циркулюють в інформаційних системах. Крім того, завдяки включенню до переліку об'єктів, на які можуть діяти якісь загрози з кіберпростору, послуг інформаційних систем це визначення терміна дозволяє мати на увазі наявність якихось загроз функціональності систем більш високого порядку, до яких в якості складових елементів входять інформаційні системи. Це положення має важливий методологічний зміст у розумінні місця і ролі проблеми кібербезпеки в контексті інших видів безпеки» [3, с.55].

На рівні національних та міжнародних стратегічних документів визначення кібербезпеки значно різняться. А значить, розрізняються і підходи не тільки до змісту відповідних стратегій, а й до змісту планів дій із забезпечення кібербезпеки. Однак транскордонний характер цієї проблеми настійливо диктує необхідність координації зусиль як на національному, так і на міжнародному рівні. Передусім, мова йде про осмислення суті кіберзагроз, змісту робіт щодо забезпечення кібербезпеки, чітке визначення цілей стратегії і власне визначення змісту самого терміну «кібербезпека» [3, с.57].

Тому тема потребує подальших наукових досліджень з ціллю закріплення переліку злочинних діянь в самостійний розділ КК України. Щодо виділення такого окремого виду безпеки як кібербезпека, видається, слід піти шляхом запозичення світового досвіду і відобразити захист кібербезпеки в національному законодавстві.

#### **Література:**

1. Дубов Д.В., Ожеван М.А. Кібербезпека: світові тенденції та виклики для України: аналітична доповідь. – К.: НІСД, 2011. – 30 с.
2. Хан Н. Майбутнє кібербезпеки: [Електронний ресурс] – Режим доступу: <http://iwp.org.ua/img/Cybersecurity.pdf>
3. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека» // Правова інформатика. – № 2(42). – 2014. – С.54-62.

#### **Щодо актуальності імплементації міжнародних стандартів кібербезпеки до національного законодавства України**

**Шуміло О.О.**

асистент кафедри кримінології та кримінально-виконавчого права  
Національного юридичного університету імені Ярослава Мудрого

**Голіна В.В.**

доктор юридичних наук, професор  
професорка кафедри кримінології та кримінально-виконавчого права  
Національного юридичного університету імені Ярослава Мудрого

Сьогодні в усьому світі відбувається об'єктивна зміна вектору розвитку суспільства: від індустріального до інформаційного, від національних стратегій розвитку до міжнародних. Розвиток інформаційного суспільства супроводжується негативними процесами протиправного використання комп'ютерних і телекомунікаційних технологій. З урахуванням специфіки феномену кіберзлочинності,

масштабів інформатизації та розвитку глобальної мережі Internet стає все менш імовірним, що злочини такого виду оминуть бодай одну державу, що ставить нові виклики науці кримінології [5, с. 67]. Транснаціональність загроз в кіберпросторі та рівень збитків під час їхньої реалізації змушують ставити проблему забезпечення інформаційної безпеки як глобальну, що вимагає зусиль всього світового співтовариства. Кількість злочинів, скоєних в кіберпросторі, зростає пропорційно числу користувачів комп'ютерних мереж, і, за оцінками Інтерполу, темпи зростання злочинності в глобальній мережі Internet є найшвидшими на планеті [1].

Так, за даними міжнародної служби щодо забезпечення безпеки в області кіберзагроз Symantec Security, щосекунди в світі піддаються кібератаці 12 осіб, а щорічно в світі реєструється близько 556 млн кіберзлочинів, збиток від яких становить понад 100 млрд дол. США [2]. Глобальна природа кіберзлочинності проявляється в її транснаціональному характері: готується і вчиняється кіберзлочин в одній країні, а шкода завдається в іншій. Так, в списку країн з високим рівнем скоєних злочинів у віртуальному середовищі Україна неодноразово обіймала найвищі позиції і водночас належить до групи найбільш незахищених від кіберзагроз держав [4]. Відповідно до останніх кримінологічних досліджень, середньорічний темп приросту кіберзлочинності в Україні протягом 2002–2015 рр. складає 107,5 % [7, с. 4], що надає могутній поштовх для вироблення своєчасних і ефективних заходів для запобігання цьому виду злочинів і запозичення найкращих практик країн ЄС.

Одним із основних міжнародних актів у цій галузі є Конвенція про кіберзлочинність (Будапештська конвенція), ухвалена Радою Європи 23 листопада 2001 р. і ратифікована Україною 7 вересня 2005 р. із деякими застереженнями і заявами [6]. Станом на 2016 р., Будапештську конвенцію ратифікували усі держави Ради Європи (за винятком Російської Федерації і Сан-Маріно), а також США, Канада, Австралія, Японія та деякі інші країни, ще понад сто держав взяли документ за основу для національного законодавства у сфері протидії кіберзлочинності [3, с. 7].

Серед ключових вимог Конвенції можна виокремити наступні:

- встановлення кримінальної відповідальності за дії, спрямовані проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними у національному законодавстві;
- створення спеціальних інститутів дотримання правопорядку у кіберпросторі;
- забезпечення належного балансу між правоохоронними інтересами і повагою до основних прав людини;
- активна участь у міжнародному співробітництві з указаних питань.

Таким чином, для того щоб національна система кібербезпеки відповідала рівню економічно розвинених країн, необхідно вжити послідовні дії з боку держави, спрямовані на підвищення ефективності та розвиток системи взаємодії учасників кіберпростору. Ці та інші положення знайшли відбиток у нещодавно затвердженій Указом Президента Стратегії кібербезпеки України, покликаний захистити життєво важливі інтереси людини і громадянина, суспільства та держави в кіберпросторі за допомогою цілісного комплексу правових, організаційних та інформаційних заходів [8]. На нашу думку, її позитивна імплементація залежатиме, перш за все, від дотримання належного балансу між захистом від кіберзагроз і забезпеченням основоположних прав людини; уникнення корупційних законодавчих новел, а також своєчасного виявлення та розробки заходів протидії новітнім протиправним практикам (фішинговим атакам, використанню зі злочинною метою хмарних сховищ і криптовалют тощо).

### **Література:**

1. Cybercrime [Electronic resource]: Interpol. Connecting Police for a Better World. – Access mode: <http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime> (date of treatment 15.04.2016). – Title from the screen.
2. Managing cyber risks in an interconnected world. Key findings from The Global State of Information Security Survey 2015 [Electronic resource]: United States Department of Labor. – Access mode: <http://www.dol.gov/ebsa/pdf/erisaadvisorycouncil2015security3.pdf> (date of treatment 15.04.2016). – Title from the screen.
3. Seger A. The Budapest Convention on Cybercrime and the Rule of Law in Cyberspace / A. Seger // Synergy. – № 59. – P. 6-10.
4. Ukraine 2014 Crime and Safety Report [Electronic resource]: United States Department of State. Bureau of Diplomatic Security – Access mode: <https://www.osac.gov/pages/ContentReportDetails.aspx?cid=16409> (date of treatment 15.04.2016). – Title from the screen.

5. Головкін Б. М. Поняття, предмет, система кримінології та її завдання на сучасному етапі розвитку / Б. М. Головкін // Питання боротьби зі злочинністю : зб. наук. пр. – Харків, 2014. – Вип. 28. – 59–68с. – 67 с.

6. Конвенція про кіберзлочинність [Електронний ресурс]: Верховна Рада України. – Режим доступу: [http://zakon0.rada.gov.ua/laws/show/994\\_575](http://zakon0.rada.gov.ua/laws/show/994_575) (дата звернення 15.04.2016). – Заголовок з екрана.

7. Кравцова М. О. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ автореф. дис. ... канд. юрид. наук : 12.00.08 / М. О. Кравцова ; Харк. нац. ун-т внутр. справ. - Харків, 2016. – 16 с. – с. 4.

8. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [Електронний ресурс]: Верховна Рада України. – Режим доступу: <http://zakon4.rada.gov.ua/laws/show/96/2016> (дата звернення 15.04.2016). – Заголовок з екрана.

### **До проблеми розуміння кіберзлочинів проти власності**

**Дорохіна Ю.А.**

кандидат юридичних наук, доцент  
доцент кафедри адміністративного, фінансового та інформаційного права  
Київського національного торговельно-економічного університету

Сучасна правова політика України ґрунтується на ліберальних ідеях, заснованих на прагненні до свободи, демократизму, гуманізму, на визнанні пріоритетності прав особи. Зокрема, як слушно наголошує Френсіс Фукуяма, «лібералізм як світоглядна та політична концепція приречений на перемогу. З огляду на значний вплив лібералізму у світі (надто на Заході та в межах безпосереднього американського впливу), а також на поширення та популяризацію ліберальних уявлень в посткомуністичній Україні, згадане положення стало майже аксіомою для багатьох українських політиків та науковців» [1]. Важливим напрямом правової політики є протидія злочинності, що покликана знизити її рівень та забезпечити стан, який відповідає потребам захисту суспільства від злочинів [2, с. 232].

Сьогодні позитивний прогрес та перехід сучасного суспільства до стадії його розвитку, як «інформаційного» обумовив підвищення цінності передачі та використання інформації. Проте сучасний прогрес світового співтовариства дістає вияв не тільки в багатьох позитивних аспектах, а й у деструктивних, злочинних і небезпечних для подальшого плідного розвитку відносин власності формах.

Так, швидкий розвиток інформаційно-комунікаційних технологій, зокрема мережі Інтернет, вплинув на збільшення способів злочинних посягань на власність. Слід наголосити, що прогрес злочинного світу завжди історично і логічно передуює виникненню потреб у врегулюванні поведінки людей в тому чи іншому напрямі. Натомість коли потреби інституціоналізуються або принаймні виявляються, вони мають оформлюватися як норма права і, в разі усвідомлення і офіційного визнання державно-організованим суспільством, ставати кримінальним законом.

Викладене, безперечно, актуалізується у зв'язку з тим, що сьогодні роль власності змінюється; особливу роль набуває так звана інформаційна власність. Це пов'язано з тим, що світова спільнота вступила в нову епоху – епоху інформаційного суспільства, в якій життєдіяльність людства певною мірою залежить від телекомунікаційних технологій, які використовуються практично у всіх сферах діяльності людини (енергетика, водопостачання, фінанси, торгівля, наука, освіта тощо).

Відповідно розвиток інформаційного простору зумовлює необхідність активізації зусиль суспільства щодо його захисту від злочинних посягань, сукупність яких вже має свою власну, відому у всьому світі назву – кіберзлочинність, яка набула широкого поширення і в сучасних умовах та становить одну з найбільш небезпечних загроз для українського суспільства. Стрімкий розвиток телекомунікацій і глобальних комп'ютерних мереж створив умови, які полегшують вчинення кіберзлочинів проти власності та утворюють нові склади. Злочинці все частіше використовують нові способи зараження комп'ютерів шкідливими програмами, які дозволяють отримувати злочинний прибуток. Так, відповідно до Звіту NCR (Norton Cybercrime Report), жертвами кіберзлочинності у 2012 р. стало 341 млн, а у 2015 р. – вже 594 млн осіб. Близько 70% інтернет-користувачів хоча б раз стикалися з шахрайством в мережі, і ці показники щорічно збільшуються [3, с. 208; 4].

Сьогодні за допомогою використання шкідливих комп'ютерних програм і програмно-технічних засобів, підключених до комп'ютерної мережі, можуть вчинятися більшість злочинів проти власності, передбачених розділом VI Особливої частини КК України. Виняток становлять лише злочини, спосіб

вчинення яких пов'язаний з безпосереднім контактом злочинця з потерпілим, а також значна частина злочинів, предметом яких може бути лише матеріалізоване майно. Від того, що злочини проти власності вчиняються шляхом використання електронно-обчислювальної техніки та новітніх інформаційно-комунікативних технологій, вони не змінюють об'єкт свого посягання; у цьому випадку відбувається приєднання додаткового об'єкту, що збільшує та якісно змінює суспільну небезпеку від злочину. У зв'язку з цим сучасна система норм, яка відображає злочини проти власності, потребує вдосконалення, оскільки вона не повною мірою враховує сучасні кіберзагрози.

Злочини проти власності, які вчиняються шляхом використання інформаційно-комунікативних технологій (кіберзлочини проти власності), характеризуються такою ознакою, як вчинення злочину щодо великого і, як правило, невизначеного кола потерпілих. Це призводить до того, що практично неможливо точно встановити розмір завданої шкоди, а подекуди цей розмір (щодо одного потерпілого) замалий для притягнення винного до кримінальної відповідальності. Таким чином, постає питання: чи може у такому випадку розмір шкоди бути ознакою складу злочину, яка відображає характер і міру суспільної небезпеки? Звісно, що ні. Злочини проти власності, які вчиняються шляхом використання інформаційно-комунікативних технологій, не можна кваліфікувати як замах на злочин у великому або особливо великому розмірі, оскільки згідно з кримінально-правовою теорією в даному випадку є невизначений (неконкретизований) умисел. За таких обставин злочин має кваліфікуватися за наслідками, що фактично настали.

На відміну від злочинів у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж і мереж електрозв'язку, основною властивістю кіберзлочинів проти власності є те, що суб'єкт злочину використовує комп'ютерні мережі як знаряддя або засіб вчинення злочину.

Щодо осіб, які вчиняють злочини проти власності шляхом використання електронно-обчислювальної техніки, необхідно зазначити, що частіше за все вони не тільки володіють спеціальними навичками в сфері користування електронно-обчислювальною технікою та відповідними пристроями, а й можуть користуватися паролями і ключами банківських програм, застосовувати свої спеціальні знання для фальсифікації програм шляхом зміни правильних вихідних даних. Зазвичай це – оперативні працівники банків різних посадових рівнів, програмісти й оператори комп'ютерів.

Корисливі кіберзлочини вчиняють і так звані «хакери» – переважно молоді люди, добре технічно і професійно підготовлені для роботи з електронно-обчислювальною технікою та зі складання комп'ютерних програм. Дослідження показують, що безпосередній несанкціонований доступ до електронно-обчислювальної техніки, систем та комп'ютерних мереж вчинюється співробітниками банків: програмістами, інженерами, операторами, які є користувачами або обслуговуючим персоналом такої техніки (41,9%) [5, с. 12]. Майже удвічі менше такий доступ використовують інші співробітники банку (20,2%); в 8,6% випадків злочин було вчинено співробітниками, які були звільнені, а у 25,5% несанкціонований доступ вчинявся сторонньою особою [6, с. 28].

Саме це додає таким злочинам унікальних властивостей, не притаманних для інших злочинних посягань. Таким чином, поняття злочинів проти власності, що вчиняються шляхом використання інформаційно-комунікативних технологій, можна визначити у вигляді сукупності заборонених кримінальним законодавством діянь, спосіб вчинення яких передбачає обов'язкове використання таких технологій (мереж) як знаряддя або засобу. До того ж, зміст об'єкту цих злочинів може бути різним і не бути пов'язаним з суспільними відносинами, що виникають в інформаційній сфері.

### **Література:**

1. Фукуяма Ф. Кінець історії та остання людина [Електронний ресурс]. – Режим доступу: <http://lib.chdu.edu.ua/pdf/posibnuku/307/40.pdf>.
2. Борисов В. І. Сучасна політика держави у сфері боротьби зі злочинністю та її кримінально-правовий напрям // Право України. – 2012. – № 1-2. – С. 232.
3. Логінова Н.І. Правовий захист інформації: Навчальний посібник. / Н.І. Логінова, Р.Р. Дробожур – Одеса: Фенікс, 2015. – С. 208.
4. 2015 Internet Security Threat Report [Електронний ресурс]. – Режим доступу: [http://www.symantec.com/security\\_response/publications/whitepapers.jsp](http://www.symantec.com/security_response/publications/whitepapers.jsp).
5. Яблоков Н.П. Криминалистическая характеристика финансовых преступлений // Вестник московского университета. Серия 11. Право. – 1999, № 1. – С. 11–13.
6. Біленчук П.Д. Комп'ютерні злочини: соціально-правові і кримінологічно-криміналістичні аспекти: Підручник / П.Д. Біленчук, М.А. Зубань – К., 1994. – С. 28.

**Задніченко С.І.**

здобувач кафедри кримінального права НАВС,  
заступник начальника організаційно-аналітичного управління –  
начальник відділу поточного та стратегічного планування ДООЗОР  
Національної поліції, полковник поліції

Неправомірна вигода включає у себе не тільки отримання грошових коштів чи іншого майна, а й переваг, пільг, послуг, нематеріальних активів. І так, тепер детальніше розглянемо понятійний аспект «нематеріальні активи». Нематеріальний актив — об'єкти інтелектуальної, в тому числі промислової власності, а також інші аналогічні права, визнані у порядку, встановленому відповідним законодавством, об'єктом права власності платника податку. Інтелектуальна власність (скорочено «ІВ», англ. intellectual property) — результат інтелектуальної, творчої діяльності однієї людини (автора, виконавця, винахідника та інш.) або кількох осіб. Право інтелектуальної власності — у найширшому розумінні означає закріплені законом права на результат інтелектуальної діяльності в промисловій, науковій, художній, виробничій та інших галузях. До інтелектуальної власності через зазначення об'єктів інтелектуальної власності відноситься авторське право і один із видів є комп'ютерні програми.

Комп'ютерна програма (англ. Computer program) — набір інструкцій у вигляді слів, цифр, кодів, схем, символів чи у будь-якому іншому вигляді, виражених у формі, придатній для зчитування (комп'ютером), які приводять його у дію для досягнення певної мети або результату (це поняття охоплює як операційну систему, так і прикладну програму, виражені у вихідному або об'єктному кодах) [2]. По іншому комп'ютерну програму визначають, як низку команд для комп'ютера, що становлять запис алгоритму однією з мов програмування[2].

Комп'ютерна програма вільного користування (вільне (відкрите) програмне забезпечення, програмне забезпечення з відкритим кодом) – комп'ютерна програма, яка розповсюджується на умовах договору приєднання (вільної публічної ліцензії), що надає особі, яка приєдналася до такого договору, безоплатний дозвіл на: використання комп'ютерної програми з будь-якою метою; доступ до вихідного коду; будь-які дослідження механізмів функціонування програми; використання механізмів (принципів) функціонування будь-яких довільних частин коду програми для створення інших програм та (або) адаптації до потреб користувача; відтворення комп'ютерної програми і розповсюдження її примірників будь-яким способом та в будь-якій формі; внесення змін і вільне розповсюдження як оригінальної комп'ютерної програми, так і зміненої, на тих самих умовах, під які підпадає і оригінальна комп'ютерної програма, якщо інше не передбачено ліцензією. Програма може записана у текстовому вигляді на мовах програмування, подана у графічному вигляді за допомогою блок-схем, занесена до пам'яті обчислювальної системи у вигляді електричних сигналів або збережена на носіях інформації у вигляді файлу.

Комп'ютерні програми, якщо їх не подано у вигляді послідовності машинних кодів системи команд процесора обчислювальної системи, необхідно попередньо перетворити в такі коди за допомогою компілятора, або виконати програму, використавши програмний інтерпретатор. Функціонально комп'ютерні програми поділяються на системні програмні засоби та прикладні програмні засоби. Основною системною програмою є операційна система, що пов'язує комп'ютерне обладнання з прикладними програмами. Призначення операційної системи — надати оточення, в якому прикладна програма виконується в зручний та ефективний манер [2] На додаток до операційної системи, до системних програм також відносяться утиліти що допомагають керувати та налаштовувати комп'ютер. Програми, основною ціллю яких є підтримка або покращення роботи користувача, називаються прикладними. До прикладних програм також відносяться утиліти, що виконують прикладні функції, наприклад, упорядкування даних.

У українському законодавстві нематеріальні активи діляться на 4 групи і одним з об'єктів права інтелектуальної власності виступає: є право власності на програми для ЕОМ. Право на публікацію, відтворення, розповсюдження і інші дії з введення в господарський обіг сукупності даних і команд, які призначені для функціонування ЕОМ і інших комп'ютерних пристроїв з метою отримання певного результату. Право власності на базу даних. Право на публікацію, відтворення, розповсюдження і інші дії з введення в господарський обіг сукупності даних (статей, розрахунків, і т.п.), які систематизовані для пошуку і обробки за допомогою ЕОМ. Право власності на науково-технічну інформацію. Об'єктом науково-технічної інформації можуть бути: результати науково-технічних, виробничих робіт і іншої науково-технічної діяльності, які зафіксовані у формі, яка забезпечує їх відтворення, використання і розповсюдження.

Оскільки Україна відноситься до континентальних правових систем, ключові положення права інтелектуальної власності містяться у Четвертій книзі Цивільного кодексу України.

Комп'ютерні програми на території України охороняються законом як літературні твори. Така охорона поширюється на комп'ютерні програми незалежно від способу чи форми їх вираження. Відповідно до п. 5 ст. 15, Закону України «Про авторське право і суміжні права» Відповідно до положень Бернської конвенції «Про охорону літературних і художніх творів», до якої Україна приєдналася (Закон України від 31.05. 95 р. №186/95-ВР) і з 25 жовтня 1995 р. стала її членом, комп'ютерні програми захищаються як літературні твори. Радою Європейських Співтовариств в травні 1991 р. прийнята Директива Ради щодо юридичної охорони комп'ютерних програм (91/250/СЄЕ) як літературних творів. Зазначені міжнародні норми гармонізовані в Законі України «Про авторське право і суміжні права», відповідно до статті 18 якого зазначено, що «Комп'ютерні програми охороняються як літературні твори. Така охорона поширюється на комп'ютерні програми незалежно від способу чи форми їх вираження».

Разом з тим, програмістів цікавить, які мотиви стали визначальними для такого поєднання. Одне з пояснень, яке не може вважатися офіційним, полягає в тому, що відповідно до норм авторського права захищається форма, в якій втілюється авторське бачення тієї або іншої ідеї, проблеми, процесів тощо. За характером форми відображення, рядки літературного твору і комп'ютерної програми мають дещо спільне; і рядки літературного твору, і рядки комп'ютерної програми автор наповнює символами — літерами або символами — операторами. Тотожність творчого процесу щодо створення форм авторських творів літератури і комп'ютерних програм стали визначальними для вибору форми захисту для комп'ютерних програм. В разі експертизи порушення авторських прав на літературний твір чи комп'ютерну програму, порівнюються відповідні тексти літературних творів, а для комп'ютерних програм — тексти зазначених програм.

Однак, з 2008 р. Україна зобов'язалася застосовувати стандарти охорони інтелектуальної власності, передбачені Угодою ТРІПС. І хоча ТРІПС, аналогічно до Закону України «Про авторське право та суміжні права», передбачає охорону комп'ютерних програм за режимом охорони літературних творів, однак не забороняє використання і режиму патентування (ст.27 ТРІПС). Це означає, що «держава-член СОТ має надати зазначені у ТРІПС права приватним особам», що і дозволяє патентувати програми.

Органом який займається реєстрацією авторських прав та патентів в Україні, є Державна служба інтелектуальної власності, яка серед іншого відповідає за «проведення експертизи заявок на об'єкти права інтелектуальної власності, видає патенти/свідчення на об'єкти права інтелектуальної власності». Законодавство, яке визначає права на інтелектуальну власність, базується на праві кожного володіти, користуватися і розпоряджатися результатами своєї інтелектуальної, творчої діяльності, які, будучи благом не матеріальним, зберігаються за його творцями і можуть використовуватися іншими особами лише за узгодженням з ними, крім випадків, визначених законодавством.

### **Література:**

1. Пастухов О.М. Авторське право у сфері функціонування всесвітньої інформаційної мережі Інтернет. Автореф. дис. ... канд. юрид. наук. - Київ, 2002. - С. 9.
2. <https://uk.wikipedia.org/wiki/>

### **Кібербезпека в Україні: сучасний стан**

**Іващенко Ю.К.**

курсант факультету підготовки фахівців  
для підрозділів органів досудового розслідування  
Дніпропетровського державного університету внутрішніх справ

**Черняк Н.П.**

кандидат юридичних наук, доцент  
доцент кафедри кримінального процесу  
Дніпропетровського державного університету внутрішніх справ

Науково-технічна революція наприкінці ХХ початку ХХІ сторіччя спричинила у всьому світі системні перетворення. Ці перетворення стали поштовхом для формування і розвитку новим глобальним субстанціям — інформаційному суспільству та інформаційному і кібернетичному просторам, які мають в наш час, практично, не обмежений потенціал та відіграють важливу роль в соціальному та економічному розвитку будь-якої зі світових країн. Водночас неконтрольоване



поширення і використання інформаційно-комунікативних технологій та інформаційно-телекомунікаційних систем призвело до отримання, не тільки переваг, а ще й до певних проблем. Саме ці аспекти визначили політичну необхідність контролю та регулювання взаємовідносин у сфері «кібернетики» та дали підстави стверджувати про актуальність процесу створення надійної системи кібернетичної безпеки, без якої може бути втрачена політична незалежність будь-якої з держав світу, до фактичного програшу нею війни невійськовими засобами та підпорядкування її національних інтересів інтересам проти бічної сторони [1; 2].

Кибербезпеку можна визначити як стан захищеності кіберпростору держави в цілому або окремих об'єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і/або національним інтересам [3, с.15]

Досягається такий стан завдяки сукупності активних захисних і розвідувальних дій, що у процесі інформаційного протиборства зусиллями поодиноких інсайдерів або організованих кіберугруповань розгортаються навколо ІР, ІКТ і ІТС.

Поширюються випадки незаконного збирання, зберігання, використання, знищення, поширення, персональних даних, незаконних фінансових операцій, крадіжок та шахрайства у мережі Інтернет. Киберзлочинність стає транснаціональною та здатна завдати значної шкоди інтересам особи, суспільства і держави, тому тематика кібербезпеки в Україні регулюється на найвищому державницькому рівні. Відсутність цілісного обговорення кібербезпекових питань у ширшому колі і є проблемою того, що в Україні досі відсутні системні нормативні документи, які описували б загрози Україні саме в кіберпросторі, визнали б їх і стали основою для цілісної державної політики з кібербезпеки. Досить умовно чи не єдиним документом, у якому прямо йдеться про кіберзагрози, – це ратифікована Верховною Радою України «Конвенція про кіберзлочинність» від 07.09.2005 р. [4]. Конвенція, хоч і стосується проблематики убезпечення кіберпростору, але, все ж таки, більше зосереджена на протидії карним діям з використанням комп'ютерної техніки (шахрайство, підроблення, поширення дитячої порнографії, порушення авторських прав та ін.).

Вирішення та унормування даної проблеми, можливе лише через створення відповідних нормативних документів. Протягом останніх років Україна, як і більшість країн світу, робить певні кроки в розбудові інформаційного суспільства, забезпечення інформаційної кібербезпеки, а також у боротьбі з кіберзлочинністю. Слід зазначити, що нормативно-правову базу в цих сферах діяльності становлять такі документи: Конвенція Ради Європи про кіберзлочинність, ратифікована Законом України від 7.09.2005 року № 2824-IV; Закони України «Про інформацію»; «Про основи національної безпеки України»; «Про Державну службу спеціального зв'язку та захисту інформації України»; «Про телекомунікації»; «Про захист інформації в інформаційно-телекомунікаційних системах»; «Про доступ до публічної інформації», «Про оборону України», «Про засади внутрішньої і зовнішньої політики»; Укази Президента України, зокрема про Доктрину інформаційної безпеки; Стратегію національної безпеки України та Воєнну доктрину України; окремі положення Кримінального кодексу України, окремі постанови Кабінету Міністрів та рішення РНБОУ [5, с.16-17].

Національна система кіберзахисту насамперед забезпечує взаємодію з питань кібербезпеки державних органів, органів місцевого самоврядування, навчальних закладів, громадських об'єднань, а також підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками об'єктів критичної інфраструктури, військових формувань, правоохоронних органів, наукових установ.

У відповідності до Стратегії кібербезпеки України основними суб'єктами забезпечення кібербезпеки є: Рада національної безпеки і оборони України; Міністерство оборони України; Державна служба спеціального зв'язку та захисту інформації України; Служба безпеки України, Національна поліція України, Національний банк України, та ін..

Отже боротьба з кіберзлочинністю полягає в здійсненні багатьох заходів, а саме: створення ефективного і зручного контакт-центру для повідомлень про випадки злочинів у сфері кібернетики та шахрайства у кіберпросторі, підвищення оперативності реагування на кіберзлочини правоохоронних органів, зокрема їх регіональних підрозділів; удосконалення процесуальних механізмів щодо збирання доказів в електронній формі, що стосуються злочину, удосконалення методів, засобів і технологій ідентифікації та фіксації кіберзлочинів, проведення експертних досліджень; запровадження блокування операторами та провайдерами телекомунікацій визначеного інформаційного ресурсу за рішенням суду; збереження даних про трафік; врегулювання питання можливості термінового здійснення процесуальних дій у режимі реального часу із застосуванням електронних документів та електронного цифрового підпису; та ін. [4].

### Література:

1. A Solution-based Examination of Local, State, and National Government Groups Combating Terrorism and Cyberterrorism. By: Matusitz, Jonathan; Breen, Gerald-Mark. Journal of Human Behavior in the Social Environment, Feb 2011, Vol. 21 Issue 2, p. 109-129, 21 p. [Електронний ресурс]. – Режим доступу: <http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN>.
2. Руководство по кибербезопасности для развивающихся стран. [Електронний ресурс]. – Режим доступу: <http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-r.pdf>.)
3. Конвенція про кіберзлочинність (набула чинності 01.07.2006) // Верховна Рада України [Електронний ресурс]. – Режим доступу: [http://zakon4.rada.gov.ua/laws/show/994\\_575](http://zakon4.rada.gov.ua/laws/show/994_575)
4. Стратегія кібербезпеки України, затверджена Указом Президента України від 15.03.2016, №96/2016
5. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. - К.: ДУТ, 2015. - 288 с.

### Правова природа та доказове значення висновку експерта у кримінальних провадженнях про кіберзлочини

**Калініна І.В.**

кандидат юридичних наук  
завідувач кафедри спеціально-правових дисциплін  
Донецького державного університету управління

Судова експертиза є найбільш кваліфікованою формою використання спеціальних знань під час доказування у кримінальному провадженні. Експертиза значно розширює пізнавальні можливості слідства та суду, дозволяючи використовувати під час досудового розслідування та судового розгляду матеріалів кримінального провадження весь арсенал сучасних науково-технічних засобів, який постійно розвивається шляхом створення нових та вдосконалення існуючих методик дослідження та знаходить все ширше застосування у судово-слідчій практиці. Висновок експерта, який, своєю чергою, складається за результатами проведення експертного дослідження, є одним із передбачених Кримінальним процесуальним кодексом України (КПК України) джерел доказів.

Висновок експерта – це письмове повідомлення про хід і результати проведеного експертом (обізнаною особою) дослідження та його висновки з вирішуваних питань.

Корені погляду на експертизу як на «особливий» доказ сягають у теорію, яка визначала експерта науковим суддею. Л. Владимиров писав, що судді не можуть критично ставитися до експертизи, бо для розуміння її треба набувати кілька років наукових занять. Їм залишається тільки слідувати авторитетним вказівкам експертів. Суд є самостійним у виборі експертів. Але оскільки останні вибрані, суддя йде слідом за ними, як «сліпий за своїм поводитирем» [1, с. 197]. Специфіка формування і змісту висновку експерта дала підставу і надалі деяким авторам вважати, що він займає особливе, виняткове місце [2, с. 85; 3, с. 83; 4, с. 37]. Такі погляди справедливо був підданий критиці вченими-процесуалістами [5, с. 724-725; 6, с. 136-137].

Отже, навіть високий науковий авторитет висновку експерта не надає йому наперед встановленої сили [7, с. 53-54]. Про це міститься пряма вказівка у статті 94 КПК України, згідно з якою цінність доказів визначається внутрішнім переконанням слідчого, прокурора, слідчого судді, суду, яке ґрунтується на всебічному, повному й неупередженому дослідженні всіх обставин кримінального провадження. Названі суб'єкти, керуючись законом, оцінюють кожний доказ з точки зору належності, допустимості, достовірності, а сукупність зібраних доказів – з точки зору достатності та взаємозв'язку для прийняття відповідного процесуального рішення. Жоден доказ не має наперед встановленої сили.

Питання про сутність висновку експерта в юридичній літературі довгий час залишалося дискусійним. Не дивлячись на проведені дослідження, повною мірою адекватне рішення не знайдено і донині.

За думкою Н. І. Клименко, висновок експерта, порівняно з іншими доказами, має специфічні риси, обумовлені його сутністю: він формується на основі використання спеціальних знань; він є вивідним знанням, а не інформативним, як інші особисті докази (показання), знання. У висновку експерта доказове значення має передусім його розумовий висновок, до якого він прийшов за результатами дослідження [8, с. 160].

Висновок експерта В.Д. Юрчишин визначив як заснований на завданні органу досудового розслідування, прокурора, слідчого або суду, сформульованому в постанові (ухвалі) про призначення експертизи, виклад експертом фактичних даних, що мають доказове значення для провадження та які встановлюються ним на основі застосування спеціальних знань в процесі експертного дослідження [9, с. 15].

Слід зазначити, що жоден із передбачених законом засобів доказування не містить у собі як складовий елемент судження про факти. Виключення складає висновок експерта. Наприклад, змістом показань свідка є відомості про факти, що спостерігалися ним, думка ж свідка про них не має доказового значення. У зміст висновку експерта (про що йдеться й у КПК України) обов'язково входять умовиводи, висновки про фактичні дані, і саме вони, в першу чергу, мають доказове значення. Отже, висновок завжди оснований на спеціальних наукових знаннях, що застосовуються експертом при дослідженні. Він обов'язково повинен містити кваліфіковану думку про встановлені обставини, без тлумачення яких експертом не буде й висновку. Тому слід погодитись з Т.В. Сахновою про те, що висновок експерта як засіб доказування характеризують, по-перше, специфіка формування фактичних даних у ході спеціального дослідження і їх професійна оцінка; по-друге, відповідність порядку одержання фактичних даних вимогам законодавства [10, с. 228].

Загрози кіберзлочинності в сучасних умовах розвитку українського суспільства ставлять нові завдання перед експертами. Адже поява нових об'єктів, які використовують для вчинення злочину, і розширення кола експертних завдань потребують удосконалення експертних технологій, упровадження в експертну діяльність сучасних апаратних приладів, які застосовують у міжнародній практиці, постійного підвищення професійного рівня експертів-комп'ютерщиків [11, с. 97-98].

Зрозуміло, що специфічні особливості судової комп'ютерно-технічної експертизи слід враховувати не лише під час перепідготовки та підвищення кваліфікації судових експертів, а й під час добору кандидатів на посади експертів. Розробка методик дослідження об'єктів комп'ютерно-технічної експертизи (у тому числі накопичувачів інформації, накладок на банкомати, диктофонів, мобільних терміналів) потребує від їх розробників (найчастіше експертів-практиків) як чіткого розуміння мети та завдань експертного дослідження, так і глибоких знань щодо принципів побудови, конструкції та функціонування досліджуваної техніки [11, с. 98].

Підсумовуючи, слід зазначити, що висновки експерта підлягають оцінці слідчим, прокурором, судом. Критерієм оцінки висновків експерта, як і інших джерел доказів, є належність, допустимість, достовірність. Основний зміст оцінки будь-яких видів судових експертиз слідчим або судом під час розслідування кримінальних правопорушень полягає у визначенні наукової обґрунтованості рішення експерта, яке знайшло відображення у його висновку. Слідчий чи суд оцінює експертний висновок за внутрішнім переконанням, що засновано на всебічному, повному й об'єктивному розгляді всіх обставин кримінального правопорушення в їх сукупності. Аналіз висновку експерта є розумовою діяльністю слідчого, яка поділяється на декілька стадій і веде до кінцевої оцінки висновку експерта в цілому щодо його обґрунтованості та достовірності.

#### **Література:**

1. Владимиров Л.Е. Учение об уголовных доказательствах: [переиздан.] / Л.Е. Владимиров. – Тула : Автограф, 2000. – 464 с.
2. Богдасарова М.А. Из практики криминалистической экспертизы документов по гражданским делам / М. А. Богдасарова// Сборник научных трудов ТАШНИИСЭ. – Ташкент, 1961. – Вып. 4. – С. 76–85.
3. Основы теории доказательств в советском уголовном процессе: учебн. пособ. / [сост. В.Д. Арсеньев]. – Иркутск: Иркутский госуниверситет им. А.А. Жданова, 1970. – 145 с.
4. Притузова В.А. Оценка заключения криминалистической экспертизы вышестоящим судом / В. А. Притузова. – М.: МГУ, 1961. – 38 с.
5. Теория доказательств в советском уголовном процессе / [под ред. Н.В. Жогина]. – М.: Юридическая литература, 1973. – 735 с.
6. Ульянова Л.Т. Оценка доказательств судом первой инстанции / Л.Т. Ульянова. – М.: Госюриздат, 1959. – 168 с.
7. Экспертизы у судовій практиці: наук.-практ. посіб. / [за заг. ред. В.Г. Гончаренка]. – К.: Юрінком Інтер, 2004. – 388 с.
8. Клименко Н. І. Судова експертологія : курс лекцій : навч. посіб. для студ. юрид. спец. вищ. навч. закл. / Н. І.Клименко. — К. : Вид. Дім «Ін Юре», 2007. – 526 с.
9. Юрчишин В. Д. Висновок експерта як джерело доказів у кримінальному процесі України: : автореф. дис. ... канд. юрид. наук : 12.00.09 / В. Д. Юрчишин. – К., 2006. – 20 с.
10. Сахнова Т. В. Судебная экспертиза / Т. В. Сахнова. – М.: Городец, 1999. – 368 с.
11. Харківський П.П. Комп'ютерно-технічна експертиза: проблемні питання / П.П. Харківський // Криміналістичний вісник. – 2014. – № 2 (22). – С. 97-100.

**Кримінальна відповідальність за комп'ютерне шахрайство – один з елементів кіберзлочинності**

**Кришевич О.В.**

кандидат юридичних наук, доцент  
професор кафедри кримінального права  
Національної академії внутрішніх справ

Встановлення кримінальної відповідальності за шахрайство, що вчинюється шляхом незаконних операцій з використанням електронно-обчислювальної техніки (комп'ютерне шахрайство), є значним кроком вітчизняних законодавців, спрямованим на боротьбу з комп'ютерною злочинністю (так званою кіберзлочинністю), складовим елементом якої є комп'ютерне шахрайство (поряд з такими небезпечними її проявами, як промисловий шпіонаж, створення незаконних електронних бірж, спортивних та політичних тоталізаторів, електронних казино тощо). Дана кваліфікуюча ознака утворює лише такі операції, здійснення яких без використання електронно-обчислювальної техніки є неможливим (здійснення електронних платежів, отримання інтернет-послуг, здійснення операцій з пластиковими платіжними картками), але якщо за допомогою такої техніки здійснюються операції, які можливі при використанні іншої техніки (набір тексту, виготовлення документа), то дана кваліфікуюча ознака відсутня.

Характеризуючи шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки, слід зазначити, що це обманне або через зловживання довірою використання можливостей і засобів такої техніки, пов'язане з умисним уведенням (закладанням) у її електронну систему відповідних даних, які ідентифікуються цією системою як такі, що начебто уведені власником (уповноваженою особою), а тому шахраю надається можливість отримати певну суму чужих грошей. Ця кваліфікуюча ознака має місце лише тоді, коли йдеться про операції, які без електронно-обчислювальної техніки здійснити неможливо (наприклад, електронні платежі чи перекази безготівкових грошей). Шахрайство може полягати у протиправному використанні як спеціальних засобів і знарядь (наприклад, пристроїв доступу до банківських рахунків або пристроїв для відтворення зображень), так і звичайної електронно-обчислювальної техніки — комп'ютерів, сканерів, принтерів тощо (наприклад, створення та подальше використання електронних листів, що дають можливість отримати товари з магазину, заміна з допомогою електронно-обчислювальної техніки PIN-коду ідентифікаційної картки системи банківського обслуговування населення, що належить іншій особі, та подальше отримання грошей з банкомату чи каси банку, внесення неправдивих даних до кредитної угоди, що створюється в електронній формі, з метою придбання автомобіля, побутової техніки тощо). Таким чином, під незаконними операціями з використанням електронно-обчислювальної техніки як кваліфікуючою ознакою шахрайства слід розуміти такі спрямовані на заволодіння чужим майном або придбання права на майно операції, в основі яких лежать обман чи зловживання довірою. Небезпечність такого шахрайства полягає у тому, що ця техніка значно полегшує вчинення шахрайства, дозволяє заволодівати значними коштами, завдаючи непоправної шкоди власникам. Злочин є закінченим з моменту фактичного одержання винним чужого майна чи права на нього (матеріальний склад).

При цьому вчинене має кваліфікуватися за ч. 3 ст. 190 КК і додаткової кваліфікації за статтями розд. XVI “Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку” Особливої частини КК не потребує. Навпаки, коли внаслідок несанкціонованого доступу до електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, зумовленого вчиненням шахрайства шляхом незаконних операцій з використанням електронно-обчислювальної техніки, відбувається витік, втрата, підроблення, блокування інформації, спотворення процесу її обробки або порушення встановленого порядку її маршрутизації, або здійснюється розповсюдження чи збут шкідливих програмних (технічних) засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), то вчинене, за наявності для цього підстав, належить додатково кваліфікувати, зокрема, за статтями 361 або 3611 КК. Пов'язано це з тим, що за даних умов ідеться про зовсім різні об'єктивні та суб'єктивні ознаки, які прямо не стосуються складу шахрайства.

Цілком нові можливості, засновані на властивостях електронної пошти, груп електронних новин та сервісу, відкриваються перед шахраями в галузі організації фінансових пірамід, фіктивних шлюбних контор, бюро працевлаштування, фірм по нібито наданню послуг тощо. Інший різновид шахрайства складається з модифікації алгоритмів, що визначають функціонування системи опрацювання

інформації про безготівкові банківські розрахунки. Відомі випадки зміни коефіцієнта перерахунку курсів валют, при цьому клієнтам банку валюта перераховується за заниженим курсом, а різниця заноситься на рахунки, контрольовані злочинцями. Також є спосіб, заснований на округленні до цілого нарахованих клієнту відсотків при виплаті, а різниця між належними і нарахованими в результаті округлення клієнту відсотками надходить на рахунок злочинця. Подібні операції через малі суми, що викрадаються, практично залишаються непомітними як для клієнтів, так і для керівництва банку. З'явився засіб розрахунку, так звана електронна готівка, яка супроводжує нові види шахрайства. Вже відомі деякі різновиди електронної готівки. У першу чергу це електронна готівка, що існує у вигляді кредитних карток. Вони використовуються як для отримання традиційних паперових грошей, так і для здійснення за допомогою спеціального устаткування купівлі товарів і оплати послуг. У віртуальних магазинах активно використовується різновид електронної готівки у вигляді електронних монеток (cibercash) [1].

Останнім часом значного поширення набули шахрайські операції з кредитними картками. Приклад, зловживаючи довірою громадянин, переконуючи «вигідно» вкласти гроші в інтернет-комерцію, потім на кредитну картку кібершахрая довірливі громадяни переказували кошти зі свого електронного гаманця або через платіжні термінали «WebMoney», зловмисник обіцяв, що після фінансових операцій у віртуальному підприємстві вони отримають, через деякий час, назад свої гроші разом із солідними відсотками, але натомість особа переказувала кошти на рахунки однієї з букмекерських контор. Громадяни повинні ставитися до пропозицій інтернет-комерції чи купівлі товарів через всесвітню мережу більш відповідально та перед тим, як переказувати кошти, перевіряти інформацію про особу чи підприємство, читати відгуки клієнтів, а в разі потреби - вимагати документального підтвердження законності цього бізнесу. Інший вид шахраїв це так звані «Кардери». До вас може звернутися людина, яка пояснить вам, що вона не може отримати товар і попросить виступити в ролі посередника, з тим, щоб потім за невелику винагороду ви переслали йому. Однак шахрай розплачується за товар краденою кредиткою, адреса одержувача вказується ваша, і, виконавши свою роботу, ви опиняєтеся співником злочинця, і вам доведеться доводити поліції, що це не ви розплачувалися краденою візиткою. Окремо варто згадати про шахраїв на інтернет-аукціонах, де торгують автомобілями. Найчастіший спосіб, це коли продавець-іноземець пропонує вам на перший погляд безпечну схему. Ви робите грошовий переказ за системою Western Union, але не на його ім'я, а на ваше власне або ім'я вашого родича. Він нібито грошей зняти не зможе з цього переказу, але побачить, що ви налаштовані серйозно і тоді вже прилетить для оформлення всіх необхідних паперів, а ви переоформляти на нього переказ. Суть в тому, що в деяких країнах переказ за системою Western Union можна отримати без паспорта тільки за реквізитами переказу (які ви йому, звичайно ж, повідомите). Після того як ви зробите переказ шахрай отримує гроші і зникає. Найкращий спосіб уникнути цього, це попросити у продавця копії документів на машину, після такого прохання шахраї відразу зникають.

Також, один з різновидів шахрайства з підробленими кредитними картками базується на викраденні інформації у вигляді пари чисел – номери кредитної картки та її PIN-коду. Це відбувається або на етапі розсилання картки споживачу, або в момент введення PIN-коду в торговий термінал чи банкомат, або в момент передачі електронним терміналом подібної інформації з каналів зв'язку. Крім того, номер кредитної картки і PIN-код можуть бути викрадені з банку або обслуговуючої організації. Після «викрадення» ідентифікаційної пари кредитної картки, як правило, виготовляється фальшива пластикова копія кредитної картки, за допомогою якої і здійснюється «загадкове зняття з рахунка». Інша можливість «загадкового зняття з рахунка» заснована на шахрайстві персоналу, обслуговуючого фінансові транзакції користувача і полягає в приписуванні їм неіснуючих операцій по витрачання коштів. Друга група шахрайств з пластиковими картками, пов'язана з використанням фантомної картки. Ці шахрайства засновані на використанні виявленого алгоритму одержання PIN-коду з номера кредитної картки, виготовленні неіснуючої пластикової картки з наступним вчиненням фінансових операцій з ними. Третю групу складають шахрайства зі справжніми кредитними картками. Входять шахрайства з викраденими або загубленими кредитними картками, а також різноманітні шахрайства, які вчинюються із застосуванням спеціальних прийомів. Шахраї відкривають багато рахунків із кредитними картками дебетового типу, і на одну кредитну картку кладеться невелика сума грошей. Для залучення клієнтів більшість банків припускає перевитрату фінансових коштів на дебетовій картці, якщо рахунок не закривається в банку. Кошти з першої картки знімаються цілком із перевитратою і переказуються на другу картку, з якої у свою чергу з перевитратою знімаються і переказуються на третю і т.д. В результаті збирається значна сума, що влаштовує шахраїв. До четвертої групи входять способи, засновані на використанні фальшивих банкоматів і торгових терміналів. Відомі випадки, коли злочинці встановлювали фальшивий банкомат і приймали в нього реальні кредитні картки, знімаючи номер PIN-коду, введений користувачем, а також готівкові кошти, котрі користувачі намагалися через

банкомат покласти на свій рахунок у банку. При спробі ж отримати готівку з банкомату з'являлося повідомлення, що в банкомат не завантажені купюри потрібної вартості. [2].

### **Література:**

1. Онлайн-банкінг облегчає користувачам життя / [Електронний ресурс]. – Режим доступу: <http://e-commerce.com.ua/5827>.
2. Огляд ринку Інтернет-торгівлі в Україні / [Електронний ресурс]. – Режим доступу: <http://www.ukrbiznes.com/analytic/marketing/10614.html>.

## **Психологічний аспект слідчих та співробітників оперативних підрозділів під час досудового розслідування кримінальних правопорушень**

**Солдатенко О.А.**

кандидат юридичних наук, доцент

доцент кафедри кримінального процесу Дніпропетровського державного університету внутрішніх справ

**Гуратов А.П.**

курсант 4 курсу ФПФПКП

Дніпропетровського державного університету внутрішніх справ

Кримінальним процесуальним кодексом України (далі – КПК України) в статті 2 визначено завдання кримінального провадження, які повинні бути досягнуті усіма визначеними законом методами та способами. Так, важливе місце у швидкому, повному та неупередженому розслідуванні кримінальних правопорушень відіграє взаємодія його суб'єктів (насамперед, слідчих органів досудового розслідування та співробітників оперативних підрозділів).

Відповідно до п. 3 ч. 2 ст. 40 КПК України слідчий уповноважений доручати проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій відповідним оперативним підрозділам. У свою чергу, під час виконання доручень слідчого співробітник оперативного підрозділу користується повноваженнями слідчого (ч. 2 ст. 41 КПК України), а доручення останнього щодо проведення слідчих (розшукових)

дій та негласних слідчих (розшукових) дій є обов'язковими для виконання оперативним підрозділом (ч. 3 ст. 41 КПК України).

Дане питання регулює окремий нормативно-правовий акт Міністерства внутрішніх справ України, а саме наказ № 700 від 14.08.2012 «Про організацію взаємодії органів досудового розслідування з іншими органами та підрозділами внутрішніх справ у попередженні, виявленні та розслідуванні кримінальних правопорушень». У вище зазначеному Наказі зазначено основні принципи взаємодії:

1. Відповідальність слідчого за швидке, повне та неупереджене розслідування кримінальних правопорушень, його самостійність у процесуальній діяльності, втручання в яку осіб, що не мають на те законних повноважень, забороняється.

2. Активне використання методик, наукових і технічних досягнень у попередженні, виявленні та розслідуванні кримінальних правопорушень.

3. Оптимальне використання наявних можливостей слідчих і оперативних підрозділів у попередженні, виявленні та розслідуванні кримінальних правопорушень.

4. Дотримання загальних засад кримінального провадження.

5. Забезпечення нерозголошення даних досудового розслідування (п. 1.3).

На нашу думку, важливе місце займають саме міжособистісні стосунки між працівниками правоохоронних органів, їх навички працювати у групі та взаємодіяти в різноманітних, іноді – екстремальних, ситуаціях. Налагодження психологічного контакту між слідчим та оперуповноваженим дає змогу підвищити ефективність проведення окремих процесуальних дій та є дієвим методом розслідування кримінальних правопорушень. Іноді в територіальних підрозділах Національної поліції виникають конфлікти між вище зазначеними працівниками через різноманітні причини, як службового, так і особистісного характеру. Весь процес досудового розслідування будується не лише на законодавчій базі, а й на досвіді правоохоронців, які беруть у ньому участь, та їх стосунках між собою.

Існує спеціальна наука – конфліктологія – завдання якої полягає у вивченні природи, сутності, функцій та механізмів соціальних конфліктів, умов їх виникнення та закономірностей розвитку, у розробці адекватних внутрішній природі та особливостям перебігу конфліктної взаємодії “технологій”

урегулювання та розв'язання конфліктів [3, ст. 23]. Її різновидом є юридична конфліктологія, яка займається виключно випадками, пов'язаними з юридичною діяльністю (в нашому випадку – під час досудового розслідування кримінальних правопорушень між працівниками слідчих і оперативних підрозділів).

Отже, взаємодія слідчих органів досудового розслідування та співробітників оперативних підрозділів під час досудового розслідування кримінальних правопорушень є його невід'ємним елементом.

Дієвість даної взаємодії прямо впливає на швидке, повне та неупереджене розслідування, і багато в чому залежить від міжособистісних стосунків між працівниками, їх особисто-ділових якостей та професіоналізму. Найбільш ефективними є ті слідчо-оперативні групи, в яких між правоохоронцями відсутні неприємні стосунки та не виникають конфліктні ситуації. Тому вважаємо за необхідне, приділяти особливу увагу психологічному аспекту взаємодії між працівниками слідчих та оперативних підрозділів, а у випадках наявності конфліктів – звертатися до методів юридичної конфліктології для їх нейтралізації.

### **Література:**

1. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 №4651-VI [Електронний ресурс]: // Законодавство України. – Режим доступу: <http://zakon1.rada.gov.ua/laws/show/4651a-17>
2. Наказ МВС № 700 від 14.08.2012 «Про організацію взаємодії органів досудового розслідування з іншими органами та підрозділами внутрішніх справ у попередженні, виявленні та розслідуванні кримінальних правопорушень» [Електронний ресурс] – Режим доступу: <http://document.ua/pro-organizaciyu-vzaemodiyi-organiv-dosudovogo-rozsliduvannj-doc119907.html>.
3. Юридична конфліктологія : Навч. посіб. для студ. вищ. навч. закл. / В.М. Іванов, О.В. Іванова. – К.: МАУП, 2004. – 224 с.

### **Принцип поваги до людської гідності під час кримінального процесу**

**Солдатенко О.А.**

кандидат юридичних наук, доцент  
доцент кафедри кримінального процесу  
Дніпропетровського державного університету внутрішніх справ

**Легкий М.І.**

курсант 4 курсу ФПФПКП  
Дніпропетровського державного університету внутрішніх справ

Набуття Україною незалежності потягнуло за собою ряд необхідних перетворень, в тому числі і в нормотворчій сфері. Свідченням даного факту є те, що українське законодавство максимально увібрало в себе світовий досвід, а особливо щодо гуманного ставлення до людини під час кримінального судочинства. Особливе місце займає така засада кримінального процесу, як повага до людської гідності, що і буде предметом нашого розгляду.

В Конституції України зміст даного принципу має місце, а саме:

- 1) людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю (ст. 3);
- 2) ніхто не може бути підданий катуванню, жорстокому, нелюдському або такому, що принижує його гідність, поводженню чи покаранню (ст. 28);
- 3) ніхто не може бути підданий катуванню, жорстокому, нелюдському або такому, що принижує його гідність, поводженню чи покаранню (ст. 55);
- 4) кожен зобов'язаний неухильно дотримуватися Конституції України та законів України, не посягати на права і свободи, честь і гідність інших людей (ст. 68).

Цілком логічним є те, що вище зазначені норми мають втілення в Кримінальному процесуальному кодексі України (далі – КПК України), а саме в ст. 11. Дана стаття включає в себе наступні положення:

— під час кримінального провадження повинна бути забезпечена повага до людської гідності, прав і свобод кожної особи;



— забороняється під час кримінального провадження піддавати особу катуванню, жорстокому, нелюдському або такому, що принижує її гідність, поводженню чи покаранню, вдаватися до погроз застосування такого поводження, утримувати особу у принизливих умовах, примушувати до дій, що принижують її гідність;

— кожен має право захищати усіма засобами, що не заборонені законом, свою людську гідність, права, свободи та інтереси, порушені під час здійснення кримінального провадження.

Б.М. Свірський вважає, що традиційно під поняттям гідності розуміють морально-етичну категорію, що означає повагу і самоповагу людської особистості, невід'ємну та невідчужувану властивість людини як вищій цінності, що належить їй від народження незалежно від того, як вона сама і довколишні люди сприймають і оцінюють її особу. Ця стаття (ст. 11 КПК України) передбачає обов'язок органів і посадових осіб, які ведуть кримінальне провадження, вживати заходів до забезпечення поваги до людської гідності, прав і свобод однихучасників процесу від посягань інших [3, с. 142]

Нажаль, в наш час працівники правоохоронних органів все ж таки допускають порушення даного принципу під час досудового розслідування, що, найчастіше, виявляється в отриманні показань у особи з застосуванням фізичної сили, тримання особи в жахливих умовах, використання нецензурних висловів та слів, які можуть завдати особі психічної травми. Але слід зауважити на тому, що процес реформування правоохоронної системи триває, і все частіше можна побачити притягнення до кримінальної відповідальності правоохоронців за вчинення дій, які принижують честь та гідність людини. Це свідчить про те, що держава вважає недопустимим вчинення таких дій посадовими особами і реагує на них відповідно до законодавства.

Отже, чинним кримінальним процесуальним законодавство України передбачено ряд принципів, серед яких особливо важливим є принцип поваги до людської гідності. Особливу увагу слід приділити практичній стороні даного питання, бо саме під час досудового розслідування мають місце порушення вище зазначеної норми працівниками слідчих та оперативних підрозділів. Правоохоронці повинні мати високий рівень правосвідомості та виконувати свої функціональні обов'язки незалежно від наявності чи відсутності захисника у особи.

#### **Література:**

1. Конституція України: Прийнята на 5-й сесії Верховної Ради України 28 червня 1996 р. // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.
2. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 №4651-VI [Електронний ресурс]: // Законодавство України. – Режим доступу: <http://zakon1.rada.gov.ua/laws/show/4651a-17>
3. Свірський Б.М. Визначення принципу поваги до людської гідності у кримінально-процесуальних нормах / Б. М. Свірський // Вісник Маріупольського державного університету. Сер. : Право. - 2013. - Вип. 6. - С. 138-145. - Режим доступу: [http://nbuv.gov.ua/UJRN/Vmd\\_u\\_pr\\_2013\\_6\\_21](http://nbuv.gov.ua/UJRN/Vmd_u_pr_2013_6_21).

#### **Експерт як важливий учасник кримінального процесу**

**Солдатенко О.А.**

кандидат юридичних наук, доцент  
доцент кафедри кримінального процесу,  
Дніпропетровського державного університету внутрішніх справ

**Любова Н.О.**

курсант 4 курсу ФПФПКП  
Дніпропетровського державного університету внутрішніх справ

Нерідко, під час здійснення слідчим своїх обов'язків щодо повного та всебічного з'ясування усіх обставин кримінального правопорушення, виникає необхідність у спеціальних знаннях. Це може виражатися у необхідності участі спеціаліста під час проведення слідчих (розшукових) дій, отриманні консультацій в тих чи інших питань, але дуже часто лише спеціаліст не в змозі надати необхідну допомогу та відповісти на усі запитання правоохоронних органів. У таких випадках потрібно звертатися до експерта.

Відповідно до Кримінального процесуального кодексу України експертом є особа, яка володіє науковими, технічними та іншими спеціальними знаннями, має право відповідно до Закону України «Про судову експертизу» на проведення експертизи і якій доручено провести дослідження об'єктів,

явищ і процесів, що містять відомості про обставини вчинення кримінального правопорушення та дати висновок з питань, які виникають під час кримінального провадження і стосується сфери її знань [1]. Отже, експертом є компетентна особа, яка володіє відповідними знаннями для того, щоб дати відповідь на питання, що виникає у правоохоронних органів під час здійснення кримінального провадження. Варто зазначити, що висновок, в якому експерт дасть відповіді на всі поставлені питання, відповідно до кримінального процесуального законодавства належить до джерел доказів. Що вимагає від слідчого призначати експертизи своєчасно, без зволікань.

Відповідно до ч.1 ст. 101 Кримінального процесуального кодексу висновок експерта – це докладний опис проведених експертом досліджень та зроблені за їх результатом висновки, обґрунтовані відповіді на запитання, поставлені особою, яка залучила експерта, або слідчим суддею чи судом, що доручив проведення експертизи [1].

Специфічність висновку експерта як процесуального джерела доказів полягає в тому, що він ґрунтується на спеціальних знаннях, якими не володіють працівники органів досудового розслідування та судової влади [2]. Тому, слідчий зобов'язаний перевірити чи дотримувався експерт при проведенні експертизи та складанні висновку вимог кримінально процесуального законодавства, об'єктивності, обґрунтованості, незалежності та повноти дослідження, чи ґрунтується висновок експерта на відомостях, які він сприймав безпосередньо і чи не вийшов він при складанні висновку за межі своєї компетенції. Також, перед залученням конкретного експерта, слідчий перевіряє чи входить складання висновку, в якому буде дано відповіді на поставлені слідчим запитання до компетенції даного експерта, а також чи не заінтересований експерт в результатах експертного дослідження.

На думку Н.А. Панько у кримінально процесуальному законодавстві потрібно чітко зазначити критерії, як реальні, так і загальнодоступні, якими слідчий та суд повинні керуватися під час оцінки висновку експерта. Слід також прописати порядок залучення спеціалістів для надання консультацій з приводу оцінки висновку експерта [3].

Зрозуміло, що висновок експерта, як і інший доказ може викликати у сторони захисту, слідчого судді та суду сумніви щодо його правильності. Для цього Кримінальним процесуальним кодексом передбачено три способи залучення експерта:

1. Сторона обвинувачення залучає експерта за наявності підстав для проведення експертизи, у тому числі за клопотанням захисту чи потерпілого.
2. Сторона захисту має право самостійно залучати експерта на договірних умовах для проведення експертизи, в тому числі обов'язкової.
3. Експерт може бути залучений слідчим суддею за клопотанням сторони захисту [1].

Отже, якщо у сторони захисту виникнуть сумніви щодо правильності складеного висновку внаслідок відсутності у експерта необхідних спеціальних знань, упередженості, заінтересованості у результатах дослідження, то вона може звернутися до слідчого судді за дорученням останнього на проведення експертизи іншим експертом.

Також, під час реалізації права на залучення експерта у сторони захисту можуть виникати деякі труднощі. Адже, нерідко, для проведення експертизи сторона захисту повинна надати документи, предмети, речі тощо. Але, оскільки ці документи та речі можуть вважатися доказами та знаходитися в матеріалах кримінального провадження, сторона захисту позбавлена можливості надати експерту потрібні зразки. У таких випадках, вона звертається до сторони обвинувачення або подає клопотання слідчому судді для проведення експертизи за дорученням останніх.

Отже, на основі вище викладеного, можемо зробити висновок, що у деяких випадках використання спеціальних знань у кримінальному провадженні є необхідним. Експерт є важливим учасником кримінального процесу, адже володіє необхідним обсягом знань, якими не володіє слідчий, прокурор, слідчий суддя та суд, для того аби відповісти на запитання, що виникли у сторони обвинувачення під час здійснення досудового розслідування. Проте, слідчий зобов'язаний перевірити та оцінити складений експертом висновок, який є процесуальним джерелом доказів, за критеріями законності, правильності, об'єктивності, неупередженості. Для цього йому потрібно володіти хоча б мінімальним обсягом знань, які потрібні для того аби дати відповідь на запитання, поставлені перед експертом та використовувати допомогу спеціалістів.

#### **Література:**

1. Кримінальний процесуальний кодекс України : чинне законодавство зі змінами та допов. станом на 28 лютого 2016 р. : ( офіц. текст ). К.: Паливода А. В., 2016. – 328 с.
2. Перепічка О. І. Оцінка висновку експерта: інформаційно-змістовий аспект / О. І. Перепічка // Європейські перспективи. - 2013. - № 8. - С. 70-75. - Режим доступу: [http://nbuv.gov.ua/UJRN/evpe\\_2013\\_8\\_16](http://nbuv.gov.ua/UJRN/evpe_2013_8_16).

### **Спеціальний суб'єкт злочину в сфері інформаційної безпеки**

**Форос Г.В.**

кандидат юридичних наук, доцент  
професор кафедри кібербезпеки  
та інформаційного забезпечення ОДУВС

**Когутенко Є.І.**

слухач 2-го курсу магістратури ННІЗДН ОДУВС

Проблема організації попередження кіберзлочинів пов'язана з певними соціальними групами, індивідами, особистостями та життєвими ситуаціями, до яких вони потрапляють. Радикальна точка зору взагалі полягає у запереченні існування особливого типу «комп'ютерного» злочинця, який має виразні відмінності від пересічного типу фахівця, службовця тощо. Відсутність зовнішніх «стигм», брутально-кримінального способу життя створює ілюзію, що дійсно «комп'ютерний» злочинець є виключенням і, теоретично, кожна «нормальна» людина за певних умов та обставин може перетнути «червону лінію» і здійснити правопорушення або злочин.

Особистість злочинця є одним з основних складових елементів предмету кримінології, але слід зазначити, що крім цього, особа злочинця (суб'єкт злочину) вивчається ще багатьма науками, а саме – криміналістикою, кримінальним правом, юридичною психологією, психіатрією і т. ін. Вагомість цієї проблеми пов'язана з тим, що злочин – це акт людської дії та бажання окремої людини, яке залежить від її сутності, характеру та психологічних особливостей. Різноманітні види діяльності у житті людини відкладають свій відбиток на особу, формують риси, які характерні для суб'єктів даної діяльності. На сучасному етапі людина знайомиться з інформаційними технологіями ще перебуваючи у віці дитини. Інформатизація та комп'ютеризація навчально-виховних закладів, використання інформаційних технологій у побуті, обумовлює набуття відповідних практичних навичок з використання інформаційно-телекомунікаційних систем, що у майбутньому може стати підставою для злочинної діяльності. Фахівці здебільшого вважають, що злочинець є індивідуальною, неповторною особистістю. І матрицю злочинця можна скласти лише з певною часткою припустимості. Однак злочинців можна диференціювати і за відповідними групами. При цьому зазвичай використовується наукове передбачення можливої злочинної діяльності. При оцінці особистості злочинця також беруться до уваги можливі й передбачувані перспективи поведінки з урахуванням його соціальної небезпеки.

Вважаємо, що дослідження суб'єкту злочинів в сфері кібербезпеки має важливе й принципове значення для організації й управління попереджувальною діяльністю в усіх її аспектах, особливо на рівні конкретних об'єктів управлінського впливу.

Згідно діючому законодавству, суб'єкт злочину - це особа, яка вчинила злочин та підлягає кримінальній відповідальності. Згідно ч. 2 ст. 18 КК спеціальний суб'єкт злочину – «є фізична осудна особа, що вчинила у віці, з якого може наставати кримінальна відповідальність, злочин, суб'єктом якого може бути лише певна особа» [1, с. 18].

Ознаки спеціального суб'єкта завжди доповнюють загальне поняття, і тому вони завжди є додатковими. До їх числа можна віднести такі ознаки, як службова особа, лікар, працівник транспорту, військовослужбовець, рецидивіст та ін. Так, службовими особами є особи, які постійно, тимчасово чи за спеціальним повноваженням здійснюють функції представників влади чи місцевого самоврядування, а також постійно чи тимчасово обіймають в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах чи організаціях посади, пов'язані з виконанням організаційно-розпорядчих чи адміністративно-господарських функцій, або виконують такі функції за спеціальним повноваженням, яким особа наділяється повноважним органом державної влади, органом місцевого самоврядування, центральним органом державного управління із спеціальним статусом, повноважним органом чи повноважною службовою особою підприємства, установи, організації, судом або законом.

Суб'єкт злочинів в сфері інформаційної безпеки може бути як загальний, так і спеціальний, але він повинен мати певний рівень знань та навичок у галузі використання новітніх технологій. Якщо зазначена особа є службовою і має можливість здійснення зазначених злочинних дій за родом своєї роботи, то за наявності всіх необхідних ознак його дії слід кваліфікувати як сукупність злочинів за

статтями передбаченими Розділом 16 Особливої частини Кримінального кодексу і відповідний службовий злочин [2, с. 385-398].

Щодо спеціального суб'єкта кіберзлочину фахівці відносять персонал, який являє собою небезпеку, та поділяють його на категорії у відповідності зі сферами діяльності. Аналізуючи статистичні дані та практичні приклади, ми можемо навести типологію осіб, яких впевнено за наявності законних підстав можна віднести до спеціального суб'єкта злочину в сфері інформаційної безпеки:

1. Особи, які вчиняють злочини як оператори комп'ютерних технологій («Операційні злочини»): оператори АЕОМ; оператори, які забезпечують роботу периферійних комп'ютерних пристроїв (принтер, сканер, модем) в організаціях, де ці пристрої сконцентровані для колективного використання; оператори, які обслуговують лінії телекомунікації.

2. Особи, які вчиняють злочини, основою яких є використання комп'ютерного програмного забезпечення – особи, у яких є колекція програмного забезпечення; системні програмісти; прикладні програмісти; достатньо підготовлені користувачі (але не фахівці за освітою щодо комп'ютерного програмування).

3. Щодо апаратної частини інформаційно-телекомунікаційних систем небезпеку становлять: інженери-системники; інженери територіальних систем (серверів тощо); інженери-зв'язківці; інженери-електроніки.

4. Певну частину осіб, які можуть вчинити кіберзлочини, становлять працівники, що займаються організаційною роботою щодо автоматизованих систем: керування комп'ютерною мережею (адміністратор комп'ютерної мережі); керування операторами (працівники інформаційних центрів, служб інформаційно-технічного забезпечення установ); керування автоматизованими базами даних (адміністратори баз даних); керування роботою з удосконалення програмного забезпечення.

5. Загрозу також можуть становити: різного роду працівники організацій та особи з інших організацій, які мають ділові стосунки, та конкуренти; працівники служби безпеки організації; працівники, які контролюють технічний захист функціонування комп'ютерів в організації.

6. Представники сервісних, консалтингових, ремонтних та інших обслуговуючих установ: працівники, які займаються сервісним обслуговуванням комп'ютерних програмних продуктів; працівники, які займаються ремонтом комп'ютерної техніки.

Особливу небезпеку можуть представляти фахівці у випадку входження ними у змову із керівниками підрозділів і служб самої комерційної структури чи зв'язаних з нею систем, а також з організованими злочинними групами, оскільки в цих випадках заподіяний збиток від вчинених злочинів і значущість наслідків істотно збільшуються. Фахівці стверджують, що майже 90% зловживань у фінансовій сфері, пов'язаних з порушеннями в галузі інформаційної безпеки, відбувається при прямій чи непрямій участі діючих або колишніх працівників банків. При цьому на злочинний шлях часто стають найкваліфіковані категорії банківських службовців, які володіють максимальними правами в автоматизованих системах, - системні адміністратори та інші співробітники служб автоматизації банків.

Таким чином, суб'єкт злочинів в сфері інформаційної безпеки може бути як загальний, так і спеціальний, але він повинен мати певний рівень знань та навичок у галузі використання інформаційних технологій, хоча законодавець не ставить це за вимогу, але це зумовлено специфікою даної групи злочинів.

### **Література:**

1. Кримінальний кодекс України [Електронний ресурс]: закон України від 05.04.2001 № 2341-14 із змін., внес. згідно із Законами України та Рішеннями Конституційного Суду: за станом на 01.05.2016, підстава 889-1904.07.2013 р. – Режим доступу: <http://zakon1.rada.gov.ua>. – Назва з екрана.

2. Уголовное право Украины: Особенная часть: Учебник / Отв. редактор д.ю.н., профессор, заслуженный деятель науки и техники Украины Е.Л. Стрельцов. – Х.: Одиссей, 2009. – 544 с.

**Форос Г.В.**

кандидат юридичних наук, доцент  
професор кафедри кібербезпеки  
та інформаційного забезпечення ОДУВС

**Никитюк В.С.**

слухач 2-го курсу магістратури ННІЗДН ОДУВС

Протягом останнього десятиліття спостерігається стрімкий розвиток інформаційно-комунікаційних технологій та широке застосування їх у державному управлінні, але нерозв'язаною залишається проблема недосконалості нормативно-правової бази.

Про актуальність нормативно-правового упорядкування і вдосконалення питань забезпечення інформаційної безпеки свідчить рівень наукових розробок та інтерес вчених й політиків, що знайшло відображення у працях: О. Баранова, К. Белякова, В. Брижка, В. Гавловського, І. Гаврилова, О. Гладківської, М. Гуцалюка, М. Жулинського, Л. Задорожньої, О. Зінченка, Г. Лазарєва, А. Марущака, А. Новицького, Б. Раціборинського, В. Хахановського, В. Цимбалюка, М. Швеця та ін.

Для створення і підтримання належного рівня захисту інформаційних систем розробляється система правових норм, що регулюють відносини в інформаційній сфері, визначаються основні напрями діяльності в цій сфері, формуються або перетворюються органи та сили забезпечення інформаційної безпеки і механізм контролю та нагляду за їх діяльністю.

Відсутність системи забезпечення інформаційної безпеки унеможливує надійне забезпечення не лише інформаційної, а й національної безпеки. Головне призначення цієї системи полягає у досягненні цілей національної безпеки в інформаційній сфері, а отже основною функцією даної системи є забезпечення збалансованого існування інтересів особи, суспільства і держави в цій сфері [1, с. 168].

На нашу думку, нормативну базу щодо забезпечення інформаційної безпеки органів виконавчої влади доцільно розглядати з урахуванням існуючої ієрархії нормативно-правових актів.

Досліджуючи систему нормативно-правового забезпечення інформаційної безпеки органів виконавчої влади, можна сказати, що фундаментальним нормативно-правовим актом є Конституція України прийнята Верховною Радою України 28 червня 1996 року. В ній є норми, що стосуються забезпечення інформаційної безпеки України в цілому та які є визначальними для побудови національної системи інформаційної безпеки, а також системи нормативно-правового забезпечення органів виконавчої влади. У частині 1 ст. 17 Конституції України зазначається, що забезпечення інформаційної безпеки України оголошено «справою всього українського народу» [2, с. 17].

Наступним рівнем в ієрархії нормативно-правового забезпечення інформаційної безпеки органів виконавчої влади є Закон України «Про інформацію», яким встановлюються загально-правові основи одержання, використання, поширення та зберігання інформації, закріплюється право особи на інформацію в усіх сферах суспільного і державного життя України, а також на систему інформації, її джерела, визначається статус учасників інформаційних відносин, регулюється доступ до інформації та забезпечується її охорона, захищається особа та суспільство від неправдивої інформації. Сфера дії Закону поширюється на інформаційні відносини, які виникають у всіх сферах життя і діяльності суспільства і держави при одержанні, використанні, поширенні та зберіганні інформації.

Разом з цим у Законі України «Про інформацію» визначення «інформаційна безпека» взагалі немає [3]. А в Законі України «Про основи національної безпеки України», який є основним орієнтиром забезпечення безпеки нашої держави, сутність «інформаційної безпеки» подано як невід'ємний складник національної безпеки України без точного визначення цього поняття [4].

Як бачимо, у наведених документах надаються лише загальні визначення терміну «інформаційна безпека» до того ж, не узгоджені між собою. Але ці документи не містять системних підходів до забезпечення інформаційної безпеки в Україні, не визначають суб'єктів інформаційної діяльності та не розподіляють повноважень між ними.

Базовим законом у сфері інформатизації на сучасному етапі є Закон України «Про Національну програму інформатизації», окрім цього Закону окремі напрямки інформаційної діяльності, захисту інформації та інформаційної безпеки регулюються такими Законами України : «Про доступ до публічної інформації», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист персональних даних» та інші.

Ми вважаємо, що більш нормативно опрацьованими є питання кібернетичної безпеки. Так, наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 10.06.2008 р. №

94 затверджено «Порядок координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах».

Питання забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах врегульовані Постановою Кабінету Міністрів України від 29 березня 2006 р. № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах». Правила, затверджені зазначеною постановою, визначають загальні вимоги та організаційні засади забезпечення захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Дія цих Правил не поширюється на захист інформації в системах урядового та спеціальних видів зв'язку.

Підводячи підсумки, хотілося б звернути увагу на те, що існуюча система нормативно-правових актів у сфері забезпечення інформаційної безпеки органів виконавчої влади України потребує удосконалення, оскільки в Україні поки що немає нормативних актів концептуального рівня, які б предметно стосувалися регулювання інформаційної сфери та забезпечення інформаційної безпеки держави. Значна кількість нормативних актів (як законів, так і підзаконних актів, неузгоджених не лише з нормами міжнародного законодавства, але й між собою) суттєво знижує ефективність цієї діяльності.

#### **Література:**

1. Інформаційне забезпечення управлінської діяльності в умовах інформатизації: організаційно-правові питання теорії і практики. Монографія. – К., 2002. – 296 с.
2. Конституція України [Електронний ресурс]: закон України від 28. 06. 1996 р. № 254к/96-ВР із змін., внес. згідно із Законами України та Рішеннями Конституційного Суду. – Електрон. дан. (1 файл). – Режим доступу: <http://zakon1.rada.gov.ua>. – Назва з екрана
3. Про інформацію [Електронний ресурс]: закон України від 02.10.1992 № 2657-12 в редакції Закону України від 25.06.2016, підстава 1405-19. – Електрон. дан. (1 файл). – Режим доступу: <http://zakon1.rada.gov.ua>. – Назва з екрана.
4. Про основи національної безпеки України [Електронний ресурс]: закон України від 19.06.2003 № 964-IV із змін., внес. згідно із Законами України від 07.08.2015, підстава 630-19. – Електрон. дан. (1 файл). – Режим доступу: <http://zakon1.rada.gov.ua>. – Назва з екрана.

#### **Криміналістичне прогнозування як стратегічний метод при проведенні обшуку**

**Теслюк І.О.**

аспірант аспірантури заочної форми навчання  
Одеського державного університету внутрішніх справ

**Цільмак О.М.**

доктор юридичних наук, професор  
професор кафедри криміналістики, судової медицини та психіатрії  
Одеського державного університету внутрішніх справ

Важливим та незамінним «озброєнням» слідчого при проведенні слідчих (розшукових) дій, у тому числі в сфері кіберзлочинності, є застосування різних методів (спостереження, аналіз, та ін.). Серед даного арсеналу, на нашу думку, слід виокремити метод криміналістичного прогнозування.

Розглянемо застосування методу криміналістичного прогнозування під час обшуку. Відповідно до ст. ст. 234 – 236 КПК України [1], підобшуком маєтись на увазі проведення на основі ухвали суду таких слідчих (розшукових) дій, які мають на меті пошук доказів, інформації чи відомостей, що мають відношення до вчиненого злочину (правопорушення).

Як відомо, під обшук підпадає особа, її житло, приміщення та транспортні засоби, тобто все, що виступає джерелом здобуття інформації, відомостей та доказів по кримінальному провадженню.

Суб'єктами криміналістичного прогнозування під час обшуку можуть бути слідчий та прокурор, а також інші учасники (слідчо-оперативна група).

*Об'єктами криміналістичного прогнозування під час обшуку є:*

- криміналістична ситуація;
- лінія поведінки слідчого;
- модель (форма) поведінки особи, яку обшуковують чи в якій проводять обшук;
- методи, способи, прийоми та засоби, які застосовуються під час обшуку;
- рішення, які приймаються в ході обшуку;
- інформація, яка отримується в ході обшуку;
- результати обшуку (знайдені предмети, що мають відношення до злочину).

*Метою криміналістичного прогнозування при проведенні обшуку є виявлення та фіксація речей, предметів, інформації, що має відношення до злочину.*

Застосовуючи метод криміналістичного прогнозування слідчий повинен вирішити ряд таких завдань як:

- припущення можливості вилучення, вилучення та фіксації знарядь злочину, цінних речей та інших предметів, що мають відношення до злочину;
- припущення можливості вилучення предметів, які є забороненими, а також зберігання та збут яких тягне за собою кримінальну відповідальність;
- визначення імовірності виявлення місцезнаходження особи, що знаходиться у розшуку, трупа, та ін.;
- передбачення імовірності виявлення майна, спричиненого злочинном, яке забезпечує відшкодування матеріальної шкоди.

В науковій літературі етапи проведення обшуку вчені визначають по різному [2-3]. Ми вважаємо, що процес проведення даної слідчої (розшукової) дії складається з підготовчої стадії та безпосередньо самого процесу обшуку, який має такі етапи: а) попередній; б) оглядовий; в) детальний. Кожен з яких пронизаний методом криміналістичного прогнозування.

Так, на *підготовчому етапі*, вивчаючи матеріали провадження, слідчий застосовує метод криміналістичного прогнозування задля ефективності результату обшуку. Отже, в першу чергу, необхідно спрогнозувати:

- об'єкти обшуку (що потрібно шукати);
- місце і час обшуку (де і коли);
- у кого проводити обшук;
- коло учасників обшуку (хто буде брати участь у проведенні);
- технічне забезпечення (які засоби фіксації);
- власну поведінку при проведенні обшуку;
- розумові процеси та поведінку особи, що приховала річ, предмети, (які розшукуються);
- поведінку інших осіб (слідчо-оперативної групи, спеціалістів, понятих, свідків);
- тактику обшуку.

*Під час обшуку, на попередньому етапі*, а саме по прибутті на місце, слідчий припускає :

- необхідність побудови уявної моделі дій пошуку;
- необхідність проникнення на місце обшуку таємно;
- необхідність проведення обшуку швидко, безшумно та результативно;
- необхідність виявлення речей або предметів, що мають відношення до злочину;
- імовірність перебування в житлі, де проводитиметься обшук інших людей, тварин (собаки);
- імовірність добровільної здачі предмету пошуку (його частини);
- імовірність перешкоджання особою проведення обшуку;
- імовірність недовіри в показаннях особи, в якій проводиться обшук;
- імовірність виникнення складних або безвихідних ситуацій.

*На оглядовому етапі* обшуку важливо спрогнозувати:

- можливість отримання нових даних про розміщення предмету пошуку, особливостей планування кімнат;
- можливість визначення найбільш вірогідних місць схову;
- можливість застосування спеціальних засобів для пошуку, технічних засобів;
- необхідність вибору особливої тактики обстеження приміщень, кімнат та ін.;
- необхідність змінити план проведення обшуку;
- можливість членів слідчо-оперативної групи виконувати певні обов'язки;
- необхідність уточнення графіку та схеми подальших дій під час обшуку;
- необхідність змінити тактику проведення обшуку.

Криміналістичне прогнозування вкрай необхідне і на *детальному етапі* проведення обшуку для того, аби спрогнозувати:

- можливість вибору того чи іншого прийому обшуку (послідовний чи вибірковий; одиничний чи роздільний, і т.д.);
- імовірність застосування й інших методів пошуку (порівняння, спостереження, мікрообшуку та ін.);
- імовірність виказування місцезнаходження предмету пошуку через поведінку особи, в якій проводять обшук та інших осіб;
- можливість вжиття певних заходів на вчинення опору зацікавленими особами або відволікання;
- можливість застосування засобів фіксації результатів обшуку (фото- та відеозйомка, освітлення, та ін.);
- імовірність того, що слідчий нічого не знайде;
- імовірність проведення повторного обшуку.

Слід зазначити, що важливе значення при формуванні прогнозних даних має творча уява слідчого, яка дозволяє передбачати (уявити) лінії поведінки учасників кримінального провадження в тій чи іншій ситуації, варіанти їх розвитку та вплив на результат розслідування слідчого. Чим ширший кругозір мислення, тим менша міра дефіциту інформації. Уявному моделюванню також сприяє володіння методом рефлексивного мислення, основу якого складають професійний та життєвий досвід слідчого. Особливе місце також відводиться пізнанню в сфері психології. На нашу думку, це є особливо важливим для побудови прогнозів.

Отже, при проведенні обшуку застосування методу криміналістичного прогнозування є дуже важливим. Опираючись на прогнозні дані, слідчий передбачає місцезнаходження, розміщення чи наявність тої чи іншої речі, предмета, що має відношення до злочину, а також припускає можливість виникнення небажаних ситуацій, з метою їх уникнення та попередження.

#### **Література:**

1. Кримінальний процесуальний кодекс України: Закон України від 13 квітня 2012 року № 4652-VI [Електронний ресурс]. – Режим доступу: <http://zakon3.rada.gov.ua/laws/show/4651-17>
2. Криміналістика: учебник / [В.Ю. Шепітько, В.- Коновалова, В.А. Журавль и др.]; под ред. В.Ю. Шепітько. - [5-е изд., перераб. и доп.]. - Х. : Право, 2011. - 464 с.
3. Криміналістика [Текст] : підручник / за ред. В. Ю. Шепітько ; Нац. юрид. акад. України ім. Ярослава Мудрого. - Київ : Вид. Дім "Ін Юре", 2001. - 684 с.

#### **Правове регулювання забезпечення безпеки осіб залучених до проведення негласних слідчих (розшукових) дій**

**Горбенюк Т.А.**

курсант 306 взводу факультету № 2

Одеського державного університету внутрішніх справ

**Андрусенко С.В.**

кандидат юридичних наук, доцент

завідувач кафедри оперативно-розшукової діяльності

Одеського державного університету внутрішніх справ

Боротьба зі злочинністю, її попередження на сучасному етапі набуває професіоналізму та організованості, через це виникає необхідність удосконалення способів і засобів отримання доказів у кримінальному провадженні. 13 квітня 2012 року Верховною Радою України було прийнято Кримінально процесуальний кодекс України (далі – КПК України) де уперше на законодавчому рівні створено окремий інститут процесуальних дій, що проводяться під час досудового розслідування у кримінальному провадженні – негласні слідчі (розшукові) дії.

Метою реформування кримінального процесу є створення і запровадження нової процедури досудового розслідування, під час якої гласними і негласними методами буде здійснюватися збирання інформації, що має значення для кримінального судочинства.

Під час виконання завдань протидії злочинності слідчі, оперативні працівники та інші учасники негласних слідчих (розшукових) дій зазвичай наражаються на небезпеку, що пов'язана із загрозою їх життю і здоров'ю. Водночас, не всі категорії зазначених осіб перебувають під захистом держави, передбаченим чинним законодавством, що об'єктивно ускладнює роботу із планування та проведення негласних слідчих (розшукових) дій.



Нормативно-правове регулювання та організаційне забезпечення здійснення заходів безпеки щодо цих осіб потребує суттєвого удосконалення.

Значного впливу національне законодавство зазнає з боку міжнародних установ та організацій [1, с. 160]. Вище наведенні обставини спонукають до аналізу світового досвіду в сфері визначення правового статусу учасників оперативно-розшукових заходів.

Зокрема, у кримінальному процесі Сполучених Штатів Америки під час доказування вини одну з вирішальних ролей відіграють показання осіб, які виступають у процесі свідками. Однак при розслідуванні справ, що пов'язані з організованою злочинністю, отримання таких доказів відбувається досить складно. Це пов'язано з тим, що не рідко очевидці відмовляються свідчити в суді, через те що побоюються за своє життя, а також за життя і здоров'я рідних, тому забезпечення їх безпеки – надзвичайно важлива проблема. Упевненість у безпеці стимулює до співробітництва із правоохоронними органами.

Один із способів використання свідчень таких осіб реалізується завдяки тому, що в американському кримінальному процесі широко використовується відеозапис показань. Наявність такого доказу робить безглуздим та недоречним усунення свідка, тому що навіть у випадку його смерті дана ним інформація відіграє свою доказову роль.

Закон покладає обов'язки на міністра юстиції Сполучених Штатів Америки вжити заходів для забезпечення безпеки таких осіб, а також членів їх родини. З цією метою за його наказом свідки, життя і здоров'я яких наражається на небезпеку в наслідок надання ними свідчень проти лідерів або учасників організованих злочинних угруповань, можуть бути оселені у спеціально пристосовані охоронювані житла [2, с. 34].

У кримінальному кодексі Німеччини також передбачені заходи, спрямовані на охорону особи, яка дає змогу виступати в процесі як свідок. Вони полягають у тому, що під час досудового розгляду замість відомостей, що свідчать про місце проживання такої особи, фіксуються лише дані про місце роботи. Але в тих випадках, коли оголошення навіть таких відомостей створює підстави для занепокоєння за життя свідка або інших осіб, свідок в праві не надавати жодних довідок, на підставі яких його можна ідентифікувати [3, с. 11].

Протягом останніх років перед вітчизняними правоохоронними органами постала необхідність забезпечення безпеки свідків і потерпілих. Це сталося через те, що багато учасників процесу стали ухилятися від участі у слідчих діях під час проведення досудового слідства та в суді для надання свідчень. Такі відмови були пов'язані із здійсненням на них злочинцями різних заходів впливу.

В Конституції України зазначається, що людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визначається в Україні найвищою соціальною цінністю. Утвердження і забезпечення прав і свобод людини є основним обов'язком держави. Україна відповідає перед людиною за свою діяльність. Ці конституційні положення повністю поширюються на всіх учасників кримінального судочинства та суб'єктів оперативно-розшукової діяльності.

Захист держави гарантується, перш за все, тим, що співробітництво особи з оперативними підрозділами у виконанні спеціальних завдань оперативно-розшукової діяльності є державною таємницею, яка охороняється законами України «Про оперативно-розшукову діяльність», [Про організаційно-правові основи боротьби з організованою злочинністю], «Про державну таємницю» та низкою інших. Захист держави поширюється на всіх осіб, залучених до виконання завдань оперативно-розшукової діяльності, незалежно від форм такого співробітництва, чи то на постійній основі чи тимчасово, як на основні угоди, так і за усною домовленістю за винагороду чи безоплатно [4, с. 70].

Найважливішим заходом правового захисту є перебування осіб, залучених до проведення негласних слідчих дій під захистом держави. Отже, держава в особі своїх представників зобов'язується виконувати всі передбачені законами України функції із забезпечення законних інтересів кожної особи, яка в будь-якій формі надає допомогу в проведенні негласних слідчих (розшукових) дій.

У разі виникнення реальної загрози життю, здоров'ю чи майну приватних осіб внаслідок їх сприяння, а також членів їх сімей чи близьких родичів ці підрозділи, що виступають від імені держави, зобов'язані вжити необхідних заходів до запобігання протиправним діям, установленню винних і притягненню їх до відповідальності.

Стаття 13 Закону України «Про оперативно-розшукову» діяльність зазначає, що особа, яка залучається до виконання завдань оперативно-розшукової діяльності, перебуває під захистом держави. У разі виникнення загрози життю, здоров'ю або майну особи, яка залучається до виконання завдань оперативно-розшукової діяльності, її захист здійснюється у порядку, передбаченому частиною третьою ст. 12 цього Закону, а ст. 12 передбачає, що «...не несе відповідальності працівник оперативного підрозділу, який заподіяв шкоду правам, свободам людини, інтересам держави під час здійснення

оперативно-розшукової діяльності, перебуваючи у стані необхідної оборони, крайньої необхідності або професіонального ризику, а так само у зв'язку із затриманням особи, в діях якої є ознаки злочину.

Сучасні злочинні угруповання та окремі злочинці обізнані в тактиці і методах оперативно-розшукової діяльності, знають кримінальне законодавство і майже завжди здійснюють перевірку своїх нових членів «На ділі». Через це співробітник вимушений брати участь у певних злочинних діях.

Ще більші можливості у правовому захисті особи при проведенні негласних слідчих дій закладені у ст. 43 Кримінального кодексу України (виконання спеціального завдання з попередження чи розкриття злочинної діяльності злочинної групи чи злочинної організації). У пункті першому цієї статті вказано, що не є злочином вимушене заподіяння шкоди правоохоронним інтересам особою, яка відповідно до закону виконувала спеціальні завдання, беручи участь в організованій групі чи злочинній організації з метою попередження чи розкриття їх злочинної діяльності особа, зазначена в частині першій цієї статті, підлягає кримінальній відповідальності лише за вчинення у складі організованої групи чи злочинної організації особливо тяжкого злочину, вчиненого умисно і поєднаного з насильством над потерпілим, або тяжкого злочину, вчиненого умисно і пов'язаного зі спричиненням тяжкого тілесного ушкодження потерпілому або настання інших тяжких або особливо тяжких наслідків [5, с. 281].

Правовий захист від притягнення до кримінальної відповідальності чи припинення кримінального провадження щодо особи, яка бере участь у проведенні негласних слідчих дій, спричиняє потребу соціального та фізичного захисту. Нажаль, через матеріальний стан правоохоронних органів не завжди є можливість здійснювати ці заходи, але слід прагнути і домагатися цього. Негласний працівник буде працювати з повною віддачею лише тоді, коли він вірить, що буде захищений при необхідності.

Варто враховувати, що за своїм змістом право на соціальний захист таких осіб містить у собі не тільки право на отримання грошової винагороди, а і права на соціальне обслуговування, покликане задовольнити особливі потреби людей, зумовлені розладом здоров'я.

Отже, сьогодні існує законодавче підґрунтя, достатнє для визначення правового статусу осіб, які беруть участь у проведенні негласних слідчих (розшукових) дій, а, отже, можуть наражатися на небезпеку і потребують захисту. Воно має бути покладено в основу розроблення правового механізму забезпечення безпеки учасників кримінального процесу.

#### **Література:**

1. Декларація основних принципів правосуддя для жертв злочинів та зловживання владою : прийнята Резолюцією 40/34 Генеральної Асамблеї ООН від 29 листопада 1985 р. // Права людини і професійні стандарти для юристів в документах міжнародних організацій. – Амстердам – К. : Укр. – Амар. бюро захисту прав людини, 1996. – С. 159-161.
2. Савченко А. В. Міжнародний досвід використання агентури правоохоронними органами держав Європи та США / [А. В. Савченко, В. В. Матвійчук, Д. Й. Никифорчук] ; під ред. Я. Ю. Кондратьєва. – К. : Нац. акад. внутр. справ України, 2004. – 60с.
3. Ромадановский К.О. Международные стандарты и принципы организации защиты участников уголовного судопроизводства / К. О. Ромадановский // Рос. следователь. – 2005. - №9. – С. 10-12.
4. Бандурка О. М. Оперативно-розшукова діяльність : [ч. II] / О. М. Бандурка. – Х. : Нац. ун-т. внутр. справ, 2002. – 335 с.
5. Янків О. Професійний ризик та його вплив на забезпечення особистої безпеки працівників ОВС / О. Янків // Актуальні проблеми управління та службово-оперативної діяльності ОВС у сучасний період розвитку державності України : матеріали наук.-практ. конф. (м. Київ, 27 жовтня 2007 р.). К., 2008. – С. 280-282.

#### **Дослідження факторів, що впливають на вчинення кіберзлочинів**

**Вікторів Д.І.**

курсант Херсонського факультету  
Одеського державного університету внутрішніх прав

**Бараненко Р.В.**

кандидат технічних наук, доцент  
Херсонського факультетуОдеського державного університету внутрішніх прав

Сучасні комп'ютерні технології відіграють все більш активну роль в економічній діяльності держави. В результаті з'явилися й активно розвиваються види злочинного посягання проти власності,

пов'язаного з використанням засобів комп'ютерної техніки та інформаційних технологій. Злочини проти власності, що здійснюються з використанням інформаційно-комунікативних технологій, характеризуються такою ознакою як «масовість», тобто вчиненням злочину щодо великого і, як правило, невизначеного кола потерпілих. За цими діями практично неможливо точне встановлення такої ознаки складу злочину як розмір заподіяної шкоди. А значить, для злочинів, скоєних таким чином, розмір збитку не може бути ознакою, що відображає характер і ступінь суспільної небезпеки діяння [1].

Розглянемо віктимологічні фактори, що впливають на вчинення даного виду злочинів у сфері комп'ютерної інформації. Під віктимологічними факторами маємо на увазі сукупність причин, що породжують жертву злочину [2].

В.Я. Рибальська трактує віктимологічні фактори в широкому сенсі слова як різні соціальні та соціально-психологічні властивості окремих осіб або груп, що реалізовані в конкретній поведінці, а також об'єктивні ситуативні обставини, які безпосередньо сприяють настанню віктимальних наслідків. А у вузькому сенсі слова – як обставини, пов'язані лише з особистістю й поведінкою потерпілого, що сприяють його віктимізації. Віктимізація – це процес перетворення особи в жертву злочину [3].

Віктимологічні фактори формуються в певних умовах конкретної ситуації. Під ними слід розуміти сукупність умов, при яких особа стає потенційною або реальною жертвою, а також особистісні характеристики вже реальних жертв злочину, які беруть участь в механізації вчинення конкретного злочину [4].

В.А. Бессонов в своїй роботі [2] розглядає термін «комп'ютерна віктимність». Автор вважає, що персональний комп'ютер зі зберігаємою у ньому інформацією сам по собі віктимний, в силу своїх технічних, споживчих властивостей. У людини-жертви завжди присутня особлива антропологічна властивість – кримінальна вразливість, а, отже, у комп'ютера, що зберігає в собі масу цінної інформації, присутня також особлива властивість – «комп'ютерна» вразливість. Таким чином, проводячи аналогію, В.А. Бессонов стверджує, що під «комп'ютерною» вразливістю мається на увазі здатність персонального комп'ютера в силу своїх технічних, споживчих властивостей бути віктимним.

Проблему попередження кіберзлочинів ще недостатньо добре вивчено. Міжнародний досвід боротьби зі злочинністю свідчить про те, що одним із пріоритетних напрямків вирішення завдання ефективної протидії сучасній злочинній діяльності є активне використання правоохоронними органами різних заходів профілактичного характеру. Останні мають вирішальне значення в складному процесі попередження злочинів і являють собою діяльність, спрямовану на виявлення та усунення причин, що породжують злочини, і умов, що сприяють їх вчиненню. Це обумовлено тим, що профілактичні заходи спрямовано проти самих витоків злочинності. Тому фахівці з протидії кіберзлочинам повинні надавати велику увагу стану профілактичної роботи та переглянути ставлення до віктимологічної профілактики. В даний час не існує якихось конкретних і повних за змістом методичних розробок з організації й тактики попередження злочинів даної категорії, а тим більше методик роботи з жертвами цих злочинів. Зарубіжні фахівці прямо говорять, що попередити кіберзлочин завжди набагато легше й простіше, ніж потім його розкрити й розслідувати [5].

В.Б. Веховим [5] виділяються три основні групи заходів попередження кіберзлочинів, що становлять у своїй сукупності цілісну систему боротьби з цим соціально небезпечним явищем, а саме:

- 1) правові;
- 2) організаційно-технічні;
- 3) криміналістичні.

До правових заходів попередження кіберзлочинів, в першу чергу, відносяться норми законодавства, що встановлюють кримінальну відповідальність за вказані протиправні діяння.

Заходи організаційно-технічного характеру можуть грати серйозну загально-профілактичну роль у боротьбі з кіберзлочинами при їх вмілому й комплексному використанні.

Криміналістична характеристика кіберзлочинів відрізняється від уже відомих криміналістичній науці злочинних посягань певною специфікою.

Сам факт появи комп'ютерної злочинності в суспільстві багато дослідників ототожнюють з появою так званих «хакерів» – користувачів обчислювальної системи, що займаються пошуком незаконних способів отримання несанкціонованого (самовільного) доступу до засобів комп'ютерної техніки й даних в сукупності з їх несанкціонованим використанням з корисливою метою [6].

На думку В.Б. Вехова [5], до першої групи «комп'ютерних» злочинців можна віднести осіб, відмітною особливістю яких є стійке поєднання професіоналізму в області комп'ютерної техніки й програмування з елементами своєрідного фанатизму й винахідливості. Ці суб'єкти сприймають засоби комп'ютерної техніки як своєрідний виклик їх творчим і професійним знанням, умінням і навичкам [7].

Саме це в соціально-психологічному плані є чинником для здійснення різних діянь, більшість з яких мають яскраво виражений злочинний характер.

Особливий інтерес в криміналістичному аспекті вивчення особистості злочинця представляють фахівці-професіонали в галузі засобів комп'ютерної техніки [5]. Вони зазвичай дуже допитливі й володіють неабияким інтелектом і розумовими здібностями. Нарощувані заходи щодо забезпечення безпеки комп'ютерних систем ними сприймаються в психологічному плані як своєрідний виклик особистості, тому вони прагнуть будь-що знайти ефективні способи докази своєї переваги. Як правило, це і приводить їх до скоєння злочину.

Кіберзлочини можуть також здійснюватися особами, які страждають на психічні захворювання.

Професійні «комп'ютерні» злочинці з яскраво вираженою корисливою метою на відміну від першої перехідної групи «любителів» і другої специфічної групи «хворих» характеризуються рецидивами здійснення комп'ютерних злочинів з обов'язковим використанням дій, спрямованих на їх приховування. Вони володіють у зв'язку з цим стійкими злочинними навичками. Злочинці цієї групи зазвичай є членами добре організованих, мобільних і технічно оснащених висококласним устаткуванням і спеціальною технікою злочинних груп і співтовариств. Саме ця група злочинців являє собою основну загрозу для суспільства, є кадровим ядром комп'ютерної злочинності як в якісному, так і в кількісному плані. На частку саме цих злочинців доводиться максимальне число скоєних особливо небезпечних посягань, наприклад до 79% розкрадань грошових коштів у великих та особливо великих розмірах і різного роду посадових злочинів, скоєних з використанням засобів комп'ютерної техніки [8].

За даними Ю.М. Батурина [9] виділяються три основні групи потерпілих від кіберзлочинів:

- 1) власники комп'ютерної системи – 79%;
- 2) клієнти, які користуються їхніми послугами, – 13%;
- 3) треті особи – 8%.

Власники системи неохоче повідомляють правоохоронні органи про факти вчинення кіберзлочину. Саме цим і пояснюється високий рівень латентності цих злочинів.

Сьогодні представляється неймовірним, що жертва кіберзлочину, яка втратила кошти, може відмовитися від розслідування. Проте, як показує практика, такий «ефект умовчання» досить широко поширений [9].

Згубна практика відмови потерпілих від кримінального переслідування кіберзлочинців дозволяє останнім уникати кримінальної відповідальності, що стимулює інших, потенційних, злочинців до скоєння нових посягань.

### **Література:**

1. Чекунов Игорь Геннадьевич. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности : автореферат дис. ... кандидата юридических наук : 12.00.08. – Москва, 2013. – 23 с.
2. Бессонов Владимир Анатольевич. Виктимологические аспекты предупреждения преступлений в сфере компьютерной информации : диссертация ... кандидата юридических наук : 12.00.08. – Нижний Новгород, 2000. – 249 с.
3. Виктимологические проблемы преступности несовершеннолетних [Текст] / В. Я. Рыбальская. – Иркутск : Изд-во ИГУ, 1983. – 228 с.
4. Зыков Даниил Алексеевич. Виктимологические аспекты предупреждения компьютерного мошенничества : диссертация ... кандидата юридических наук : 12.00.08. – Владимир, 2002. – 211 с.
5. Вехов В.Б. Компьютерные преступления. Способы совершения методики расследования [Текст] / В.Б. Вехов. – М., 1996. – 182 с.
6. О законе против «хакеров» // Проблемы преступности в капиталистических странах. – 1990. – № 7. – С. 62-63.
7. Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность [Текст] / Ю.М. Батурин, А.М. Жодзишский. – М.: Юрид. лит., 1991. – С. 158.
8. Полевой Н.С. и др. Правовая информатика и кибернетика [Текст]: Учебник. – М.: Юрид. лит., 1993. – С. 253.
9. Батурин Ю.М. Проблемы компьютерного права [Текст] / Ю.М. Батурин. – М.: Юрид. лит., 1991. – 272 с.

**Власенко А.В.**  
студент факультету права  
Донецького юридичного інституту МВС України

**Делія Ю.В.**  
кандидат юридичних наук, доцент,  
доцент кафедри загально-правових дисциплін  
Донецького юридичного інституту МВС України

Досліджуючи дане питання в першу чергу слід з'ясувати що являє собою торгівля людьми. Вона є однією з галузей кримінального бізнесу, що розвивається найбільш стрімкими темпами в світі. Торгівля людьми дає мільйонні прибутки і поступово витісняє торгівлю зброєю та наркотиками.

За оцінками експертів у світі щороку від двох до чотирьох мільйонів осіб стають жертвами торгівлі людьми. Особливо це стосується жінок та дітей. Отже, для когось це – «Великий бізнес», а для когось – це крах надій і сподівань на краще майбутнє [1].

Стрімко розвивається використання Інтернету, як для вербування жертви, так і для реклами послуг. Зустрічі між жертвами та клієнтами організовуються за допомогою спеціальних веб-сайтів. Жертви швидко змінюються, залишаючись в одному місті не більше ніж на 1-2 дні. Ілюзія анонімності і масова кількість онлайн-послуг збільшує як обережність, так і рентабельність цих послуг, що робить дуже важкою ідентифікацію правопорушників з використанням лише традиційних методів поліції [2, с.179].

Для даної протиправної діяльності використовуються апаратні та програмні засоби. До *апаратних засобів*, які використовуються для вчинення злочинів у сфері торгівлі людьми найчастіше відносять:

- персональні комп'ютери та сервери;
- ноутбуки та нетбуки;
- планшети;
- мобільні телефони;
- телевізори з функцією SMART;
- системи фото- та відео фіксації;
- банківське обладнання;
- спеціально виготовлені апаратно- програмні засоби, тощо.

Найбільш поширеними *програмними технологіями*, які використовуються для вивчення протиправної діяльності у кіберсфері є:

- спеціально створені веб-сайти;
- комп'ютерні соціальні мережі;
- дошки оголошень;
- електронна пошта;
- чати;
- мультимедійні засоби спілкування;
- засоби шифрування, тощо.

Правопорушниками створюються активні веб-сайти пошуку моделей, шлюбні агенції тощо, які слугують основою для вербування потенційних жертв торгівлі людьми. Також можна знайти багато сайтів ескорт агентств, які слугують для надання ескорт-партнерів клієнтам, переважно для сексуальних послуг.

Правоохоронним органам часто доводиться здійснювати первинний пошук інформації про певні об'єкти в мережі. Найбільш проблемним питанням залишається встановлення особи та визначення її місцезнаходження за мережними ідентифікаторами, тобто за тими обліковими даними, які особа залишила по собі в мережі. Як правило, такими ідентифікаторами виступають адреса електронної пошти, нікнейм у форумі, профіль соціальної мережі тощо. Вказана проблема часто обумовлена підвищеним рівнем анонімності, що реалізується за допомогою різного роду розподілених ресурсів (проксі-сервери, шели) та використанням спеціалізованих захищених мереж (TOR, I2P) [3, с. 256].

Для здійснення ефективної протидії роботі онлайн-торгівлі людьми потрібні спільні, узгоджені дії підрозділів боротьби з кіберзлочинністю та підрозділів боротьби зі злочинами пов'язаними із торгівлею людьми.

У межах пошуку та протидії в мережі можуть застосовуватись різні інструменти. Багато в чому конкретна методика залежить від наявності ситуації, тому оперативному працівнику та слідчому для ефективної реалізації завдання слід бути не лише юридично, але й технічно обізнаним працівником та

постійно підвищувати свій професійний рівень, відслідковуючи новітні методики та розробки, які зможуть допомогти у вирішенні завдань протидії злочинності.

#### **Література:**

1. Що таке «торгівля людьми»: [електронний ресурс]. – Режим доступу: [http://psihossoc.ucoz.ru/torgivlia/torgivlja\\_ljudmi.pdf](http://psihossoc.ucoz.ru/torgivlia/torgivlja_ljudmi.pdf).
2. Справочное руководство ОБСЕ по обучению полиции: Торговля людьми/ серия публикаций ДТУ/ОВСВПД, том 12, 2013. – 210с.
3. Бандурка О.М. Оперативно-розшукова компаративістика: монографія / О.М. Бандурка, М.М. Перепелиця, О.В. Манжай та ін. – Х.: Золота миля, 2013. – 352с.

### **Передові юридичні доктрини в інформаційному праві в період незалежності України**

**Никитюк В.О.**

магістр 2-го курсу Факультету №4 Одеського державного університету внутрішніх справ

**Ісмайлов К.Ю.**

кандидат юридичних наук,  
завідувач кафедри кібербезпеки та інформаційного забезпечення  
Одеського державного університету внутрішніх справ

Новаційні теорії правового змісту або іншими словами передові юридичні доктрини набувають сьогодні поширення і в інформаційному праві, як науковому напрямку юриспруденції, як галузевому напрямку в системі права і як дисциплінарному курсу підготовки правників всіх спеціалізацій. Актуальність цього питання загострюється в умовах інформаційної конфронтації України на міждержавному рівні з Російською Федерацією, на етапі, поки що, недосконалості розвитку інформаційного суспільства в українських реаліях.

Сьогодні в інформаційно-правовому науковому просторі утворюється декілька концептуальних підходів. Серед таких, в першу чергу, доцільно виокремити: доктрину галузевості інформаційного права в системі національного права і законодавства; теорію охоплення галуззю інформаційного права інститутів електронного права та права високих технологій; доктрину розширеного тлумачення права на інформацію; доктрину розширеного тлумачення видів і форм джерел інформаційного права; вчення про особливих суб'єктів інформаційно-правових відносин; вчення про інформаційний суверенітет держави; вчення про інформаційні правопорушення та інформаційно-правову відповідальність.

На протязі останніх двадцяти років означені наукові проблеми були сферою досліджень таких вітчизняних вчених-юристів як: В.Д. Гапотій, К.Ю. Ісмайлов, Т.Є. Мураховська А.А. Письменицький, В. М. Супрун, О.С. Рождественська, О.В. Синєокий, С.В. Стасюк, В.С. Цимбалюк та інших.

Зокрема, В.С. Цимбалюк, в контексті доктрини інформаційного суспільства та категоріального становлення предмету і методології інформаційного права звертається до питань галузевої характеристики цього напрямку юриспруденції в своїй монографії «Інформаційне право: концептуальні положення до кодифікації інформаційного законодавства» 2011 року. Визначено ознаки інформаційного права, наведено загальну характеристику його основних інститутів. Одночасно, обґрунтовується необхідність реформування інформаційного законодавства, запропоновано методику його кодифікації [1].

Денісова О.С. в дисертації «Роль преси у правовому інформуванні громадян України», 2002 року, також йдеться про галузеві ознаки інформаційного права в інституціональному аспекті крізь особливості ролі ЗМІ в інформаційному соціальному обороті. Так, нею розглянуто проблеми теорії правового інформування та права на правову інформацію, визначаються такі класифікаційні види правового інформування як нормативно-правове і ненормативно-правове, що вперше удосконалює розуміння поширення інформації про правову дійсність на науковому юридичному рівні [2].

Безумовно інноваційним є дослідження дисертація В.М. Супруна, який в своїй роботі «Теоретико-правові основи інформаційного суверенітету» 2010 року формулює авторський підхід до визначення поняття «інформаційний суверенітет», як виняткового права України відповідно до Конституції і законодавства України, нормами міжнародного права самостійно і незалежно, з дотриманням балансу інтересів особи, суспільства і держави визначати і здійснювати внутрішні і геополітичні національні інтереси в інформаційній сфері; державну внутрішню і зовнішню інформаційну політику; розпоряджатися власними інформаційними ресурсами; формувати інфраструктуру національного

інформаційного простору; створювати умови для його інтеграції в світовий інформаційний простір і гарантувати інформаційну безпеку держави [3].

У дисертаційному дослідженні Т.Є. Мураховської «Формування нових галузей в системі права України» 2011 року на теоретико-правовому рівні автором загострюється постановка наукового питання про розуміння інформаційного права як комплексної галузі, та здійснюється порівняння наукових концепцій щодо розуміння галузевих ознак в системі права [4].

Питання розширеного підходу до правових джерел інформаційного права піднімає в своєму науковому дослідженні «Акти судової влади в системі джерел права України» (2012 р.) Ісмаїлов К.Ю. Зокрема йдеться про активне застосування в практичному правовому обороті останніх років, наукових обґрунтуваннях та навчальній літературі в якості форм інформаційного права та джерел інформаційного законодавства і права таких інструментів, як різноманітні акти судової влади. Йдеться не тільки про законодавчо визнані в Україні, в якості джерел права і законодавства, актів Європейського суду з прав людини, але й актів національної судової влади. Зокрема офіційних Рішень Конституційного Суду України, Постанов Верховного Суду України, Керівних роз'яснень Пленуму Верховного Суду України. Автором наводяться приклади актів судової влади саме зі сфери інформаційно-правового обороту, що значною мірою вплинули на інформаційно-правові відносини в Україні. Показовим, зокрема, є приклад з Рішення Конституційного Суду України у справі за конституційними поданнями 51 народного депутата України про офіційне тлумачення положень статті 10 Конституції України щодо застосування державної мови органами державної влади, органами місцевого самоврядування та використання її у навчальному процесі в навчальних закладах України (справа про застосування української мови) (справа від 14.12.1999 № 10-рп/99). Означене рішення суттєвим чином вплинуло на інформаційно-мовний обіг правовідносин в Україні, що призвело як до позитивних, так і до негативних юридичних наслідків [5].

Також, до питань становлення галузі інформаційного права, свободи засобів масової інформації на шляху формування громадянського суспільства і правової держави звертається і А.А. Письменицький, який в дисертації 1997 року «Взаємодія держави і засобів масової інформації» [6] та монографії 2012 року «Загальна теорія інформаційного права» [7]. На основі аналізу теоретичної правової літератури і нормативно-правових актів дослідив аспекти взаємодії засобів масової інформації з гілками державної влади, роль засобів масової інформації в становленні і розвитку демократії, проблеми і сфери правового регулювання діяльності засобів масової інформації, шляху і перспективи розвитку інформаційного права і законодавства. В означених роботах в якості одного з новачків цих елементів виступає і авторська категоріальна конструкція розширеного тлумачення права на інформацію: «як права кожного на пошук і отримання, виготовлення, використання і зберігання, поширення і захист інформації, в будь-який вільно обраний спосіб і не залежно від кордонів» [7].

Останнім часом актуалізується і питання охоплення інформаційним правом сфери відносин щодо високих технологій і, зокрема нанотехнологій. Так, у своїй роботі «Інформаційне право України та електронне право високих технологій Електронний курс лекцій» доцент О.В. Синєокий, у 2010 році, ставить питання розгляду формування самостійного правового інституту електронного права та інституту права високих технологій в галузі інформаційного права. Сьогодні, на думку автора, ми наблизилися до розуміння високотехнологічної теорії як окремої підгалузі інформаційного права. Зокрема, до високих технологій можна віднести оптоволоконні, інтегрально-волоконні, лазерні, комп'ютерні, цифрові, космічні, нанотехнології та деякі інші, але обов'язковою ознакою є створення на протязі останніх 30-40 років, тобто з початку 60-х років ХХ ст. до теперішнього часу. Потрібно визнати, що до цього часу відсутнє в законодавстві повноцінне або, хоча б єдине визначення такого поняття як «високі технології» та похідних і суміжних термінів. Звідси постає проблема відсутності повноцінного нормативно-правового регулювання суспільних відносин, що виникають в цій галузі [8].

Таким чином, з наведеного вище можна зробити наступні висновки:

Сьогодні в науковому юридичному середовищі формується підхід до комплексу теорій, що визначають розвиток категоріального апарату інформаційного права як до новачків концепцій, що несуть в собі авторські наопрацювання передового категоріального апарату.

Доцільно вбачати в узагальненому розумінні новачків вектор розвитку наукових інформаційно-правових досліджень як фундаментально-правових, що формують основи загальної теорії інформаційного права.

Потребою сьогодення в національній юриспруденції і, зокрема, у здійсненні публічних навчально-популяризаційних форм поширення інформаційно-правових матеріалів підкреслювати персоналізаційну роль науковців України в фундаментально-правових, засадничих досягненнях оновлення категоріального апарату. Це буде відповідати таким вимогам законодавства про вищу освіту, що стосуються необхідності обов'язкового внесення у викладання курсу «Інформаційне право України»

авторського доробку науковців, як відповідного ідеям Болонського процесу.

Ідейні, що закладаються концепціями «особливого суб'єкту інформаційних правовідносин», «теорії специфічності об'єкту інформаційних правовідносин», «теорії розширеного підходу до джерел інформаційного права», «теорії інформаційно-правової відповідальності», «інформаційних правопорушень» змістовно змінюють наукове сучасне правове розуміння всієї теорії правових відносин, а також теорії форм права, теорії системи права, теорії правопорушення і юридичної відповідальності.

### **Література:**

1. Цимбалюк В.С. Інформаційне право: концептуальні положення до кодифікації інформаційного законодавства : монографія / В.С. Цимбалюк. - К.: «Освіта України», 2011. – 426 с.
2. Денісова О.С. Роль преси у правовому інформуванні громадян України. Дис...канд. юр. наук. - Харків: Національний університет внутрішніх справ. - 2003, 186 с.
3. Супрун В.М. Теоретико-правові основи інформаційного суверенітету [Текст]: автореф. дис. ... канд. юрид. наук: 12.00.01 / Супрун Володимир Миколайович ; Харк. нац. ун-т внутр. справ. - Х., 2010. - 20 с.
4. Мураховська, Т.Є. Формування нових галузей в системі права України [Текст] : дис. ... канд. юрид. наук : 12.00.01 / Мураховська Тетяна Єгорівна ; Харк. нац. ун-т внутр. справ. – Х., 2011. – 233 с.
6. Стасюк С.В. Об'єкт інформаційних правових відносин: загальнотеоретичний аспект [Текст] : автореф. дис. ... канд. юрид. наук: 12.00.01 / Стасюк Світлана Валентинівна ; Маріуп. держ. ун-т. – Маріуполь, 2012. - 20 с.
5. Ісмайлов К.Ю. Акти судової влади в системі джерел національного права України: монографія / К.Ю. Ісмайлов. – Донецьк: Вид-во «Ноулідж» (Донецьке відділення), 2014. – 116 с.
6. Письменицький А.А. Взаємодія держави і засобів масової інформації [Текст] : автореф. дис... канд. юрид. наук: 12.00.01 / Письменицький Андрій Анатолійович; Університет внутрішніх справ. – Х., 1997. – 22 с.
7. Письменицький А.А. Загальна теорія інформаційного права: монографія / А.А. Письменицький, В.Д. Гапотій. – Мелітополь: ТОВ «Видавничий будинок ММД», 2012. – 300 с.
8. Синєокий О.В. Інформаційне право України та електронне право високих технологій : [електронний ресурс] (електронний курс лекцій українською мовою) / Автор – доцент кафедри кримінального права та правосуддя ЗНУ, к.ю.н., доцент О.В. Синєокий ; Запорізький національний університет; Національна бібліотека України ім. В.І. Вернадського [цифрова мікроформа e-text]. – Запоріжжя : ЗНУ, 2010. – 215 ел. с. = 15 ум. друк. арк. : іл. ; сх. // <http://www.nbu.gov.ua/>

### **Використання правоохоронними органами сучасних інформаційно-аналітичних технологій у протидії тіньовій економіці в Україні**

**Мукоїда Р.В.**

кандидат юридичних наук, доцент  
професор кафедри ОРД факультету № 1 ОДУВС

**Шелехов А.О.**

кандидат юридичних наук, доцент  
завідувач кафедри АД ОВС та економічної безпеки  
факультету № 2 ОДУВС

Для якісної реалізації функцій будь якого державного інституту, в якому обробляється багато інформації, необхідна організація спеціальної інформаційно - аналітичної діяльності. Головне завдання цієї діяльності повинно полягати в зборі, узагальненні, обробці, аналізі та зберіганні інформації. Це в свою чергу буде створювати механізм прийняття перевірених і значущих управлінських рішень.

Одна з основних завдань цієї діяльності полягає не просто в механічному зборі і накопиченні інформації, а в постійній інтеграції в інші важливі сфери діяльності, тісна і тривала взаємодія з різними соціальними інститутами і організаціями.

Необхідною для інформаційно-аналітичної роботи є взаємодія і з іншими інформаційно - допоміжними структурами, сферою діяльності яких традиційно є упорядкування інформаційного простору, оптимізація та координація переміщення інформаційних потоків, забезпечення збереження накопиченої інформації. До допоміжних структур можна віднести як стародавні винаходи людської



цивілізації (архіви і бібліотеки), так і сучасні структури, що виробляють різні, в тому числі і мережеві електронні ресурси.

Проте головне завдання інформаційно - аналітичної діяльності повинно і суттєво відрізняється від завдань допоміжних структур, в число яких входить, наприклад, бібліографування, реферування, анотування, створення і об'єднання різних баз і банків даних. А інформаційно - аналітична діяльність, ґрунтуючись на діяльності допоміжних служб, оперуючи підсумками їх кінцевими інформаційними результатами, виробляє трансформацію інформації, стикаючись і перетинаючись в цій сфері з виробництвом нового знання, сценаріїв і способів вирішення тієї чи іншої задачі. Аналітика об'єднується з наукою на основі інформаційного механізму пізнання і наукового підходу до аналізу реальності.

Таким чином, інформаційна аналітика на основі аналізу та інтерпретації наявних припущень, фактів, теорій покликана виявляти в них об'єктивні закономірності і тенденції, визначати рушійні ними механізми і причинно - наслідкові зв'язки.

Разом з тим існує відмінність аналітики і науки в тому, що перша, ґрунтуючись на наукових знаннях і загальних закономірностях, проводить оцінку фактів і подій, пророкуючи їх подальший розвиток з урахуванням не тільки властивих їм характеристик, але і цілого ряду факторів. До них можна віднести протистояння різних сил, протистояння інтересів. Науковий же аналіз перш за все забезпечує об'єктивні, фундаментальні закономірності спостерігаючи і вивчаючи, повторювані істотні зв'язку об'єктів, узагальнені параметри процесів.

Одним з державних інститутів, де проводиться збір, узагальнення, обробка інформаційних потоків з метою прийняття перевірених і ефективних управлінських рішень, є МВС України та його структурні підрозділи.

В сучасних умовах криміногенна обстановка, що характеризується поширеністю злочинних діянь, наприклад, в сфері економіки, вимагає інноваційних підходів до постановки та вирішення проблем інформаційно - аналітичного та оперативного забезпечення. Необхідним є використання методичних розробок, інструментів і механізмів, заснованих на застосуванні інформаційно - аналітичних технологій, що сприяють протидії злочинності взагалі і економічної злочинності зокрема. Дані заходи повинні сприяти забезпеченню ефективності діяльності органів правопорядку і бути затребуваними державою і суспільством.

Одним з механізмів впливу і контролю над криміногенною ситуацією в країні в цілому і економічної діяльності зокрема є таке поняття, як «оперативне обслуговування». Деякі дослідники і практики, порівнюючи різні підходи у визначенні поняття оперативного обслуговування, вказували на те, що в умовах наявності в економіці різних форм власності, постійних змін законодавчої бази, оперативне обслуговування може здійснюватися тільки в рамках компетенції оперативних служб правоохоронних органів.

Одночасно інші дослідники і практики пропонують використовувати поняття «інформаційне забезпечення», при цьому характеризуючи його як систему збору, накопичення та аналізу різних голосних і оперативних даних і явищ, пов'язаних з причинами злочинності.

У процесі вдосконалення понятійного апарату організація інформаційного забезпечення об'єктів економіки трансформувалася в систему організаційних і оперативних - тактичних заходів, що гарантують належну своєчасну поінформованість про стан і зміну оперативної обстановки в сфері економіки держави чи регіону і комплексне використання наявних сил і засобів у вирішенні завдань з протидії економічним злочинам. Ефективність протидії зумовлена чітким розмежуванням сфер дії різних правоохоронних органів (по боротьбі з майновими злочинами, щодо протидії організованій злочинності, боротьби зі злочинами проти особистості (убивства, зґвалтування), забезпечення економічної безпеки і боротьби з корупцією).

Тому інформаційне забезпечення можна визначити як систему оперативно - розшукових заходів щодо збору, узагальнення, накопичення, аналізу і зберігання інформації, що характеризує оперативну обстановку на певному об'єкті або сегменті економіки, спостереження за її змінами, своєчасному виявленні, попередженні і розкритті скоєних злочинів.

У наукових дослідженнях останніх років акцентувалася увага на тому, що сутність інформаційного забезпечення полягає в комплексі як традиційних (агентурний метод, особистий розшук), так і нетрадиційних (аналітична розвідка, внутрішня розвідка) заходів. Ці заходи в цілях прийняття перевірених і значущих управлінських рішень, доповнюючи один одного, забезпечують надходження до оперативного підрозділу, інформації про економічні об'єкти (сфери) або напрями економіки.

Таким чином, впровадження більш розширеного переліку використовуваних в процесі здійснення правоохоронними органами методів збору, обробки, накопичення і аналізу різних видів інформації дозволяє інформаційне забезпечення визначати як систему оперативно - розшукового моніторингу,

який передбачає безперервне спостереження, аналіз, оцінку і прогноз стану оперативної обстановки на об'єкті, в галузі, комплексі, сфері економіки з метою забезпечення ефективної діяльності щодо виявлення, попередження та розкриття скоєних там злочинів.

### **Компетенція кіберполіції з протидії ввезенню, виготовленню, збуту і розповсюдженню порнографічних предметів**

**Біба А.В.,**  
студентка 2-го курсу  
Донецького юридичного інституту МВС України

**Пекарський С.П.**  
кандидат юридичних наук  
доцент кафедри СДАД  
Донецького юридичного інституту МВС України

У сучасних умовах розвитку громадянського суспільства використання інформаційних технологій не має меж. Віртуальний простір переймає від суспільства все підряд, у тому числі й злочинні прояви. І тому кожна науково-розвинена країна зіткнулась з кіберзлочинністю.

Слід зазначити, що серед підрозділів Національної поліції [1] Департамент кіберполіції [2,с.3] безпосередньо протидіє злочинам, які вчиняються з використанням електронно-обчислювальних машин (комп'ютерів), телекомунікаційних та комп'ютерних інтернет-мереж і систем. Саме тому предметом даного дослідження є компетенція кіберполіції з протидії ввезенню, виготовленню, збуту і розповсюдженню порнографічних предметів.

З точки зору кримінального права [4] загальним об'єктом кіберзлочинів є персональні данні, банківські рахунки, паролі та інша особиста інформація як фізичних осіб, так і бізнесу та державного сектору. Саме тому підтримуємо висновок, що кіберзлочинність є загрозою не тільки на національному, а й на глобальному рівні [5]. Своєю чергою статтею 301 Кримінального кодексу України передбачено відповідальність за ввезення, виготовлення, збут і розповсюдження порнографічних предметів [4, ст. 301]. Частина 4 даної статті кваліфікуючою ознакою даного злочину визнає дії, вчинені щодо творів, зображень або інших предметів порнографічного характеру, що містять дитячу порнографію, або примушування неповнолітніх до участі у створенні творів, зображень або кіно- та відеопродукції, комп'ютерних програм порнографічного характеру [4, ч. 4 ст. 301]. Дана інформаційна продукція відноситься до протиправного контенту, протидія якому відноситься до компетенції кіберполіції.

Об'єктом даного злочину є суспільні відносини, які складаються з приводу протидії поширенню порнографії. Порнографія - це вульгарно-натуралістична, цинічна, непристойна фіксація статевих актів, самоцільна, спеціальна демонстрація геніталій, антиетичних сцен статевого акту, сексуальних збочень, замальовок з натури, які не відповідають моральним критеріям, ображають честь і гідність людини, спонукаючи негідні інстинкти [6]. Безпосередньо предметом даного злочину є твори, предмети або інші зображення порнографічного характеру, які у назві ст. 301 скорочено визначені як порнографічні предмети. Саме тому нам необхідно визначитися з поняттям «порнографічні предмети». Отже під «порнографічними предметами» законодавець визнає предмети [6]:

а) які становлять матеріальний предмет - річ (книги, фільми, фотопродукція, аудіо-, відеопродукція, у т. ч. реклама, картини, скульптурні зображення тощо);

б) змістом яких є детальне зображення анатомічних чи фізіологічних деталей сексуальних дій чи які містять інформацію порнографічного характеру. Форма зображення цієї сфери життя людей є неприйнятною з погляду суспільної моралі, загальновизнаних правил сором'язливості, прихованості відповідних стосунків від сторонніх осіб;

в) призначені для збудження статевої пристрасті інших осіб, провокування їх статевої агресії. Тому предметом злочину, передбаченого ст. 301, є лише твори, інші предмети, призначені для збуту чи розповсюдження, а не для власного користування;

г) не мають іншого призначення - мистецького, наукового, просвітницького тощо. Тому не можуть визнаватися предметом даного злочину відповідні ілюстрації в медичній чи юридичній літературі тощо;

д) іншими особами (яким вони демонструються чи мають демонструватися) сприймаються саме як порнографічні і збуджують статеву пристрасть [6].

Отже приходимо до висновку, що кіно- та відеопродукція, комп'ютерні програми порнографічного характеру є різновидом предмета аналізованого злочину, за наявності якого дії з ними оцінюються як кваліфікований вид злочину (ч. 2, ч.4 ст. 301 КК України). Це кіноплівки, відеоплівки, комп'ютерні дискети та цифрові носії інформації, на яких містяться фільми чи їхні окремі фрагменти відповідного змісту і призначення, або ж порнографічні відеоігри [6].

На підставі вищевказаного кримінально-правового аналізу злочину, що досліджується нам необхідно визначити компетенцію кіберполіції з протидії даним злочинам. Отже Департамент кіберполіції Національної поліції України є міжрегіональним територіальним органом Національної поліції України, який відповідно до законодавства України забезпечує реалізацію державної політики у сфері протидії кіберзлочинності, здійснює інформаційно-аналітичне забезпечення керівництва Національної поліції України та органів державної влади про стан вирішення питань, віднесених до його компетенції [3]. Участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, учинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, а також сприяння в порядку, передбаченому чинним законодавством, іншим підрозділам Національної поліції України у попередженні, виявленні та припиненні кримінальних правопорушень відноситься до завдань кіберполіції [3].

Окрім завдань до функцій Департаменту кіберполіції відноситься:

- визначення, розроблення та забезпечення реалізації комплексу організаційних і практичних заходів, спрямованих на попередження та протидію кримінальним правопорушенням у сфері протидії кіберзлочинності;
- у межах повноважень ужиття необхідних оперативно-розшукових заходів щодо викриття причин і умов, які призводять до вчинення кримінальних правопорушень у сфері протидії кіберзлочинності;
- у межах компетенції розроблення рекомендації для підвищення професійного рівня і поінформованості органів Національної поліції України, а також, громадськості про результати діяльності кіберполіції;
- внесення в установленому порядку пропозицій щодо вдосконалення законодавства у сфері протидії кіберзлочинності, а також участь у розробленні та опрацюванні проектів законодавчих та інших нормативно-правових актів у цій сфері;
- відповідно до чинного законодавства створення та забезпечення функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні злочинів, пов'язаних з комп'ютерними системами та даними, переслідуванні осіб, що обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі;
- аналіз та систематизація даних про кримінальні правопорушення, учинені у сфері протидії кіберзлочинності та з використанням високих технологій, що надходять від громадян каналами кол-центрів, електронними листами та терміналами зворотного зв'язку;
- участь в організації та проведенні навчальних та науково-практичних заходів з питань протидії кіберзлочинності (тренінгів, конференцій, семінарів тощо);
- інші повноваження відповідно до вимог чинного законодавства [3].

Отже, на підставі проведеного дослідження приходимо до висновку, що саме Департамент кіберполіції уповноважений законодавством України протидіяти протиправному контенту, одним із проявів якого є обіг порнографічних предметів, якій здійснюється з використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

#### **Література:**

1. Про Національну поліцію : Закон України від 02 липня 2015 р. № 580-VIII // Відомості Верховної Ради України. – 2015. – № 40-41. – с. 379.
2. Структура Національної поліції [Електронний ресурс]. – Режим доступу: <http://www.npu.gov.ua/uk/publish/article/1795723>
3. Департамент кіберполіції Національної поліції України [Електронний ресурс]. – Режим доступу: <https://www.npu.gov.ua/uk/publish/article/1816252>
4. Кримінальний кодекс України від 05.04.2001 [Електронний ресурс]. – Режим доступу: <http://zakon3.rada.gov.ua/laws/show/2341-14/page9>
5. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби [Електронний ресурс]. – Режим доступу: <http://www.gurt.org.ua/articles/34602/>
6. Кримінальний кодекс України. Науково-практичний коментар. [Електронний ресурс]. – Режим доступу: <http://uazakon.ru/ukr/bku/301/default.htm>

**Компетенція кіберполіції з протидії ввезенню, виготовленню, збуту або розповсюдженню творів, що пропагують культ насильства і жорстокості, расову, національну чи регіональну нетерпимість та дискримінацію**

**Кушнарьова К.О.**

студент 2-го курсу

Донецького юридичного інституту МВС України

**Пекарський С.П.**

кандидат юридичних наук

доцент кафедри СДАД

Донецького юридичного інституту МВС України

Проблема дитячої жорстокості з'явилася не сьогодні, вона є актуальною ще з давніх часів, тому зараз, на жаль, вона стала повсякденною, і багато з дорослих на це не звертають уваги, запевняючи себе, що їх дитина особлива та ніколи жорстокості не проявить. Але, на нашу думку, це є самою великою помилкою батьків, адже протягом свого дорослішання дитина всмоктує всю оточуючу інформацію навколо себе немов губка, і, навіть, якщо дитина дійсно «ідеальна», вона з легкістю може освоїти всю «не ідеальність» іншої дитини, або, навіть, дорослої людини, думку якої може вважати авторитетною. Слід вказати, що відповідно до ст. 6 Сімейного кодексу України правовий статус дитини має особа до досягнення нею 18-ти років [1, с. 20].

Відомо, що розвиток особистості відбувається поступово, причому для початкових етапів характерна недосконалість або навіть і відсутність моральної позиції. Свідомою людиною дитина ще має стати, крок за кроком, під керівництвом дорослих: батьків, учителів, друзів тощо. Як правило, особа у дитячому віці ще перебуває під впливом власних імпульсів і настроїв.

Моральні бар'єри, які впорядковують життя дорослої людини, дитиною не засвоєні. До того ж, дитина ще не завжди вміє співвідносити свої вчинки та їх наслідки. Адже і в багатьох дорослих «сверблять руки», коли їх хтось дратує своєю поведінкою, і лише значними вольовими зусиллями їм вдається себе стримувати. Прожиті роки, набутий життєвий досвід, засвоєні моральні настанови привчили їх дотримуватися суспільних норм.

Дитина ж ще не набула подібного досвіду, не засвоїла необхідних моральних уроків, у неї «руки сверблять» недовго їй розправа над однолітками, меншими, слабшими відбувається миттєво. Отже, на нашу думку, дитина може вчинити жорстоко від незнання, від нерозуміння, що крик і плач товариша - свідчення страждання й болю, завданих нею. Якщо дитина не навчена розуміти і співпереживати, вона не здатна правильно оцінювати й відчувати чужі страждання [2].

Саме тому ми приходимо до висновку, що жорстокість у наш час проявляється дуже часто відносно будь-кого. Чинниками жорстокості в першу чергу є оточуючи тебе люди. Для маленької дитини поведінка, думка батьків є найголовнішою, їх вчинки самі вірні і тому, дивлячись на те, як себе поведуть батьки вдома, дитина починає себе вести так у середовищі (дитячі садки, школа, інститут) по відношенню до оточуючих, тому що вона впевнена, що це є правильно, адже так роблять батьки. Якщо її ідеали серед дорослих дозволяють собі вирішувати особистісні проблеми за допомогою використання фізичної сили, ненормативної лексики, то дитина автоматично «намотує собі на вуса», що всі проблеми повинні вирішуватися саме так. Практика свідчить, що найпростіший засіб впливу в сімейному вихованні - покарання. Але якщо дитина не розуміє, за що її покарано, то вона відчуває лише спантеличеність і роздратування. Покарання сприймається нею як свавілля з боку дорослих. Тому вислів «викорінити жорстокість» парадоксальний за суттю. Насилля не лікується насиллям. Нерозуміння усувається роз'ясненням. Якщо дитина вчинила жорстоко з нерозуміння, необхідно його розвіяти, детально пояснивши, що вона скоїла. Дуже часто фізичне покарання переходить до постійної практики [2].

Але батьки, як правило, якщо не мають певних недоліків у психічному розвитку, виховують свою дитину згідно з нормами моралі, закону, пояснюючи їй, що є добре, а що погано, тому не викликає сумніву, що жорстокості можна навчитися. Якщо дитина виховується в такому середовищі, де жорсткі, безжалісні зіткнення є буденною справою, вона з легкістю засвоює наочні зразки поведінки. Тим більше, що зразки сучасної масової культури, до яких діти дуже чутливі, також переважно нав'язують стереотипи саме жорстокої поведінки.

Для сучасних дітей, що живуть у часи віртуального життя, коли будь-яку інформацію можна дістати через мережу, саме вона стає головним чинником, котрий розвиває в дитині схильність до жорстокості. Саме через таке активне використання мережі, виникло нове поняття злочинності –

кіберзлочинність, яка також проявляється у розповсюдженні відеороликів, фото-кадрів з зображенням жорстокості, вбивств, знущанням над людьми та тваринами тощо.

Саме тому ст. 300 Кримінального кодексу України передбачена відповідальність за ввезення, виготовлення або розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію [3]. Об'єкт даного злочину виступають моральні засади суспільства в частині розповсюдження інформації про прийнятні способи поведінки людей, засоби вирішення конфліктів. Отже ми наголошуємо на аксіомі, що інтересам суспільства відповідає необхідність обмеження в поширенні серед населення чи навіть повна відсутність творів, в яких вихваляються, видається за норму поведінки застосування грубої фізичної сили, розправа над потерпілим, катування і навіть заподіяння смерті. Такі інформаційні продукти безумовно деформують психіку людей, особливо молоді, сприяють росту злочинності.

Предметом даного злочину є твори, що пропагують культ насильства і жорстокості. Ці твори характеризуються такими ознаками:

а) становлять собою матеріальний предмет, тобто матеріалізовані у формі писаних чи відповідно розмножених (надрукованих) текстів, фільмів, магнітофонних записів, комп'ютерних програм на носіях інформації;

б) їхній зміст полягає у демонстрації актів насильства і жорстокості (сцени та епізоди з проявами садизму, тортур, катування, смакування страждань жертви, безжальності тощо в таких творах становлять головну частину сюжету);

в) призначаються для пропаганди культу насильства і жорстокості. Це означає, що відповідні прояви не засуджуються, а видаються за поведінку правильну і таку, яка заслуговує на наслідування, поширення. Оскільки пропаганда передбачає поширення і роз'яснення певних положень серед широких верств, то предметом даного злочину є лише твори, призначені для збуту або розповсюдження, а не для власного використання;

г) не мають іншого призначення - наукового, історичного тощо. Не можуть, наприклад, визнаватися предметом виготовлення творів, що пропагують культ насильства і жорстокості, дані оперативних зйомок, які провадяться працівниками правоохоронних органів.

Об'єктивна сторона злочину полягає в таких діях щодо творів, які пропагують культ насильства і жорстокості: 1) ввезення в Україну; 2) виготовлення; 3) зберігання; 4) перевезення; 5) інше переміщення; 6) збут; 7) розповсюдження; 8) примушування до участі в їх створенні [4]. Окрім того слід вказати на використання злочинцями електронно-обчислювальних машин (комп'ютерів), телекомунікаційних та комп'ютерних інтернет-мереж і систем у своїх злочинних намірах. Оскільки твори, що пропагують культ насильства і жорстокості відносяться до протиправного контенту то серед підрозділів Національної поліції саме співробітники Департаменту кіберполіції уповноважені протидіяти даним злочинним діям [5; 6].

Підводячи підсумок зазначаємо, що нами на підставі кримінально-правового аналізу злочину, що досліджується, визначена компетенція кіберполіції з протидії ввезенню, виготовленню, збуту або розповсюдженню творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію.

### **Література:**

1. Науково-практичний коментар до Сімейного кодексу України: Видання друге, доповнене / Харитонов Є.О., Харитонova О.І., Білоусов Ю.В. та ін. За ред. Є.О. Харитонova. – Х.: ТОВ «Одіссей». – 2008. – 560 с.
2. Дитяча жорстокість [Електронний ресурс]. – Режим доступу: <http://pedrada.km.ua/document/dityacha-zhorstokist.html>
3. Кримінальний кодекс України від 05.04.2001 [Електронний ресурс]. – Режим доступу: <http://zakon5.rada.gov.ua/laws/show/2341-14/page9>
4. Коментар до статті 300. Ввезення, виготовлення або розповсюдження творів, що пропагують культ насильства і жорстокості [Електронний ресурс]. – Режим доступу: <http://yurist-online.com/ukr/uslugi/yuristam/kodeks/024/297.php>
5. Структура Національної поліції [Електронний ресурс]. – Режим доступу: <http://www.npu.gov.ua/uk/publish/article/1795723>
6. Департамент кіберполіції Національної поліції України [Електронний ресурс]. – Режим доступу: <https://www.npu.gov.ua/uk/publish/article/1816252>  
<http://zakon3.rada.gov.ua/laws/show/2341-14/page9>

**Окремі проблеми правового забезпечення кібернетичної безпеки в Україні в умовах розвитку інформаційного суспільства**

**Хлевицький В.Б.**

кандидат юридичних наук, с.н.с.,  
в.о. завідувача сектору

Науково-дослідного інституту  
інформатики та права НАПрН України

Досвід провідних країн світу свідчить про те, що ефективність державного управління, темпи соціально-економічного розвитку суспільства, рівень обороноздатності держави та її безпеки на етапі переходу від постіндустріального суспільства до суспільства інформаційного усе більше залежить від стану захищеності інформаційної сфери. Це, зокрема, стосується інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, що забезпечують функціонування органів державної влади, місцевого самоврядування, військової організації держави, фінансової і кредитно-банківської системи, автоматизованих систем керування технологічними процесами стратегічно важливих для економіки та безпеки держави промислових підприємств, об'єктів життєзабезпечення та підвищеної небезпеки (енергетики, транспорту, телекомунікацій, хімічної та переробної промисловості, тепло-, водопостачання та ін.) – тобто тих, що становлять так звану «критичну інфраструктуру» держави [1-2].

З урахуванням прагнення України інтегруватись в Європейський Союз, одним з головних її пріоритетів згідно із Законом України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 рр.» [3] є побудова орієнтованого на інтереси громадянина, відкритого для всіх і спрямованого на розвиток інформаційного суспільства, в якому кожен міг би створювати і накопичувати інформацію та знання, мати до них вільний доступ, користуватися і обмінюватися ними, щоб надати можливість кожній людині повною мірою реалізувати свій потенціал, сприяючи суспільному і особистому розвитку та підвищуючи якість життя. Паралельно актуалізуються питання створення належних, насамперед, правових умов для забезпечення безпечного використання національної інформаційної інфраструктури, надійного її захисту від кібернетичних загроз як одного з визначальних чинників для забезпечення кібернетичної безпеки особи, суспільства і держави.

Джерелом кібернетичних загроз можуть бути не тільки міжнародні злочинні групи хакерів, добре обізнані у сфері інформаційних технологій злочинці, а й іноземні державні органи, терористичні угруповання, недержавні організації, політичні структури та неформальні об'єднання екстремістського спрямування, транснаціональні корпорації та фінансово-промислові групи тощо. Зростає загроза використання проти України кібернетичних засобів як з середини держави, так і з-за меж її кордонів. Такою ж реальною є загроза використання української інформаційної інфраструктури як "транзитного майданчику" для приховування кібернетичної атаки на інформаційні ресурси третьої держави, що може розцінюватись провідними країнами як дії держави з відповідними наслідками політичного, економічного, правового і воєнного характеру. Вказані чинники перевели проблему боротьби з кіберзлочинністю із загально-кримінальної у військово-політичну, про що свідчить.

Активність з боку провідних країн світу у кіберпросторі, глибинні зміни у їх зовнішній та внутрішній інформаційній політиці, формування потужних транснаціональних злочинних груп, що спеціалізуються на злочинах в кіберпросторі – все це обумовлює необхідність створення в Україні ефективної національної системи кібернетичної безпеки (далі - НСКБ), що знайшло підтримку на рівні вищого політичного керівництва держави.

Так, пунктом 4.12. оновленої «Стратегії національної безпеки України», введеної в дію Указом Президента України від 26.05.2015р. №287/2015 [4] визначено, що одним з основних напрямів державної політики національної безпеки України у сфері забезпечення кібербезпеки і безпеки інформаційних ресурсів є створення національної системи кібернетичної безпеки, що підтверджено рішенням Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України", затвердженим Указом Президента України № 96/2016 [5].

За оцінкою фахівців, створення НСКБ, насамперед, потребуватиме законодавчого визначення наступних питань:

- структура системи державного управління у сфері кібернетичної безпеки, склад, завдання, режими функціонування НСКБ;
- порядок інформаційного обміну між її складовими елементами, їх повноваження щодо протидії кіберзагрозам;
- механізми державно-приватного партнерства та залучення громадськості до забезпечення

кібернетичної безпеки;

– критерії віднесення об'єктів до таких, що мають становлять критичну інформаційну інфраструктуру України та потребують першочергового захисту від кібернетичних атак, порядок формування їх переліку, повноваження владних структур щодо його розробки, затвердження та подальшого ведення.

Крім того, важливе місце у створенні НСКБ має займати належне кадрове забезпечення, створення ефективної системи підготовки кадрів, у т.ч., враховуючи транснаціональний характер кіберзагроз, - з можливим залученням іноземних фахівців.

Суттєву профілактичну роль у питанні кібербезпеки відіграє удосконалення кримінального законодавства, розвиток якого у порівнянні з темпами впровадження та опанування кримінальними елементами сучасних інформаційних технологій, вочевидь пригальмований. Слід зазначити, що цей чинник суттєво ускладнює боротьбу з кібернетичними загрозами внаслідок недостатньої гармонізації чинного законодавства з вимогами Конвенції про кіберзлочинність, ратифікованої Постановою Верховної Ради України від 7 вересня 2005 року № 2824 [6-7]. Зокрема, йдеться про Кримінальний, Кримінальний процесуальний кодекс, Закони України «Про телекомунікації», «Про банки та банківську діяльність», «Про захист інформації в інформаційно-телекомунікаційних системах» та ін. у частині:

- надання правоохоронним органам повноважень щодо видачі обов'язкових до виконання приписів володільцями комп'ютерних даних (провайдерів і операторів телекомунікацій, іншими юридичними та фізичними особами), про термінове фіксування та подальше зберігання комп'ютерних даних, які потрібні для розкриття злочину на термін до 90 днів із можливістю подальшого продовження терміну до 3 років;

- встановлення вимог із надання провайдером телекомунікацій правоохоронним органам інформації для ідентифікації постачальників послуг і маршруту, яким було передано інформацію.

Кримінальний процесуальний кодекс України (далі - КПКУ), який набрав чинності 19 листопада 2012р., також потребує узгодження з положеннями Конвенції Ради Європи «Про кіберзлочинність» у частині належної імплементації статей 17, 19, 20, 21, 30, 33, 34, які передбачають розкриття та збирання в режимі реального часу даних про рух інформації в комп'ютерній системі, обшук та арешт комп'ютерних даних, перехоплення змісту інформації в телекомунікаційних мережах тощо.

Негласні слідчі дії, які відповідають зазначеним статтям Конвенції, передбачені чинним КПКУ, а саме, ст. 263 «Зняття інформації з транспортних телекомунікаційних мереж» та ст. 264 «Зняття інформації з електронних інформаційних систем», які є різновидом втручання у приватне спілкування.

Відповідно до ст. 246 КПКУ, втручання у приватне спілкування проводиться виключно у кримінальному провадженні щодо тяжких або особливо тяжких злочинів. Проте, передбачені розділом XVI Кримінального кодексу України (окрім ч. 2 ст. 361 та ч. 3 ст. 362) не є тяжкими.

Водночас, в процесуальному законодавстві багатьох країн-учасниць Конвенції про кіберзлочинність є окремі норми, які встановлюють особливий порядок перехоплення та розкриття інформації про рух даних в комп'ютерній системі під час розслідування кіберзлочинів, навіть якщо вони не є тяжкими.

З урахуванням реалій сьогодення, окремі норми вітчизняного законодавства також втрачають свою актуальність.

Так, незважаючи на визначену законодавством компетенцію органів держбезпеки та внутрішніх справ, виключне право провадження попереднього слідства при розслідуванні злочинів, передбачених Розділом XVI Кримінального Кодексу України, віднесено до підслідності органів внутрішніх справ. Такий підхід не враховує специфіку завдань, які мають виконувати вказані правоохоронні органи, що потребує чіткого розмежування за компетенцією. Спроба такого розмежування знайшла відображення в законопроекті «Про основні засади забезпечення кібербезпеки України» (реєстр. № 2126а від 14.04.2016 р.) [8]. Проте, зазначена норма вимагає внесення додаткових змін та доповнень у кримінальне та кримінальне процесуальне законодавство, розробка яких є перспективним завданням для науковців та практиків.

#### **Література:**

1. Довгань О.Д., Климчук О.О., Панченко В.М. та ін. Організаційно-правові засади критичної інфраструктури України від кіберзагроз : моногр. – К. : Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2013. – 244 с.
2. Недільніченко В.Д. Розвиток інформаційних технологій і національна безпека України // Національна безпека: український вимір.- 2009.- №3 (22). – С. 43-57.

3. Закон України від 9 січня 2007 року №537-V “Про основні засади розвитку інформаційного суспільства в Україні з 2007 - 2015 роки” // Відомості Верховної Ради України.-2007.-№12.-Ст.102.
4. Указ Президента України від 26.05.2015р. №287/2015«Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України"[Електронний ресурс] //Офіційний сайт Верховної Ради України. – Режим доступу : <http://zakon.rada.gov.ua>.
5. Указ Президента України від 15 березня 2016 року N 96/2016 “Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “Про Стратегію кібербезпеки України” [Електронний ресурс] // Офіційний сайт Верховної Ради України. – Режим доступу : <http://zakon.rada.gov.ua>.
6. Про кіберзлочинність: Конвенція Ради Європи // Офіц.вісн.України.-2007.-№65.-Ст.2535.-С.107.-10 верес.- Код акта 40846/2007.
7. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 7 верес. 2005 р. №2824- IV // Урядовий кур'єр.- 2005.-№185.-верес.
8. Проект Закону України «Про основні засади забезпечення кібербезпеки України» (реєстр. № 2126а від 14.04.2016р.)[Електронний ресурс] //Офіційний сайт Верховної Ради України. – Режим доступу : <http://w1.c1.rada.gov.ua>

### **Використання європейського досвіду в організації роботи поліції України**

**Шелехов А.О.**

кандидат юридичних наук, доцент  
завідувач кафедри адміністративної діяльності  
ОВС та економічної безпеки  
Одеського державного університету внутрішніх справ

**Корнієнко М.В.**

кандидат юридичних наук, доцент  
професор кафедри адміністративної діяльності  
ОВС та економічної безпеки  
Одеського державного університету внутрішніх справ

У даному матеріалі досліджено напрями та шляхи використання в Україні європейського досвіду з організації діяльності і навчання поліцейських на прикладі роботи поліції в Естонській Республіці. Висвітлені на нашу думку передові та перспективні напрями удосконалення поліцейської діяльності в Естонії, які доцільно було б запровадити під час реформування Національної поліції України, трансформуючи їх під наші реалії.

В рамках «Програми обміну поліцейськими 2016» Європейського поліцейського коледжу (CEPOL) з 04 по 09 вересня 2016 року відвідали Республіку Естонію і ознайомились зі структурою та роботою правоохоронних органів в державі.

В Україні відбувається реформуванням правоохоронної системи та впровадженням нових підходів у діяльність Міністерства внутрішніх справ України згідно зі стандартами, принципами та нормами розвинутих європейських країн. Однією з найбільш прогресивних країн пострадянського простору яка на нашу думку досягла значного успіху у реформуванні правоохоронної системи є Естонська Республіка. В Естонії функціонування поліції супроводжується високим рівнем соціальної довіри з боку населення і це є одним із головніших критеріїв оцінки її діяльності. Також під час співпраці поліції і населення вживається термін партнерство. Партнерство як один з видів взаємодії, який ґрунтується на очікуванні, що партнер по взаємодії буде поводитись згідно з очікуваннями співробітництва.

Партнерство у сучасному розумінні - це вид взаємовідносин між різними суб'єктами, який полягає у виробленні єдиної позиції з тих чи інших питань, організації спільних дій. Специфікою партнерства є збереження кожним з партнерів відносної самостійності в основних аспектах діяльності [1, с. 427].

Етимологічний словник української мови визначає, що термін партнер в українську мову запозичений з французької, в свою чергу французьке "partenaire" походить від англійського "partner", яке вживається у кількох значеннях, зокрема, "співспадкоємець", "поділ", "частина" тощо [2, с. 300].

Відносно практики поліцейської діяльності зарубіжних країн, як правило, на означення процесів співпраці поліції з населенням, вживається термін поліція громади чи общинна поліція, тотожним до



якого є термін "партнерство з населенням" [4, с. 5-6]. Результати діяльності поліції у Естонській Республіці є досить високі і тому для України цей досвід роботи в поліцейській діяльності є дуже актуальним.

Систему Національної безпеки Естонської Республіки становлять: Президент країни, Парламент та комітет по національній обороні, на наступному рівні заходиться Прем'єр - міністр, ступенем нижче знаходиться Департамент інформації і координаційне бюро по безпеці та національній обороні, на наступному рівні системи знаходяться Міністерства, так в Міністерство фінансів входить (податковий та митний департамент), до Міністерства юстиції належить (прокуратура), до Міністерства внутрішніх справ (Департамент поліції і прикордонної охорони та поліція безпеки), до Міністерства оборони відноситься (Генеральний штаб сил оборони, Центр кіберзахисту та Центр оборонних досліджень) та Міністерства закордонних справ належить (Комітет по стратегічним товарам).

Розглянемо більш докладніше які ж органи входять до Міністерства внутрішніх справ: це Департамент поліції прикордонної служби, рятувальний департамент, поліція безпеки, Академія внутрішньої безпеки, центр розвитку інформаційних технологій, рятувальний центр.

Звернемо увагу що Міністерство внутрішніх справ Естонської Республіки розробляє стратегічні напрямки, методи і повноваження кожного вищевказаного органу, а також являється координатором в кожній сфері. Так наприклад Департамент поліції та прикордонної охорони (ДППО) був створений у 2010 році завдяки об'єднанню трьох департаментів (Департаменту поліції, Департаменту прикордонної охорони, Департаменту громадянства і міграції). На основі поліцейських префектур та прикордонних округів були сформовані чотири регіональні префектури Пыхьяская префектура (північна), Идаская префектура (південна), Лыунаская префектура (східна), Ляэнеская префектура (західна). На сьогодні в Департаменті поліції та прикордонної охорони працює 5443 з них 4077 поліцейських, 868 державних службовців та 498 додаткового персоналу.

Департамент поліції та прикордонної охорони виконує такі основні завдання як: забезпечення охорони зовнішніх кордонів Європи, провадження відносно адміністративних і кримінальних правопорушень та їх профілактика, здійснення охорони правопорядку в середині держави та визначення громадянства та видача документів

Важливим критерієм довіри роботи поліції є її відкритість для громадян. Формування довіри до поліції це є щоденна, кропітка робота всіх підрозділів ДППО, адже знання про її досягнення та проблеми, а відтак подальше ставлення та оцінка виконаної роботи складаються як з безпосереднього досвіду спілкування з її працівниками, так і з інформації, яку громадяни отримують із різних джерел, у тому числі з засобів масової інформації.

Діяльність засобів масової інформації в частині контролю за діяльністю Національної поліції України визначається положеннями Конституції України [3], Законами України «Про Національну поліцію» [9], «Про інформацію» [8], «Про доступ до публічної інформації» [6], «Про інформаційні агентства» [7], «Про телебачення і радіомовлення» [11], «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування засобами масової інформації» [10], «Про державну підтримку засобів масової інформації та соціальний захист журналістів» [5] та ін.

Окремої уваги потребує вдале запровадження підрозділів оперативної інформації чи так званого центру єдиного виклику екстреної допомоги «112». Підрозділи поліції оперативної інформації розташовані у 4 префектурах і здатні у разі потреби, брати на себе функції одне одного. Вони цілодобово приймають і обслуговують термінові виклики та також відповідають за управління ресурсами оперативної допомоги і обміну інформації.

Двухступиневе керування підрозділів оперативної інформації здійснюється наступним чином: на першій ступені (організатор допомоги) приймає дзвінок термінові допомоги, обробляє і реєструє в базі даних, якщо є виклик на місце події передається на другу ступень. На другій ступені організовується відправлення ресурсу для вирішення питання прийнятого першим ступенем. Також для зручності і чіткості в роботі при прийнятті повідомлення йде чітке розподілення по пріоритетах на три частини: А (alfa) подія чи стан потерпілого не критичний, також немає загрози життю чи майну; В (bravo) подія чи стан постраждалого важкий чи інформація про стан постраждалого відсутня, є загроза заволодіння майном чи знищення майна або затриманий правопорушник; С (charlie) подія потребує термінового втручання поліції, стан потерпілого критичний він потребує швидкої допомоги з боку медичних працівників чи рятувальників.

В Естонії приділяється багато уваги питанням боротьби з корупцією. Питаннями попередження, виявлення і боротьбою з корупцією займаються три окремі служби: «Бюро по боротьбі з корупційними злочинами», «Поліція безпеки» та «Внутрішній контроль департаменту поліції і прикордонної охорони». Бюро складається з чотирьох регіональних підрозділів і займається винними діями посадовців, хабарами в приватному секторі і злочинами, пов'язаними з перешкоджанням вільному

здійсненню виборчого права. Поліція безпеки займається корупційними злочинами високо посадовців, а внутрішній контроль департаменту поліції і прикордонної охорони корупційними діяннями поліцейських. В Республіці Естонії під злочинами, пов'язаними з корупцією, розуміють -привласнення, зловживання довірою, отримання, посередництво, дача хабара, використання впливу в корупційних цілях, підробка документів посадовою особою, використання підроблених документів, порушення вимог здійснення державних замовлень, порушення обмеження на вчинення дій, отримання та давання хабара в приватному секторі. Законодавець в Естонії визначає хабар як згоду посадової особи прийняти обіцяні йому або третій особі майно або інші пільги або прийняття ним майна чи інших пільг в якості винагороди за використання ним свого службового становища. Також в Естонії визначені ознаки корупційної небезпеки - це отримання пільг або додаткового доходу посадовця, цим схиляючи чиновника до нечесних дій, ставлячи під сумнів хорошу репутацію установи. Найбільш часті корупційні порушення є присвоєння майна (фіктивні рахунки, шахрайство у вигляді забирання додому майна, палива, маркірованого палива, майна на рахунок осіб, які перебувають під опікою, підробка звітів бухгалтерії; порушення обмеження на здійснення дій (рішення щодо себе або афілійованої особи); адміністрування установи (пайовою участю в установі виносяться рішення щодо себе або афілійованої особи, паливо і паливне масло, відрядження, фіктивні рахунки, забирання додому майна, хабар за замовлення на виконання робіт, приписка робочих годин, пов'язаних з виконанням проекту), а також в більшості випадків, підробка документів. Все вище викладене займає не великий відсоток у виявлених правопорушеннях пов'язаних з корупційними діяннями в Естонській Республіці. Дуже багато уваги приділяється превенції корупційних проявів у державних службовців у вигляді (соціальних відеороликів та соціальної реклами, роз'яснювальних лекцій і тренінгів і таке інше).

Питаннями підготовки та перепідготовки поліцейських в Естонській Республіці займається Академія безпекових наук яка розташована у місті Таллінн, в якій вчиться 890 кадетів і працює близько 250 осіб, та яка є вищим навчальним закладом у відомчому підпорядкуванні Міністерства внутрішніх справ Естонії і готує на базі професійної, вищої і магістерської освіти фахівців для установ, що відповідають за внутрішню безпеку країни (в тому числі поліція, прикордонна охорона, юстиція, рятувальна, податкова і митна служба). Поряд з основним комплексом навчальних будівель, що знаходяться в Таллінні, академія має в своєму розпорядженні кілька навчальних центрів в різних частинах Естонії: в Харьюском повіті (Коледж поліції і прикордонної охорони в Мурасте), в Пярнуському повіті (Поліцейська школа в Пайкузе) і в Ляене-Віруском повіті (Рятувальний коледж в Вайке-Маарів).

Серед новел організації навчального процесу в Академії безпекових наук Естонської Республіки цікавим для детального розгляду і подальшого введення в навчальний процес для вузів зі специфічними умовами викладання системи Міністерства внутрішніх справ України є: по-перше закріплення за курсантами з початку навчання вогнепальної зброї яка буде супроводжувати його під час проходження всієї служби у поліції; по-друге під час проходження практики курсанти які в майбутньому стануть патрульними поліцейськими, до речі вони навчаються півтора року і отримують по закінченню диплом спеціаліста, а в перспективі (перехід на дворічну підготовку), з викладачем по графіку заступають на патрулювання міста і займаються в першу чергу профілактичною роботою також складання протоколів за порушення правил дорожнього руху, з початку навчання у курсантів виховується самостійність в прийнятті рішення і вмінні спілкуванні з громадянами; по-третє курсанти під час навчання отримують спеціальні сертифікати які дають їм право керувати службовим автотранспорт, використовувати табельну вогнепальну зброєю і спец засобами, під час кадрових переміщень додатково ніяких іспитів і заліків не здається; по-четверте курсантів не залучають на чергування і на господарські роботи, для того щоб не відволікати від навчання. В навчальному процесі також широко застосовується комп'ютерна система XVR, яка дозволяє моделювати різні не штатні події, а також приймати курсантами швидке, правильне рішення, що в подальшому буде слугувати гарною практикою в чіткому алгоритмі дій при не штатних ситуаціях.

Підсумовуючи діяльність Департаменту поліції та прикордонної охорони Естонської Республіки можна зробити загальний висновок, що у діяльності поліції на сучасному етапі діє підхід, в основі якого лежить орієнтація поліції на задоволення потреб громадян, які виступають клієнтами, замовниками послуг, які надає поліція. З одного боку партнерство, а з іншого боку служіння і задоволення потреб кожної людини яка потребує допомоги, поставлено в центр діяльності поліції Естонії.

#### **Література:**

1. Большая энциклопедия [текст] : в 62 томах. / гл. ред. С. А. Кондратов. — М. : ТЕРРА, 2006 — Т.35 : Охрана - Пейзаж. — М., 2006. — 591 с.

2. Етимологічний словник української мови : у 7 томах [редкол.: О. С. Мельничук та ін.] — К.: Наукова думка, 1983. Т.4: Н-П.-К., 2003 -656 с.
3. Конституція України від 28 липня 1996 р. [Електронний ресурс] – Режим доступу: <http://zakon.rada.gov.ua/>.
4. Наилучшая практика построения партнерства между полицией и обществом. Составлено Старшим полицейским советником при Генеральном секретаре ОБСЕ. [Електронний ресурс] — Вена : Отдел стратегических вопросов полицейской деятельности ОБСЕ, 2008. — Режим доступу : <http://polis.osce.org/library>.
5. Про державну підтримку засобів масової інформації та соціальний захист журналістів : закон України від 23.09.1997 р. [Електронний ресурс] — Режим доступу : <http://www.zakon.rada.gov.ua/>.
6. Про доступ до публічної інформації : закон України від 13.01.2011 р. [Електронний ресурс] — Режим доступу : <http://zakon.rada.gov.ua/>.
7. Про інформаційні агентства : закон України від 28.02.1995 р. [Електронний ресурс] —Режим доступу : <http://zakon.rada.gov.ua/>.
8. Про інформацію : закон України від 02.10.1992 р. [Електронний ресурс] —Режим доступу : <http://zakon.rada.gov.ua/>.
9. Закон України Про Національну поліцію / від 02.07.2015 року Відомості Верховної Ради України. – 2015. – № 580. – Ст. 378.
10. Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації: закон України від 23.09.1997 року [Електронний ресурс] —Режим доступу : <http://zakon.rada.gov.ua>.
11. Про телебачення і радіомовлення :Закон України від 21.12.1993 року [Електронний ресурс] — Режим доступу : <http://www.zakon.rada.gov.ua/>.

### **Сучасні проблеми кіберзлочинності: міжнародний аспект**

**Небеська М.С.**

кандидат юридичних наук  
доцент кафедри теорії та історії держави і права  
Одеського державного університету внутрішніх справ

Розвиток високих інформаційних технологій є масштабним динамічним процесом, що має постійний та цілеспрямований характер. Внаслідок цього постійно вдосконалюються існуючі або створюються нові способи оброблення інформації, підвищується швидкість передачі даних, з'являються нові види каналів зв'язку, виникають раніше невідомі або недосяжні послуги. З іншого боку, все це приваблює злочинний світ, оскільки виступає підґрунтям для виникнення більш складних, високотехнологічних схем кримінальної діяльності, створює вищий рівень організованості.

Сучасна злочинність, яка є породженням перехідного періоду розвитку суспільства, за своїми якісними і кількісними ознаками суттєво відрізняється від злочинності минулих років. Сьогодні злочинність більш масштабна, професійна, організована та технічно оснащена. Сучасний стан злочинів у сфері високих інформаційних технологій характеризується тим, що їх кількість не має тенденцій до зменшення, а навпаки, спостерігається постійне зростання та розширення існуючих меж. Цілком очевидно, що гострота проблем у цій сфері боротьби стає потенційною небезпекою для держави та вимагає прийняття неординарних рішень, кардинальних змін стереотипних підходів до її вирішення, розроблення нових форми боротьби зі злочинністю, але враховуючи при цьому пріоритетність інтересів людини й громадянина.

Протидію будь-якому злочину або їх групі можна визначити як систему правових, організаційних, методичних заходів, які забезпечуються певними юридичними науками процесуального циклу, такими як кримінальне право, кримінальний процес, кримінологія, криміналістика, судова експертиза, оперативно-розшукова діяльність, а також адміністративне право. Слід підкреслити, що специфіка злочинів проти інформаційної безпеки виражається в тому, що при вчиненні протиправних дій злочинець, як правило, практично не залишає матеріальних слідів своєї діяльності або вони є незначними. Через це працівникам правоохоронних органів доводиться мати справу з такою специфічною групою слідів як інформаційні, що вносить корективи в процес дослідження способу вчинення злочину і супроводжуючих його відповідних слідів.

Поступове покращення якості обслуговування в ІТ-сфері спричинило різкий сплеск злочинності у сфері високих інформаційних технологій та інших антигромадських проявів, пов'язаних з інформаційними і телекомунікаційними технологіями. Такі перетворення становлять серйозну загрозу

демократичним перетворенням і безпеці всіх без винятку країн світу. Зазначене примусило правоохоронні органи держав світу вдосконалювати відповідні правові інструментарії, пристосовуючи їх до нових технологій. За останні роки відмічається тенденція до створення та подальшої реорганізації у складі правоохоронних органів (поліції, органів сектору безпеки) держав світу спеціалізованих підрозділів з протидії комп'ютерній злочинності. Все частіше держави виходять з ініціативами щодо протидії злочинності у сфері високих інформаційних технологій. З огляду на гостроту та актуальність питання боротьби з цим явищем у стратегічній перспективі, сьогодні особливої уваги набуває проблематика формування організаційної та функціональної структури, існуючої у правоохоронних органах підрозділів по боротьбі з комп'ютерними злочинами, яка сьогодні не відповідає поставленим перед ними завданням. Тому, вивчення та впровадження зарубіжного досвіду із зазначеного питання є досить необхідним і важливим для України. На сучасному етапі розвитку зацікавленість з боку провідних країн світу та міжнародних організацій до проблем кібербезпеки викликана зростанням кількості кіберзлочинів; проникненням інформаційних, телекомунікаційних та інформаційно-телекомунікаційних технологій в усі сфери життєдіяльності; посиленням уваги до агресивних дій у кіберпросторі з боку злочинних формувань і деяких країн [1, с. 32].

Певний інтерес викликає організація боротьби з комп'ютерною злочинністю, а також інших напрямів захисту кіберпростору у Сполучених Штатах Америки.

Інтенсивний контроль за кримінальною діяльністю в мережі Інтернет здійснює ФБР США. У складі ФБР США у 1996 році створено Кіберпідрозділ, який функціонує на правах окремого управління в структурі ФБР. На Кіберпідрозділ покладено функцію надання допомоги іншим підрозділам ФБР у розслідуванні злочинів, вчинених з використанням комп'ютерних і телекомунікаційних технологій. Кіберпідрозділ ФБР має чотири відділи: протидії незаконним втручанням у роботу комп'ютерних мереж, протидії дитячій порнографії, протидії шахрайствам, протидії порушенням у сфері інтелектуальної власності. У лютому 2003 року в США розроблено та опубліковано «Національну стратегію захисту кіберпростору», в якій наведено послідовний та комплексний підхід до захисту життєво важливих комунікаційних технологій американської нації [2, с. 260].

У Французькій Республіці в 1994 році було створено «Службу протидії зловживанням у сфері інформаційних технологій». Даний підрозділ підпорядковується Управлінню паризької кримінальної поліції, основним завданням якого є боротьба з «інтелектуальним» піратством і «хакінгом». У лютому 2008 року Міністр внутрішніх справ Франції Мішель Алліот-Марі оприлюднив французьку Стратегію з питань боротьби з кіберзлочинністю. Мета Стратегії - співпраця між приватним бізнесом (постачальником інформаційно-телекомунікаційних послуг) і правоохоронними органами з метою обміну інформацією та об'єднання зусиль у боротьбі з кіберзлочинністю. Для реалізації Стратегії було визначено основні завдання:

- покращення співробітництва з операторами електронних комунікацій, що прискорить передачу інформації поліції та жандармерії;
- створення належних умов для адекватної протидії кіберзлочинності з боку поліції та жандармерії, для чого слід використовувати всі відомі національні та міжнародні нормативно-правові акти, розробляти новітні й модернізувати існуючі технічні засоби, що знаходяться у розпорядженні поліції та жандармерії, удосконалювати методи щодо упередження такого виду злочинності [3, с.245 ].

У 1994 році в складі поліцейського управління м. Мюнхен (Німеччина) було створено спеціальну групу по боротьбі зі злочинами у сфері високих технологій. Пізніше у структурі федеральної поліції Німеччини створено групу «Технології», до складу якої входить понад 60 працівників кримінальної поліції, техніків, інженерів і вчених різних спеціальностей. Їх завданнями є як самостійне розслідування високотехнічних злочинів, так і сприяння роботі інших підрозділів, проведення досліджень і створення нових програмно-апаратних засобів для поліції, міжнародне співробітництво. Корисним є досвід Німеччини щодо створення національних систем по контролю за діяльністю Інтернет-сайтів, що використовуються в терористичних цілях. Так, з метою інформаційного забезпечення та координації всіх спеціальних і правоохоронних органів Німеччини, задіяних у боротьбі з тероризмом, для пошуку, аналізу та контролю за вищевказаними веб-сайтами на початку 2007 року розпочав свою роботу «Інтернет-центр Німеччини», який: щоденно готує інформаційне повідомлення; раз на 10 днів видає інформаційний бюлетень щодо існуючих тенденцій та їх оцінки; невідкладно інформує з термінових питань [4, с. 36].

Розвиток багатьох країн світу свідчить про співіснування усталених і нових форм злочинної діяльності, що охоплюють, у першу чергу, слабко контрольовані чи неконтрольовані державою сфери, втручаються в економіку, політику, ідеологію та соціальні відносини. Це проявляється й у вчиненні злочинів у сфері високих інформаційних технологій або використанні їх можливостей при вчиненні

тероризму, торгівлі людьми та розповсюдженні порнографії. Вивчення та впровадження позитивного зарубіжного досвіду із зазначеного питання є необхідним і важливим для України.

Важливо зазначити, що в Україні створена і діє досить розгалужена система забезпечення безпеки інформації. Наявна певна законодавча база, яка складається із Законів України «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про державну таємницю» тощо. Є чинними низка указів Президента та постанов Кабінет Міністрів України, якими регульовано конкретні напрями діяльності в галузі захисту інформації. Але чинне кримінальне та кримінально-процесуальне законодавство України наразі не забезпечує надійного захисту від кіберзлочинності.

Дослідження зарубіжного досвіду свідчить про те, що на сучасному етапі оперативно-розшукова профілактика злочинів повинна також ґрунтуватися на вивченні основних тенденцій розвитку злочинності. Це передбачає застосування нових підходів до реалізації аналітичних розробок щодо інформаційно-психологічних впливів, спрямованих на боротьбу з комп'ютерною злочинністю.

### **Література:**

1. Телійчук В. Г. Способи вчинення злочинів у сфері використання електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку та заходи протидії [Текст] / В. Г. Телійчук // Держава та регіони. Сер. : Право. - 2014. - № 2. - С. 31-37.
2. Гіда О. Ф. Міжнародні ініціативи у сфері посилення інформаційної безпеки та протидії організований злочинності [Текст] / О. Ф. Гіда // Боротьба з організованою злочинністю і корупцією (теорія і практика). - 2012. - Вип. 1. - С. 258-266.
3. Бутузов В. М. Міжнародний досвід: ініціатива правоохоронних органів Франції з протидії комп'ютерній злочинності [Текст] / В. М. Бутузов // Боротьба з організованою злочинністю і корупцією (теорія і практика). - 2008. - Вип. 19. - С. 240-246.
4. Бойченко О. В. Особливості оперативно-розшукової протидії комп'ютерній злочинності [Текст] / О. В. Бойченко, М. М. Новиков // Форум права. - 2010. - № 1. - С. 34.

### **Актуальні питання нормативно-правового забезпечення аналітично-інформаційної системи Національної поліції України**

**Свиріпа І.В.**

курсант 402 взводу факультету №1  
Одеського державного університету внутрішніх справ

**Небеська М.С.**

кандидат юридичних наук  
доцент кафедри теорії та історії держави і права ОДУВС

XX століття характеризується як століття комп'ютеризації усіх сфер життєдіяльності суспільства, впровадження новітніх розробок науково-практичного прогресу в практичну діяльність як окремого індивіда, так і держави в цілому.

Станом на сьогоднішній день, інформаційні системи широко використовуються в усіх галузях життєдіяльності суспільства та надзвичайно ефективно виконують покладені на них завдання. Процес комп'ютеризації призводить до поступової заміни людської праці у рутинних монотонних операціях, тобто є їй гідним правонаступником.

Сучасний період розвитку цивілізації, в цілому, можна характеризувати як глобальне інформаційне суспільство, в якому практично уся діяльність людей здійснюється на основі використання послуг, які надаються інформаційними системами.

Широке впровадження на світовому рівні комп'ютеризованих (автоматизованих, комп'ютерних) інформаційно-технологічних систем поряд із поліпшенням взаємодії між окремими людьми, їх спільностями, суспільствами, цілими народами, державами висуває багато актуальних проблем, які потребують наукового дослідження, обґрунтування і практичного вирішення [1].

Важливим є те, що інформаційна система має особливе значення для правоохоронних органів, що пояснюється наявністю великого спектра інформації: від звичайних облікових даних у комп'ютерних системах про громадян до стратегічних державних програм. Окрім цього, як відомо основою прийняття найбільш ефективних заходів, у будь-якій ситуації, є своєчасно отримана достовірна інформація.

Дослідженням актуальних питань щодо впровадження та розвитку аналітично – інформаційної системи Національної поліції України, займалися такі вчені, як: П.Д. Біленчук, В.С. Безрученко, Є.С. Дубоносов, Ю.С. Шумшученко, Д.Я. Семир'янов та ін.

В умовах сьогодення успіх будь-якої сфери людської діяльності безпосередньо залежить від його рівня забезпечення необхідною інформацією, що безумовно стосується і діяльності Національної поліції України. Стосовно цього не можна не погодитись з Г.М. Бірюковим, який зазначив, що вміло організована та ефективно діюча система інформаційного забезпечення дозволяє правоохоронним органам ефективно вирішувати завдання, що стоять перед ними [2].

Поява величезної кількості інформаційних систем у різних сферах людської діяльності була ініційована необхідністю вирішення завдання щодо накопичення та обробки інформації для неодноразового використання. У кожній з таких систем було відображено частину інформації про об'єкт. Створення інформаційних систем такого типу призвело до того, що інформація про значну кількість об'єктів матеріального світу розсіялася по різних інформаційних системах, як за рівнем зосередження так і службовою та відомчою належністю [1, с. 3].

Довідкова література, надає нам поняття систем, які стосуються досліджуваної нами проблеми.

Інформаційно-правова система–організаційно впорядкована сукупність нормативно-правових документів (масивів документів), за допомогою яких суб'єкт управління (орган, посадова особа), застосовуючи інформаційні технології, у тому числі засоби обчислювальної техніки та зв'язку, забезпечує процес розробки та прийняття рішень у сфері законодавства, застосовної та правоохоронної діяльності. Інформаційно-правова система є комплексною сукупністю елементів, яка включає до свого складу методи, процедури, інформаційні ресурси (масиви документів, фонди документів, архіви, банки даних, бази знань, автоматизовані інформаційні системи (мережі).

Проте, важливо зазначити, що у науці та практичній діяльності правоохоронних органів існує також таке поняття, як інформаційно-аналітичне забезпечення.

Інформаційно-аналітичне забезпечення – це сукупність компонентів з організації діяльності щодо виявлення осіб і фактів, які становлять оперативний інтерес, збору, передачі та обробки інформації, аналітичних методів її аналізу, внутрішніх і зовнішніх каналів її транспортування (зв'язків) та, власне, інформацію. Інформаційно-аналітичне забезпечення повинно послідовно реалізовувати принципи єдності процесів пошуку, організації та опрацювання інформації за допомогою застосування технічних засобів збору, накопичення, опрацювання і передачі інформації в поєднанні з використанням аналітичних методів математичної статистики і моделей прогнозно-аналітичних розрахунків [3, с. 23].

Д. Я. Семир'янов виділяє дві функції інформаційно-аналітичної роботи правоохоронних органів. По-перше, інформаційно-аналітична робота задовольняє потреби працівників різних підрозділів в інформації, необхідній для ефективного вирішення основних завдань з виявлення та розкриття злочинів. Терміни «виявити» й «розкриття» є синонімами в юридичному трактуванні і їх використання в даному контексті цілком обґрунтовано. Так, термін «виявлення» означає робити явним щось раніше не помічене, знаходити, а «розкриття» – це викрити, відкрити вже відоме. По-друге, на підставі аналізу й узагальнення масиву даних про види і форми порушень законодавства інформаційно-аналітична робота дозволяє здійснити складання прогнозів розвитку криміногенної обстановки, зокрема, визначити майбутню динаміку найбільш небезпечних правопорушень [4, с. 10].

З вищезазначеного можна зробити висновок, що аналітично – інформаційне забезпечення Національної поліції України посідає одне з провідних місць у піраміді необхідних заходів, невід'ємних при виконанні покладених на поліцейських обов'язків. Звідси актуальності набуває питання щодо нормативно – правового забезпечення функціонування аналітично – інформаційної системи в органах і підрозділах Національної поліції України.

Важливо відмітити, що головним підрозділом у системі інформаційно-аналітичного забезпечення діяльності органів і підрозділів Національної поліції України є Департамент інформаційної підтримки та координації поліції «102» Національної поліції України, який організовує і здійснює заходи, передбачені законодавством України, що спрямовані на інформаційно-аналітичне інформаційно-пошукове забезпечення правоохоронної діяльності та захист персональних даних при їх обробці в структурних підрозділах апарату Національної поліції України, головних управліннях Національної поліції України в Автономній Республіці Крим та м.Севастополі, областях, м.Києві, між регіональних територіальних органах Національної поліції України, їх структурних (відокремлених) підрозділах (далі – органи і підрозділи поліції).

Основними завдання Департаменту є: координація діяльності органів і підрозділів поліції щодо забезпечення наповнення та підтримання в актуальному стані персонально-довідкового та дактилоскопічного обліків; організація інформаційно-аналітичної та інформаційно-пошукової діяльності поліції здійснюється відповідно до Конституції України, законів України, указів Президента

України та актів Кабінету Міністрів України, інших актів законодавства, відповідно до законодавства формування баз даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України; Участь в реалізації меж компетенції поліції державної політики у сфері інформатизації, координація виконання державних програм з цього напрямку апаратом Національної поліції України.

Проте, не зважаючи на, виокремлення органами законодавчої влади завдань даного Департаменту, в сфері його функціонування є наявна велика кількість прогалин, що стосується в першу чергу неналежним законодавчим закріпленням та нормативно – правовою регламентацією.

Так, зазначено, що Департамент здійснює свої функції на основі Конституції України, Закону України «Про захист персональних даних», Закону України «Про Національну поліцію». Проте чи достатньо цього для функціонування цілого Департаменту, і де законодавчий акт, який регулюватиме виключно роботу даного Департаменту. На жаль, дане питання не вирішене органами як законодавчої так і виконавчої влади, тому спостерігається нагальна проблема нормативного забезпечення подальшої роботи аналітично – інформаційної системи Національної поліції України.

Отже, діючого органу державної влади та людини яка його очолює надзвичайно мало для належного виконання покладених на нього завдань, адже для результативної роботи апарату потрібна належна та чітка регламентація та координація його дій. Процес реорганізації Національної поліції є позитивним процесом, проте його тривалість позначається на функціонуванні абсолютно усіх підрозділів, що призводить до гальмування системи в цілому.

### **Література:**

1. Бірюков В.В. Інформаційно-довідкове забезпечення розслідування злочинів : навчальний посібник / Бірюков В.В. – Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренко, 2009. – 112 с.
2. Бірюков Г.М. Базы данных и компьютерные сети в практике работы органов внутренних дел : учебное пособие / [Бірюков Г.М., Михно А.А., Никифорчук Д.И., Лебеденко В.И. ]. – Луганск : РИО МВД, 2001. – 65 с.
3. Безрученко В.С. Напрями вдосконалення інформаційно-аналітичного забезпечення підрозділів податкової міліції. Проблеми удосконалення законодавства і практики протидії злочинності у сфері господарської діяльності : збірник наукових праць за матеріалами Міжнародного науково-практичного семінару; 10 грудня 2009 року. / Національний університет ДПС України, НДІ фінансового права. – К. : Вік. прінт, 2009. – 278 с
4. Семир'янов Д.Я. Автореферат дисертації на здобуття ступеня канд. юрид. наук. – Ірпінь, 2004 – С. 10.

**СЕКЦІЯ 2**

**АДМІНІСТРАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ**

**Адміністративно-правове регулювання у сфері забезпечення кібербезпеки в Україні**

**Нікітенко О.І.**

доктор юридичних наук, професор,  
Заслужений юрист України,  
завідувач кафедри публічного та приватного права  
факультету права та міжнародних відносин  
Київського університету імені Бориса Грінченка

**Журавель І.В.**

студент IV курсу  
Херсонського університету

У статті проводиться дослідження щодо адміністративно-правового регулювання забезпечення внутрішньої кібернетичної безпеки в Україні.

Акцентується увага щодо адміністративно-правового забезпечення кібернетичної безпеки держави обґрунтовується доцільністю розробки організаційно-правових засад регулювання цих відносин і відповідає проекту Закону України «Про основні засади забезпечення кібербезпеки України».

Адміністративно-правове регулювання кібербезпеки в Україні та її забезпечення залишаються недостатньо врегульованими на законодавчому рівні. Недостатньо висвітлені в наукових і методичних розробках, не враховуються сучасні загрози вітчизняному кіберпростору.

За часів незалежності України галузь інформаційних технологій розвивалася практично без підтримки з боку держави, що часто не відображали реального стану справ. Основний комплекс переваг інформаційних технологій у системі державного управління практично не застосовується [1].

Інформаційні відносини щодо забезпечення кібернетичної безпеки в державі, врегульовані чинним законодавством, Законом України «Про інформацію», «Про науково-технічну інформацію», «Про доступ до публічної інформації, проте не існує єдиного законодавчого правового акту.

Питаннями адміністративно-правового регулювання у сфері кібербезпеки присвячені наукові роботи науковців: О.А. Баранова, В.М. Бутузова, Д.В. Дубова, О.В. Орюва, Ю.М. Супрунова, О.О. Тихомирова. Комплексному аналізу дослідження адміністративно-правового регулювання у сфері забезпечення кібербезпеки не було приділено достатньої уваги.

Закон України «Про основи національної безпеки України» зазначає, що правовою основою внутрішньої безпеки є Конституція України і Закони України [2].

Інформаційна внутрішня безпека в Україні повинна забезпечуватися шляхом проведення цілісної державної програми відповідно до Конституції та чинного законодавства України і норм Європейського права шляхом реалізації Концепції адміністративної реформи України [3] та Правової доктрини України [4].

Важливу роль у дослідженні правової природи внутрішніх загроз інформаційної безпеки відіграє їх класифікація, яка дає змогу виявити різні сторони цього явища, а також виробити певні механізми протидії. У науковій літературі відсутній єдиний підхід до визначення критеріїв класифікації загроз інформаційного та захисту скоєння злочинів у сфері кібернетичної злочинності.

Нормами п. 4.12 стратегії національної безпеки від 26 травня 2015 року визначено пріоритети забезпечення кібербезпеки і безпеки інформаційних ресурсів що вона є основою для прийняття розробленою Стратегією кібербезпеки [5].

І.В. Арістова вважає, що для дослідження загроз інформаційної безпеки та протидії їм необхідно виходити зі змісту цього поняття. Важливо звернути увагу на те, що з точки зору термінології безпека буквально, у вузькому значенні, означає саме відсутність загрози. Необхідно звернутися до здобутків «загальної теорії безпеки, як системи знань про захищеність людини від загроз» [6].

Таким чином, дослідження цієї проблематики показало, що адміністративно-правове регулювання у сфері забезпечення кібербезпеки в Україні є невід'ємною частиною нашого суспільства і потребує докорінних змін з юрисдикційної точки зору і покращення законодавчого підґрунтя забезпечення кібербезпеки в державі, таким вимогам, на нашу думку, відповідає проект Закону України «Про основні засади забезпечення кібербезпеки України».



**Література:**

1. Informatsiyna skladovaderzhavnoyipolitykytaupravlinnya [Tekst]: monohrafiya / S.H. Solovyov, O.Ye.Bughatyy, Yu. V. Nesteryak [tain] ; zazah. red. N.V. Hrytsyak; Nats. akad. derzh. upr. pryPrezydentoviUkrayiny, Kaf. inform. politykytaelektron. uradyuvannya. – Kyiv : K.I.S., 2015. – 319 с.
2. Закон України від 19 червня 2003 р. № 964 – IV // Відомості Верховної Ради. – 2003. - №39. – 351 с.
3. Указ Президента України Про заходи щодо впровадження Концепції адміністративної реформи України від 22 липня 1998 р. №810/98 // Офіційний вісник України. – 1999. - №21. – 32-76 с.
4. Правова доктрина України: у 5 т. – Х. : Право, 2013. Т.1: Загальнотеоретична та історична юриспруденція / В.Я.Тацій, О.Д.Святоцький, С.І. Максимов та ін.; за заг. ред. О.В.Петришина. – 692 с.
5. Про стратегію кібербезпеки України: Указ Президента України від 15.03.2016 №96/2016 // Урядовий кур'єр. – 2016. – 52 с.
6. Арістова І.В. Інформаційна безпека людини як споживача телекомунікаційних послуг: монографія/ І.В. Арістова, Д.В. Сулацькію: НДІ інформатики і права Нац. акад. прав. наук України. – К.: Право України, 2013. – 184 с.

**Створення системи кібернетичної безпеки в Україні: деякі актуальні питання**

**Козюра В.Д.**

кандидат технічних наук, доцент  
доцент кафедри інформаційних систем та технологій  
Національної академії Служби безпеки України

**Хорошко В.О.**

доктор технічних наук, професор  
професор кафедри Безпеки інформаційних технологій  
Національного авіаційного університету

Кількість деструктивних інцидентів у сфері комп'ютерних та Інтернет-технологій за період з 2005 по 2015 рік збільшилася приблизно у 2,7 рази. Саме тому найбільш пріоритетним напрямом керівництво України вважає реформування системи забезпечення кібернетичної безпеки. Це є одним з головних напрямів забезпечення конфіденційності, цілісності та доступності інформації в національних інформаційних ресурсах від кібернетичних атак шляхом створення в інформаційно-телекомунікаційних системах (ІТС) комплексних систем захисту інформації з підтвердженою відповідністю.

Враховуючи таке вже зараз у Адміністративному та Кримінальному кодексах України до переліку протиправних дій у кіберпросторі віднесено:

- несанкціоноване втручання в роботу комп'ютерів та ІТС;
- несанкціонований збут або розповсюдження інформації з обмеженим доступом;
- створення та використання шкідливих програмних та технічних засобів;
- несанкціоновані дії з інформацією, яка обробляється в комп'ютерах та комп'ютерних мережах;

- здійснення незаконного доступу до інформації в ІТС;
- незаконне виготовлення чи розповсюдження копій баз даних тощо.

Протидіяти таким діям на теренах України спроможні:

- центральні органи виконавчої влади, які реалізують державну політику у сфері інформатизації та телекомунікацій, захисту державних інформаційних ресурсів в ІТС, а також криптографічного та технічного захисту інформації;
- органи державної влади, підприємства, організації (зокрема приватних) та установи, які експлуатують об'єкти критично важливої інфраструктури або здійснюють господарську діяльність у сфері захисту інформації в ІТС;
- Національний банк України, який формує та реалізує державну політику із забезпечення інформаційної та кібербезпеки банківських установ;
- підрозділи спеціального призначення, що виконують завдання із забезпечення кібернетичної безпеки;
- оператори (провайдери) телекомунікацій тощо.

Все це, з огляду на тенденції розвитку національного кібернетичного простору, потребує від

України координації зусиль державного і приватного секторів у протидії новим викликам в інформаційній сфері та вказує на необхідність подальшого секторального вироблення принципів і механізмів реагування на можливі комп'ютерні інциденти.

Серед підрозділів та формувань спеціального призначення найбільше навантаження в ході вирішення завдань кібернетичного лягає на:

- Державну службу спеціального зв'язку та захисту інформації (ДССЗІ) України, що реалізує державну політику в сфері захисту інформації в інформаційно-телекомунікаційних мережах;
- Службу безпеки (СБ) України, що реалізує державну політику в сфері охорони інформації з обмеженим доступом, яка є власністю держави;
- Міністерство внутрішніх справ (МВС) України, що здійснює досудове слідство у справах про злочини у сфері інформаційних технологій;
- Міністерство оборони (МО) України, що планує та реалізує заходи протидії і нейтралізації кіберзагроз національним інтересам України у воєнній сфері, впровадження новітніх інформаційних технологій у сфері оборони;
- Службу зовнішньої розвідки України (СЗР).

З моменту здобуття незалежності Україна прагне створити комплексну систему протидії внутрішнім і зовнішнім загрозам власному кібернетичному простору, однак існує низка проблем, що заважають нашій державі це зробити:

- деградація науково-технічного потенціалу, нерозвиненість інноваційної системи в інфосфері та низький рівень конкурентоздатності в ній;
- значна уразливість інфосфери через надмірно широке впровадження до неї іноземних програмних та матеріально-технічних засобів;
- непрозорість розподілу обов'язків між відомствами, правоохоронними органами та силовими структурами, які спеціалізуються на проблемах кіберзахисту та їх незадовільне кадрове забезпечення;
- відсутність загальнонаціонального координаційного центру, який був би спроможним узгоджувати та координувати діяльність правоохоронних органів, силових структур і відомств щодо протидії реальним загрозам інформаційному та кіберпростору України;
- відсутність єдиного понятійно-термінологічного поля кібербезпеки України, як головної складової інформаційної безпеки, та системних нормативно-правових документів, які б регламентували діяльність відомств, правоохоронних і силових структур у сфері кіберзахисту.

Такий стан фактично є каталізатором для реалізації втручань і загроз в інфосферу України, результатом чого може стати порушення управління державою, її інституціями та окремими об'єктами критично важливої інформаційної інфраструктури. Це вимагає від керівництва країни формування надійної системи кібернетичної безпеки шляхом започаткування низки міжвідомчих, а можливо й міждержавних ініціатив на кшталт:

- проведення аналізу ІТ ринків та організації взаємодії ІТ мереж;
- визначення понятійно-категорійного апарату і потенційних загроз власній кібернетичній безпеці;
- формування критеріїв віднесення об'єктів кіберпростору до критично важливої інформаційної та кіберінфраструктури;
- удосконалення механізмів надання взаємодопомоги у технічних і методологічних аспектах випереджувального виявлення джерел, фіксації та оперативного обміну інформацією про факти здійснення кібератак;
- вироблення та реалізації єдиної науково-технічної політики щодо захисту державних інформаційних ресурсів та ІТ інфраструктури від деструктивного кібервпливу;
- створення нової сучасної навчально-наукової бази для підготовки фахівців;
- розробки єдиних механізмів аудита та сертифікації програмно-апаратних комплексів, використовуваних у державних та військових системах управління;
- модернізації існуючих та розробки нових захищених інформаційних технологій;
- організації міжвідомчої взаємодії та координації державних органів при оцінюванні реальних і потенційних загроз в інформаційній сфері, а також вироблення та реалізації заходів щодо їх усунення;
- удосконалення міждержавних консультативних механізмів з питань законодавчого забезпечення і регулювання діяльності у сфері боротьби з кіберзлочинністю і кібертероризмом та внесення змін до низки існуючих нормативно-правових актів України;
- створення міжнародного експертного центру з питань регулювання взаємовідносин у галузі

телекомунікацій та зв'язку тощо.

Було б раціональним удосконалити організаційно-правові норми міжнародної взаємодії з питань боротьби з кіберзлочинністю і кібертероризмом та запропонувати світовій спільноті внести зміни і доповнення до низки існуючих міжнародних нормативно-правових документів.

У результаті це дасть можливість:

- провести огляд кібербезпекової сфери держави, що дозволив би більш чітко визначити сучасний стан її нормативного забезпечення та основних проблем, які мають бути вирішені вже найближчим часом;
- розробити на підґрунті моделей розвитку світового кібернетичного простору власну модель та реалізувати її;
- впорядкувати політику України у сфері інформаційної та кібербезпеки і виробити так звані загальні правила поведінки у кіберпросторі;
- визначитись з розбіжностями між військовими та цивільними об'єктами в інформаційному та кіберпросторах і сформулювати вимоги щодо безпеки для ключових доменів;
- визнати міжнародним злочином проведення кібератак і кібероперацій на об'єкти інформаційної та кіберінфраструктури України, які спроможні привести до виникнення техногенних катастроф або надзвичайних ситуацій.

### **Особливості безпечної роботи з інформацією в МВС та Національній поліції України**

**Манжай О.В.**

кандидат юридичних наук, доцент  
доцент кафедри кібербезпеки факультету № 4  
Харківського національного університету внутрішніх справ

В умовах розвитку інформаційного суспільства, активного впровадження електронного урядування, переходу державних органів на електронний документообіг в Україні все гостріше постає питання якісної розбудови системи інформаційної безпеки як в державі в цілому, так і в окремих державо утворюючих суб'єктах – правоохоронних органах. Особливої актуальності це питання сьогодні набуває для реформованої Національної поліції України як суб'єкта системи кібербезпеки, визначеного Стратегією кібербезпеки України [1].

Потрібно звернути увагу, що на рівні Президента України, Кабінету Міністрів України постійно приймаються підзаконні нормативно-правові акти, спрямовані на убезпечення працівників державних органів під час роботи з інформаційними ресурсами. У цьому сенсі можна, наприклад, назвати Постанову Кабінету Міністрів України «Деякі питання використання доменних імен державними органами в українському сегменті Інтернету» від 21.10.2015 № 851.

У Міністерстві внутрішніх справ України та Національній поліції України також було прийнято низку нормативно-правових актів, які мають на меті убезпечити працівників від необачного ставлення до роботи з інформаційними ресурсами. Серед таких документів можна виділити, наприклад, Наказ Національної поліції України від 07.12.2015 № 176 «Про запобігання негативним наслідкам використання інтернет-ресурсів російських провайдерів», у якому серед іншого працівникам Національної поліції рекомендується утриматись від застосування російських інтернет-ресурсів у позаслужбовий час та наводиться конкретний перелік ресурсів, заборонених до використання у службовий час, за виключенням певних обставин.

Оскільки останнім часом все більша частка суспільства користується у повсякденному житті соціальними мережами, то окрему увагу хотілося б звернути на вимоги безпеки, яких повинні дотримуватись працівники Національної поліції у цій сфері.

Серед іншого потрібно пам'ятати про *заборону*:

- обміну інформацією з обмеженим доступом нествореними телекомунікаційними каналами;
- передачі облікових даних (імені користувача та паролю), а також відомостей про них (які можуть сприяти скиданню паролю через систему його відновлення) стороннім особам;
- переходу за гіперпосиланнями в сумнівних повідомленнях;
- розміщення фотографій особистого характеру, які можуть дискредитувати особу або орган, у якому вона працює;
- використання у повідомленнях неприйнятних виразів;
- використання «простих» відповідей на секретні питання у системі відновлення паролів тощо.

Також під час роботи в мережі слід пам'ятати, що *необхідно*:

- дотримуватись вимог до складності застосовуваних паролів;
- встановити на своєму робочому місці антивірус та фаєрвол;
- використовувати окремий телефонний номер, невідомий іншим особам, під час реєстрації чутливих профілів (банківський обліковий запис тощо);
- дотримуватись правил надійного збереження особистих даних;
- бути обережним із розміщенням інформації в мережних ресурсах, що використовують для роботи сервери недержавних країн;
- періодично перевіряти Інтернет на наявність фальшивих мережних профілів, асоційованих із працівником поліції та/або його близькими родичами;
- зберігати пильність та навчити близьких правилам безпечної поведінки в мережі;
- регулярно ознайомлюватися із новинами у сфері інформаційної безпеки, які можуть вплинути на особисту безпеку працівника поліції.

Наостанок пропонуємо пошукати свої особисті дані, у тому числі паролі за допомогою пошукових систем. Результат може Вас здивувати!

### **Література:**

1. Стратегія кібербезпеки України, затверджена Указом Президента України від 15 березня 2016 року № 96/2016 [Електронний ресурс]. – Режим доступу: <http://zakon5.rada.gov.ua/laws/show/96/2016>.

### **Кібербезпека інтелектуальної власності у відкритій мережі інтернет**

**Кіянчук В.М.**

студент автомобільного відділення  
Автотранспортного коледжу ДВНЗ КНУ

**Делія Ю.В.**

кандидат юридичних наук, доцент,  
доцент кафедри загально-правових дисциплін  
Донецького юридичного інституту МВСУ України

Науково-технічна революція на початку XXI століття спричинила в усьому світі глибокі системні перетворення. Завдяки поєднанню досягнень у сфері новітніх інформаційно-комунікаційних технологій із надбаннями, що постали на базі стрімкого розвитку інформаційно-телекомунікаційних систем, сформувалися принципово нові глобальні субстанції — інформаційне суспільство, а також інформаційний та кібернетичний простори, які мають нині практично необмежений потенціал і відіграють провідну роль в економічному та соціальному розвитку кожної країни світу [3, с. 4].

В юридичній науці захист авторських прав в Інтернеті розглядались у працях Ю.М. Батуріна, В.І. Жукова, В.О. Калятіна, С.В. Малахова, С.В. Петровського, І.М. Рассолова, Г.А. Сverdлика, А.А. Карцхії, Л.С. Сімкіна та інших. Незважаючи на окремі правові дослідження цієї проблематики, захист авторських прав в мережі Інтернет до цих пір не отримав достатнього висвітлення в юридичній літературі.

При подальшому розвитку всесвітньої мережі Інтернет, проблема захисту права на інтелектуальну власність набуває дедалі більшої актуальності та необхідності її висвітлення для широких верств населення. Не секрет, що сьогодні Інтернет настільки завоював прихильність українців, що став одним з найголовніших засобів розповсюдження інформації ділового, рекламного, просвітницького та розважального характеру. Майже кожен власник бізнесу або просто особа, яка володіє будь-якою інформацією, що має пізнавальний або комерційний характер, використовує для її розміщення Інтернет ресурси. Разом з цим виникає необхідність у захисті такої інформації від посягань тих користувачів мережі, які не бажають самостійно створювати контент, а лише копіюють інформацію з ресурсів інших осіб. Захистити авторські права в мережі Інтернет стає дедалі важче, оскільки наявні правові інструменти не відповідають реаліям, а єдиний на сьогодні механізм захисту – ініціювання судового розгляду – не завжди ефективний [1, с. 152].

За загальним порядком захист права інтелектуальної власності здійснюється в Україні судом у цивільних або кримінальних справах. Зокрема такі норми містять статті 442 ЦКУ та 176 ККУ. Основна мета цивільно-правової відповідальності - не покарання за недотримання встановленого правопорядку,

а відшкодування заподіяної шкоди, а кримінально-правова відповідальність полягає у обмеженні прав і свобод засудженого, але, насправді, визначені у нормах санкції переважно є меншими, ніж отримана вигода, або ж справа взагалі не порушується, через нехтування правоохоронними органами правами на інтелектуальну власність [2, с. 34].

За даними оприлюдненими на початку лютого 2016 року Спеціального щорічного звіту Міжнародного альянсу інтелектуальної власності щодо захисту прав власності (International Intellectual Property Alliance), який є відомим за назвою «список 301», Україна є лідером у рейтингу держав-порушників права інтелектуальної власності. Необхідно визнати, що в українському суспільстві не прийнято платити за права інтелектуальної власності, такі як легальна аудіо- і відеопродукція та ліцензоване програмне забезпечення, розміщені в мережі Інтернет. Так, за даними корпорації Microsoft за 2015 рік, майже 85% її продукції, якою користуються в українських державних установах, – не є ліцензійною.

Контроль за порушенням права інтелектуальної власності у мережі Інтернет є досить складним. Саме через це, в умовах сьогодення українським авторам необхідно самостійно піклуватися про захист своїх законних прав заздалегідь, за допомогою використання різноманітних технічних засобів захисту, які дозволяють створювати технологічні перешкоди порушенню авторського права або суміжних прав. Серед таких засобів можна виділити наступні:

- Саморуйнування електронного документа при несанкціонованому копіюванні;
- Криптографічні конверти, тобто програмне забезпечення, яке зашифровує твори так, що доступ до них може бути отриманий лише із застосуванням належного ключа до шифру;
- Твори з обмеженою функціональністю, коли автор подає лише частину інформації, приміром, зміст книги чи деякі її розділи. Цей метод широко використовується для передплати Інтернет видань;
- Серед організаційних засобів захисту прав інтелектуальної власності виділяються наступні:
  - Апаратні засоби, які вимагають від користувача придбання і встановлення певного пристрою.
  - Виконувані програми, які працюватимуть під час конкретного сеансу зв'язку та стиратимуться з оперативної пам'яті комп'ютера після закінчення роботи;
  - Централізоване обчислення, тобто програми, що не є частиною інтерфейсу комп'ютера користувача, а залишаються на сервері продавця - комп'ютер користувача повинен встановлювати контакт з сервером щоразу, як використовується програма;
  - Цифрові сертифікати, зокрема електронний файл – цифровий сертифікат, якими користувався Цифрові сертифікати посвідчується як власник публічного ключа;
  - Клірингові центри, наділені повноваженнями з ліцензування своїх авторських прав на твори;
  - Продаж фізичних копій, тобто «hardware» – продаж обладнання-носіїв інформації (На відміну від «software» – програм в електронному вигляді).

Отже, питання кібербезпеки інтелектуальної власності у відкритій мережі Інтернет мають комплексний характер: разом із забезпеченням діючої нормативно-правової бази з боку держави, сам автор мусить використовувати різні організаційно-технічні методи із захисту своєї інтелектуальної власності у мережі Інтернет. Найбільшою проблемою у захисті авторських прав є те, що нормативно-правова база України не узгоджена з реаліями сьогодення та суттєво відстає у ефективному правовому регулюванні цього питання, тому вдосконалення й адаптування правових основ для забезпечення права інтелектуальної власності у мережі Інтернет є необхідним і пріоритетним завданням держави.

### **Література:**

1. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В.Л. Бурячок, В. Б. Толубко, В.О. Хорошко, С.В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015.— 288 с.
2. Жаров В.О. Захист права інтелектуальної власності: навчальний посібник / В.О. Жаров. – К.: ЗАТ «Інститут інтелектуальної власності», 2003. – 64 с.
3. Рассолов И.М. Право и Интернет: теоретические проблемы / И.М. Рассолов. – 2-е изд., доп. – М.: Норма, 2009. – 210 с.

**Аналіз активності у деструктивних мережних співтовариствах для прогнозування сплесків  
протиправної діяльності**

**Манжай І.А.**

завідувач навчального відділу  
Харківського економіко-правового університету

У березні 2016 року в Україні було затверджено Стратегію кібербезпеки України [1], яка серед іншого передбачає створення системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій.

Одним з методів виявлення відповідних загроз може бути проведення аналізу активності у деструктивних мережних співтовариствах. Такий аналіз може бути здійснено на декількох рівнях, першим з яких є статистичний аналіз взаємозв'язку відповідних груп між собою та відслідковування відповідної активності в цих групах напередодні певних подій, що мають протиправний характер.

Під час проведення експерименту нами було здійснено спостереження протягом трьох місяців у період з 04.06.2015 до 05.08.2015 за діяльністю шести деструктивних груп антиукраїнської спрямованості у соціальних мережах. Двічі на день (вранці та ввечері) фіксувалася кількість учасників у кожній групі, кількість залишених повідомлень та коментарів до них.

На початку аналізу одержаних даних було встановлено попарно коефіцієнти кореляції (R) для досліджуваних груп за інтенсивністю зміни кількості учасників (табл. 1).

Таблиця 1 – Коефіцієнти кореляції

	Група 1	Група 2	Група 3	Група 4	Група 5	Група 6
Група 1	1					
Група 2	-0,8183017	1				
Група 3	0,16402811	0,40660713	1			
Група 4	0,94885004	0,95161622	0,1456132	1		
Група 5	0,95673251	0,92427899	0,1080685	0,994109734	1	
Група 6	0,92109977	0,97130884	-0,214496	0,995278783	0,9837147	1

Протягом подальшого дослідження було виявлено сплеск (спад) активності у групах із міцним кореляційним зв'язком ( $|R| > 0,5$ ) під час загострення або тимчасового пом'якшення ситуації на сході України або у відносинах між Російською Федерацією та Україною (кількісна зміна досліджуваних параметрів відмінна від звичайної). Причому, в окремих групах такі зміни відбувалися напередодні знакових подій, що може свідчити про певний зв'язок між учасниками (координаторами) таких груп та безпосередніми організаторами (замовниками, виконавцями) протиправних дій.

Описана закономірність, на нашу думку, є характерною не лише для досліджуваних, але й для інших деструктивних співтовариств, у тому числі тих, які здійснюють протиправні дії у кіберсфері.

Таким чином, відповідний аналіз дає можливість спрогнозувати настання певних негативних подій. Знаючи це, можна більш ґрунтовно дослідити мережні дані на предмет інформації про заплановані протиправні дії. У якості методології для такого аналізу пропонується використовувати загальноприйняті методики, застосовувані у рамках американської та європейської моделі кримінального аналізу (розвідки) [2], [3].

Отже, аналіз активності відповідних груп у соціальних мережах, форумах тощо може бути використано правоохоронними органами для попередження злочинності та оперативного реагування на події, які відвернути не вдалося.

**Література:**

1. Стратегія кібербезпеки України, затверджена Указом Президента України від 15 березня 2016 року № 96/2016 [Електронний ресурс]. – Режим доступу: <http://zakon5.rada.gov.ua/laws/show/96/2016>.
2. Манжай О. В. Кримінальна розвідка та її співвідношення з оперативним обслуговуванням / О. В. Манжай, Є. О. Жицький // Jurnalul Juridic National: Teorie si Practică. – 2015. – № 3(13). – С. 100-105.

3. Манжай О. В. Аналіз методології кримінальної розвідки в зарубіжних країнах / О. В. Манжай // Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка. – 2016. – № 3(75). – С. 256-265.

## **Парадигмальна трансформація концепції інформаційної безпеки**

**Нашинець-Наумова А.Ю.**

кандидат юридичних наук, доцент,  
доцент кафедри публічного та приватного права  
Київського університету імені Бориса Грінченка

Поняття інформаційної безпеки в повному обсязі включає забезпечення захисту та безпеки інформації, інформаційного ресурсу. У прямому розумінні «захист інформації» – це недопущення будь-якого впливу на інформацію, яку хтось повинен зберегти в певному стані. Інформаційна безпека включає: 1) безпеку інформації; 2) безпеку споживачів від інформації. З точки зору права виникають два напрями регулювання. Перший пов'язаний з встановленням певних загальних правил щодо інформації як предмета суспільних відносин. При цьому від імені держави встановлюються правила і вимоги, висловлені змістом інституту правового режиму. Другий напрям являє собою правове регулювання відносин з приводу використання інформації, сформованої з урахуванням її правового режиму та правового статусу власника або власника ресурсу і правового статусу споживача інформації [1, с. 8].

Сьогодні склалися дві основні тенденції у визначенні поняття і структури інформаційної безпеки. Представники першого напрямку пов'язують інформаційну безпеку тільки з інститутом таємниці. Представники іншого – пропонують поширити сферу інформаційної безпеки практично на всі питання та відносини в інформаційній сфері, по суті, ототожнюючи інформаційну безпеку з інформаційною сферою. Відзначимо, що проблеми інформаційної безпеки зачіпають всі рівні науково-технологічного забезпечення – від теоретичних основ і міжнародних стандартів до оперативного адміністрування.

Коли ми говоримо про безпеку будь-якого об'єкта, ми маємо на увазі можливість виконання ним покладених на нього завдань незалежно від зовнішніх або внутрішніх деструктивних факторів. Якщо ми говоримо про безпеку людини або соціуму, тобто інформаційної системи з самомодифікуючою метою, то предмет дослідження становить можливість реалізувати ці цілі в кожен конкретний момент часу. І в цьому випадку під безпекою ми розуміємо не тільки можливість контролю деструктивних процесів і явищ по відношенню до нас, скільки можливість домінувати над ними. Перевага над чим-небудь складає сутність безпеки.

Очевидно, що інформаційна безпека не є явищем найвищого порядку і може розглядатися тільки ґрунтуючись на парадигмі соціальної безпеки, використовуючи її методологічний потенціал. Тому доцільним є з'ясування поняття «безпека» як базової категорії для дослідження інформаційної безпеки. Оскільки безпека за своєю сутністю є соціальним явищем, то серед усього розмаїття поглядів необхідно звернути увагу на філософсько-соціологічне розуміння, яке має стати фундаментальною частиною системного підходу до розуміння явища безпеки, що дозволить на науковому (доктринальному) рівні уникнути використання у визначеннях таких неоднозначних і суперечливих понять, як «захищеність», «інтереси», «потреби» та «загрози», відобразивши при цьому синергетичний бік явища безпеки [2, с. 253]. Підґрунтя такого підходу окреслене Г.Івашенком. Наголошуючи на недосконалої загальнопоширеного визначення безпеки через стан захищеності життєво важливих інтересів особи, суспільства і держави від внутрішніх та зовнішніх загроз, він зазначає, що основою усвідомлення його повинен стати дієвий підхід, напрацьований соціальною філософією та теоретичною соціологією. Однак це не означає, що безпеку можна формально розуміти як вид діяльності у відриві від її результатів, умов, у яких вона здійснюється, та можливостей функціонування суб'єкта в цих умовах. З цієї позиції безпеку пропонується розглядати як «сукупність умов існування суб'єкта, якими він оволодів (осягнув, засвоїв, створив) у процесі самореалізації, і які він, таким чином, здатний контролювати» [3, с.58].

Інформаційна безпека є складовим компонентом загальної проблеми інформаційного забезпечення людини, держави і суспільства. Вона орієнтована на захист значимих або вже згаданих суб'єктів інформаційних ресурсів, законних інтересів. Зміст поняття «інформаційна безпека» розкривається у практичній діяльності, наукових дослідженнях, а також нормативно-правових документах.

Так, в розділі XV «Інформаційна безпека як складова частина національної безпеки України» запропонованого проекту Інформаційного кодексу зазначається, що інформаційна безпека – це стан

захищеності життєво важливих інтересів особи, суспільства та держави, який виключає можливість заподіяння їм шкоди через неповноту, невчасність і недостовірність інформації, через негативні наслідки функціонування інформаційних технологій або внаслідок поширення законодавчо забороненої чи обмеженої для поширення інформації [4]. Слід зазначити, що у науковій літературі поки бракує єдиного консолідованого погляду на зміст поняття «інформаційна безпека». Для одних воно відображає стан, для інших процес, діяльність, здатність, систему гарантій, властивість, функцію. Відтак постає необхідність в угрупованні напрямів визначення аналізованого поняття [5, с.76]. Сьогодні також відсутня норма, яка б містила дефініцію поняття «інформаційна безпека», враховуючи різницю між інформаційною безпекою та безпекою інформації. Так, наприклад, Ю.А. Фісун, характеризує інформаційну безпеку як «стан захищеності інформаційного середовища, який відповідає інтересам держави, за якого забезпечується формування, використання і можливості розвитку незалежно від впливу внутрішніх та зовнішніх інформаційних загроз» [6, с. 89]. Такої ж позиції притримуються і розробники концепції інформаційної безпеки центру Разумкова, а також деякі українські дослідники, які вважають за необхідне визначати інформаційну безпеку як стан захищеності. Так наприклад, Гасеський В.К., Авраменко В.А. [7, с.123] визначають інформаційну безпеку як стан захищеності життєво важливих інтересів особи, суспільства та держави, який виключає можливість заподіяння їм шкоди через неповноту, невчасність і недостовірність інформації, через негативні наслідки функціонування інформаційних технологій або внаслідок поширення законодавчо забороненої чи обмеженої для поширення інформації, у той час як О.Г. Додонов визначає інформаційну безпеку як стан захищеності інформаційного простору, який забезпечує формування та розвиток цього простору в інтересах особистості, суспільства та держави [8, с. 65].

Проте, якщо проаналізувати зміст та напрямки досліджень поняття інформаційної безпеки, можна виокремити декілька підходів окреслення сутності цього феномену, а саме розуміння інформаційної безпеки в якості: – стану захищеності інформаційного простору; – процесу управління загрозами та небезпеками, що забезпечує інформаційний суверенітет України; – стану захищеності національних інтересів України в інформаційному середовищі; – захищеності встановлених законом правил, за якими відбуваються інформаційні процеси в державі; – стану захищеності національних інтересів країни в інформаційній сфері; – до суспільних відносин, пов'язаних із захистом життєво важливих інтересів людини і громадянина, суспільства та держави від реальних та потенційних загроз в інформаційному просторі; – важливої функції держави; – невід'ємної частини політичної, економічної, оборонної та інших складових національної безпеки.

Узагальнивши, можна підсумувати, що: по-перше, достатньо стрімкий розвиток наукових досліджень в сфері забезпечення інформаційної безпеки у 90-х роках минулого століття змінився науковою байдужістю до цього питання, адже жодних концептуальних документів по інформаційній безпеці досі не прийнято; по-друге, аналіз наукових праць з питання інформаційної безпеки показує, що в цілому дана проблема досліджена неповно. Більшість наукових розробок представлена у вигляді лекцій, практичних посібників, монографій тощо. Це обумовлено такими причинами:

- інформаційна безпека згадується в сотнях нормативних актів, безпосередньо її захисту вже 15 років присвячуються десятки документів, серед яких Доктрина інформації безпеки, укази президентів, декілька рішень РНБО, міжнародні документи про співробітництво в межах СНД. Але в жодному з них немає визначення цього поняття, і що, власне, захищається, можна намагатися зрозуміти з переліку численних загроз та заходів щодо їх подолання.
- актуальним залишається встановлення сутнісних характеристик інформаційної безпеки шляхом дослідження підходів до визначення цього поняття.
- при дослідженні питання інформаційної безпеки спостерігається однобічність та поверховість (зокрема, взагалі не досліджувалась змістовна складова, яка виражається в захисті суспільства від поширення недостовірної або маніпулятивної інформації).
- тривалий час безпека інформації залишалася закритою, що не дозволяло повною мірою вивчати питання інформаційної безпеки як всередині, так і ззовні неї. Такий стан призвів до того, що наукові дослідження та обґрунтування здійснювалися обмеженим колом вчених, що призвело до однобічності і суб'єктивізму сформованих наукових положень та висновків.

### **Література:**

1. Рибальський О.В. Основи інформаційної безпеки та технічного захисту інформації [Текст]: посібник для курсантів ВНЗ МВС України / О.В. Рибальський, В.Г. Хахановський, В.А. Кудінов. – К.: Вид-во НАВС, 2012. –



104 с.

2. Нижник Н.Р. Національна безпека України (методологічні аспекти, стан і тенденції розвитку) [Текст] : навчальний посібник / Н.Р. Нижник, Г.П. Ситник, В.Т. Білоус. – Ірпінь : Акад. ДПС України, 2000. – 304 с.
3. Данільян О.Г. Національна безпека України: сутність, структура та напрямки реалізації [Текст] : навчальний посібник / О.Г. Данільян [та ін.]. – Х. : Фоліо, 2002. – 285 с.
4. Потреба часу – створення Інформаційного кодексу України [Електронний ресурс] / Режим доступу: [http://comin.kmu.gov.ua/control/uk/publish/article?art\\_id=70301&cat\\_id=64654](http://comin.kmu.gov.ua/control/uk/publish/article?art_id=70301&cat_id=64654).
5. Ліпкан В.А. Теоретичні основи та елементи національної безпеки України [Текст] / В.А. Ліпкан; Національна академія внутрішніх справ України. – К. : Текст, 2003. – 599 с.
6. Фисун Ю.А. Материали конференции «Проблемы внутренней безопасности России в XXI веке». – М. : Фонд «Отечество», 2001.
7. Захист інформаційних ресурсів в інформаційно-телекомунікаційних системах. – К., 2001.
8. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія / О.Г. Додонов, В.П. Горбулін, Д.В. Ланде. – К.: Інтертехнологія, 2009. – 164 с.

### **Деякі психологічні особливості осіб, що вчиняють злочини у сфері високих технологій**

**Даніч М.А.**  
курсант 2-го курсу 201 взводу  
факультету №3 ОДУВС

**Добровольська О.О.**  
викладач кафедри психології та педагогіки  
факультету №3 ОДУВС

Сучасний світ практично неможливо уявити без нових інформаційних технологій, в основі яких лежить широке використання комп'ютерної техніки та новітніх засобів комунікацій. Сьогодні комп'ютери впроваджуються в різноманітні галузі людської діяльності. Останнім часом в Україні значно зросла кількість Інтернет користувачів, адже підключення до глобальної мережі стало доступним та зручним. Популярність Інтернету не випадкова, адже він забезпечує цілодобовий доступ до величезної кількості інформації, швидку передачу даних, можливість проведення банківських, торгових, біржових операцій, переказ коштів і багато іншого. Для багатьох людей він став цілим світом, віртуальним світом. Як і в реальному світі, так і в віртуальному, де панує комп'ютерна інформація, трапляються, злочини - кіберзлочини.

Грунтуючись на специфічних особливостях кіберзлочинів, їх ознаках, а також на аналізі положень «Конвенції про злочинність у сфері комп'ютерної інформації», ми можемо поділити дані злочини на чотири групи:

- перша група - злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем;
- друга група — злочини, безпосередньо пов'язані з комп'ютерами;
- третя група — злочини, пов'язані із вмістом контенту;
- четверта група — злочини, пов'язані з порушеннями авторського права і суміжних прав.

Більш детально ми розглянемо злочини другої групи, а точніше інтернет-шахрайство, тобто «фішинг». Головним завданням фішинг шахрая є отримання вашого логіна і пароля від певного сайту, з подальшим їх використанням, тобто це може бути логін і пароль вашого банківського кабінету або номер і пінкод вашої картки для виведення ваших грошей на свій рахунок. Так само досить часто використовують фішинг для доступу до акаунтів в соціальних мережах. У будь-якому випадку якщо пароль і логін став відомий шахраям наслідки будуть неприємні.

Фішинг – один із популярних нині кіберзлочинів, і людей на нього спонукають різні мотиви. Ми знаємо, що найчастіше причетні до скоєння кіберзлочинів колишні співробітники компаній або банківські службовці: Загалом, це такі особи які, працюють в компаніях не менше 4 років; першими приходять і останніми йдуть з роботи; користуються відпустками дуже рідко, або взагалі не беруть відпустку; намагаються будь якими способами завоювати довіру адміністрації, навіть підлабузництвом та занадто добре знайомі з роботою систем захисту інформації і мають ключі від основних замків службових приміщень [1, с. 6].

Також для фішингу характерна так звана мотивація «просто для розваги», яка притаманна підліткам. Проте, ця мотивація має особливий характер тому, що злочин скоюється не через злий намір, а задля фінансової вигоди або ж доведення одноліткам своєї значущості. Також до фішингу можна віднести емоційну мотивацію, через яку особи можуть здійснити непоправну шкоду тільки для себе і потім довго шкодувати.

Всі кіберзлочини характеризуються саме латентністю та знаннями в комп'ютерних технологіях. Проте, не обов'язково бути професійним комп'ютерним злочинцем з яскраво вираженою корисливою метою чи особою, особливістю якої є стійке сполучення професіоналізму у сфері комп'ютерної техніки та програмування з елементами своєрідного фанатизму та винахідливості [2, с. 38–39]. Для фішингу достатньо мати базовий рівень знань в області комп'ютерів та мереж для створення злочину. Його особливість полягає в тому, що скоїти саме цей злочин може особа будь-якого віку, достатньо тільки розуміти, як можна розробити план махінації та володіти фотошопом.

На нашу думку, на відміну від переважної більшості звичайних злочинів, вчинення кіберзлочину не вимагає, як правило, будь-яких пересувань або прийняття будь-яких активних фізичних дій. Кіберзлочинець при реалізації свого злого умислу перебуває вдома, в інтернет-клубі, місці з безкоштовним доступом в Інтернет, будь-якому іншому обраному їм місці, яке для нього є комфортним або, принаймні, знайомим і звичним. Тому кіберзлочинці можуть не відчувати, або відчувати в значно меншій мірі, дискомфорт, страх бути випадково виявленим і затриманим [3, с. 4].

Значна частина комп'ютерних злочинів здійснюється індивідуально. Але сьогодні росте тенденція співучасті в групових посяганнях. Криміальна практика свідчить про те, що 38% злочинців діяли без співучасників, тоді як 62% скоювали злочин в складі організованих злочинних угруповань.

Таким чином, ми бачимо, що комп'ютерна злочинність – це міжнародне явище, рівень якої тісно пов'язаний з економічним рівнем розвитку суспільства у різних державах та регіонах. При цьому, Україна на наш погляд, має можливість використати досвід більш розвинутих країн для запобігання та викриття злочинів. Загальні тенденції, злочинні засоби та заходи запобігання в різні відрізки часу є однаковими для різних країн, що базуються на єдності технічної бази цих злочинів. А з метою попередження таких злочинів необхідне подальше проведення досліджень соціального та криміналістичного профілю типового комп'ютерного злодія.

#### **Література:**

1. Іванченко О.Ю. кримінологічна характеристика кіберзлочинності, запобігання кіберзлочинності на національному рівні / О.Ю. Іванченко // Актуальні проблеми вітчизняної юриспруденції — 2016 — № 3. — 172-176 с.
2. Бутузов В.М. Документування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку при проведенні дослідчої перевірки : наук. практ. посіб. / [В.М. Бутузов, В.Д. Гавловський, Л.П. Скалосуб та ін.]. — К. : Вид. дім “Аванпост-Прим”, 2010. — 245 с.
3. Косенков А. Н. о применении юридической психологии в борьбе с киберпреступностью / А. Н. Косенков. //Библиотека криминалиста. —2013. — № 5. — с. 207-217

#### **Термінологічна невизначеність у сфері кібербезпеки**

**Політова А.С.**

кандидат юридичних наук, доцент  
доцент кафедри кримінально-правових дисциплін та судових експертиз  
Донецького юридичного інституту МВС України

Протягом останніх років на різних рівнях проведено багато форумів, семінарів та конференцій міжнародного і національного масштабу, присвячених різноманітним аспектам кібербезпеки. Разом з тим, постає проблема визначення поняття «кібербезпека», оскільки воно активно використовуються в офіційних документах провідних країн світу та «безпекових» організацій, але досі відсутнє загальноприйняте та однозначне його тлумачення.

У 2011 році Д.В. Дубов та М.А. Ожеван у аналітичній доповіді «Кібербезпека: світові тенденції та виклики для України» запропонували визначення «кібербезпеки» як стан захищеності кіберпростору в цілому або окремих об'єктів його інфраструктури від ризику стороннього кібернетичного впливу (кібератак), за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз особистим, корпоративним та/або національним

інтересам [1, с. 26]. Подібної точки зору щодо визначення поняття «кібербезпеки» дотримується і О.В. Коломієць.

Існує й інші підходи до його тлумачення. Так, зокрема, деякі вітчизняні вчені трактують кібербезпеку як захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у сфері функціонування інформаційно-телекомунікаційних систем [2, с. 165-171].

Також висловлюється думка, що кібербезпека – це безпека інформації та інфраструктури в цифровому середовищі, що її забезпечує. Кібербезпека передбачає досягнення і збереження властивостей безпеки в ресурсах організації або користувачів, що спрямовані на запобігання відповідним кіберзагрозам.

Отже, вищевикладене свідчить, що термінологічне поле сфери кібербезпеки держави досі залишається фрагментарним, що унеможлиблює формування дієвих нормативно-правових документів з протидії кіберзагрозам [1, с. 30].

Аналіз деяких міжнародно-правових актів щодо протидії кіберзлочинності показав про відсутність загальноприйнятого визначення «кібербезпеки». Так, зокрема, Конвенція про кіберзлочинність 2001 р., ратифікована Україною 07.09.2005 та набув чинності 01.07.2006, дає визначення «комп'ютерна система», «комп'ютерні дані», «постачальник послуг». У Конвенції також визначено перелік кіберзлочинів, до яких відносяться: правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, нелегальне перехоплення, втручання у дані, втручання у систему, зловживання пристроями); правопорушення, пов'язані з комп'ютерами (підrobка пов'язана з комп'ютерами та шахрайство, пов'язане з комп'ютерами); правопорушення, пов'язані зі змістом (правапорушення, пов'язані з дитячою порнографією) та правопорушення, пов'язані з порушенням авторських та суміжних прав [3].

Що ж стосується законодавства України, то у Стратегії національної безпеки, затвердженій Указом Президента України від 26.05.2015 №287/2015, серед актуальних загроз національній безпеці України виділено п. 3.7. розділу 3 Актуальні загрози національній безпеці України, у якому зазначено: «Загрози кібербезпеці і безпеці інформаційних ресурсів: уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак; фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом» [4].

Також у Стратегії визначено основні напрями державної політики національної безпеки України. Щодо кібербезпеки, то у п. 4.12. Забезпечення кібербезпеки і безпеки інформаційних ресурсів відзначено, що пріоритетами забезпечення кібербезпеки і безпеки інформаційних ресурсів є:

- розвиток інформаційної інфраструктури держави;
- створення системи забезпечення кібербезпеки, розвиток мережі реагування на комп'ютерні надзвичайні події (CERT);
- моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації;
- розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів;
- забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, відмова від програмного забезпечення, зокрема антивірусного, розробленого у Російській Федерації;
- реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації з урахуванням практики держав - членів НАТО та ЄС;
- створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони;
- розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікація співпраці України та НАТО, зокрема в межах Трестового фонду НАТО для посилення спроможностей України у сфері кібербезпеки [4]. Проте визначення «кібербезпеки» відсутнє.

Аналізую невизначеність поняття «кібербезпека», деякі вчені відзначають, що у нормативно-правових актах доволі розповсюдженим є поняття «інформаційна безпека». Так, зокрема, Д. В. Дубов відзначає, що у вітчизняному нормативно-правовому полі визначення поняття «інформаційна безпека» зафіксоване у Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки». У ньому під інформаційною безпекою розуміється стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний

вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації. Внесення в дане визначення проблеми «негативних інформаційних впливів», на його думку, багато в чому розмиває поле «інформаційної безпеки», що дозволяє постійно включати до нього нові елементи безпекової сфери, штучно розмиваючи предметне поле цього поняття [5, с. 121].

Слід відзначити, що питання врегулювання термінологічної невизначеності у сфері кібербезпеки було зроблене у проекті Закону про внесення змін до Закону України «Про основи національної безпеки України» щодо кібернетичної безпеки України (реєстр. №2483 від 07.03.2013), де пропонувалося запровадити до термінології національного законодавства нові поняття, зокрема, «кібернетична безпека» та «кібернетичний простір». Згідно із проектом, «кібернетична безпека (кібербезпека) – це стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі; кібернетичний простір (кіберпростір) – це середовище, яке виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем» [6].

Таким чином, навіть «поверхневий» аналіз нормативно-правових актів України вказує, що вітчизняне нормативно-правове поле у сфері кібернетичної (інформаційної) безпеки оперує термінами визначень яких фактично немає. Це питання потребує скорішого врегулювання, оскільки чітке окреслення поняття «кібербезпека» дасть змогу більш ефективно протидіяти кіберзлочинності.

### **Література:**

1. Кібербезпека: світові тенденції та виклики для України. – К.: НІСД, 2011. – 30 с. : [Електронний ресурс]. – Режим доступу: [http://www.niss.gov.ua/content/articles/files/kyber\\_bezpeka-aab17.pdf](http://www.niss.gov.ua/content/articles/files/kyber_bezpeka-aab17.pdf)
2. Мельник С.В. До проблеми формування понятійно-термінологічного апарату кібербезпеки / С. В. Мельник, О.О. Тихомиров, О.С. Ленков // Збірник наукових праць Військового інституту Київського національного університету ім. Т. Г. Шевченка. – 2011. – №30. – С. 165-171.: [Електронний ресурс]. – Режим доступу : [http://www.nbuv.gov.ua/portal/natural/Znpviknu/2011\\_30/Zbirnik\\_30\\_28.pdf](http://www.nbuv.gov.ua/portal/natural/Znpviknu/2011_30/Zbirnik_30_28.pdf).
3. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07.09.2005 №2824-IV // Відомості Верховної Ради України. – 2006. – № 5-6. – Ст. 71. : [Електронний ресурс]. – Режим доступу : [http://zakon2.rada.gov.ua/laws/show/ru/994\\_575/print1447087919957738](http://zakon2.rada.gov.ua/laws/show/ru/994_575/print1447087919957738)
4. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26 травня 2015 року № 287/2015 : [Електронний ресурс]. – Режим доступу:<http://zakon2.rada.gov.ua/laws/show/ru/287/2015/paran14#n14>
5. Дубов Д. В. Стратегічні аспекти кібербезпеки України / Д. В. Дубов // Стратегічні пріоритети. – 2013. – №4 (29). – 119-126 с.
6. Проект Закону про внесення змін до Закону України «Про основи національної безпеки України» щодо кібернетичної безпеки України (реєстр. №2483 від 07.03.2013) : [Електронний ресурс]. – Режим доступу: [http://w1.c1.rada.gov.ua/pls/zweb2/webproc4\\_2?id=&pf3516=2483&skl=8](http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2?id=&pf3516=2483&skl=8)

### **До питання кібернетичної безпеки в Україні**

**Гончаров М.В.**

студент 4 курсу Донецького юридичного інституту  
МВС України (м. Кривий Ріг)

Формування в Україні інформаційного суспільства можливе за умови широкої інтеграції сучасних технологій автоматизованої обробки даних у всі сфери економіки, державного управління та суспільної діяльності. Це різко збільшує залежність реалізації життєво важливих інтересів осіб, суспільства та держави від належного функціонування інформаційно-телекомунікаційних систем, за допомогою яких й забезпечується така реалізація.

Таким чином, питання захисту життєво важливих інтересів людини, суспільства та держави у кіберпросторі набуває особливого значення. Потребує подальшого розвитку механізм захисту приватного життя особи при користуванні кіберпростором, при автоматизованій обробці персональних даних [1].

За останні роки глобальний кіберпростір усе більшою мірою розглядається всіма державами світу як один із найважливіших безпекових пріоритетів, оскільки його, функціонування стає визначальним чинником розвитку економіки, військового, соціального та інших секторів.

Відповідно до ст. 6 Конституції України державна влада в Україні здійснюється на засадах її поділу на законодавчу, виконавчу та судову. Органи законодавчої, виконавчої та судової влади здійснюють свої повноваження у встановлених Конституцією межах і відповідно до законів [2].

Серед органів державної влади важливе місце посідають органи виконавчої влади, що здійснюють функції державного управління у сфері кібернетичної безпеки.

Ситуація, що склалася сьогодні в Україні, вимагає від держави прийняття необхідних рішень, спрямованих на формування єдиної моделі кібернетичної безпеки для забезпечення нормального життєвого рівня своїм громадянам і в той же час дана політика має набути концептуального характеру. Адже сфера державної політики, спрямованої на захист життєво важливих інтересів особи, суспільства і держави, реалізація яких залежить від належного функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, створює необхідні передумови для розвитку виробництва, науки, освіти, культури, у цілому всіх галузей людського розвитку, в тому числі і досягнення економічних успіхів.

У таких умовах виняткового значення для забезпечення національних інтересів та їх захисту на міжнародному рівні набуває ефективність механізмів забезпечення кібербезпеки держави та вирішення тих проблем, які виникають на шляху їх розбудови [3, с. 119].

Політичне й економічне реформування, конституційне закріплення права приватної власності і підприємницької діяльності, роздержавлення, утвердження приватної власності, розвиток самоврядування змінили форми державно-управлінської діяльності, форми регулювання суспільних відносин: зменшилась необхідна участь держави в економічних, інформаційних процесах.

Суб'єктами державного управління виступають не лише державні органи, а й підприємці, об'єднання громадян, страхові фонди та ін. Значно змінюється співвідношення централізації і децентралізації в управлінні у зв'язку з перерозподілом більшого обсягу повноважень від верхніх до середніх і нижчих рівнів управління [4, с. 117].

Найсуттєвіші зміни у змісті, спрямованості державного управління зумовлені принципово новими відносинами між особистістю і суспільством, державою і громадянином, коли людина визнається в Україні найвищою соціальною цінністю. Права і свободи людини, їх гарантії визначають зміст і спрямованість діяльності держави.

Процеси державотворення в Україні вимагають дальшого підвищення якості державного керівництва у сфері забезпечення кібернетичної безпеки, розвитку методів управління з врахуванням специфіки цієї сфери суспільних відносин.

Можна визначити такий зміст державного управління у сфері забезпечення кібернетичної безпеки в Україні:

- правове регулювання відносин шляхом прийняття законодавчих актів, рішень державних органів, спрямованих на реалізацію державної політики у цій сфері;
- розгляд Верховною Радою України, Президентом України, Кабінетом Міністрів України, найважливіх питань відносно кібербезпеки, визначення пріоритетів державної політики в цій сфері, а також розробка та реалізація комплексних програм;
- достатнє фінансування і матеріально-технічне забезпечення у зазначеній сфері тощо [5, с. 364].

Отже, забезпечення належного рівня кібернетичної безпеки є необхідною умовою розвитку інформаційного суспільства. Тому, розбудова дієвої системи кібернетичної безпеки є однією з найнагальніших завдань забезпечення національної безпеки України.

#### **Література:**

1. Пояснювальна записка до проекту Закону України «Про кібернетичну безпеку України» [Електронний ресурс]. – Режим доступу: <http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=7240&pf35401=264849>
2. Конституція України від 28 червня 1996 року // Відомості Верховної Ради України. – 1996. – №30. – Ст. 141.
3. Дубов Д. В, Стратегічні аспекти кібербезпеки в Україні / Д. В. Дубов // Стратегічні пріоритети № 4(29). – 2013. – С. 119.
4. Административное право: Учебник / Под ред. Ю.М. Козлова, Л.Л. Попова. – М., Юридическая литература, 1999. – 450 с.
5. Державне управління: теорія і практика / за загальною редакцією В.Б. Авер'янова. – К.: Юрінком Інтер, 1998. – 431 с.

## Сутність та зміст громадського порядку і його адміністративно-правової охорони

**Припутень Д.С.**

кандидат юридичних наук  
старший викладач кафедри адміністративного права,  
процесу та адміністративної діяльності ОВС  
Дніпропетровського державного університету внутрішніх справ

**Кожушна О.В.**

курсант 4 курсу ФПФПКП  
Дніпропетровського державного університету внутрішніх справ

Побудова правової держави потребує удосконалення всіх суспільних відносин і, в першу чергу, відносин, що складають зміст громадського порядку. Питання охорони громадського порядку завжди були, є і будуть актуальними для цивілізованого суспільства. Вони мають як наукове, так і практичне значення, оскільки зміст громадського порядку, активність його охорони впливають на стабільність прав громадян, всебічне задоволення їх матеріальних і духовних потреб.

Саме у сфері громадського порядку реалізується значна частина особистих прав громадян, важливі політичні свободи, соціально-економічні та культурні права. Гарантії прав і свобод громадян у даній сфері традиційно розглядаються як загальні умови реалізації прав і свобод або спеціальних (юридичних) засобів, які не завжди забезпечують надійну реалізацію, охорону, а в необхідних випадках і захист порушених прав. Демократизація України, використання світових стандартів захисту прав і свобод людини і громадянина, прагнення України стати повноправним учасником світової спільноти роблять наукові дослідження з питань охорони громадського порядку надзвичайно актуальними.

Так, загальнотеоретичні положення організації громадського порядку, його охорони досліджувалися у наукових працях О.М. Бандурки, Ю.П. Битяка, І.П. Голосніченка, М.І. Єропкина, А.П. Ключніченка, М.В. Корнієнка, М.В. Лошицького, В.П. Нагребельного, Ю.О. Тихомірова, В.Є. Чиркіна, К.В. Шоріна та інших учених.

Зазначимо, що саме поняття «громадський порядок» прийшло з наполеонівської Франції в царську Росію на початку XIX століття. У той час була проведена чітка межа між кримінальною поліцією і поліцією адміністративною, на яку був покладений обов'язок «охороняти громадський порядок в кожній місцевості». Проте поступово на рубежі XIX-XX століть поняття «громадський порядок» витісняють інші – спорідненні йому поняття: «благочиння», «благополуччя», «благоустрій» [1, с. 84].

Так, К.С. Бельський зазначає, у самому загальному виді під громадським порядком необхідно розуміти правильне розміщення людей і речей у місцях, які мають суспільне значення, шляхом установлення їх правового статусу за допомогою моральних, правових та естетичних норм [2].

В той же час, громадський порядок у широкому розумінні містить усю систему суспільних відносин, які виникають внаслідок дотримання та реалізації соціальних норм, принципів, ідей, які діють у суспільстві в усіх сферах життя та є суспільно необхідними та найбільш важливими для даного економічного і політичного устрою, поведінки громадян, державних організацій та громадських об'єднань [3, с. 191]. У такому значенні громадський порядок є об'єктом охоронного впливу всіх соціальних інститутів держави.

Таким чином, ми погоджуємось з В.І. Мельником, що громадський порядок – це складне соціальне явище, забезпечення якого вимагає комплексного підходу. Виходячи з норм чинного законодавства та практики діяльності правоохоронних органів, можна зробити висновок, що зміст громадського порядку складають такі системи суспільних відносин:

- система суспільних відносин, що забезпечує життя, здоров'я, честь і гідність громадян;
- система суспільних відносин, що забезпечує збереження власності;
- система суспільних відносин, що забезпечує нормальну діяльність підприємств, установ, організацій, посадових осіб і громадян [4, с. 40].

Обов'язковим елементом громадського порядку є засоби регулювання суспільних відносин, які утворюють зміст громадського порядку: правові, а також інші соціальні норми – норми моралі, звичаї, релігійні норми, правила громадського співжиття. За їх допомогою встановлюються права та обов'язки учасників суспільних відносин, визначаються заборони на вчинення певних дій, а також можливість і порядок застосування санкцій.

З іншого боку, громадський порядок, у вузькому розумінні, визначається як морально-правовий стан суспільства, при якому компетентні органи виконавчої влади шляхом поліцейського нагляду забезпечують безпеку і правомірну поведінку громадян в громадських місцях, вільне використання

ними своїх прав і свобод, а також упорядкування громадських місць, яке сприяє трудовій діяльності та відпочинку громадян [5].

Адміністративно-правова охорона громадського порядку представляє собою виконавчо-розпорядницьку діяльність органів державного управління, що складаються з встановлених обов'язкових правил поведінки, створення необхідних умов для їх виконання, а також здійснення адміністративного нагляду і вжиття заходів впливу.

Адміністративно-правова охорона – це діяльність, що здійснюється в трьох основних напрямках:

- нормотворчому – коли створюються закони й інші нормативні акти з адміністративно-правових питань охорони правопорядку;
- правозастосовних, що визначені в проведенні в життя встановлених державою правил у сфері громадського порядку;
- правоохоронного – включаючи заходи забезпечення встановленого порядку і застосування заходів впливу до правопорушників [5].

Підводячи підсумки, потрібно зазначити, що громадський порядок як вид безпеки виступає важливим елементом правової основи життєдіяльності громадян і являє собою систему суспільних відносин, яка виникає і розвивається в процесі спілкування її учасників переважно в громадських місцях, і регулюється правовими та іншими соціальними нормами, дотримання яких забезпечує особисту і громадську безпеку людей.

В той же час, вдосконалення системи організації охорони громадського порядку з метою підвищення її ефективності, на нашу думку, передбачає більш активне залучення громадян до охорони громадського порядку в поєднанні з посиленням координуючої ролі органів місцевого самоврядування в охороні громадського порядку.

#### **Література:**

1. Ярмачі Х.П. Сутність та зміст громадського порядку і його охорони / Х.П. Ярмачі // Актуальні проблеми держави і права. – 2005. – С. 84-91
2. Вельский К.С. Полицейское право: Лекционный курс. – М.: Дело и сервис, 2004. – С. 240.
3. Олійничук Р.П. Еволюція та сучасний зміст поняття «громадський порядок» у теорії кримінального права / Р.П. Олійничук // Право і суспільство. Питання кримінального права і кримінології. – 2012. – № 3. – С. 190-194
4. Мельник В.І. Організаційні аспекти удосконалення охорони громадського порядку в сільській місцевості / В.І. Мельник // Науковий вісник Херсонського державного університету. Серія «Юридичні науки». – 2015. – Вип. 1 (Том 3). – С. 40-42
5. Організація діяльності міліції громадської безпеки: мультимедійний навч. посіб. [Електронний ресурс] / С.Ф. Константинов, С.Г. Братель, О.Ю. Дрозд, В.М. Білик та ін. Нац. акад. внутр. справ. – Режим доступу: <http://www.naiu.kiev.ua/books/ODGMV/new-page.html>

#### **Початкові дії спеціаліста під час огляду місця події за фактом порушення працездатності комп'ютерної системи**

**Скачкова Т.Ю.**

кандидат юридичних наук, доцент  
доцент кафедри спеціально-правових дисциплін  
Донецького державного університету управління  
м. Маріуполь, Україна

Стрімкий розвиток новітніх інформаційних технологій та їхнє впровадження в життя обумовили появу злочинності в галузі комп'ютерної інформації. Для України цей вид злочинності є відносно новим, але для багатьох розвинених країн проблеми, що виникають у зв'язку з даним видом злочинності, давно стали першочерговими й такими, що потребують невідкладного рішення.

Багато людей дізнаються про злочини даної категорії лише тоді, коли вони тією чи іншою мірою зачіпають їх інтереси. Тому для повного й об'єктивного розкриття й розслідування злочинів вищевказаної категорії необхідно не тільки знати, але й розуміти мотиви й механізм здійснення злочинів у галузі інформаційних технологій.

Перш, ніж приступати до такого «мистецтва» як хакінг, кіберзлочинець проведе попередній збір всієї інформації про комп'ютерну мережу, що його зацікавила. Для пошуку інформації кіберзлочинець

використає відкриті джерела в Internet: адреси й місця розташування Web-вузлів; номери телефонів організації, що його зацікавила; контактну інформацію й адреси електронної пошти.

Одержати таку відкриту інформацію можна, скориставшись пошуковими системами Internet та спеціалізованими пошуковими ресурсами.

Встановивши адреси або доменні імена комп'ютерів, кіберзлочинець переходить до зондування комп'ютерної мережі, тобто визначенню комп'ютерів, підключених у цей момент до Internet. Ці операції кіберзлочинець може проводити з використанням програм traseroute, Visual Route, Neo Trace та ін. Вищевказані програми дозволяють визначити географічне положення комп'ютерів, які зацікавили кіберзлочинця.

Якщо при зондуванні кіберзлочинець установить, що на шляху до мережі, яка атакується, встановлені апаратні брандмауери або маршрутизатор або програмний брандмауер, то він намагатиметься знайти в них уразливість за допомогою такої багатофункціональної утиліти як Nmap (Network Mapper) або за допомогою інших спеціалізованих програм [1, с. 2].

Особливістю огляду місця події на даному етапі є те, що об'єкти, що підлягають огляду, тобто комп'ютерні системи й мережні устрої, перебувають у працюючому стані. Необхідно виключити або звести до мінімуму внесення змін у комп'ютерні системи або мережні устрої спеціалістом правоохоронних органів або персоналом, відповідальним за безпеку комп'ютерної мережі.

Для реагування на дії кіберзлочинця необхідно вивчити журнали реєстрації подій систем виявлення вторгнень, апаратних або програмних брандмауерів, маршрутизаторів, xDSL-модемів. Для цього необхідно застосовувати програми, у працездатності й правильності результатів яких фахівець упевнений. Іншими словами, необхідно виключити або звести до мінімуму використання програм наявних у комп'ютерній системі, що оглядається [1, с. 2].

Для вивчення журналів реєстрації подій систем виявлення вторгнень, апаратних або програмних брандмауерів, маршрутизаторів, xDSL-модемів нами рекомендується використовувати наступні програми. Для проведення вибірки з журналу по заданому параметрі в операційних системах сімейства Windows - Power Grep.exe, egrep.exe; в операційних системах сімейства UNIX - grep, egrep [2, с. 3].

Після зондування кіберзлочинець переходить до сканування мережі, тобто визначення її топології, використовуючи такі утиліти як ping, icmpenum і ін. Кращими утилітами даного класу вважаються Nmap, Ping Sweeper виробництва компанії Solar Winds, та Pinger, яка написана хакерами із групи Rhino9. Далі йде процес визначення відкритих портів у системі. Порти - це місця входу в систему, встановлені різними програмами й процесами, що очікують підключення. Для цих цілей зловмисник може використати вищезгадану програму Nmap, програми Super Scan, Ip Eye, сканери Whisker, Nikto. Він може також скористатися й так званим «швейцарським армійським ножом» - багатофункціональною програмою nc -Net Cat [1, с. 2].

На даному етапі діяльності кіберзлочинця, спеціаліст правоохоронних органів, крім журналів система виявлення вторгнень і маршрутизаторів, що ведуться в комп'ютерних мережах, повинен також вивчити журнали Web-серверів, DNS-серверів, поштових серверів і серверів баз даних за допомогою вищезгаданих програм, для виявлення IP-адреси або IP-адрес, засобів і методів, використовуваних кіберзлочинцем [1, с. 2].

Зібравши достатні на комп'ютерну мережу або комп'ютерну систему, кіберзлочинець перейде до проникнення в комп'ютерну мережу або комп'ютерну систему та інвентаризації користувальницьких ресурсів і облікових записів.

Якщо кіберзлочинець знайшов уразливості в комп'ютерах мережі або комп'ютерній системі й скористався ними, він одержав доступ у мережу. Але тепер йому необхідно закріпитися, тобто розширити свої привілеї, щоб використати ресурси мережі не один раз. Для цього кіберзлочинець може використати такі програми як реєстратори натискань клавіш на клавіатурі- Invisible Key Logger Stealth (IKS), аналізатори мережних пакетів - Dsniff, Grep, BUTTSniffer, NetXRay, програми переспрямування портів - fpipe, datarpipe, пакет програм Winaf та ін. [1, с. 2].

Після того, як кіберзлочинець набув певних прав у комп'ютерній мережі, він намагатиметься сховати факт своєї присутності й залишити потайний хід. Для цього він може скористатися як командами операційних систем – attrib +h, так і програмами Win2K Resource Kit. Також може використати набори «відмичок» - rootkit - AFXRootkit2005, HackerDefender v1.0, FU\_Rootkit, OpenBSD rootkit, Adore 0.54, LKM Rootkit, BDW, які під час свого виконання приховують від стандартних засобів моніторингу операційної системи зазначені програми, каталоги, процеси й відкриті порти або використати пакувальники файлів і бібліотек - StealthPE, UPX, FSG [1, с. 2].

Далі всі програми, якими користується кіберзлочинець, можуть бути упаковані в один архів, за допомогою програми EliteWrap. Ця програма дозволяє поєднувати кілька програм для асинхронного й непомітного розпакування й виконання. Також кіберзлочинець може використати програми



віддаленого адміністрування - Net Bus, Sub Seven 2.2, Back Orifice, Institution2004, може скористатися методами тунелювання (DNS, HTTP, SNMP, ICMP) [1, с. 2].

На даному етапі діяльності кіберзлочинця, фахівець залучений до огляду, повинен вивчити журнали системних подій, файли обліку доступу в комп'ютерну систему, файли паролів, списки доступу маршрутизатора, журнали систем виявлення вторгнень, інформаційне наповнення накопичувачів на жорстких магнітних дисках, наявні в скомпрометованій комп'ютерній системі.

При завершенні свого злочинного діяння кіберзлочинець повинен переконатися, що пророблена їм робота не пропаде, а для цього йому в більшості випадків, необхідно перезавантажити операційну систему атакowanego комп'ютера з використанням програм операційної системи. Для цього кіберзлочинець також може скористатися exploitami або привести систему до стану «відмови в обслуговуванні» DoS (Denied of Service) шляхом «бомбардування» комп'ютера пакетами ICMP (Smurf-атака) або UDP (Fraggle- атака) з використанням посилюючої мережі (DDoS) [1, с. 2].

Таким чином, під час огляду місця події, при розслідуванні злочинів в галузі інформаційних технологій, тобто досліджуючи скомпрометовані комп'ютерні системи або комп'ютерні мережі, або мережні устрої спеціаліст повинен: вивчити журнали системних подій, файли обліку доступу в комп'ютерну систему, файли паролів, списки доступу маршрутизатора, журнали систем виявлення вторгнень журнали Web-серверів, DNS-серверів, поштових серверів, серверів баз даних, xDSL-модемів; застосовувати програми, у працездатності й правильності результатів яких фахівець упевнений; виключити або максимально знизити можливість зміни досліджуваної комп'ютерної системи; максимально задокументувати всі дії кіберзлочинця шляхом створення файлів-доказів, виявлення всіх встановлених кіберзлочинцем програмних засобів, а також необхідно створити файл із контрольними сумами всіх виявлених та створених речових доказів; записати створені файли-докази, виявлені програмні засоби та файл з контрольними сумами на виключно на носій з можливістю однократного запису (CD-R, DVD-R); упакувати носій з файлами-доказами з дотриманням правил і передати носій особі, що керує проведенням огляду місця події.

Підбиваючи підсумок, хочеться відзначити що спеціаліст, який бере участь в огляді місця події при розслідуванні злочинів у галузі інформаційних технологій повинен бути хакером - мати спеціальні знання в галузі різних операційних систем, комп'ютерних мереж і технологій передачі інформації в комп'ютерних мережах, уміти на досить високому рівні досліджувати комп'ютерну систему й знаходити уразливості, знати програмні інструменти які використовують кіберзлочинці й постійно відслідковувати інформацію про нові уразливості в програмах та появу нових програмних інструментів.

#### **Література:**

1. Вакка Д. Секреты безопасности в Internet / Д. Вакка. – Диалектика. - К., 1997 г.
2. Стенг Д. Секреты безопасности сетей / Д. Стенг. – Диалектика. - К., 1996 г.
3. Чирилло Д. Обнаружение хакерских атак. Для профессионалов / Д. Чирилло. - С.-П. - 2002 г.

#### **Кібертероризм як різновид тероризму**

**Баркар Р.І.**

студент магістратури факультету № 4  
Одеського державного університету внутрішніх справ

**Форос Г.В.**

к.ю.н., доцент  
професор кафедри кібербезпеки інформаційного забезпечення  
Одеського державного університету внутрішніх справ

Стрімке збільшення кількості персональних комп'ютерів, вільний доступ до Інтернету і швидкий розвиток ринку новітніх технологій змінили і способи проведення дозвілля, і методи ведення бізнесу, але також змінюються і способи вчинення злочинів. Злочинність в сфері інформаційних технологій відкриває нові можливості для діяльності злочинців. З огляду на національну безпеку України, спостерігається небезпечна тенденція, пов'язана зі збільшенням технічної і технологічної залежності держави від транскордонних проявів кібертерористів. Стан інформаційно-телекомунікаційних систем і рівень їх захисту є одним з найважливіших факторів, що впливають на інформаційну безпеку держави.

Сьогодні, в залежності від політичних цілей терористів, сферою терористичної діяльності стає весь світ, механізмом терористичних дій – насильство відносно цивільних громадян, а його головним об'єктом – суспільство та громадська думка. У сучасних умовах, коли арсенал терористів поповнюється новітніми зразками зброї, сучасними засобами та технологіями отримання, передання, обробки та збереження інформації, а їх організаційні структури ускладнилися і набули міжнародного характеру, гостро встає питання про виявлення і забезпечення надійним захистом потенційних об'єктів терористичних зазіхань, і як наслідок систем національної безпеки держав.

На підставі проведеного аналізу наукових джерел та нормативно-правових актів, на наш погляд, серед різновидів тероризму (національного, міжнародного, ідеологічного, релігійного, кримінального) можна виділити такий вид як технологічний. Цей вид тероризму має складний зміст. Згідно, Закону України «Про боротьбу з тероризмом» він містить в собі ядерний тероризм, хімічний тероризм та кібернетичний тероризм. А саме, технологічний тероризм – це злочини, що вчиняються з терористичною метою із застосуванням ядерної, хімічної, бактеріологічної (біологічної) та іншої зброї масового ураження або її компонентів, інших шкідливих для здоров'я людей речовин, засобів електромагнітної дії, комп'ютерних систем та комунікаційних мереж, включаючи захоплення, виведення з ладу і руйнування потенційно небезпечних об'єктів, які прямо чи опосередковано створили або загрожують виникненням загрозливого надзвичайної ситуації внаслідок цих дій та становлять небезпеку для персоналу, населення та довкілля; створюють умови для аварій і катастроф техногенного характеру [1, с. 1].

Сучасні інформаційно-комунікативні технології забезпечують відносно невеликі терористичні групи могутньою та дієвою зброєю, своєрідним ретранслятором насильства. Таким чином, можна стверджувати, що за сучасних міжнародних реалій значну зовнішню загрозу для України становить розповсюдження інформаційного тероризму.

На наш погляд, враховуючи високий рівень громадської небезпеки вид цих видів тероризму їх слід розглядати як самостійні види тероризму. Так, інформаційний (кібернетичний) тероризм - це новий вид терористичної діяльності, орієнтований на використання різних форм і методів тимчасового або незворотного виведення з ладу інформаційної інфраструктури держави або її елементів, а також за допомогою протиправного використання інформаційної структури для створення умов, що тягнуть за собою тяжкі наслідки для різних сторін життєдіяльності особистості, суспільства і держави [2, с.13]. Його різновидом є кібернетичний тероризм, який полягає в використанні сучасних інформаційних технологій, і в першу чергу Інтернету, коли така зброя застосовується з метою пошкодження важливих державних інфраструктур (таких як енергетична, транспортна, урядова).

Серед наукових та практичних працівників немає єдності у термінологічному позначенні даного виду терористичної діяльності. Такий вид тероризму вони називають по-різному: «інформаційний тероризм», «комп'ютерний тероризм», «кібертероризм», «технологічний тероризм», «віртуальний тероризм», тощо. При цьому зміст зазначених понять визначається по-різному. Складність у формулюванні цих понять існує, очевидно, як через неможливість виділення єдиного об'єкта злочинного посягання, так і достатньо великої кількості предметів злочинних посягань з погляду їх кримінально-правової охорони.

На думку вчених, найбільшу небезпеку представляє кібертероризм, а саме тероризм спланований, вчинений чи скоординований в кіберпросторі, тобто в терористичних акціях використовуються новітні досягнення науки і техніки в галузі новітніх інформаційних технологій. Кібератаки здатні завдати інформаційно-телекомунікаційним системам на основних інфраструктурах значної шкоди. Для терористів електронні засоби обробки інформації мають певні переваги у порівнянні з фізичними. Так, з їх допомогою, можна діяти віддалено і анонімно, вони значно дешевше і не потребують вибухових засобів та місій самогубців.

Аналіз наукових праць, спеціальної літератури та повідомлень засобів масової інформації свідчить про той факт, що вирізняють абсолютно новий вид тероризму – віртуальний. Це тероризм, при якому у терористів є можливість доступу до інформаційно-комп'ютерних технологій, за допомогою яких вони створюють видимість терористичної кампанії або окремого терористичного акту, якого насправді немає, чим можливе досягнення потрібного терористам психологічного впливу на широкую аудиторію. Особливістю сучасного тероризму є активне використання інформаційно-психологічного впливу як важливого елемента маніпуляції свідомістю людей. Не таємниця, що сьогодні засоби комунікацій, що оперують, трансформують та дозують інформацію, стають головним інструментом впливу в сучасному суспільстві. Для підвищення ефективності здійснення стратегій використовуються найсучасніші інформаційні технології, які допомагають перетворити публіку в об'єкт маніпулювання. Тому роль засобів масової інформації полягає в дії на користь суспільству, а не терористів. Висвітлення подій у засобах масової інформації не повинно працювати для досягнення терористичних цілей, а сприяти

вихованню у свідомості людей неприйняття методів насильства й шантажу, підтримці дій влади, а також навчанню прийомам особистої і колективної безпеки в ситуаціях, пов'язаних з терористичними погрозами.

Таким чином, кібертероризм – це новий вид терористичної діяльності, спрямований на використання можливостей інформаційних систем та комп'ютерних технологій з метою порушення або знищення значних державних інфраструктур.

#### **Література:**

1. Про тероризм [Електронний ресурс]: Закон України № 638-IV від 02.10.92.– Режим доступу: <http://zakon1.rada.gov.ua>. – Назва з екрану
2. Коршунов В.О. Політичний тероризм: інформаційні методи боротьби: автореф. дис. на здобуття наук. ступеня канд. пол. наук: спец. 23.00.02 «Політична інститути та процеси» /Коршунов В.О. – Дніпропетровськ., 2008. – 18 с.

#### **Інформаційне суспільство та кібербезпека**

**Кондрашева К.С.**

студентка магістратури факультету № 4  
Одеського державного університету внутрішніх справ

**Форос Г.В.**

к.ю.н., доцент  
професор кафедри кібербезпеки та інформаційного забезпечення  
Одеського державного університету внутрішніх справ

В умовах глобалізації швидкими темпами формується новий тип людської формації – «інформаційне суспільство». Однією з основних характеристик новітньої формації є швидкий обмін інформацією, розвиток усіх сфер людської діяльності за допомогою знань. Перехід будь-якої країни до інформаційного суспільства вимагає переосмислення, а у окремих випадках і розробки нових механізмів регулювання відносин, що виникають між громадянами, їх об'єднаннями та державою. Побудова інформаційного суспільства – закономірний і невідворотний результат розвитку цивілізації. Всі сфери суспільного життя пронизані різноманітними інформаційними відносинами. Суспільна формація визначається нині ступенем використання сучасних інформаційно-телекомунікаційних технологій, а динаміка розвитку суспільства – швидкістю передачі інформації.

Термін «інформаційне суспільство» зайняв стале місце в лексиконі зарубіжних політичних діячів різного рівня, і саме з ним зв'язують майбутнє своїх країн багато керівників. Основу теорії інформаційного суспільства заклали Ф. Махлуп, Д. Белл, З. Бжезинський, Ж. Фурасте, Дж. Мартін, О. Тоффлер та інші. Саме в їх наукових працях і доповідях були сформовані основні ознаки та перспективи інформаційного суспільства. Вони вказували, що інформаційне суспільство – це різновид постіндустріального суспільства. Значний вклад в розвиток даного напрямку наукової думки вніс О. Тоффлер, який визначив три основні цивілізації, які виникли в ході глобальних соціотехнологічних революцій. Першою була аграрно-реміснична революція, результатом якої було виникнення історично першої цивілізації в основі виробництва якої були землеробські та ремісничі технології. Друга соціотехнологічна революція отримала назву індустріальної. Її результатом стало виникнення індустріальної і урбаністичної цивілізації, в рамках якої склалися господарства, орієнтовані на індивідуально-групову ініціативу. Наступна, третя соціотехнологічна революція отримала назву інформаційна, і полягає в процесі інформатизації всіх сфер життєдіяльності суспільства та людини [1, с. 12-14].

Проведений аналіз наукових праць надає можливість виділити три базові характеристики інформаційного суспільства. По-перше, інформація використовується як економічний ресурс, по-друге, інформація стає предметом масового споживання у населення, і по-третє, швидкими темпами формується та зростає інформаційний сектор економіки.

Перехід будь-якої країни до інформаційного суспільства вимагає переосмислення, а у окремих випадках і розробки нових механізмів регулювання відносин, що виникають між громадянами, їх об'єднаннями та державою. Конституція України закріпила право кожного вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб, за винятком спеціально

визначених у законі обставин (ст. 34 Конституції України). Але здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку, з метою запобігання заворушенням чи злочинам, для охорони життя і здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошення конфіденційної інформації для підтримання авторитету неупередженості правосуддя.

Інформаційна політика визначає закони функціонування інформаційної сфери. Коли ефективно працює система ЗМІ суспільства, це дає змогу швидко вирощувати нову еліту, активно обговорювати нові проекти, сприяти прозорості влади, наближати її дії до населення. Законом взаємодії влади і населення є адекватне функціонування комунікації між владою і населенням. Не тільки населення має чути владу, а й влада має прислухатися до думки і слова свого населення.

Інформаційна безпека полягає в аналізі загроз, які можуть виникнути в інформаційній сфері, і створенні умов для запобігання їхньому виникненню. У першу чергу це стосується різноманітних технічних аспектів передавання й обробки інформації.

Якщо розглядати проблему формування інформаційного суспільства в цілому, то специфіка сучасного етапу полягає в тому, що подальший прогрес інформаційних і телекомунікаційних технологій залежить не тільки від досягнень у галузі технологій, а від того наскільки швидко будуть пристосовані до нових реалій старі норми, які регулюють традиційно різні сектори, - телекомунікації, телебачення та інші засоби масової інформації.

При цьому слід особливу увагу приділяти захисту інформації та інформаційно-телекомунікаційних систем. Недаремно однією з основних складових системи забезпечення національної безпеки називають інформаційну безпеку. Поняття інформаційної безпеки в сучасному світі надзвичайно широке, а останнім часом із нього виокремлено поняття кібербезпеки. *В науковій літературі кібербезпека визначається як безпека інформації та інфраструктури в цифровому середовищі, що її забезпечує.* Кібербезпека передбачає досягнення і збереження властивостей безпеки в ресурсах організації або користувачів, що спрямовані на запобігання відповідним кіберзагрозам.

Однак слід пам'ятати, що заходи інформаційної безпеки, - це засоби забезпечення інтересів суспільства, а не самоціль. Їх здійснення не повинно перешкоджати здійсненню громадянами права на вільний доступ інформації, що не становить державної, військової, комерційної чи медичної таємниці. Вільний доступ до несекретної інформації органів влади є одним з законних засобів громадського контролю, який дозволяє спрямовувати дії влади на задоволення інформаційних потреб громадян.

Потреба забезпечення інформаційної безпеки викликана, по-перше, необхідністю забезпечення національної безпеки в цілому; по-друге, існуванням таких загроз інформаційній сфері країни, які можуть принести значний збиток загальнонаціональним, регіональним і локальним інтересам; по-третє, необхідністю врахування того, що за допомогою інформації можна впливати на свідомість та поведінку людей.

Вважається, що в майбутньому існуватиме кілька типів інформаційного суспільства, як колись існували кілька моделей індустріального суспільства. Ключовими ознаками для визначення типу суспільства будуть такі: ступінь забезпечення рівних прав доступу громадян до основного ресурсу – інформації, ступінь участі у житті суспільства та самореалізації людей із обмеженими фізичними можливостями.

### **Література:**

1. Беляков К.И. Управление и право в период информатизации. Монография. – Киев: из-во «КВІЦ», 2001. - 308 с.
2. Копылов В.А. Информационное право. – М.: Юристъ. – 1998. – 257 с.
3. Арістова І. В Державна інформаційна політика: організаційно-правові аспекти. – Х.: УВС, 2000. – 368 с.

### **Щодо розмежування понять «кібербезпека» та «інформаційна безпека»**

**Форос Г.В.**

к.ю.н., доцент

професор кафедри кібербезпеки

та інформаційного забезпечення

Одеського державного університету внутрішніх справ

Останнім часом проблема безпеки в кіберпросторі виділяється як одна із глобальних проблем сучасності. Згідно діючому законодавству, одним із головних напрямів державної інформаційної

політики є створення загальної системи охорони інформації. Так, Конституція України, що стала гарантом побудови демократичної правової держави, не могла не врахувати загальносвітових тенденцій інформатизації суспільства. Тому ряд її статей визначають забезпечення інформаційної безпеки як одну з найважливіших функцій держави і мають стати запорукою розвитку національного інформаційного законодавства. Згідно, Закону України «Про Національну програму інформатизації», інформаційна безпека - невід'ємна частина політичної, економічної, оборонної та інших складових національної безпеки [1].

В науковій та спеціальній літературі інформаційна безпека розглядається як елемент або підсистема національної безпеки. У Законі України «Про основи національної безпеки України» визначено дев'ять основних напрямів державної політики національної безпеки в різних сферах життєдіяльності. До однієї з них належить інформаційна, що дає усі підстави стверджувати, що інформаційна безпека є ваговою складовою національної.

Досить тривалий час поняття «кібербезпека» та «інформаційна безпека» в науковій та спеціальній літературі, ототожнювали або розглядали кібербезпеку як складову інформаційної безпеки. Але у «Стратегії національної безпеки України» надається розмежування понять кібербезпека та інформаційна безпека, шляхом визначення загроз інформаційній безпеці та загроз кібербезпеці і безпеці інформаційних ресурсів [2].

Так, до загроз інформаційній безпеці віднесено ведення інформаційної війни проти України; відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства. Загрози кібербезпеці і безпеці інформаційних ресурсів визначаються в уразливості об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак, а також у фізичній і моральній застарілості системи охорони державної таємниці та інших видів інформації з обмеженим доступом.

Не спиняючись на визначенні загроз, було встановлено Пріоритети забезпечення інформаційної безпеки до яких віднесено забезпечення наступальності заходів політики інформаційної безпеки на основі асиметричних дій проти всіх форм і проявів інформаційної агресії; створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них; протидія інформаційним операціям проти України, маніпуляціям суспільною свідомістю і поширенню спотвореної інформації, захист національних цінностей та зміцнення єдності українського суспільства; розробка і реалізація скоординованої інформаційної політики органів державної влади; виявлення суб'єктів українського інформаційного простору, що створені та/або використовуються Росією для ведення інформаційної війни проти України, та унеможливлення їхньої підривної діяльності; створення і розвиток інститутів, що відповідають за інформаційно-психологічну безпеку, з урахуванням практики держав - членів НАТО; удосконалення професійної підготовки у сфері інформаційної безпеки, впровадження загальнонаціональних освітніх програм з медіа культури із залученням громадянського суспільства та бізнесу.

На думку вчених, інформаційна безпека – це стан захищеності інформаційного простору, що забезпечує формування та розвиток цього простору в інтересах особистості, суспільства та держави. В межах даного напрямку існує визначення інформаційної безпеки як стану, тенденції розвитку, умов життєдіяльності соціуму, його структур, інститутів та установ, за яких забезпечується збереження якісної, з об'єктивно обумовленими інноваціями в ній, вільної, відповідно власній природі функціонування інформації. Ряд представників цього напрямку розглядають інформаційну безпеку як стан, що характеризується відсутністю небезпеки, тобто чинників та умов, які загрожують безпосередньо індивіду, спільноті, державі з боку інформаційно-комунікаційного середовища.

Інформаційна безпека дає гарантію того, що досягаються наступні цілі: конфіденційність інформації; цілісність інформації і пов'язаних з нею процесів; доступність інформації, коли вона потрібна; облік усіх процесів, пов'язаних з інформацією, тобто завдяки інформаційній безпеці виконуються функції щодо дотримання вимог, які ставляться до інформації.

Пріоритетами забезпечення кібербезпеки і безпеки інформаційних ресурсів є: розвиток інформаційної інфраструктури держави; створення системи забезпечення кібербезпеки, розвиток мережі реагування на комп'ютерні надзвичайні події (СЕКТ); моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації; розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів; забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, відмова від програмного забезпечення, зокрема антивірусного, розробленого у Російській Федерації; реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації з урахуванням практики держав - членів НАТО та ЄС; створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони; розвиток міжнародного

співробітництва у сфері забезпечення кібербезпеки, інтенсифікація співпраці України та НАТО, зокрема в межах Трестового фонду НАТО для посилення спроможностей України у сфері кібербезпеки.

В науковій літературі кібербезпека визначається як безпека інформації та інфраструктури в цифровому середовищі, що її забезпечує. Кібербезпека передбачає досягнення і збереження властивостей безпеки в ресурсах організації або користувачів, що спрямовані на запобігання відповідним кібер загрозам.

В Україні найбільше від кібератак страждають впливові медіа, фінансові інститути та державні установи. При цьому на сьогодні зростає не тільки кількість атак на інформаційну інфраструктуру, але і їх складність. Зловмисники використовують різні види атак: фізичні (атаки на телевізійні вежі), DDoS-атаки (на сайти Центрвиборчкому, Верховної Ради та ключових ЗМІ), зломи інформаційних ресурсів (сайту ЦВК, електронних скриньок політиків і журналістів), атаки на мобільні мережі (перехоплення переговорів мобільного зв'язку).

Отже, інформаційна безпека являє собою одне з найважливіших понять в юридичній науці і в різних сферах людської діяльності. Сутність і комплексність цього поняття обумовлюється характером сучасного інформаційного суспільства. Аналіз різних підходів до визначення змісту поняття «інформаційна безпека» дає змогу зауважити про недоцільність жорсткого обрання тієї чи іншої позиції. Наведені вище підходи до визначення поняття інформаційної безпеки дають змогу розглядати дану проблему комплексно та системно. Інформаційна безпека є і властивістю, і атрибутом інформаційного суспільства, і діяльністю, і результатом діяльності людини, спрямованої на забезпечення певного рівня безпеки в інформаційній сфері.

Інформаційна безпека є невід'ємною частиною загальної безпеки — чи то національної, чи то регіональної, чи то міжнародної. Аналіз інформаційної безпеки передбачає розгляд сукупності таких об'єктивних чинників: потреб громадян, суспільства, держави та світового співтовариства; уразливості індивідів, суспільства та держави від детальних технологій; наявності широкого кола загроз і небезпек, якими має управляти система забезпечення інформаційної безпеки.

Зміст поняття «інформаційна безпека» розкривається у практичній діяльності, наукових дослідженнях, а також нормативно-правових документах. Варто зазначити, що у науковій літературі поки відсутній єдиний консолідований підхід до змісту понять «інформаційна безпека» та «кібер безпека».

### **Література:**

1. Про Національну програму інформатизації [Електронний ресурс]: закон України від 04.02.1998 № 74/98-ВР із змін., внес. згідно із Законами України від 01.08.2016, підстава 922-19. – Електрон. дан. (1 файл). – Режим доступу: <http://zakon1.rada.gov.ua>. – Назва з екрану.
2. Про Стратегію національної безпеки України [Електронний ресурс]: указ Президента України від 06.05.2015 № 287/2015. – Електрон. дан. (1 файл). – Режим доступу: <http://zakon1.rada.gov.ua>. – Назва з екрану.
3. Кормич Б.А. Інформаційна безпека: організаційно-правові основи. Навч. посібник. – К.: Кондор, 2004. – 384 с.

### **протидія кіберзлочинності як складова інформаційної безпеки держави**

**Новіцький О.І.**

студент 2 групи 3 курсу Факультету №4  
Одеського державного університету внутрішніх справ

**Косаревська О.В.**

кандидат педагогічних наук, доцент,  
доцент кафедри кібербезпеки та інформаційного забезпечення  
Одеського державного університету внутрішніх справ

Розвиток сучасних інформаційних технологій та їх впровадження в усі без винятки сфери життя обумовив виникнення якісно нових загроз національній та міжнародній безпеці. За останні десятиріччя такі загрози як транснаціональна кіберзлочинність, кібертероризм, застосування кібернетичної зброї перетворились із потенційних та гіпотетичних на цілком реальні, а протидія ним на пріоритетне завдання усього сектора національної безпеки і оборони.

У доктрині інформаційної безпеки України [1] окремою загрозою визначено лише прояви комп'ютерної злочинності та тероризму, що загрожують функціонуванню національних інформаційно-телекомунікаційних систем. Але в сучасних реаліях глибокого латентного проникнення кіберзлочинності у суспільне та державне життя комп'ютерні злочини є складовою всіх загроз негативного інформаційного впливу. Фундаментальною умовою ефективної протидії кіберзлочинності є достатній рівень інформаційно-правової культури суспільства та професійної підготовки фахівців із забезпечення інформаційної безпеки. Інформаційна безпека згідно законодавства України визначена як стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через [2,3]:

- неповноту, невчасність та невірогідність інформації, що використовується;
- негативний інформаційний вплив;
- негативні наслідки застосування інформаційних технологій;
- несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації.

Загроза інформаційній безпеці України - це сукупність умов та чинників, які становлять небезпеку інтересам держави, суспільства і особи через негативний інформаційний вплив на свідомість та поведінку громадян, інформаційні ресурси та інформаційно-технічну інфраструктуру. Згідно Закону України «Про основи національної безпеки України» основними інформаційними загрозами національній безпеці є [4]:

- обмеження доступу громадян до інформації;
- поширення засобами масової інформації культу насильства, жорстокості, порнографії;
- комп'ютерна злочинність та комп'ютерний тероризм;
- розголошення інформації, яка становить державну та іншу, передбачену законом таємницю;
- поширення недостовірної, неповної або упередженої інформації

Існує багато технологій здійснення негативного впливу на інформаційну сферу життєдіяльності суспільства. Вони можуть застосовуватись спецслужбами, терористичними та екстремістськими організаціями та угрупованнями, кримінальними структурами, тощо. І можливість такого використання видається досить реальною [5].

В сучасних умовах нагальною стає проблема координації діяльності правоохоронних структур та правового унормування зон відповідальності відомств, процедур взаємодії та засобів комплексного реагування на загрози кібербезпеці держави, а також значної роботи із попередження таких злочинів [6]. В Україні органом, на який покладаються повноваження щодо створення та функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні злочинів, пов'язаних з комп'ютерними системами та даними, переслідуванні осіб, що обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі, є Міністерство внутрішніх справ України [7].

Враховуючи наведене доцільна розробка наступних напрямів [8,9]:

- поширення інформації щодо правил безпечного користування мережею Інтернет;
- внесення теми онлайн-безпеки у шкільну програму для дітей віком від 7 до 14 років, а також у програму навчання та підвищення кваліфікації вчителів;
- вивчення та використання міжнародного досвіду боротьби з кіберзлочинністю;
- визначення поняття “дитяча порнографія” у законодавстві України;
- передбачити законодавством України покарання за виробництво і володіння матеріалами, що характеризуються як дитяча порнографія;
- вдосконалення ресурсної бази підрозділів МВС щодо боротьби та запобігання кіберзлочинів;
- на законодавчому рівні затвердити процедуру блокування Інтернет-ресурсів, що містять інформацію в порушення українського законодавства;
- створення зони довіри в українському сегменті Інтернету.

Актуалізація кіберзагроз вплинуло і на діяльність Служби безпеки України, як одного з центральних елементів у забезпеченні національної кібербезпеки. У 2012 році в структурі СБУ був утворений Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки

Основними завданнями які вирішує Департамент є насамперед:

1. протидія зовнішнім та внутрішнім загрозам спрямованим на:
  - урядові телекомунікаційні системи, державні інформаційні ресурси, системи електронного урядування;

- об'єкти критичної інформаційної інфраструктури держави (у тому числі об'єкти енергетики, зв'язку, транспорту, життєзабезпечення, фінансової системи, сектору національної безпеки і оборони тощо);

- національну систему технічного та криптографічного захисту інформації;

2. боротьба з кібертероризмом, використанням мережі Інтернет з терористичною метою;

3. боротьба з кіберзлочинністю, що становить загрозу життєво важливим інтересам держави, її національній безпеці;

4. контроль за обігом спеціальних засобів негласного отримання інформації, захист прав громадян від протизаконного застосування спецтехніки.

Підсумовуючи слід наголосити, що в умовах глибокого латентного проникнення кіберзлочинності у суспільне та державне життя, її подолання стає наріжним комнем на шляху розбудови інформаційного суспільства і входження України у світовий інформаційний простір. Гарантувати ефективну протидію кіберзлочинності може лише застосування комплексних підходів до забезпечення інформаційної безпеки. Встановлення місця протидії кіберзлочинності у системі забезпечення інформаційної безпеки з метою визначення необхідних її складових та урахування особливостей є важливою умовою формування ефективної державної політики забезпечення інформаційної безпеки, у межах якої доцільно розглядати протидію кіберзлочинності.

### **Література:**

1. Про Доктрину інформаційної безпеки України : Указ Президента України від 8 липня 2009 року № 514/2009 [Електронний ресурс]. – Режим доступу : <http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=514%2F2009>.

2. Закон України «Про інформацію» // ВВР. – 2003. – № 48.

3. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» // ВВР. – 2007. – № 12.

4. Закон України «Про основи національної безпеки України» // ВВР. – 2006. – № 14.

5. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи / В. Петрик // Юридичний журнал. – 2009. – № 5. – С. 45–46 ([www.justinian.com.ua](http://www.justinian.com.ua)).

6. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування. Аналітична записка [Електронний ресурс]. – Режим доступу: <http://www.niss.gov.ua/articles/454>.

7. Литовченко И.В. И др. Дети в интернете: как научить безопасности в виртуальном мире / И.В. Литовченко и др.. – К.: Изд. дом “Аванпост-Прим”, 2010. – 234 с.

8. Про внесення зміни до ЗУ "Про ратифікацію Конвенції про кіберзлочинність" (ВВР), 2011, N 5, ст.32 ) [Електронний ресурс]. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/2532-17>

9. Региональный обзор об изображениях сексуального насилия над детьми посредством использования информационных и коммуникационных технологий в Беларуси, Молдавии, России и Украине [Електронний ресурс]. – Режим доступу: [www.ecpat.net](http://www.ecpat.net).

### **Кіберзлочини у фінансово-банківській сфері: скімінг та способи його викорінення**

**Шутило С.В.**

магістр 1-го курсу Факультету №4  
Одеського державного університету внутрішніх справ

**Косаревська О.В.**

кандидат педагогічних наук, доцент,  
доцент кафедри кібербезпеки інформаційного забезпечення  
Одеського державного університету внутрішніх справ

Сучасне суспільство це суспільство інформаційних технологій, що базується на повсякденному використанні комп'ютерної техніки, мереж зв'язку, мобільних засобів комунікації та інших технічних засобів. Щоденна робота урядових структур, банківської, енергетичної, транспортної та інших систем неможлива без надійної роботи комп'ютерної техніки та засобів комунікацій. Інформаційні технології стали постійним супутником сучасної людини не лише на робочому місці, вони увійшли майже в усі сфери людського життя.



Банківська система України є однією зі сфер, де найбільш широко та активно використовуються сучасні можливості інформаційних технологій та мережі Інтернет. А враховуючи, що зазначені технології використовуються для грошових переказів, зазначена сфера привертає все більшу увагу злочинців. Несанкціоноване списання коштів з банківських рахунків, шахрайство з платіжними картками, втручання в роботу інтернет-банкінгу, розповсюдження комп'ютерних вірусів, DDoS-атаки на інтернет-ресурси, шахрайство в інформаційних мережах це не вичерпний перелік кіберзлочинів, тобто злочинів у сфері інформаційних та комп'ютерних технологій.

За оцінками експертів щорічні збитки від діяльності кіберзлочинців перевищують 100 млрд дол. США. Підготовка та вчинення кіберзлочину здійснюється практично не відходячи від «робочого місця», тобто такі злочини є доступними, оскільки комп'ютерна техніка постійно дешевшає, злочини можна вчинювати з будь-якої точки планети, у будь-якому населеному пункті, а об'єкти злочинних посягань можуть знаходитись за тисячі кілометрів від злочинця. Крім того, доволі складно виявити, зафіксувати і вилучити криміналістично-значущу інформацію при виконанні слідчих дій для використання її в якості речового доказу[1].

В наш час банківські пластикові картки впевнено займають одне з головних місць в системі фінансово-економічних відносин громадян. Проте разом з перевагами використання даного засобу електронного розрахунку або зберігання грошового капіталу, пересічний громадянин може стикнутися з деякими проблемними ситуаціями, що можуть загрожувати його економічному добробуту. Однією з таких проблем є шахрайство з використанням віртуального електронного простору (кіберпростору), коли зловмисник з одного боку використовує конфіденційні реквізити електронних платіжних карток для особистого збагачення, а з іншого використовує пластикові електронні картки для отримання коштів, які були зараховані на рахунок від довірливих громадян.

Взагалі, способів шахрайства з використанням пластикових карт існує велика кількість. Це зумовлено цілою чергою чинників, що сприяють поширенню шахрайств, наприклад в сфері благодійності до них слід віднести: а) легкий доступ до електронної мережі Інтернет в яких розміщуються оголошення про надання допомоги; б) шахрайство не вимагає спеціальної освіти, потрібні лише елементарні знання роботи з банківськими картками та мережею Інтернет; в) особа, що вчиняє шахрайські дії залишається невідомою для потерпілої особи; г) після вчинення даного злочину залишаються специфічні сліди за якими складно встановити конкретну особу злочинця

Одним із таких видів злочинів, що вчиняються у фінансово-банківській сфері, є скімінг (анг. *skimming*), коли під час використання АТМ (*automated teller machine*), POS (*point-of-sale*), PIN-паду (далі – термінал) з банківської платіжної картки сторонніми особами нелегально і потайки копіюється зміст магнітної стрічки такої картки.

Скімінг з'явився на початку 90-х років минулого сторіччя і з того часу тільки набирає обертів, як з кількості скоєних злочинів, так і в плані безперервного удосконалення прийомів та технічних засобів, що використовуються злочинцями. Розрізняють два типи скімінгового обладнання. В першому випадку, скімінгове обладнання приєднується до слоту карткового приймача терміналу і зчитує інформацію замість самого пристрою. У цьому випадку користувач картки доступу до рахунку не отримує. В іншому випадку, людина отримує доступ до рахунку, але згодом дізнається про несанкціоноване зняття коштів. В обох випадках зловмисники різними способами також дізнаються про PIN-код картки, наприклад: шляхом використання прихованих камер, накладних клавіатур тощо. Інформація з магнітної стрічки переноситься на нову пластикову картку і використовується при безпосередньому знятті грошей через банкомат, оплаті товарів чи послуг через Інтернет, або продається третім особам. Такі ж схеми можуть траплятися і на точках продажу, депокупці розплачуються за послуги картками. Відповідно достатистики, зловмисники не залишаються на одному місці. Данні зчитуються і майже одразу виготовляється клон-картка та проходить нелегальне знімання коштів, злочинець переїжджає на інше місце (іншу країну). В більшості випадків несанкціоновані операції здійснюються у вечірній або нічний час, а також у вихідні дні, коли банківські установи не працюють і факт крадіжки встановлюється згодом [2].

Серед різноманітної інформації стосовно правил безпечної поведінки особи щодо запобігання скімінгу можна виділити наступні аспекти: звертати увагу на підозрілі предмети на терміналі, не застосовувати силу при вкладанні картки у приймач банкомату, негайно інформувати банк про будь-яку підозру. Безперечно, факт невиявлення скімінгового обладнання клієнтом не виключає відповідальності банківської установи стежити за відсутністю нелегально встановленого обладнання на власному терміналі: кардрідерами, накладками на клавіатуру, камерами тощо [4].

Деякі фірми-виробники виготовляють термінали з приймачем пластикової картки, що конструктивно ускладнює приєднання зовнішнього зчитувального пристрою. Також виробники

використовують сигналізацію, що спрацьовує при спробі несанкціонованого приєднання скімінгового обладнання до терміналу.

Інша технологія запобігання скімінгу – коли швидкість з якою картка входить до терміналу змінюється і не є постійною, що є важливим для вдалого зчитування інформації скімінговими пристроями. Також, картка примусово рухається зад і вперед під час зчитування. Ще один спосіб боротьби зі скімінгом отримав назву Magneprint, що полягає в використанні притаманної тільки для даної магнітної стрічки унікальної характеристики «шуму» для диференціювання поміж справжньою картою та її клоном.

В процесі еволюції боротьби зі скімінгом, на шляху до впровадження технології EMV (Europay, MasterCard and Visa), була використана технологія «Chip and PIN system», мета якої полягає в ідентифікації і підтвердженні власника картки за допомоги мікрочипу, що розміщується на платіжній картці. Додатково фінансові установи використовують програмне забезпечення і проводять моніторинг транзакцій на рахунок, розміру та географії витрат, встановлюють обмеження на суму транзакції.

Одним із дієвих напрямків боротьби зі скімінгом є перехід на мікропроцесорні пластикові картки (EMV-технологія) і відмова від магнітної стрічки. На даний час процес остаточного переходу на чипові технології не завершився, термінали працюють комбіновано і приймають магнітні стрічки, що ісприяє скімінгу. В таких умовах для боротьби з проблемою підробки картки із забезпеченням збереження ПІН-коду (колізловмисник з різних причин не володіє ПІН-кодом) полягає у використанні виробниками і власниками терміналів удосконалених і більш захищених способів оновлення сесійних ключів в алгоритмі 3DES (стандарт ANSI X9.24) та шифрування даних для ПІН-коду (стандарт ANSI X9.8). Як відомо, передавання даних ПІН-блоку від терміналу до хостової системи банку відбувається у зашифрованому вигляді. Найбільш захищеним на даний час вважається алгоритм шифрування 3DES який і має використовуватись у процесінгових системах банків.

Таким чином, ефективним способом викорінення скімінгу є глобальний перехід банківської системи на EMV-картки та невикористання магнітної стрічки для запису і зчитування інформації.

#### **Література:**

1. Про затвердження Типологій легалізації (відмивання) доходів, одержаних злочинним шляхом, у 2013 році : наказ Держ. служби фінанс. моніторингу від 25 груд. 2013 р. № 157 [Електронний ресурс]. – Режим доступу: [http://cct.com.ua/2014/25.12.2013\\_157.htm](http://cct.com.ua/2014/25.12.2013_157.htm).
2. Schmidt L. Warning signs [Електронний ресурс] / Lucinda Schmidt. – Режим доступу: <http://moneymanager.smh.com.au/articles/2003/10/15/1065917445606.html>
3. Wisconsin Bankers Association Warns Consumers, Asks for Help In Identifying ATM Card Skimming Scam [Електронний ресурс]. – Режим доступу: [http://www.wisbank.com/Media/Press%20Releases/PR\\_ATM\\_Card\\_Skimming\\_Scam.htm](http://www.wisbank.com/Media/Press%20Releases/PR_ATM_Card_Skimming_Scam.htm).
4. Costa C. MasterCard International Hosts First Global Risk Management Symposium [Електронний ресурс] / Christina Costa. – Режим доступу: <http://www.mastercardintl.com/cgi-bin/newsroom.cgi?id=706>.

#### **Кібербезпека як один з факторів забезпечення національної безпеки держави**

**Гітрук О.О.**

курсант Херсонського факультету  
Одеського державного університету внутрішніх справ

**Бараненко Р.В.**

кандидат технічних наук, доцент  
Херсонського факультету  
Одеського державного університету внутрішніх справ

У сучасному світі все більше виробництв і послуг спираються на інформаційні технології. Виробництво й постачання енергії, очищення і постачання питної води, керування транспортом, освітлення міст, зв'язку, доступ людей до інформації, охорона здоров'я, оплата товарів і послуг, волевиявлення під час виборів і референдумів, і навіть електронне урядування – все це реалії нашого життя. Людство сьогодні залежить від безперервності та коректності функціонування комп'ютерних систем як об'єктів критичної інфраструктури, й атаки з боку та засобами кіберпростору на такі системи спричиняють реальні загрози для безпеки людей і суспільства.

*Кібербезпека* – це безпека інформації та інфраструктури в цифровому середовищі, що її забезпечує. Кібербезпека передбачає досягнення і збереження властивостей безпеки в ресурсах організації або користувачів, що спрямовані на запобігання відповідним кіберзагрозам.

В залежності від виду загроз кібербезпеку можна розглядати як забезпечення стану захищеності особистості, суспільства, держави від впливу неякісної інформації; інформації та інформаційних ресурсів від неправомірного впливу сторонніх осіб; інформаційних прав і свобод людини й громадянина.

В інформаційному праві інформаційна безпека – це одна із сторін розгляду інформаційних відносин у межах інформаційного законодавства з позицій захисту життєво важливих інтересів особистості, суспільства, держави та акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами [1].

До суб'єктів інформаційної безпеки відносяться: держава, що здійснює свої функції через відповідні органи; громадяни; суспільні або інші організації і об'єднання, що володіють повноваженнями по забезпеченню інформаційної безпеки у відповідності до законодавства [2].

У першу чергу загрози інтересам держави також можуть проявлятися у вигляді отримання протиправного доступу до відомостей, що складають державну таємницю, до іншої конфіденційної інформації, розкриття якої може нанести збитки державі. Проте найбільш небезпечними джерелами загроз інтересам держави в інформаційному суспільстві може стати неконтрольоване розповсюдження інформаційної зброї.

Поняття інформаційної зброї визначається як сукупність засобів, методів і технологій, що забезпечують можливість силового впливу на інформаційну сферу протилежної сторони з метою руйнування її інформаційної інфраструктури, системи управління державою, зниження духовного потенціалу суспільства.

Серед найбільш серйозних завдань, які можуть вирішуватися за допомогою сучасної інформаційної зброї, можна виділити наступні [3]: створення атмосфери бездуховності та аморальності, негативного відношення до культурної спадщини противника; маніпулювання суспільною свідомістю та політичною орієнтацією соціальних груп населення держави з метою створення політичної напруги та хаосу; дестабілізація політичних відносин між партіями, об'єднаннями та рухами з метою провокації конфліктів, розпалювання недовіри, загострення політичної боротьби, провокування репресій проти опозиції, провокація взаємного знищення; зниження інформаційного забезпечення влади та управління, інспірація помилкових управлінських рішень; дезінформація населення про роботу державних органів, підрив їхнього авторитету, дискредитація органів управління; провокування соціальних, політичних, національних і релігійних сутичок; ініціювання страйків, масових заворушень та інших акцій економічного протесту; ускладнення прийняття органами важливих рішень; підрив міжнародного авторитету держави, її співробітництва з іншими країнами; нанесення втрат життєво важливим інтересам держави в політичній, економічній, оборонній та інших сферах.

Руйнівний вплив інформаційної зброї в інформаційному суспільстві може бути більш потужним та ефективним, ніж це уявляється зараз. Це є особливо небезпечним в умовах жорсткого протистояння нашої країни ворожій агресії Російської Федерації.

Сьогодні в Україні найбільше від кібератак страждають впливові медіа, фінансові інститути та державні установи. При цьому зростає не тільки кількість атак на інформаційну інфраструктуру, але і їх складність. Зловмисники використовують різні види атак: фізичні (атаки на телевізійні вежі), DDoS-атаки (на сайти Центрвиборчкому, Верховної Ради та ключових ЗМІ), зломи інформаційних ресурсів (сайту ЦВК, електронних скриньок політиків і журналістів), атаки на мобільні мережі (перехоплення переговорів мобільного зв'язку) [4].

Найбільшим позитивним моментом є затвердження «Стратегії кібербезпеки України» [5], що регулює основні положення у сфері реалізації державної політики з цього питання.

Незважаючи на це ситуація у сфері вітчизняної кібербезпеки характеризується наявністю суттєвих проблем [6]:

1) незадовільне кадрове забезпечення відомств відповідними фахівцями у сфері інформаційної безпеки. Якість підготовки фахівців за різноманітними спеціальностями сфери інформаційної безпеки багато в чому є незадовільною. Існує брак матеріальних і нематеріальних стимулів для залучення висококласних фахівців (молодих спеціалістів) до структур, задіяних у забезпеченні безпеки вітчизняного кіберпростору;

2) незважаючи на зусилля спеціальних відомств Україна досі залишається вразливою в кіберпросторі. Актуальною є проблема створення національної операційної системи (принаймні для використання у системі органів державної влади), відновлення вітчизняних потужностей з виробництва

матеріально-технічної телекомунікаційної бази (особливо для потреб закритих відомчих інформаційних систем), стимулювання з боку держави створення національного антивірусу.

В умовах жорсткого протистояння з кіберпідрозділами країни-агресора першочергову значимість також має завдання захисту об'єктів критичної інфраструктури, до якої експерти відносять енергетичні та транспортні магістральні мережі, нафто- й газопроводи, морські порти, канали швидкісного та урядового зв'язку, системи життєзабезпечення (водо- й теплопостачання) мегаполісів, утилізації відходів, служби екстреної допомоги населенню та служби реагування на надзвичайні ситуації, високотехнологічні підприємства й підприємства військово-промислового комплексу, а також центральні органи влади. Захист критичної інфраструктури ствердився як важливий напрям політики у сфері безпеки країн-членів ЄС і НАТО [7].

Необхідність забезпечення безпеки об'єктів критичної інфраструктури може спричинити певні юридичні проблеми, пов'язані з тим, що значна частина цих об'єктів може перебувати в приватній власності, отже, правоохоронні органи можуть не мати можливості законно (в моніторинговому режимі) отримувати відомості про їх стан, параметри безпеки (характер програмного забезпечення, рівень захищеності тощо), що можуть бути критично важливими при забезпеченні їх безпеки на державному рівні.

Питання цивільної та військової безпеки у кіберпросторі останнім часом дедалі більше ототожнюються. Під тиском військових чинників в Україні й світі спостерігається тенденція до напрацювання норм національного та міжнародного права, які не лише регулюють поведінку різних державних та недержавних, військових та невійськових суб'єктів у кіберпросторі, а й безпосередньо стосуються тих специфічних ситуацій, що окреслюються поняттям «кібервійна».

Тому Україні доречно продовжити активні кроки на шляху розбудови власної системи кібербезпеки. На думку експертів [6] доцільно пришвидшити підготовку та подальше прийняття Верховною Радою України Законопроекту про кібернетичну безпеку України, варто розглянути можливість внесення до Закону України «Про інформацію» поняття «інформація про об'єкти критичної інфраструктури» з метою забезпечення правоохоронних органів (зокрема Єдиної загальнодержавної системи протидії кіберзлочинності) необхідною інформацією про стан об'єктів критичної інфраструктури, що перебувають у приватній власності.

#### **Література:**

1. Литвиненко О. Інформація і безпека / О. Литвиненко // Нова політика. – 1998. – № 1. – С. 47-49.
2. В.В. Лук'янова, А.Ю. Лаутар Інформаційна безпека в умовах розвитку інформаційної системи // Вісник Хмельницького національного університету. – 2013. – № 2. Т. 3. – С. 97-101.
3. [https://uk.wikipedia.org/wiki/Інформаційна\\_війна](https://uk.wikipedia.org/wiki/Інформаційна_війна)
4. Степаненко О.П. Формування системи інформаційної безпеки в банківському секторі України / О.П. Степаненко // Моделювання та інформаційні системи в економіці : зб. наук. пр. – 2015. – Вип. 91. – С. 17-35.
5. Указ Президента України № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» від 15.03.2016.
6. Дубов Д.В., Ожеван М.А. Кібербезпека: світові тенденції та виклики для України. – К.: НІСД, 2011. – 30 с.
7. Бірюков Д.С. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні / Д.С. Бірюков, С.І. Кондратов. – К.: НІСД, 2012. – 96 с.

#### **Щодо сучасного стану інформаційно-аналітичного забезпечення початкового етапу досудового розслідування та перспективи його розвитку**

**Бухонський С. О.**

аспірант кафедри кримінального  
процесу та криміналістики КПУ,  
завідувач сектору

Херсонського науково-дослідного  
експертно-криміналістичного центру МВС України,

На сьогодні інформація набуває визначального провідного фактора у всіх сферах життєдіяльності суспільства, стає його рушійною силою, що дозволяє констатувати створення "інформаційного суспільства". Головний зовнішній прояв інформаційного суспільства – це інтенсивне насичення всіх

його ланок і інституцій інформаційними продуктами та комп'ютерно-телекомунікаційними технологіями.

Виходячи із цього, можна припустити, що ці тенденції притаманні всім ієрархічним рівням управління суспільством і державою.

Останнім часом різко загострилася криміногенна обстановка в Україні. У зв'язку з цим дуже збільшився потік інформації, що надходить на адресу правоохоронних органів, зросла кількість управлінсько-розпорядчих й інших документів, які потребують негайного реагування та виконання. Збільшився обсяг ручних довідкових картотек та існуючих банків даних, які досягли тієї межі, коли наявні технічні засоби і технології не дозволяють оперативної та доброякісної обробляти інформацію, що надходить.

Уведення в дію нового Кримінального процесуального кодексу України ініціювало перетворення інформаційно-аналітичне забезпечення ОВС у цілісну систему, спрямовану на узагальнення результатів їхньої діяльності.

Інформаційне забезпечення органів внутрішніх справ України є одним із пріоритетних завдань, що поставили на сучасному етапі їхнього розвитку та вимагають більш інтенсивного використання криміналістичних обліків, своєрідність яких полягає в тому, що інформація в них формується за допомогою експертів-криміналістів із використанням сучасної криміналістичної техніки й технологій. Також на їхній основі проводяться дослідження з метою підтвердження результатів узагальненої цими обліками інформації, актуалізації її як доказів.

У цьому плані, метою даної роботи є визначення основних напрямів аналізу та узагальнення сучасного стану роботи органів МВС України з обліковою інформацією, актуальність яких обумовлена постійним удосконаленням криміналістичної техніки і комп'ютерних технологій та їхнього впровадження в практичну діяльність ОВС і, зокрема, розслідування злочинів.

Конкретним завданням виступу є аналіз й удосконалення процесів упровадження методик використання новітніх досягнень науки і техніки, та розкриття нових можливостей роботи з обліковою інформацією, отриманої з місця події.

Використання сучасних комп'ютерних технологій, дозволяє фіксувати та обробляти інформацію в найкоротші строки, уникаючи складних лабораторних процесів.

Практикою накопичено позитивний досвід застосування комп'ютерних технологій для фіксації і обробки криміналістично значущої інформації та використання отриманих результатів під час розслідування злочинів [1, с. 3-4].

Основні методи сприйняття та фіксації інформації, що застосовуються під час розслідування злочину, аналогічні методам, що використовуються в інших сферах діяльності для виявлення й обробки різної за своєю фізичною природою інформації.

На шляху реалізації Концепції Національної програми інформатизації, а також: Наказу МВС України Про створення Інтегрованої інформаційно-пошукової системи органів внутрішніх справ України, інших [2-3] актуальне постійне вдосконалення роботи з обліковою інформацією, отриманої з місця події.

Перспектива у цьому напрямку нам убагацькається у тому, що за умов визначення базової для МВС України автоматизованої системи, всі інші системи повинні бути сумісними з базовою чи поступово доводитись до сумісності.

Аналіз практики засвідчує зазначають, що своєчасне отримання та узагальнення різноманітної інформації та статистичних даних є надзвичайно важливим у роботі з попередження злочинів та здійснення ефективного кримінального провадження, встановлення і розшуку злочинців. Раціональне на вміле використання автоматизованих баз даних створює необхідні умови отримати та ефективно скористатися необхідною інформацією.

У цьому контексті, нами, в своїх попередніх дослідженнях, були розроблені та запропоновані пропозиції щодо реформування та вдосконалення існуючої системи інформаційно-аналітичного забезпечення кримінального провадження – сформульована власна концепція "Автоматизованої системи криміналістичних обліків (кримінальної реєстрації)" [4].

Для узагальнення та апробації емпіричного матеріалу дослідження, нами були розроблені цільові анкети. За якими, Інститутом права імені Володимира Сташиса Класичного приватного університету, за темою: "Інформаційно-аналітичне забезпечення початкового етапу досудового розслідування" планується проведення відповідного анкетування різних сторін кримінального провадження (див. додаток – фрагмент примірника анкети).

Заплановано отримати відповіді на запитання у таких номінаціях: "Найефективніші (доцільні) способи збирання інформації", "Узагальнення типових способів збирання інформації щодо судових експертиз і криміналістичних досліджень", "Узагальнення видів обліку інформації з місця події, які

використовуються на практиці", "Типологія перспективних категорій об'єктів криміналістичних обліків", "Виокремлення видів обліків сучасної системи кримінальної реєстрації, які потребують автоматизації (комп'ютеризації) за допомогою створення відповідного програмного забезпечення", "Узагальнення видів обліків, які є найбільш інформаційними для проведення експертиз і спеціальних досліджень", "Шляхи покращення системи кримінальної реєстрації", "Узагальнення та виокремлення категорій злочинів (і злочинців) криміналістичні обліки за якими відсутні", "Пропозиції стосовно систематизації існуючих обліків", "Визначити, які категорії працівників ОВС матимуть право доступу до відповідних обліків", "Узагальнення особливостей використання в кримінальному провадженні інформації, отриманої з різних обліків" тощо.

На завершення зазначимо, що подальше вдосконалення Системи дозволить оптимізувати: роботу з криміналістичними та іншими обліками; поліпшить взаємодію окремих підрозділів ОВС та поліції, на всеукраїнському та міжнародному рівнях, та з іншими державними інституціями.

### **Література:**

1. Бирюков В.В. Научные и практические основы использования компьютерных технологий для фиксации криминалистически значимой информации: Монография (МВД Украины, Луган. акад. внутр. дел МВД имени 10-летия независимости Украины; Науч. ред. канд. юрид. наук, доц. И.В. Попов). – Луганск: РИО ЛАВД, 2002. – 264 с.
2. Про Національну програму інформатизації: Закон України від 04.02.98 № 74/98-ВР // Відомості Верховної Ради України. – 1998. - № 27-28. - С. 181; 2002. - № 1. – С. 3.
3. Про Концепцію Національної програми інформатизації: Закон України від 04.02.98 № 75/98-ВР // Відомості Верховної Ради України. – 1998. - № 27-28. - С. 182.
4. «Актуальні напрями вдосконалення інформаційно-аналітичного забезпечення кримінального провадження (автоматизована система криміналістичних обліків)» – Міжнародний науковий журнал Вищого навчального закладу Словацької Республіки «Пан'європейський університет» «Visegrad journal on human rights». – №2/2. - 2016. – 177 с.

### **Д о д а т о к**

Дослідження проводить кафедра кримінального процесу та криміналістики Інституту права імені Володимира Сташиса Класичного приватного університету. Тема: «Інформаційно-аналітичне забезпечення початкового етапу досудового розслідування»

### **А н к е т а (фрагмент)**

(окремо для: слідчих, прокурорів, суддів, експертів, поліцейських та викладачів)

*Пропонуємо Вам висловити свою думку з наступних питань:*

1. Регіон \_\_\_\_\_
2. Місце роботи (звання, посада) \_\_\_\_\_
3. Стаж роботи (за спеціальністю) \_\_\_\_\_
4. Наявність допусків для участі у процесуальних дій \_\_\_\_\_
5. Якими способами Ви збираєте докази:
  - 5.1. опитуванням: очевидців події, свідків, сусідів, родичів, колег потерпілого/потерпілої, зацікавлених осіб, осіб, які обізнані з чужих слів, спеціалістів у певній галузі, експрес-дослідження, фото/аудіо/відео запис тощо;
  - 5.2. допитом: підозрюваного, обвинуваченого, потерпілого, свідка, експерта;
  - 5.3. оглядом, виявленням, дослідженням, зберіганням речових доказів;
  - 5.4. оглядом, зберіганням, вилученням, дослідженням документів, які містять ознаки речових доказів;
  - 5.5. інше \_\_\_\_\_
6. Якими способами Ви збираєте докази щодо експертиз і досліджень під час:
  - 6.1. прийняття рішення про призначення судової експертизи (дослідження), про задоволення клопотання про проведення експертизи;
  - 6.2. проведення експертизи;

6.3. розгляду клопотань експертів (про недостатність досліджувального матеріалу, його непридатність, встановлення строків, витребування нових матеріалів; про необхідність уточнення питань, поставлених експерту; можливість відповіді на додаткові запитання; про необхідність залучення інших фахівців, проведення комплексної чи комісійної експертизи; про необхідність експертом ознайомитися з іншими матеріалами справи; про неможливість відповіді на питання, що виходять за межі спеціальних знань експерта; під час допиту експерта (в тому числі, допит іншою стороною в якості експерта особи, яка під час дачі показань, висловила думку або висновок, що ґрунтується на спеціальних знаннях, якщо суд не визнав їх допустимими доказами)

7. Які види обліку інформації з місця події Ви застосовуєте на практиці? (постійно, часто, не часто, не застосовую) \_\_\_\_\_

8. Якими категоріями об'єктів Ви б доповнили криміналістичні обліки?

### **Кібератаки та кібертероризм: поняття та особливості реалізації атак в кіберпросторі**

**Касюк О.О.**

слухач магістратури факультету № 1  
Одеського державного університету внутрішніх справ

**Романов О.Д**

фахівець відділу організації аналітичної роботи та контролю  
Одеського державного університету внутрішніх справ

Злочинні дії з організації різного роду кібератак, несанкціонованого доступу до чужих сайтів, створення «сайтів-двійників» вийшли за межі тих країн, які за темпами зростання значно випереджають та переважають інші види організованої злочинності. Більш того, останніми роками кібератаки отримали істотну фінансову підтримку та високоякісні комунікації, охопивши всі види злочинів, скоєних у інформаційно-телекомунікаційній сфері [1]. Проте й досі немає чіткого визначення відповідних понять, зокрема й такого поняття, як «кібератака». З огляду на це, Д. Дубов і М. Ожеван кваліфікують «кібератаку» як цілеспрямовану дію, що реалізується в кіберпросторі за допомогою технічних можливостей цього простору та призводять до досягнення несанкціонованих цілей, таких як, порушення конфіденційності, цілісності, авторства, доступності інформації, деструктивних інформаційно-психологічних впливів на свідомість та психічний стан громадян [2; 3].

С. Мельник, О. Тихомиров та О. Ленков розглядають «кібератаку» як результат використання технічних недоліків механізмів безпеки сучасного кіберпростору з метою дезорганізації роботи його елементів [2]. Узагальнюючи вищезазначене, можна сформулювати наступне визначення поняття «кібератаки». «Кібератака» - це сукупність узгоджених щодо мети, змісту та часу дій або заходів - так званих кіберакцій, спрямованих на певний об'єкт впливу з метою порушення конфіденційності, цілісності, доступності, спостережуваності або авторства інформації, що циркулює в ньому, з урахуванням її уразливості, а також порушення роботи ІТ-систем і мереж зазначеного об'єкта [1].

Характерною особливістю кібератак є миттєвість їх здійснення. Звідси слід виокремити основні ознаки кібератаки, серед яких:

1. За метою впливу на об'єкт атаки. Цей вплив може бути спрямований, наприклад, на порушення цілісності або конфіденційності інформації, її захищеності від несанкціонованого доступу а також на порушення живучості системи та надійності її функціонування.

2. За принципом впливу на об'єкт атаки:

- із використанням прихованих каналів (шляхів передавання інформації, що дозволяють двом процесам обмінюватися нею у спосіб, який порушує політику безпеки;
- застосування прав суб'єкта системи до об'єкта (файлів даних, каналів зв'язку тощо).

3. За характером впливу на об'єкт атаки:

- активний вплив (користувач виконує деякі дії, що виходять за рамки його обов'язків і порушують наявну політику безпеки, наприклад розкриття пароля);
- пасивний вплив (користувач прослуховує лінії зв'язку між двома вузлами мережі).

4. За способом впливу на об'єкт атаки, зокрема на систему дозволів (захоплення привілеїв), а також безпосередній доступ до даних, програм, служб, каналів зв'язку з використанням привілеїв та інші.

Також набула поширення класифікація, запропонована компанією Internet Security Systems Inc. Скоротивши кількість можливих категорій кібератак до п'яти, фахівці компанії умовно виокремили з них такі, що мають на меті:

1. сприяти збору інформації;
2. сприяти спробам несанкціонованого доступу до інформації;
3. досягти стану відмови в обслуговуванні;
4. імітувати підозрілу активність;
5. чинити вплив на операційні системи.

Найбільш поширеними способами здійснення кібератак, наприклад, П.Нойман вважає сніфер пакетів та IP-спуфінг, DoS і DDoS атаки, паролльні атаки, атаки на рівні додатків типу логічних бомб і троянських коней, вірусні атаки й так звані ін'єкції.

Сніфер пакетів - це програма, яка використовує мережний інтерфейс, функціонуючи в так званому нерозбірливому режимі. Вона перехоплює мережний трафік, призначений для інших вузлів, та здійснює його подальший аналіз. Застосування програми дає змогу виявити паразитний, вірусний і за кільцьований трафік; перехопити будь-який призначений для користувача незашифрований, а іноді й зашифрований трафік із метою отримання паролів та іншої інформації; локалізувати несправність мережі або помилку конфігурації мережних агентів [3].

Представники інституту System Administrator and Network Security (США) та Центру із захисту національної інфраструктури при ФБР (США) зробили спільну заяву про те, що здійснення кібератак поступово стає потужним засобом ведення інформаційних воєн між державами, а мережа Інтернет - незамінним «інструментом кіберпланування» [4], яка забезпечує сучасним терористам анонімність, можливість керувати і координувати дії при підготовці та здійсненні терактів. Тобто, згідно із [4; 5] та твердженням інших фахівців, тероризм останнім часом зробив якісний крок у своєму розвитку й еволюціонує в напрямку, який можна назвати «мережною війною».

Такий стан справ призвів до появи принципово нового різновиду терористичних дій у віртуальному просторі – «кібертероризму». Власне, як термін це поняття в ІТ-лексиконі з'явилося приблизно в середині 1980-х років. Саме тоді один із наукових співробітників США Беррі Колін уперше впровадив його в офіційний обіг. Згідно з Конвенцією Ради Європи 2001 року щодо кіберзлочинів, засобами кібертероризму можуть виступати комп'ютерна система, комп'ютерні дані а також дані трафіку.

Кібертероризм - це суспільно-небезпечна діяльність, що свідомо здійснюється в кіберпросторі (або з використанням його технічних можливостей) окремими особами або організованими групами з терористичною метою та реалізується ними через заздалегідь сплановані й політично вмотивовані кібератаки на ІТС з використанням високих технологій.

Власне спектр впливу кібертероризму є достатньо широким - від нав'язування хибних рішень або панічних настроїв до проникнення в канали й системи зв'язку та навігації. Результатом таких дій може бути, наприклад, введення хибного IP або порушення цілісності роботи критично важливих елементів інформаційної або кібернетичної інфраструктури держави, ускладнення міжнародних відносин або інші негативні наслідки, що створюють небезпеку для життя і здоров'я населення. Тим самим головними особливості кібертероризму є:

- висока ефективність кібератак;
- просторово-часова невизначеність джерела кібератаки та його віддаленість від об'єкта атаки;
- часова невідповідність між власне кібератакою та процесом її підготовки;
- можливість організації складних кібератак одночасно на різні ІТС із різних напрямів тощо.

Кібератаки та кібертероризм як головні складові кіберзлочинності посідають не останнє місце серед низки загроз національній безпеці та інтересів України. Їх поширення активно впливають на:

- здатність молоді швидко опановувати технічні новинки, про які ще вчора вони не мали жодного уявлення;
- темпи комп'ютеризації (кількість комп'ютерів в Україні щорічно подвоюється) та стрімке збільшення кількості інтернет-користувачів.

Таким чином, кібератаки та кібертероризм на сьогодні є одними з головних загроз, що зустрічаються в інформаційно-телекомунікаційній системі. Виокремлення різновидів та особливостей кібератак і кібертероризму дає більш чітку регламентацію властивостей, притаманним даним явищам. Для кожної держави, яка піклується про безпеку інформаційного простору як у середині держави так і за її межами, забезпеченні захисту даних, одним з головних напрямків організації та координації зусиль у протидії кіберзлочинам є впровадження стійкого механізму для кіберзахисту власної ІТ-



інфраструктури, протистоянню фізичному руйнуванню технічних засобів, дезорганізації роботи інформаційних систем та мереж, а також запобігання порушення функціонування об'єктів нападу.

### **Література:**

1. Бурячок, В.Л. Основи формування державної системи кібернетичної безпеки: монографія / В. Л. Бурячок. - К.: НАУ, 2013. - 432 с.
2. Гнатюк, С. О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи / С.О. Гнатюк// Безпека інформації.— 2013.— Т. 19, № 2.— С. 118–129.
3. Дубов Д.В. Кібербезпека: світові тенденції та виклики для України / Д.В. Дубов, М.А. Ожеван. - К.: НІСД, 2011. - 30 с.
4. Бутузов, В.М. Протидія комп'ютерній злочинності в Україні (системно структурний аналіз): монографія / В.М. Бутузов.— К.: КІТ, 2010.— 145 с.
5. Старостина Е. Терроризм и кибертерроризм — новая угроза международной безопасности // [Електронний ресурс]. - Режим доступу: <http://www.crime-research.ru/articles/starostina>

### **Проблеми розслідування злочинів щодо порушення авторського права на комп'ютерні програми**

**Ігнатушко Ю.І.**

кандидат юридичних наук  
доцент кафедри інформаційних технологій  
Національна академія внутрішніх справ

Актуальною проблемою сьогодення учасників відносин у сфері використання комп'ютерного програмного забезпечення є його правовий захист.

Відносна новизна виниклих проблем, стрімке нарощування процесів комп'ютеризації суспільства ставлять перед правоохоронними органами складні питання боротьби з цим новим соціально-правовим явищем і зокрема проблему виявлення та розслідування злочинів щодо порушення авторського права на комп'ютерні програми.

Відповідно до Закону України «Про авторське право і суміжні права» і Бернської конвенції «Про охорону літературних і художніх творів», комп'ютерні програми охороняються як літературні твори.

Така охорона поширюється на комп'ютерні програми незалежно від способу чи форми їх вираження [1].

Розвиток комп'ютерної техніки та інформаційних технологій призвели до появи «комп'ютерних злочинів». Найчастіше вони трактується як злочини, що пов'язані з електронно – обчислювальною технікою (ЕОМ) та порушенням авторського права на комп'ютерні програми (програмні продукти).

Комп'ютерні злочини, як правило, мають економічне підґрунтя. Такі злочини спрямовані на отримання програм обробки даних, результатів науково – конструкторських досліджень, відомостей про збут продукції, баз даних тощо.

Комп'ютерні програми є об'єктом авторського права й охороняються як літературні твори[2, с. 17].

Встановлення авторської - правової охорони на національному рівні автоматично означає і міжнародну охорону комп'ютерних програм.

На сьогоднішній день в Україні сформовано законодавчу базу щодо створення, відтворення, розповсюдження комп'ютерних програм, визначено основні вимоги щодо розпорядження майновими правами на них та суворе покарання за неправомірне їх використання [3, с. 53].

Порушенням авторського права можуть бути наступні дії:

- тиражування та поширення примірників комп'ютерних програм на носіях інформації без дозволу власника авторських прав;
- незаконне поширення програмних продуктів через телекомунікаційні мережі (електронна пошта, Інтернет, тощо);
- продаж комп'ютерної техніки разом з незаконно встановленим програмним забезпеченням.

Одним з найефективніших методів виявлення та документування незаконної діяльності з тиражування і поширення контрафактної продукції є контрольна закупівля, що включає комплекс оперативно – розшукових дій які забезпечують придбання продукції з ознаками контрафактності та подальше її вилучення і направлення для дослідження.

Необхідно здійснити заходи щодо виявлення та вилучення предметів правопорушення (матеріальні носії з записаними контрафактними комп'ютерними програмами), ліцензійних договорів, ліцензій на комп'ютерні програми, голографічних сертифікатів підтвердження справжності (ліцензійності) комп'ютерних програм та інших матеріалів, які спеціально використовувались для виготовлення контрафактних примірників програм.

Як показує практика, бувають випадки коли продавець контрафактний примірників комп'ютерних програм стверджує, що не знав, що товар – контрафактний, що він вважав, що якщо є накладна на компакт-диски, то вони ліцензійні, тому необхідно критично оцінювати його твердження.

Подібного роду заяви затриманого розповсюджувача контрафактної продукції є спробою ухилитися від адміністративної або кримінальної відповідальності.

Щоб спростувати такі неправдиві твердження, необхідно отримати і документально зафіксувати наступні дані:

- встановити коли та на яких посадах правопорушник працював раніше, чи мав він за своєю роботою чи фахом відношення до інформаційних технологій;
- з'ясувати, чи був ознайомлений правопорушник з нормативними актами, що регламентують порядок продажу окремих видів товарів, зокрема з вимогами законодавства про захист права споживачів, якщо так, то як продавець інформував споживачів про походження товару, визнаного контрафактним;
- з'ясувати, чи притягувалася дана особа до адміністративної чи кримінальної відповідальності за правопорушення пов'язані з обігом контрафактної продукції або порушень правил торгівлі.

У випадку, коли особа, яка використовувала неліцензійні комп'ютерні програми, стверджує, що не знала, що використовувана нею програма є неліцензійною, потрібно враховувати, що така ситуація дійсно можлива при введенні користувача в оману продавцем програмного забезпечення чи комп'ютерної техніки з встановленим програмним забезпеченням.

У тих випадках, коли користувачем було укладено договір з організацією чи фізичною особою на встановлення і технічне супроводження комп'ютерних програм, які згодом виявляються контрафактним, всю повноту відповідальності буде нести продавець такого неліцензійного програмного забезпечення, якщо не буде доведено, що мала місце попередня змова сторін з метою мінімізації витрат, необхідних для придбання легальних ліцензійних комп'ютерних програм.

Бувають випадки, коли керівництво підприємства, організації стверджує, що не знало що співробітниками організації використовують неліцензійні комп'ютерні програми. Проте, про операційні системи та спеціальне програмне забезпечення (програми обліку, системи проектування тощо) керівництво та бухгалтер підприємства знати зобов'язані, хоча б з тієї причини, що всі легально придбані програмні продукти повинні бути поставлені на баланс.

Як загальний висновок треба зазначити, що використання і впровадження сучасних інформаційних технологій привело до появи нових видів злочинів, зокрема, до порушень роботи автоматизованих систем і несанкціонованому доступу до комп'ютерної інформації, порушення авторського права. По своєму механізму, способам вчинення ці злочини мають визначену специфіку, яка характеризується високим рівнем латентності і низьким рівнем розкриваємості, а окремі види таких злочинів мають транснаціональний характер.

Підсумовуючи сказане, слід зазначити, що система і структура сучасного правового регулювання використання комп'ютерного програмного забезпечення потребує певного вдосконалення механізму державного контролю, одним з аспектів якого є забезпечення пріоритету закону.

### **Література:**

1. Про авторське право і суміжні права: Закон України // Відомості Верховної Ради України. – 1994. – № 13. – 64 с.
2. Дмитришин В. С. Інтелектуальна власність на програмне забезпечення в Україні / В. С. Дмитришин, В. П. Бережанська. – К. : Вірлен, 2005. – 312 с.
3. Інформаційні технології в правозастосовній практиці : навч. посіб. / В. Г. Хахановський, В. А. Кудінов, В. М. Смаглюк. – К. : Нац. акад. внутр. справ, 2015. – 112 с.

**Ком'яга А.В.**

старший викладач кафедри  
спеціальної та фізичної підготовки  
Одеського державного університету внутрішніх справ

Розвиток сучасного світового простору, на сьогоднішній день, характеризується впровадженням в усі сфери функціонування суспільства нових інформаційно-телекомунікаційних технологій, що мають великий вплив на усі аспекти життєдіяльності суспільства і держави.

Роль інформаційної сфери, актуальність якої невпинно зростає, активно впливає на стан політичної, економічної, військової та інших складових держави. Тому інформаційна безпека набуває великого значення у загальній системі забезпечення інтересів суспільства і держави.

Широкий спектр проблем забезпечення інформаційної безпеки особи, суспільства і держави, розвитку інституту кібербезпеки, забезпечення недоторканності приватного життя і захисту прав людини на доступ до інформації, захисту інформаційних систем, ресурсів і мереж, розширення застосування інформаційних технологій у державному управлінні та при наданні державних послуг, а також інші проблеми інформаційної безпеки потребують системного правового регулювання на основі ретельного аналізу чинного законодавства України та світової правозастосовної практики.

Так, проблемою сучасного суспільства постає глобальне перенесення соціальною, економічною та політичною активності окремих індивідів у кіберпростір, який, в свою чергу, стає складовою частиною модернізованого суспільства, а отже і потребує відповідного адміністративно-правового регулювання відносин, що виникають у зазначеній сфері.

Питанням правового регулювання кібербезпеки в Україні, присвячено наукові праці таких вчених: В.М. Бутузова, С.В. Демедюка, О.В. Орлова, О.О. Тихомирова та ін.

Для вирішення питань, які є актуальними, щодо кіберпростору та забезпечення кібербезпеки в нашій державі, необхідно визначити ключові поняття, які зможуть дати орієнтир в побудові превентивних заходів.

Як відомо, суспільство характеризується певним ступенем організованості та упорядкування, що вимагає узгодження потреб, та інтересів окремої людини та співтовариства людей [1], тому, відповідно, суспільство повинно здійснювати адміністративно-правове регулювання відносин, у тому числі, у сфері забезпечення та організації кібербезпеки.

Варто зазначити що особливо актуальним і важливим сьогодні стає уточнення адміністративно-правового статусу такого елементу механізму адміністративно-правового регулювання забезпечення кібербезпеки в Україні, як правові засади регулювання відносин у сфері кібербезпеки, оскільки розвиток суспільних відносин у зазначеній сфері явно випереджає розвиток права й виявляються тенденції формування «подвійного стандарту», коли норм закону потрібно дотримуватися, але тільки не в мережі [2, с. 138].

Законодавство держави повинно бути однозначним, проте сучасний стан чинного законодавства дещо відстає від темпів розвитку сучасності, в першу чергу це стосується розвитку інформаційно-телекомунікаційних систем, тому у виключних випадках органам державної влади доводиться звертатись до світового законодавства, що значно відрізняється від законодавства України. Проте є актуальним для сьогоднішнього стану розвитку кіберзлочинності та забезпечення кібербезпеки.

Так, щодо діючого законодавства у даній сфері діяльності, актуально зауважити, що правовою основою є норми Конституції України, зазначені й інші закони України, міжнародні договори, згода на обов'язковість яких надана Верховною Радою України [3].

Окремі, важливі аспекти адміністративно – правового регулювання кібербезпеки в Україні, відображено в правових нормах законодавчого рівня, наприклад: Закон України «Про Державну службу спеціального зв'язку та захисту інформації» від 23 лютого 2006 року, «Про державну таємницю» від 21 січня 1994 року тощо.

Підзаконний рівень адміністративно-правового регулювання кібербезпеки складають нормативно-правові акти Президента України, Верховної Ради України, Кабінету Міністрів України, Ради національної безпеки та оборони України, та ін.

Так, наприклад нормами Указу Президента України «Про рішення Ради національної безпеки і оборони України» від 8 червня 2012 року, «Про нову редакцію Воєнної доктрини України» від 8 червня 2012 року, у якості кіберзагроз воєнно-політичній обстановці у світі визначено поширення кібертероризму, кібернетичних атак та ядерну, хімічну промисловість, оборонно-промисловий комплекс, об'єкти, на яких зберігається озброєння, військова техніка та боєприпаси, інших потенційно

небезпечних об'єктів, які Україна вважає намірами або діями інших держав такі дії, що створюють умови для виникнення воєнного конфлікту та застосування воєнної сили проти неї. [4].

Окрім цього важливим нормативно-правовим актом щодо регулювання забезпечення та організації кібербезпеки в Україні слід віднести один з актів Кабінету Міністрів України, а саме «Про схвалення Стратегії розвитку інформаційного суспільства в Україні» від 15 травня 2015 року.

Дані нормативно – правові акти, різного рівня юридичної сили, дають змогу зрозуміти, що органи державної влади прикладають чимало зусиль для забезпечення належного рівня кібербезпеки в нашій державі. І, незважаючи на те, що розвиток науки і техніки на крок попереду, адміністративно – правове регулювання все ж таки впливає на рівень злочинності в кіберпросторі, а також має не аби який вплив у напрямку протидії кіберзлочинності в Україні.

### **Література:**

1. Алексеев С.С. Теория государства и права: [учебник для юр. вузов и факультетов] / Алексеев С.С. [Електронний ресурс]. – Режим доступу.: <http://www.lawbook.by.ru/theory/Alexeev/cont.shtml>.
2. Степанов В.Ю. Державна інформаційна політика: проблеми та перспективи: [монографія] / Ю.В. Степанов. –Х.: Ви-дво «С.А.М.», 2011. – 548с.
3. Про основи національної безпеки України: закон України від 19 червня 2003 року №964 // Відомості Верховної Ради України. – 2003. –№ 39. – Ст. 351.
4. Про державну таємницю: офіц. Текст Закон України від 21 січня 1994 року №3855 // Відомості ВРУ. – 1994. - № 16. – Ст. 93.

### **Проблеми визначення поняття адміністративного розсуду**

**Бааджи Н.А.**

викладач кафедри іноземних мов

Одеського державного університету внутрішніх справ

У сучасних умовах стрімкої правотворчої діяльності в Україні першорядного значення набуває проблема підвищення рівня захисту прав та свобод громадян. Особливе місце на шляху здійснення адміністративної реформи належить виробленню принципово нових механізмів, які дозволять максимально регламентувати діяльність правозастосовних органів. Існуюча система правозастосування в державному управлінні є недосконалою. Однією з багатьох причин є нечіткість та непрозорість процедур і критеріїв прийняття рішень у багатьох сферах суспільного життя, що уможливорює корупційні діяння зі сторони посадових осіб. Отже важливим суб'єктом правозастосування в данному випадку виступають органи публічної адміністрації, а їх діяльність на будь-якому етапі тісно пов'язана з застосуванням адміністративного розсуду.

Категорія «розсуд» у праві є багатоаспектною. Тому аналізуючи її вкрай важливо мати на увазі те, що вона відноситься до суб'єктивної сторони правомірної поведінки.

Причина із-за якої так важливо дослідження адміністративного розсуду у діяльності органів публічної адміністрації полягає в тому, що норми права дещо надмірно узагальнені, і на думку дослідника Р. Давіда призводить до того, що «норми не є більш достатньо надійним керівництвом для практики, але в той самий час норми повинні бути настільки узагальнені, щоб регулювати певний вид відносин, а не застосовуватись, подібно судовому рішення, лише в конкретній ситуації» [4, с. 70].

У вітчизняній доктрині, а також і в юридичній літературі в цілому досі не склалось єдиного підходу щодо визначення розсуду. Суперечності в науковій сфері щодо чіткого визначення поняття з'явилися давно та й досі тривають.

Тому в науковій літературі й досі спостерігається насторожене відношення до розсуду як об'єкта вивчення. В деякій мірі це пов'язано як із самими ознаками розсуду, так і небезпекою свавілля, яке досить часто асоціюється з ним.

А.А. Маліновський визначає розсуд як «вибір суб'єктом певної цілі та способів її досягнення або як можливість виражати свою волю та приймати рішення незалежно від волі інших осіб» [8, с. 102]. Але дане визначення є суперечливим, тому що правозастосовник завжди діє в інтересах громадянина, справа якого вирішується, а тому керівним елементом у вираженні волі правозастосовника повинен бути перш за все закон і, по-друге, суспільний інтерес. Також А.А. Маліновський виділяє два складових елемента розсуду, а саме: «розсуд за вибором суб'єктивного права, тобто розумова діяльність, в рамках якої здійснюється аналіз тих можливостей, які надає діюче законодавство для задоволення інтересу» та друга складова, яка «пов'язана з розумовою діяльністю з вибору варіантів поведінки, направленою на

задоволення свого інтересу в рамках конкретного суб'єктивного права» [8, с.102]. Але знову, інтерес, про який йдеться у визначенні дослідника не є суб'єктивним інтересом правозастосовника, а інтересом суспільним.

Як пише видатний російський правознавець П.І. Люблінський: «Громадяни боялися не розсуду судді, а його свавілля, вони протестують не проти влади судді визначати справедливість в окремих випадках, а проти надмірності її ставлення в залежність від неї основних прав громадянина [6, с. 2].

Питання щодо відокремлення понять «розсуд» та «свавілля» виникли досить давно, та не без причини. Ще імператор Юстиніан звертав увагу на те, що «люди, які проводили судові розгляди, навіть за існування різноманітних законів, використовували в судах лише де-які з них, тому судові справи розглядались більш волею судді, ніж авторитетом закону» [11, с. 11.].

В науковій літературі існують різноманітні визначення даного поняття. Наприклад, найпростіше визначення адміністративному розсуду дає Авер'янов В.Б., який визначає його, як надане органу виконавчої влади чи посадовій особі право самостійного вибору варіанту поведінки, рішення чи передбачуваного наслідку правової норми найбільш виразно виявляється через інститут адміністративного (або вільного) розсуду [2, с. 265].

зарубіжний дослідник А. Барак з цього приводу писав, що вільний розсуд — це повноваження, якими наділяється особа наділена владою, вибирати між двома або більше альтернативами, коли альтернатива законна. Отже, це вибір лише із законних альтернатив. Якщо законна альтернатива не закріплена нормою права, то і розсуду в даному випадку бути не може. Досить часто в своїй монографії «Судейское усмотрение» він звертається до неконкретності або колізій правових норм, неналежній кодифікованості адміністративного законодавства, наявності оціночних понять, і що найважливіше - низького рівня правової культури державних службовців [3].

В юридичній літературі прийнято вважати, що необхідність розсуду з'являється тоді, коли норма права не передбачає конкретного варіанту дій, а надає посадовим особам органів публічної адміністрації можливість вибору певної моделі поведінки (або ступеню свободи дій) при вирішенні певної підвідомчої справи [1, с. 265-266].

Наприклад, Лазарев Б.М. вважає, що розсуд – це термін для позначення визначеного законом ступеня оперативної самостійності органу держави у прийнятті рішення про те вступати, чи не вступати в дію у тому чи іншому випадку, у виборі моменту вступу в дію і найбільш доцільного, на переконання органу, вирішення питання з декількох допустимих законом варіантів. Розсуд, в даному розумінні, він розглядає як вольовий бік співвідношення доцільності та законності [5, с. 92], чим повністю співпадає в думці з відомим ізраїльським суддею та дослідником Аароном Бараком.

А в противагу Б. М. Лазарев зазначає: "Якщо б кожен крок органів був пов'язаний з настанням заздалегідь визначених наслідків, то ці органи були б неспроможні активно впливати на процеси, що відбуваються в житті, а їх діяльність в значній мірі втратила б творчий характер" [5, с. 94].

Також О. Лагода писав, що не слід вважати, що певна свобода чи самостійність посадової особи в виборі певного варіанту дії, керуючись законністю та доцільністю є суперечливим концепції «правової держави», говорячи про те, що закон є вищою мірою доцільності й протиставляти дані категорії неможливо [7, с. 109].

А дослідник Д. М. Чечот, і зовсім, визначив розсуд як право органу чи посадової особи приймати рішення за власною волею, що не пов'язана рамками його законності [12].

Досить повною та найменш суперечливою, на розсуд автора, є думка К. Комісарова, що розсуд не слугує ні способом, ні підставою підміни законності доцільністю. Його призначення полягає в тому, щоб у випадку відсутності прямого абсолютно визначеного вказання, знайти таке з ряду запропонованих законом рішень, яке найточніше відповідає ідеї законодавця [9, с. 49].

В монографії колективного авторства А. Луньова, С. Студенікіна, Ц. Ямпольського розсуд розглядається тільки у зв'язку з законом. Проте, автори справедливо, на думку автора, підкреслюють, що в сфері застосування закону вибір рішення повинен бути пов'язаний з метою, яка вказується законодавцем або витікає з сенсу закону [10, с. 63].

Тому необхідно сказати, що без чіткого визначення поняття адміністративний розсуд, буде неможливим передбачити виникнення негативних наслідків від зловживання владою зі сторони органів публічної адміністрації. А ті прогалини в праві, яких можна було б уникнути, тільки стануть глибшими.

### **Література**

1. Адміністративне право України. Академічний курс: Підруч.: у двох томах: том 1. Загальна частина / Ред. колегія В. Б. Авер'янов (голова). – К.: «Юридична думка», 2004. – 584 с., С.265-266
2. Адміністративне право України (В.Б. Авер'янов). Для студентів, аспірантів і викладачів вищих навчальних закладів. – «Юридична думка», 2004. – С.265

3. Барак Аарон. Судейское усмотрение. Перевод с английского. – М.: НОРМА, 1999. – 376 с.
4. Давид Р. Жоффре-Спинози К. Основные правовые системы современности / пер с фр. В.А. Туманова. – М.: 2003.
5. Лазарев Б. М. Компетенция органов управления / Б. М. Лазарев – М. Юрид. лит., 1972. – 280 с., С. 94.
6. Люблинский П.И. Основания судейского усмотрения в уголовных делах // Санкт-Петербург, 1904. – С.2
7. Лагода О. Адміністративний розсуд та межі його застосування / О. Лагода // Право України. – 2006. – № 12. – С. 109-112.
8. Малиновский А. А. Усмотрение в праве // Государство и право. 2006. № 4. – С. 102.
9. Комиссаров К. И. Судебное усмотрение в советском гражданском процессе / К. И. Комиссаров // Советское государство и право. – 1969. – № 4. – С.49-56., с. 49
10. Социалистическая законность в советском государственном управлении / Лунев А. Е., Студеникин С. С., Ямпольская Ц. А.; Под общ. ред.: Студеникин С. С. – М.: Юрид. изд-во СССР, 1948. – 136 с., С.63
11. Томсинов В.А. О сущности явления, называемого рецензией римского права // Вестн. Моск. ун-та. Сер. 11, Право. - 1998. - № 9. - С.11.
12. Чечот Д. М. Административная юстиция (теоретические проблемы) / Д. М. Чечот. – Л.: ЛГУ: Наука, 1973 – 134 с.

### **Кіберзлочинність як злочин транснаціонального характеру**

**Любчик В.Б.**

кандидат юридичних наук, доцент,  
підполковник поліції  
професор кафедри оперативно-розшукової діяльності  
факультету №1 Одеського державного університету внутрішніх справ

**Слободянюк О. О.**

курсант 414 взводу  
факультету №3 ОДУВС

Актуальність: Розвито інтернету, поширення глобальних мереж, доступ широкого кола осіб до світової бази інформаційних ресурсів – основні вимоги формування інформаційного суспільства. Саме до становлення такого прагне й Україна. На щастя, розвиток технічних можливостей постійно розвивається, вдосконалюється, створюються все нові й нові технології. Однак, разом з цими позитивними моментами з'являються й нові причини для хвилювань, адже наскільки б не були розвинені технологічні можливості – можливості людського розуму, винахідливості та винахідливості завжди більші. Саме тому сьогодні людство стикнулося з такою глобальною проблемою як злочинність, пов'язана з використанням ЕОМ – кіберзлочинність. Дану проблему вище названо глобальною і це не перебільшення, адже саме з початком інтеграційних та глобалізаційних процесів почався процес вірусного поширення кіберзлочинності. Однією з кримінологічних характеристик кіберзлочинності в науковій літературі є її транснаціональний характер, а тому, лише досконало вивчивши дану особливість такого виду злочинної діяльності можна говорити про створення певної системи її протидії, боротьби та попередження.

Тематика кіберзлочинності має велике поширення серед науковців, що займаються питаннями права, правоохоронної та правозахисної діяльності, серед яких: В. Бабакіна, В.М. Бутузов, А.М. Ключко, В. Кудінов, С.Ю. Лисенко, Г.Ю. Маклаков, В.В. Пивоваров, О.О. Тихомиров, С. Черніченко та інші.

Проблема поширення кіберзлочинності є досить новою для нашого суспільства, тому важливо виявити шляхи її поширення, та осередки її розповсюдження. Та в першу чергу бажано розглянути саме поняття кіберзлочинності, під якою розуміють - злочини, які вчиняються за допомогою або через комп'ютерні системи чи пов'язані саме з комп'ютерними системами, тобто із сукупністю пристроїв, із яких один чи більше у відповідності до певної програми виконують автоматичну обробку даних[1, С. 414].

Транснаціональний або ж міжнародний характер таких правопорушень викликаний цілим рядом факторів, приділивши увагу уваги ми зможемо наблизитись до сутності та змісту комп'ютерної

злочинності. Так, глобальність і транскордонність комп'ютерних і телекомунікаційних мереж, можливість маніпуляцій злочинця з ідентичністю (тобто використання чужих імен, адрес, паролів і т.п.) створює ситуації, коли злочинець знаходиться на одному континенті, злочин безпосередньо вчиняється на іншому, а наслідки злочину настають на третьому. Більше того, в останні кілька років у зв'язку з появою і поширенням ботнетів - мереж інфікованих комп'ютерів, які проводять атаки незалежно від користувачів, ситуація ускладнилася ще більше: злочинець, сотні атакуючих комп'ютерів і потерпілий від злочину можуть перебувати на території більш ніж двох або трьох держав[2]. Саме це є однією з проблем, які постають перед органами, що здійснюють розслідування злочинів та виявлення осіб винних у їх вчиненні, оскільки перебуваючи в одній країні, діючи там - злочинні наслідки наставатимуть у зовсім іншому місці, довести в такому випадку причинно-наслідковий зв'язок досить складно. Міжнародні комп'ютерні мережі, такі як Інтернет, є відкритим середовищем, що дає користувачам можливості чинити певні дії за межами кордонів держав, у яких вони перебувають.

У той же час оперативні або слідчі дії правоохоронних органів повинні обмежуватися територією власної держави, що в свою чергу викликає суттєві труднощі. Ще однією проблемою транскордонності є те, що відкритість глобальних інформаційних мереж надає можливість користувачам вибирати таку юрисдикцію, яка відповідає їхнім цілям. Тобто, користувачі можуть вибирати ті країни, в яких певні діяння, здійснені в кіберпросторі, не визначаються як кримінальнокарані. Такі країни можуть створювати привабливі можливості для протиправних дій осіб з тих держав, де такі дії, згідно внутрішнього законодавства, підпадають під кримінальну відповідальність. Наявність інформаційних притулків[3].

Транснаціональний характер протиправних дій доводить, що вони можуть здійснювати свою діяльність з території власної або третьої держави, а також з тих територій, в яких недостатньо розвинений режим протидії. Злочинців зазвичай приваблює відсутність фізичного контакту з потерпілими, складність виявлення, фіксування та вилучення криміналістично-значущої інформації у віртуальному просторі[4, с. 94].

Поряд з поняттям кіберзлочинності використовують поняття кіберпростору, під яким розуміють простір, сформований інформаційно-комунікаційними системами, у якому проходять процеси перетворення (створення, зберігання, обміну та знищення) інформації, представленої у вигляді електронних комп'ютерних даних[1, с. 416]. Як бачимо з визначення, кіберпростір не обмежений рамками державних кордонів, певної територіальної юрисдикції, що в свою чергу також пояснює таку особливість кіберзлочинності як транскордонний характер. З огляду на це постає питання створення єдиного простору міжнародного співробітництва у сфері боротьби з кіберзлочинністю, лише таким чином правоохоронні органи будуть в рівних умовах зі злочинцями, які вчиняючи злочини не обмежуються будь-якими рамками та кордонами.

Окремо потребує уваги таке, на жаль, поширене сьогодні явище як кібервійна та, тісно пов'язане з нею комп'ютерне шпигунство. Дані явища напевно найяскравіше розкривають міждержавний характер кіберзлочинності. Сьогодні застосування засобів кібервійни є одним з основних способів вчинення злочинів, які за Кримінальним законодавством, визначаються як такі, що посягають на територіальну цілісність та конституційний лад держави. Вся інформація глобального поширення, що знаходиться у відкритому доступі для кожного жителя планети, незалежно від приналежності до певної держави, при правильному її застосуванні може стати зброєю масового ураження, протистояти якій практично неможливо.

Враховуючи визначення кіберзлочинності як злочинів міжнародного характеру, слід визначити такі проблеми, вирішення яких має стати перспективним курсом кожної держави у сфері боротьби з кіберзлочинністю. Перш за все те, що боротьба з кіберзлочинністю для урядів багатьох країн не є пріоритетом, що не дозволяє визначити об'єктивний рівень небезпеки від комп'ютерних злочинів у багатьох державах. Також проблемою є відставання, внаслідок стрімкого розвитку новітніх технологій, правових норм від умов використання цих технологій в економіці та суспільстві, у тому числі зі злочинною метою. Як приклад, високий ступінь анонімності у мережі Інтернет, що дає можливість отримувати великі злочинні доходи з мінімальним ризиком викриття, провокує до вчинення нових видів злочинів. Неабиякою перешкодою сьогодні є брак конструктивного міжнародного співробітництва у протидії кіберзлочинності, наприклад, у багатьох державах, які ратифікували Конвенцію про кіберзлочинність, ратифіковану Україною 07.09.2005 року, досі не створили національні контактні пункти. Саме прийняття даної Конвенції стало вагомим кроком на шляху визнання кіберзлочинності злочинами глобального, міжнародного характеру.

Проблемою також є відсутність у багатьох державах належної взаємодії між правоохоронними відомствами та приватним бізнесом (телекомунікаційними компаніями та компаніями, що надають

послуги Інтернет) з питань надання необхідної інформації (доказів у електронному вигляді) та її збереження в комп'ютерних системах[5, с. 85].

Враховуючи все вищезазначене можна зробити такий цілком логічний висновок, що питання боротьби, протидії, попередження та розкриття кіберзлочинів може бути вирішене лише за умови налагодження ефективного діалогу між державами та їх правоохоронними органами, а кожна держава окремо зобов'язана виконувати ті певні вимоги, що мінімізують умови поширення кіберзлочинності.

#### **Література:**

1. Бельський Ю. Щодо визначення поняття кіберзлочину / Ю. Бельський// Юридичний вісник – 2014. - №6. – С. 414.
2. Антикібер – Кіберзлочинність: проблеми боротьби і прогнози[Електронний ресурс] – Режим доступу: [http://anticyber.com.ua/article\\_detail.php?id=140](http://anticyber.com.ua/article_detail.php?id=140).
3. Аналітичний огляд наукових статей з проблем протидії кіберзлочинності № 4 (О.О.Тихомиров, В.М. Бутузов, В.А. Кудінов) - [Електронний ресурс] – Режим доступу:<http://inter.criminology.onua.edu.ua/?p=10549>.
4. Гринчак І. В. Кіберзлочинність як злочин міжнародного характеру / І. В. Гринчак // Науково-інформаційний вісник – 2015. - №12. – С. 94.
5. Бутузова В.М “Злочини із застосуванням сучасних інформаційних технологій” - [Електронний ресурс]- / В. М. Бутузова // Науково-практичний журнал “Боротьба з організованою злочинністю і корупцією (теорія і практика)” - 2003. – №7. – Режим доступу:<http://inter.criminology.onua.edu.ua/?p=10549>.

#### **Роль та місце зворотного зв'язку в процесі здійснення управлінської діяльності**

**Колодніцький Р.М.**  
курсанта 414 взводу  
факультету №3 ОДУВС

**Медведенко С.В.**  
начальник відділу кадрового забезпечення  
Одеського державного університету внутрішніх справ

Система управління за своєю природою є досить складним і багатоплановим явищем, бути на чолі якого зовсім не проста річ, кожна така система в певний період свого становлення переживає певні проблеми. Підтвердженням цього положення є численні повстання, мітинги, страйки. Саме такий період сьогодні переживає й наша держава, свідками чого ми й є.

Події, які ми сьогодні можемо спостерігати, потрібно розцінювати ніяк інакше як неправильно обрані методи управління державою загалом та кожною її сферу окремо. На жаль, для нашого суспільства досі не є близьким такий інститут суспільного управління як «інститут взаємодії», «зворотного зв'язку». Правильно застосовуючи його та адекватно реагуючи на отриману завдяки йому інформацію можна було б уникнути цілого ряду непорозумінь та, цілком вірогідно, що сьогодні Україна перебувала б на порядок вище за рівнем свого розвитку порівняно з даним етапом. Враховуючи це, на нашу думку цілком доцільно детальніше вивчити перспективу зворотнього зв'язку для управління та можливості пристосування його до наявного в нас механізму, виробивши особливу специфічну його модель.

Дослідженням цього питання займалися багато вчених, зокрема це: Т.П. Абдулова, О.В. Новак, В.Я. Малиновський, О.С. Поважний, С.М. Попов, Г.Н. Татарінова, А.В. Халецький та інші. Як і при будь-якому дослідженні першим чому приділяється увага є розкриття теоретичного змісту та сутності досліджуваного питання. Проблеми прямих і зворотних зв'язків у системі державного управління заслуговують самої пристальної уваги. Одні вчені називають прямі зв'язки жорсткими і свавільними (сильна рука), без яких неможливо забезпечити ефективне управління соціальними процесами. Інші вважають, що у прямих зв'язках «зверху-вниз» домінує свавілля, а зворотні зв'язки «знизу-вверх» носять в основному хаотично-випадковий характер у вигляді нескінченних прохань, пропозицій, вимог, критичних зауважень. Проте як би не називали державне управління, якщо управлінський вплив не доходить до керованого об'єкта, не впливає на життя людини та її діяльність, то подібне управління втрачає будь-який смисл. Усі його елементи починають діяти розрізнено, суперечливо, знищуючи один одного у конкурентній боротьбі. Мистецтво управління як раз і складається у тому, щоб через



посередництво багатоманітних і розумно об'єднаних між собою інститутів, форм, процедур і соціальних технологій прямого і зворотного зв'язку (включаючи багатопартійність, парламентську опозицію, незалежність місцевої влади, вільну пресу, інші складові громадянського суспільства) забезпечити високоефективне функціонування управляючої системи. Прямі зв'язки – це вплив керованого суб'єкта (органа, посадової особи) на об'єкт, у яких переважно представлений вплив зверху вниз, хоча управлінський вплив може бути і горизонтальним, координуючим. Прямі зв'язки можуть бути постійними, часовими та несистематичними, м'якими та активними, командними і навіть силовими [1, с. 86].

У свою чергу зворотний зв'язок - це процес обміну змістовною та оціночною реакцією партнерів на інформацію і поведінку один одного.

Розрізняють такі форми соціального зворотного зв'язку:

1) Свідомо або несвідомо дозований. Часто керівники надають неповну або неточну інформацію, щоб приховати деякі обставини або запобігти негативним реакціям персоналу;

2) Прямий і опосередкований. Прямий зворотний зв'язок характеризується відвертою і однозначною формою повідомлення. Опосередкований зворотний зв'язок — це обмін завуальованими реакціями, щоб ввести партнера в оману або скоригувати його поведінку. Він може бути також зумовлений неможливістю з морально-етичних норм висловлюватися прямо й відверто. Такий зворотний зв'язок негативно позначається на процесі управління.

3) Позитивний або негативний зворотний зв'язок. Особливе значення таких зворотних зв'язків між керівником і підлеглим зумовлене процесом сприймання інформації. Обмеженнями для негативного зворотного зв'язку з боку підлеглого можуть бути: побоювання можливих неприємних наслідків для себе; соціально-культурний фактор (норми, традиції, які обмежують критичні висловлювання); психологічне напруження. Щодо керівників, то негативну зворотну інформацію щодо підлеглих вони часто розглядають як ефективну форму управлінського спілкування. Висловлювання можуть принижувати людську гідність підлеглого. Як наслідок, виникають комунікативні бар'єри в спілкуванні, конфлікти. Разом з тим негативний зворотний зв'язок в управлінському спілкуванні має об'єктивну основу, оскільки не всі працівники однаково ставляться до своїх функціональних обов'язків. Завдання полягає в тому, щоб керівник знаходив найбільш ефективні форми негативного зворотного зв'язку [2].

Як бачимо сутність зворотного зв'язку розкривається через цілий ряд категорій, оцінюючи які слід враховувати безліч нюансів, зокрема як об'єктивних так і суб'єктивних. Яка ж все ж таки роль зворотного зв'язку в процесі здійснення державного управління, та чи справді він є настільки важливим та необхідним для управлінської діяльності? Перш за все, слід сказати, що у системі державного управління виділяють два типи зворотних зв'язків: об'єктні і суб'єктні, кожен з яких присутній в усіх управлінських відносинах, однак виражають різні аспекти та сторони управління. Об'єктні зворотні зв'язки відображають рівень, глибину, адекватність сприйняття об'єктами управління управлінських впливів суб'єкта державного управління. Відсутність або неповнота змістовних і правдивих об'єктних зворотних зв'язків не дозволяє визначати раціональність і ефективність організації та діяльність суб'єкта державного управління та виробляти заходи їх підвищення. Погано в такому разі уявляються й потреби, інтереси та цілі об'єктів управління. Суб'єктні зворотні зв'язки характеризують доцільність і раціональність власної, внутрішньої організації і діяльність суб'єкта державного управління загалом, його підсистем, лапок і окремих компонентів. Вони дають змогу побачити, зрозуміти й оцінити, як кожний нижчий рівень реагує на рішення й дії вищого, наскільки і яким чином він враховує їх у своїй діяльності, яке його реальне відношення до вищого рівня тощо. До суб'єктних зворотних зв'язків належать: контроль, аналіз та оцінка організації і діяльності державних органів, виконання своїх обов'язків з боку посадових осіб, звіти, інформація тощо [3]. Продовжуючи дану тему потрібно сказати, що кожен з цих видів має по-своєму важливе значення та відіграє свою виключну роль, що в комплексі підвищує загальний рівень управління та його здатність до вдосконалення, шляхом вивчення, оцінки та вирішення виникаючих питань. Зворотний зв'язок потрібен і керівникам – від своїх працівників. Підлеглі можуть надати управлінцю цінну інформацію про ефективність процедур і процесів, оцінити лідерську ефективність [4].

Провівши паралель із сьогодишньою ситуацією в Україні, можемо з упевненістю сказати, що багатьох речей можна було б уникнути, якби зв'язок між державою, в особі органів державної влади та їх посадовців з одного боку, та суспільством, громадянами, населенням - з іншого, був налагоджений.

Активна взаємодія між урядом і громадянами повинна існувати в усіх сферах суспільного життя, однак вона особливо необхідна у сфері захисту прав людини. Участь громадян у виробленні політичного курсу, управлінні державою на демократичних засадах через встановлені законом форми безпосереднього співробітництва, а також через дозволена законом діяльність громадських організацій,

незалежний нагляд за діяльністю органів управління як основи механізмів стримувань і противаг неможлива без забезпечення вільного доступу до інформації та відкритого обговорення рішень влади.

Відкритість органів державного управління, згідно з вимогами нормативних документів Парламентської Асамблеї Ради Європи, у контексті розбудови правової, демократичної, суверенної держави є не лише умовою виконання рекомендацій Ради Європи, а й необхідністю на сучасному етапі державного будівництва.

За роки членства України в Раді Європи почали створюватися і поступово впроваджуватися в життя механізми залучення громадськості до вироблення та реалізації відкритої та прозорої державної політики. Відчувається нагальна потреба наукового дослідження таких механізмів, однак у науковій літературі не спостерігається інтересу до цієї проблеми. Чинна Конституція України гарантує громадянам достатньо широкі права та можливості участі в різних формах у процесі прийняття рішень органами державного управління України (ст. 5, 36, 38, 40, 55, 69). Проте в Конституції України, як і в інших нормативно-правових актах, не виписано чіткі механізми для реального забезпечення проголошених прав.

Аналіз нормативно-правової бази забезпечення правових гарантій участі громадян у виробленні та реалізації управлінських рішень за досліджуваний період свідчить, що не тільки не опрацьовані такі гарантії, а й жоден чинний нормативно-правовий акт не регламентує чітких процедур щодо забезпечення громадян з боку Верховної Ради України, Кабінету Міністрів України, окремих міністерств та інших центральних органів державного управління інформацією стосовно обговорюваних цими органами питань, прийнятих рішень, проектів та механізмів прийняття важливих для суспільства рішень [5]. Даний зв'язок може мати вигляд різного роду референдумів, якщо говорити в масштабі країни, соціальних опитувань, співпраці з громадськими організаціями, які представляли б інтереси певної категорії населення, і, звичайно, не останнє місце в цьому переліку займають ЗМІ. Взагалі, в нашій чомусь стало такою традицією, що яка б справа не була, чого б вона не стосувалась, але по-справжньому вона набирає обороту лише після оприлюднення в ЗМІ. Такого роду зворотній зв'язок не можна назвати ідеальною його формою, однак як варіант заслуговує на життя, як приклад у вигляді газет та журналів державного рівня, де кожен свідомий громадянин, який має певні пропозиції щодо управління зм'яг би висловити їх, будучи впевненим у тому, що його почують. Звертаючись до законодавства слід зазначити певні зрушення в даному питанні. Трансформації всіх сфер суспільного життя, розпочаті на основі курсу реформ Президента України, визначають необхідність вдосконалення зворотного зв'язку влади та громадськості. Зворотний зв'язок може відбуватися через:

- 1) функціонування громадських рад при органах влади;
- 2) проведення громадських слухань (консультацій);
- 3) підготовку громадської експертизи діяльності органів влади;
- 4) опитування громадської думки (якісні та кількісні) [6].

Ще одним аспектом зворотного зв'язку є його розкриття як одного з принципів управління. Враховуючи те, що основною особливістю принципів є їх основоположний характер, тобто подальша діяльність в даній сфері обов'язково повинна відповідати даним положенням. Так, принципу зворотного зв'язку належить фундаментальна роль для соціального управління: там, де цей принцип порушується чи взагалі відсутній, там відсутній і спотворений смисл і результати соціально-орієнтованого управління. У загальній формі даний принцип зводиться до наступного: у будь-якій взаємодії основу (суб'єкт інформації та управління) і об'єкт інформації та управління неминуче змінюються місцями. Отже, і в процесі соціально-орієнтованого управління відбувається зворотний вплив об'єкта управління на його суб'єкт. Принцип зворотного зв'язку передбачає у якості необхідного моменту обмін інформацією [1, с. 98].

В умовах циклічності процесу управління вступає в дію закон зворотного зв'язку. Його вміле використання в процесі управління дозволяє, з одного боку, більш ефективно організовувати досягнення поставленої мети, з іншого - накопичувати досвід вирішення управлінських проблем, маючи інформацію не тільки про прийняті рішення, а й інформацію про результати їх реалізації. Облік отриманих раніше результатів і висновків, зроблених на підставі їх аналізу, дозволяє управлінцю удосконалювати свою управлінську майстерність. Власні знахідки і помилки для управління-практика допомагають більш впевнено знаходити і реалізовувати стратегічні рішення, оскільки він більш впевнено може представляти очікуваний результат прийнятого рішення [7].

#### **Література:**

1. Попов С.М. Зворотній зв'язок у парадигмі саморегуляції соціальних систем [Електронний ресурс]. - Режим доступу: [http://www.nbuv.gov.ua/old\\_jrn/soc\\_gum/Nzkit/2011\\_9/7.pdf](http://www.nbuv.gov.ua/old_jrn/soc_gum/Nzkit/2011_9/7.pdf)

2. Підручник: Політологія - Сутність зворотного зв'язку, його значення для ефективного управління [Електронний ресурс]. – Режим доступу : [http://lubbook.org/book\\_358\\_glava\\_52\\_54.Sutn%D1%96st\\_zvorotnogo\\_zv%E2%80%99.html](http://lubbook.org/book_358_glava_52_54.Sutn%D1%96st_zvorotnogo_zv%E2%80%99.html)
3. Підручник: Державне управління [Електронний ресурс]. - Режим доступу: <http://subject.com.ua/political/governance/58.html>
4. Інтелект-проект Інновація - Зворотний зв'язок: є альтернатива - 17.08.2016 - [Електронний ресурс] / Режим доступу: <http://innovations.com.ua/ua/blogs/finance/19713/zvorotnij-zv-yazok-je-alternativa/>
5. Халкевський А.В. Зв'язки органів державної влади з громадськістю: інформаційна взаємодія / А.В. Халецький // Державне управління, удосконалення й розвиток [Електронний ресурс]. – Режим доступу: <http://www.dy.nayka.com.ua/?op=1&z=547>
6. Організація зворотного зв'язку влади та громадськості: проблемні питання. Аналітична записка [Електронний ресурс]. – Режим доступу: <http://www.niss.gov.ua/articles/392/>
7. Стратегічний менеджмент - Дія закону зворотного зв'язку [Електронний ресурс]. - Режим доступу: [http://stud.com.ua/18610/menedzhment/zakonu\\_zvorotnogo\\_zvyazku](http://stud.com.ua/18610/menedzhment/zakonu_zvorotnogo_zvyazku)

### **Створення інформаційного середовища взаємодії та роботи у сфері запобігання та протидії легалізації (відмиванню) доходів**

**Мукоїда Р.В.**

кандидат юридичних наук, доцент  
професор кафедри ОРД факультету № 1  
Одеського державного університету внутрішніх справ

**Аносенков А.А.**

кандидат юридичних наук, доцент  
доцент кафедри АП та АП факультету № 2  
Одеського державного університету внутрішніх справ

Державний фінансовий моніторинг відповідно до основних завдань, визначених статтею 18 Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» [2] у 2015 році забезпечив функціонування єдиної державної інформаційної системи у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (ЄІС).

Єдина державна інформаційна система у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення забезпечує цілодобові та безперервні технологічні процеси щодо здійснення отримання, первинної та аналітичної обробки, гарантованого зберігання інформації від суб'єктів фінансового моніторингу, а також підтримку інформаційного середовища взаємодії та роботи самостійних структурних підрозділів Державного фінансового моніторингу. ЄІС функціонує в цілодобовому режимі (24 на 7) відповідно до регламентів, затверджених наказами Державного фінансового моніторингу.

На сьогодні ЄІС понад 12 років перебуває в експлуатації. Протягом 2003 – 2015 років значно розширився перелік суб'єктів первинного фінансового моніторингу, що мають забезпечувати подання інформації та вимоги щодо інформаційної взаємодії з ними.

Враховуючи нові вимоги законодавства, розвиток інформаційних технологій, підвищення вимог міжнародних стандартів з протидії відмиванню доходів та фінансуванню тероризму і розповсюдженню зброї масового знищення (Рекомендації FATF, що затверджені Пленарним засіданням FATF 16 лютого 2012 року) до оперативності реагування на загрози безпеці суспільству, збільшення загроз безпеці інформаційних ресурсів, необхідність вдосконалення технологій взаємодії органів влади з іншими суб'єктами, зокрема з використанням засобів мережі Інтернет, необхідною стала потреба у модернізації ЄІС.

Відповідно до вимог Базового Закону розроблені заходи вдосконалення та розвитку ЄІС.

Зокрема прийнято постанову Кабінету Міністрів України від 14.05.2015 №299 «Деякі питання Єдиної державної інформаційної системи у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення», якою затверджено Положення про єдину державну інформаційну систему у

сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення та перелік інформаційних ресурсів баз даних цієї системи [1].

Положенням про ЄІС встановлюється порядок визначення державних інформаційних ресурсів та порядку надання доступу до них для забезпечення функціонування Єдиної системи, а також засади функціонування та розвитку цієї системи.

З метою економії бюджетних коштів п. 13 Положення про ЄІС запроваджено дві технології обміну інформацією між Держфінмониторингом та іншими суб'єктами ЄІС: на запит, що формується Держфінмониторингом до інформаційного ресурсу розміщеного на функціональній системі у суб'єкта ЄІС, або шляхом регулярного надання суб'єктом інформаційних ресурсів баз даних для їх оновлення у сховищі даних.

Перелік інформаційних ресурсів баз даних ЄІС, що затверджено постановою, забезпечує додаткове надання інформації до баз даних ЄІС з 8 нових інформаційних ресурсів, а саме відомостей:

- про документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус;
- Єдиного реєстру розпорядників бюджетних коштів та одержувачів бюджетних коштів;
- про державну реєстрацію юридичних осіб та фізичних осіб-підприємців;
- про осіб, яким повідомлено про підозру у вчиненні кримінальних правопорушень у сфері легалізації доходів, одержаних злочинним шляхом, і фінансування тероризму;
- про задекларовані витрати, що враховуються при визначенні об'єкту оподаткування платників податків;
- про доходи, що враховуються при визначенні об'єкту оподаткування страхових компаній;
- про фінансові інструменти, що перебувають у власності торговця цінними паперами за станом на останній день кварталу (крім цінних паперів власних випусків);
- з Єдиного реєстру об'єктів державної власності.

Зміни у зазначеному переліку передбачають створення функціональних підсистем у Державній міграційній службі України, Державній реєстраційній службі України, Генеральній прокуратурі України та модифікацію функціональних підсистем у трьох державних органах Міністерстві внутрішніх справ України, Державній фіскальній службі України, Державній прикордонній службі України.

У зв'язку зі змінами переліку інформаційних ресурсів баз даних та складу суб'єктів ЄІС функціональні підсистеми ЄІС у Державній регуляторній службі України та Державній службі України з питань геодезії, картографії та кадастру згорнуті. Також, у зв'язку зі зміною технології обміну інформацією демонтовані функціональні підсистеми у Міністерстві економічного розвитку і торгівлі України, Національній комісії з цінних паперів та фондового ринку, Національній комісії, що здійснює державне регулювання у сфері ринків фінансових послуг, Державній фінансовій інспекції України, Службі безпеки України, Міністерстві фінансів України, Фонді державного майна України, та обладнання Головного комутаційного центру інформаційно-телекомунікаційної системи фінансового моніторингу (Державне підприємство «Українські спеціальні системи»).

З метою вдосконалення єдиної інформаційної системи у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення та на виконання заходів з основних напрямків розвитку цієї системи відповідно до вимог законодавства Держфінмониторингом розроблена програма «Модернізація інформаційної системи у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення».

Розпочата Держфінмониторингом модернізація має забезпечувати відповідність національної системи протидії відмиванню коштів та фінансуванню тероризму і розповсюдженню зброї масового знищення Стандартам FATF, інтеграцію додаткових інформаційних ресурсів органів державної влади до ЄДІС, заміну застарілого апаратного та програмного забезпечення, удосконалення комплексної системи захисту інформації у відповідності до нових загроз її безпеки.

### **Література:**

1. Деякі питання Єдиної державної інформаційної системи у сфері запобігання та протидії легалізації [...]. Кабінет Міністрів України; Постанова, Положення, Перелік від 14.05.2015 № 299
2. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення. Верховна Рада України; Закон від 14.10.2014 № 1702-VII.//Відомості Верховної Ради (ВВР), 2014, № 50-51, с.2057

**Розовик І.В.**

здобувач вищої освіти 4-го курсу  
факультету № 2 ННІ № 1  
Національної академії внутрішніх справ

**Шевчук О.Ю.**

кандидат юридичних наук, доцент,  
доцент кафедри СТ та ОРД ННІ №1  
Національної академії внутрішніх справ

Враховуючи провідну роль інформатизації в економіці України та її стрімку криміналізацію, сьогодні особливої актуальності набуває внесення значущих змін і доповнень до чинного законодавства і відомчих нормативних актів, які б забезпечили нормальне функціонування інформаційних систем і мереж, створили б умови для мінімізації криміногенних процесів, своєчасного виявлення і попередження кіберзлочинів. Криміногенна ситуація у сфері використання інформаційних технологій вимагає комплексного підходу як з боку правоохоронних органів, так і з боку інших зацікавлених відомств.

Так, у серпні 2003 року на розгляд Верховної Ради України було внесено проект Закону України «Про моніторинг телекомунікацій» [1] за поданням Кабінету Міністрів України. Цей Закон визначає правові та організаційні засади моніторингу телекомунікацій, регулює відносини суб'єктів у сфері моніторингу телекомунікацій під час провадження оперативно-розшукової, контрозвідувальної та розвідувальної діяльності з метою забезпечення безпеки громадян, суспільства і держави.

Що стосується міжнародного досвіду, то 30 травня 2002 року Європарламент відмінив положення Директиви про захист персональних даних у сфері комунікацій 1997 року [2], яке обмежувало зберігання персональних даних користувачів Інтернет. Країнам ЄС було дозволено вимагати від Інтернет-провайдерів і телекомунікаційних компаній, щоб ті фіксували, систематизували та зберігали комунікаційні дані своїх клієнтів, включаючи дані про трафік, місцезнаходження власника мобільного телефону, ідентифікаційні дані відправників і отримувачів SMS-повідомлень і осіб, що телефонували. Відповідні закони були прийняті в Бельгії, Франції, Іспанії, Данії, Великобританії, Фінляндії. Тим самим Європарламент законодавчо закріпив існування так званої системи «Ешелон».

«Echelon» – частина угоди UKUSA, яка представляє систему вибіркового контролю за трафіком на ключових супутниках Intelsat, транслюючи більшість міжнародних розмов, трафіку Інтернет, електронної пошти, факсів і телексів. Її опорні пункти розташовані в США, Новій Зеландії, Австралії, Гонконгу, Великобританії.

У США існує система «Carnivore», яка дозволяє відслідковувати та аналізувати електронну пошту. Окремий комп'ютер сканує всю кореспонденцію користувачів поштового сервера. З цього масиву інформації програма відбирає файли, які належать конкретному користувачеві [4, с. 30].

Прийняття закону, який би регулював відносини в сфері телекомунікацій, конче необхідне для України, бо це відповідає нагальним потребам правоохоронних органів та вимогам європейського законодавства, підвищує інвестиційну привабливість інформаційно-телекомунікаційної галузі шляхом встановлення чітких і прозорих норм.

За механізмом і способами здійснення злочини у сфері інформаційних технологій є специфічними і, як вже згадувалось раніше, мають високий рівень латентності.

Що стосується прогнозування тенденцій кіберзлочинності на близьку перспективу, то представляється можливим відзначити деякі з них:

1. Постійна динаміка збільшення світової і вітчизняної аудиторії Інтернет та кількості комп'ютерів дає підстави для передбачення збільшення динаміки кіберзлочинності. Зважаючи на стрімке зростання користувачів Інтернет в Україні та щорічне зростання кількості комп'ютерів з динамікою 1,5 – 2 рази, можна прогнозувати лише незначне збільшення кількості розкритих кіберзлочинів (приблизно до 60 – 65 по Україні).

Активно розвиваючись, кримінальне середовище в інформаційній сфері вже сформувало свій віртуальний осередок. «Надбанням» цього середовища є поява «тіньового» IT-ринку, існування якого підтверджено зафіксованими фактами продажу кримінального товару. Так чи інакше, майбутнє цього ринку вже визначене і в подальшому буде тільки розвиватись, а його віртуальний товар вже представляє собою серйозний засіб для вчинення реальних злочинів;

2. Найближчим часом прогнозується збільшення випадків вимагання грошей у компаній шляхом погроз блокування он-лайн-ресурсів за допомогою DoS-атак;

3. Все більше і більше комп'ютерних вірусів застосовуватимуться злочинцями з конкретною метою – одержати гроші, а не з метою вандалізму, як було в минулі часи, віруси і шпигунські програми все частіше гіпотетично використовуватимуться також і в політичних цілях;

4. Зростатиме кількість злочинів в Інтернет, вчинюваних організованими злочинними угрупованнями, які ведуть свою діяльність в міжнародних масштабах. Зростаючий інтелектуальний потенціал молоді дозволяє злочинним угрупованням вже сьогодні привертати до себе нових людей різними способами, частіше – шляхом погроз та шантажу. Організовані злочинні угруповання активніше використовуватимуть нові технології і направлятимуть в університети молодих людей, які стануть фахівцями в цій сфері;

5. У зв'язку зі зростаючою кількістю Інтернет-магазинів, супермаркетів, які пропонують свої послуги та товари через Інтернет, зростатиме кількість шахрайств у цій сфері діяльності.

З огляду на зазначене, вважаємо за доцільне вжити заходів:

1. Верховній Раді України прийняти Закон України «Про моніторинг телекомунікацій»;

2. Кабінету Міністрів України:

– розробити проекти постанов щодо вжиття першочергових заходів, спрямованих на зниження рівня хуліганської і кримінальної активності в Інтернет, що регламентуватиме роботу постачальників Інтернет-послуг та їх клієнтів, провайдерів і операторів IP-телефонії, а саме: запровадити практику ідентифікації користувача Інтернет шляхом надання ідентифікаційного коду особи оператору зв'язку, при подачі письмової заяви про укладення договору на надання послуг;

– розробити та ввести в дію систему з попередження шахрайств [3, с. 58], в Інтернет з метою проведення інвентаризації та сертифікації сайтів компаній і фірм, основною сферою діяльності яких є торгівля та надання послуг (у тому числі сайтів з азартних ігор, лотерей, аукціонів), які проводять розрахунки між продавцем та покупцем за допомогою засобів електронного зв'язку;

– всебічно сприяти створенню у вітчизняному сегменті Інтернет-сайтів, висвітлюючих діяльність правоохоронних органів у сфері протидії кіберзлочинності.

#### **Література:**

1. Проект Закону України «Про моніторинг телекомунікацій» № 4042 від 07 серпня 2003 року. // ЛПА: ЗАКОН.

2. Ястребов Д.А. Институт уголовной ответственности в сфере компьютерной информации (опыт международно-правового сравнительного анализа) / Д.А.Ястребов // Гос. и право. – 2005. – № 1.

3. Деякі шляхи протидії викликам в інформаційному просторі країни // Основні тенденції проявів організованої злочинності в сучасних умовах (зб. наук.-аналіт. матеріалів). – К.: МНДЦ, 2014. – Вип. 1. – 182-186 с.

4. Борьба зі злочинами у сфері комп'ютерної інформації: проблеми та шляхи їх вирішення: матеріали міжвуз. наук.-практ. конф. 14 груд. 2007 р. / Донецький юрид. ін-т. – Донецьк: Донец. юрид. ін-т, 2008. – 242 с.

#### **Правове регулювання поширення інформації в мережі інтернет**

**Саакян М.Б.**

доктор юридичних наук, професор

професор кафедри ОРД

Одеського державного університету внутрішніх справ

Процеси глобалізації та інформатизації, які набувають всесвітніх масштабів, призвели до належної реакції зі сторони міжнародної спільноти, яка знайшла своє вираження у міжнародно-правових актах, спрямованих на врегулювання основних положень протікання зазначених процесів. До ключових документів, прийнятих міжнародним співтовариством у сфері інформатизації, слід виділити: Окінавську хартію глобального інформаційного суспільства, Конвенцію про захист осіб стосовно автоматизованої обробки даних особистого характеру, Директиву 95/46/ЄС Європейського Парламенту та Ради Європи «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних», Угоду про співробітництво в галузі інформації та інші документи.

Ключовим серед цих документів є Окінавська хартія глобального інформаційного суспільства, яка визначає, що інформаційно-комунікаційні технології є одним із найважливіших чинників, що впливають на формування суспільства ХХІст. Крім цього, у документі визначено обсяг необхідних

завдань, виконання яких є необхідним для побудови інформаційного суспільства. З огляду на те, що розвиток процесів глобалізації та інформатизації супроводжується експансією злочинних структур у вказані сфери життя суспільства, держави, учасниці Хартії, зобов'язались забезпечити здійснення ефективних заходів у боротьбі зі злочинністю у комп'ютерній сфері.

До того ж потребує розгляду Конвенція про кіберзлочинність (далі Конвенція). Передумовою, що детермінувала прийняття Конвенції, стала експансія кримінальних структур у сферу використання високих інформаційних технологій та їх використання для здійснення злочинної діяльності. Так, у преамбулі Конвенції зазначено, що держави-члени Ради Європи та інші держави, які підписали Конвенцію, стурбовані ризиком того, що комп'ютерні мережі та електронна інформація може також використовуватись для вчинення кримінальних правопорушень, і того, що докази, пов'язані з такими правопорушеннями, можуть зберігатись і передаватись такими мережами.

Зважаючи на специфіку сфери правового регулювання, у Конвенції визначені окремі інноваційні положення процесуального права, спрямовані на забезпечення інтересів кримінального судочинства. Так, на виконання норм Конвенції держави зобов'язані на законодавчому рівні забезпечити:

- надання можливості компетентним органам видавати ордери або іншим подібним шляхом здійснювати термінове збереження визначених комп'ютерних даних, включаючи данні про рух інформації, які зберігалися за допомогою комп'ютерної системи, зокрема, у випадку, коли існують підстави вважати, що такі комп'ютерні дані особливо вразливі до втрати чи модифікації (ст. 16);

- зберігання і підтримання цілісності комп'ютерних даних протягом такого періоду, який буде необхідним для того, щоб компетентні органи мали можливість отримати дозвіл на їх розкриття з максимальним терміном у 90 днів(ст. 16);

- зберігати конфіденційність факту проведення таких процедур протягом періоду, визначеного її внутрішньодержавним законодавством (ст. 16);

- забезпечити термінове збереження даних про рух інформації, незважаючи на те, один чи більше постачальників послуг залучені до передачі такої інформації (ст. 17);

- забезпечити термінове розкриття обсягу даних про рух інформації, достатнього для ідентифікації постачальника послуг і маршруту, яким була передана інформація (ст. 17);

- надання компетентним органам повноважень арештовувати або вчиняти інші подібні дії щодо комп'ютерних даних. Такі заходи включатимуть повноваження: на арешт або подібні дії щодо комп'ютерної системи або її частини, або комп'ютерного носія інформації, копіювання і збереження копії таких комп'ютерних даних, збереження цілісності відповідних даних, заборону доступу або вилучення таких даних з комп'ютерної системи (ст. 19).

У Конвенції чітко окреслено поняття «інформація про користувача послуг», під якою розуміється будь-яка інформація у формі комп'ютерних даних чи в іншій формі, яка знаходиться у постачальника послуг, належить користувачам його послуг, не є даними про рух даних або власне даними змісту інформації та за допомогою якої можна встановити:

- тип комунікаційної послуги, яка використовувалась, її технічні положення і період користування послугою;

- особистість користувача послуг, поштову або географічну адресу, телефони та інший номер доступу, інформацію про рахунки і платежі, яку можна отримати за допомогою угоди або домовленості про постачання послуг.

Отже, розглянута Конвенція встановлює досить широке коло повноважень правоохоронних органів щодо протидії інноваційним формам злочинної діяльності та використання високих інформаційних технологій у боротьбі зі злочинністю. Крім того, значну увагу приділено визначенню обов'язків постачальників інтернет-послуг щодо співпраці з правоохоронними органами. Проте національне законодавство України сьогодні не приведено у відповідність із стандартом, передбаченим Конвенцією. В наш час норми міжнародного права у внутрішніх правовідносинах використовуються ще досить рідко, тому говорити про них як про правову основу діяльності поліції некоректно.

Одним із ключових досягнень в процесі розвитку високих інформаційних технологій, без сумніву, є побудова та функціонування глобальних інформаційних мереж, зокрема Інтернет. Інтернет поступово охоплює дедалі нові й нові сфери нашого життя, перетворюючись у стандартний канал соціальних комунікацій. У сферу Інтернет постійно і органічно впливають такі галузі економіки, як зв'язок, засоби масової інформації, консультаційні послуги. З'являються нові соціальні групи, формується нова ідеологія, новий спосіб життя.

Зараз перед багатьма державами світу постає питання щодо можливості впливу права як найбільш могутнього соціального регулятора на Інтернет, оскільки інформаційні потоки поступово стають важелями управління соціальними процесами. Виникнувши як суто технічний засіб передачі інформації, Інтернет перетворився на соціальне явище, що звертає на себе увагу фахівців різних наук, в

тому числі й юриспруденції. Такий погляд поділяє низка науковців. Зокрема, Е. Кеєв зазначає, що необхідність регулювання правом інтернет-відносин пов'язана з тим, що право обирає нові напрями і відвідує нові території, з'являється дедалі більш на екранах, ніж на папері. У своїй роботі «Право у цифровому світі» Е. Кеєв зазначає, що право входить у світ нових рухливих просторів і нових відносин, туди, де індивідуальні і колективні можливості сполучення усе більше зростають; місце, де воно зіштовхується з новими визначеннями і з новими очікуваннями. У зв'язку з інтенсивним розвитком сучасних суспільних відносин в інформаційній сфері, серед яких найбільш розповсюдженими є доступ до інформаційних ресурсів в мережі Інтернет і використання інформаційних послуг, у тому числі електронної пошти, регулювання інтернет-відносин, вважає В.М. Наумов, стає одним з найактуальніших завдань сучасного законодавства і права. Схожий погляд висловлює А. Чучківська, зазначаючи, що в мережі Інтернет активно йде електронний документообіг, який охоплює формування, обробку, відправлення та одержання, перевірку і використання електронних документів.

Але у наукових колах існує інша думка, яка полягає в тому, що інтернет-відносини не можуть бути врегульовані правом. Так, Д. Пост упевнений, що комп'ютерна мережа Інтернет не піддається централізованому врегулюванню чи регламентації, і це питання можна вирішити лише в майбутньому.

Але ж видається, що мережа Інтернет все ж таки може виступати об'єктом правового впливу, і більш того, такий вплив є необхідним на сучасному етапі. Найбільш ефективно використання високих інформаційних технологій в оперативно-розшуковій діяльності відбувається у відповідному симбіозі з глобальною мережею, яка сама виступає продуктом інтеграції високих технологій. Відсутність правових норм щодо статусу мережі, визначення окремих його складових, юрисдикційних меж та інших аспектів значно знижує ефективність використання високих інформаційних технологій в ОРД. Існує й інший аспект проблеми, власне, наддержавний характер глобальних мереж об'єктивно потребує розвитку міжнародно-правового регулювання у цьому напрямі. Як зазначають вчені, у глобальному інформаційному просторі кримінально-правова політика кожної держави здійснює безпосередній вплив на кримінологічну ситуацію в цілому. Присутність у глобальних мережах національних сегментів, у яких не криміналізовані окремі діяння, призводить до того, що злочинці активно освоюють зазначені сегменти. Втрата з боку держави правового контролю за суспільними відносинами у досліджуваній сфері означає відмову від одного з найефективніших способів отримання різного виду соціально корисної інформації, якою є дані про підготовку чи безпосереднє вчинення злочинів.

Аналіз світових тенденцій свідчить, що міжнародна юридична практика виробила два основних підходи до правового регулювання глобального інформаційного простору. Так, умовно можна виділити такий підхід, що передбачає тотальний контроль з боку держави над усіма правовідносинами в інформаційній сфері, наявність жорсткої цензури інформаційних ресурсів у межах політичної ідеології країни, мінімізації саморегулювання відносин учасниками інформаційної діяльності.

З огляду на те, що мережа Інтернет виступає свого роду міжнародним феноменом, який певним чином впливає на всі країни, існує необхідність розробки уніфікованого законодавства. Вважаємо, що одним з ефективних способів гармонізації національних законодавств є підготовка модельних законів, які акумулюють у собі основні принципи, вироблені міжнародним правом. Особливістю таких актів є те, що вони не обов'язкові для виконання, а лише орієнтують держави на основні концептуальні положення, яких слід дотримуватись під час розроблення та прийняття аналогічних законів.

Перший суттєвий крок в окресленому напрямі було зроблено Парламентською Асамблеєю країн СНД, яка ухвалила проект модельного закону «Про Інтернет». Серед головних проблем, вирішуваних у законі, такі: визначення основних термінів, зокрема: «Інтернет», «управління Інтернетом», «доменне ім'я», «сайт» (ст. 2); закріплення кола суб'єктів правовідносин у мережі Інтернет (ст. 3); закріплення деяких положень протидії використанню мережі Інтернет у злочинних цілях (ст. 13); визначення місця та часу вчинення дій, які мають юридичні наслідки (ст. 11).

Звернімо увагу на два суттєві положення названого проекту. Зокрема, ст. 11 передбачає, що «юридично значущі дії, вчинені за допомогою мережі Інтернет, визнаються вчиненими на території держави, якщо дії були вчинені особою під час перебування на території держави». Таким чином, зроблено спробу юридичного врегулювання місця вчинення юридично значущих дій через мережу Інтернет та вирішено окремі питання юрисдикції. Проте найважливіше значення у проекті закону, без сумніву, має ст. 13, у якій наголошено, що держава вживає законодавчих та інших заходів з метою протидії використанню мережі Інтернет в злочинних цілях. Для виконання цього завдання держава зобов'язує операторів інтернет-послуг зберігати інформацію про користувачів та надані їм послуги не менше шести місяців і надавати вказані відомості на запит судових та правоохоронних органів. Це положення значно підвищить ефективність взаємодії оперативних підрозділів та провайдерів і, як наслідок, дозволить отримувати з найменшими затратами значну кількість оперативно-розшукової інформації про особу.



З нашого погляду, у законі доцільно передбачити й відповідальність провайдерів щодо попередження особи, якій надаються послуги, про зацікавленість нею правоохоронних органів, адже, як засвідчує практика оперативних підрозділів ДСБЕЗ, означені випадки трапляються досить часто. Але проект закону не передбачає обмежень щодо розміщення інформації та відповідальності власників сайтів, щодо інформації, на них розміщеної. Такі положення, по суті, надають власникам сайтів та провайдерам широкі можливості для саморегулювання відносин у цій сфері.

Отже, підсумовуючи викладене, слід зазначити, що прийняття відповідного закону у нашій країні є вкрай необхідним, оскільки вказаний канал соціальних комунікацій зараз можна використовувати і для розвитку суспільних відносин, і як засіб для вчинення антисоціальних, в тому числі й злочинних дій. За відсутності правового регулювання діяльності користувачів, організацій і держави в мережі виникає і закріплюється подвійний стандарт – закон має виконуватись, але не в мережі. До того ж прийняття відповідного закону, по-перше, оптимізує роботу суб'єктів ОРД щодо отримання оперативно-розшукової інформації та різнопланової інформації довідкового характеру; по-друге, стане вагомим кроком у напрямі вдосконалення правового статусу інформації, отриманої з мережі; по-третє, значно посилить правову основу для забезпечення державної політики протидії злочинності у сфері високих інформаційних технологій; по-четверте, сприятиме врегулювання проблемних питань інших галузей права щодо правовідносин в мережі Інтернет.

Крім того, прийняттям Закону України «Про Інтернет» можна здійснити імплементацію норм міжнародного права, зокрема, Конвенції про кіберзлочинність, у національне законодавство України.

### **Література:**

1. Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних: директива 95/46/ЄС Європейського Парламенту та Ради Європи від 24 жовтня 1995 р.
2. У співробітництво у галузі інформації: Угода від 09.10.1992 р. – Офіційний Вісник України – 2004 - № 40
3. Наумов В.Б. Правовое регулирование распространения информации в сети интернет: автореферат дис. к.ю.н. – Екатеринбург. – 2003. – 24 с.
4. Чучківська А. Електронна комерція: деякі проблеми правового регулювання. Право України – 2003 - №7 – 112 с.
5. Тихомиров Ю.А. Курс сравнительного правоведения – М. – НОРМА, 1996

### **Особа злочинця як елемент криміналістичної характеристики злочинів у сфері мобільних телекомунікацій**

**Нерубашенко І.Ю.**

студент 2-го курсу магістратури факультету № 2  
Навчально-наукового інституту заочного та дистанційного навчання ОДУВС

**Янковий М.О.**

кандидат юридичних наук, доцент  
доцент кафедри криміналістики, судової медицини та психіатрії ОДУВС

Розбудова і розвиток України як правової соціальної демократичної держави вимагає всебічного забезпечення прав та свобод людини і громадянина. Стаття 41 Конституції України проголошує, що кожен має право володіти, користуватися і розпоряджатися своєю власністю, результатами своєї інтелектуальної та творчої діяльності. Право приватної власності є непорушним. Ніхто не може бути протиправно позбавлений права власності [1].

В час стрімкого розвитку науки і техніки, в тому числі інформаційних технологій та телекомунікаційних послуг, набув широкого використання стільниковий зв'язок. За статистичними даними мобільний телефон в Україні має практично кожний другий дорослий і кожна третя дитина; він допомагає створювати інформаційний простір, де людина почуває себе комфортно і безпечно, сучасній людині вже важко уявити своє життя без цього надбання техніки. Поряд з цим, засоби стільникового зв'язку все частіше стають предметами злочинного посягання, а також широко використовуються для маскування діяльності злочинних груп.

Вивчення особи злочинця являє собою складну комплексну проблему, що потребує різнобічного підходу. Існує декілька напрямків дослідження даного об'єкта: кримінологічне, кримінально-правове, кримінально-процесуальне, судово-психологічне, виправно-трудове та криміналістичне. Усі вони, як справедливо зазначається у криміналістичній літературі, становлять єдине ціле – правове дослідження особи і вимагають єдиного підходу [2, с. 46].

З урахуванням завдань, які вирішуються в кримінальному провадженні, можемо зазначити, що вивчення особи злочинця має важливе значення. Практичних працівників слідчих підрозділів, перш за все, у форматі криміналістичної характеристики під час опису структури особи злочинця цікавлять ознаки, які корелюються з іншими її елементами, оскільки, відображаючись в обстановці скоєння злочину у вигляді матеріальних та ідеальних слідів, вони можуть бути використані при їх розслідуванні [3, с. 116].

Обсяг вивчення особи злочинця обмежується конкретними завданнями тієї чи іншої стадії кримінального процесу. Слідчі та працівники оперативних підрозділів Національної поліції при розкритті злочинів використовують узагальнену інформацію про особу злочинця, зосереджену в груповій криміналістичній характеристиці. Зрозуміло, що така інформація має орієнтовний характер, оскільки являється результатом узагальнення багатьох однорідних кримінальних проваджень. Тому ці типові дані про особу підозрюваного, що містяться в груповій криміналістичній характеристиці, використовуються по конкретному кримінальному провадженні, що знаходиться в провадженні слідчого, для висунення та перевірки слідчих версій.

На нашу думку, вивчаючи особу злочинця як елемент криміналістичної характеристики злочинів у сфері мобільних телекомунікацій необхідно з'ясувати наступні дані:

- а) соціальні – соціальний стан, освіта, національність, сімейний стан, професія тощо;
- б) психологічні – світогляд (світосприйняття), переконання, знання, навички, звички, емоції, почуття, темперамент;
- в) біологічні – стать, вік, особливі прикмети;
- г) фізичні дані – сила, зріст, вага та деякі інші.

Як справедливо зазначається у криміналістичній літературі, одним з важливих завдань криміналістики є створення типологічних моделей злочинця щодо різних видів злочинів, зокрема вчинених у сфері мобільних телекомунікацій. У цьому плані криміналістами розроблено чимало різних класифікацій ознак злочинців [4, с. 76]. Серед них найбільш прийнятною для практики, на наш погляд, є класифікація, розроблена М.О. Селівановим. Він пропонує поділити всі властивості злочинця на власні та відносні [5, с. 132]. Із власних ознак злочинця в криміналістичних характеристиках в основному відбиваються такі, як стать, вік, інтелектуальний та фізичний розвиток, морально-психологічний образ, володіння певними професійними навичками, злочинним досвідом і т.д. Криміналістичний інтерес мають і різноманітні прояви відносних характеристик злочинця. Серед них – спосіб життя злочинця, прояв особистості в основних сферах діяльності, співвідношення місця проживання, роботи злочинця з місцем вчинення злочину, особливості правового, пільгового стану особи (посада, дипломатичний імунітет) тощо.

Крім того важливим є встановлення чинників, що мають вплив на формування і здійснення злочинної мети, створення злочинної групи, розподіл ролей між співучасниками тощо. Щодо стереотипу неповнолітнього злочинця, то ця група відрізняється яскраво вираженою антисоціальною спрямованістю поведінки; недисциплінованістю; конфліктністю; схильністю до вживання алкогольних напоїв та наркотичних засобів; незацікавленістю навчанням; об'єднанням в неформальні групи за місцем проживання; явною неповагою до оточуючих.

Резюмуючи, зазначимо, що розглянутий нами елемент криміналістичної характеристики злочинів у сфері мобільних телекомунікацій є інформаційною моделлю особи злочинця і має своїм призначенням на підставі даних про типові елементи злочинної діяльності певної категорії осіб оптимізувати процес висунення та перевірки версій з метою швидкого, повного та об'єктивного розслідування цієї категорії кримінальних проваджень.

#### **Література:**

1. Конституція України [Електронний ресурс] : закон України від 28. 06. 1996р. № 2952-VI із змін., внес. згідно із Законами України : за станом на 01. 02. 2011р. – Електрон. дан. (1 файл). – Режим доступу : <http://zakon1.rada.gov.ua>. – Назва з екрану.
2. Гауман Л.Д. Расследование грабежей и разбойных нападений: уч. пособие[Текст] / Л.Д. Гауман, С.С. Степичев. – М. :РЮ МВД СССР, 1987. – 110 с.
3. Біленчук П.Д. Криміналістика : підручник для вищих навч. закл. [Текст] / П.Д. Біленчук, В.В. Головач, М.В. Салтевський ; під ред. П.Д. Біленчука. – К.: Право, 1997.–254с.
4. Самойлов Г.А. Личностная информация, фиксирующаяся в следах преступления [Текст] / Г.А. Самойлов // Труды ВШ МООП СССР. – М., 1972. – Вып. 34. – С. 20-33.
5. Селиванов Н.А. Советская криминалистика: система понятий[Текст] / Н.А. Селиванов. – М. : Юрид. лит., 1982. – 152 с.

### **СЕКЦІЯ 3**

## **ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ В БОРОТБІ З КІБЕРЗЛОЧИННІСТЮ**

### **Використання інформаційних технологій і системна підприємствах енергетики України**

**Кузьменко Б.В.**

доктор технічних наук, професор,  
професор кафедри автоматизації  
та комп'ютерно-інтегрованих технологій  
Академії муніципального управління м. Київ

Інформаційна технологія - це сукупність методів і способів отримання, обробки, представлення інформації, спрямованих на зміну її стану, властивостей, форми, змісту і здійснюваних в інтересах користувачів. ІТ грають серйозну стратегічну роль в розвитку кожної країни. Їх значення швидко збільшується за рахунок того, що ІТ : активізують і підвищують ефективність використання інформаційних ресурсів, забезпечують економію сировини, енергії, корисних копалини, матеріалів і устаткування, людських ресурсів, соціального часу; реалізують найбільш важливі і інтелектуальні функції соціальних процесів; займають центральне місце в процесі інтелектуалізації суспільства, в розвитку системи освіти, культури, нових (екранних) форм мистецтва, популяризації шедеврів світової культури і історії розвитку людства; забезпечують інформаційну взаємодію людей, сприяють поширенню масової інформації; швидко асимілюються культурою суспільства, знімають багато соціальних, побутових і виробничих проблем, розширюють внутрішні і міжнародні економічні і культурні зв'язки, впливають на міграцію населення по планеті; оптимізують і автоматизують інформаційні процеси в період становлення інформаційного суспільства; грають ключову роль в процесах отримання, накопичення, поширення нових знань по цим трьом напрямкам.

Нові ІТ дозволяють оперативно відстежувати діяльність злочинних співтовариств на принципово іншому рівні. На наш погляд, представляє значний інтерес досвід спецслужб США в розробці і застосуванні систем "Oasis" (ЦРУ) і "Magic Lantern" (ФБР), які дозволяють не лише контролювати інформаційний обмін злочинних співтовариств, але і "зламувати" комп'ютери підозрюваних, впроваджувати в них "трояни" (програми-віруси, що дозволяють відстежувати інформацію в певному комп'ютері).

Нині має місце формування і зростання злочинного шару, що спеціалізується на наданні і забезпеченні технологічних рішень (програмні, апаратні засоби, інформаційні) іншим представникам злочинного співтовариства для реалізації їх злочинних задумів з використанням телекомунікаційної інфраструктури. Така спеціалізація вже має місце, наприклад, при організації DDos- атак, коли продаються готові бот-сети або персональні дані, що включають рахунки у банках і реквізити банківських карток. Наявність подібної тенденції свідчить про те, що відбувається активне проникнення в інфотелекомунікаційне середовище загальнокримінальної злочинності. Це, передусім, шахраї шантажисти, вимагачі і тому подібне категорії злочинців, які використовують телекомунікаційні засоби загального користування для реалізації своїх злочинних задумів. Це повною мірою відноситься і до Інтернету, і до стільникового зв'язку. Найактивніше нині вони поринули в Інтернет, уміло використовуючи його специфіку. Також серйозною проблемою залишається використання телекомунікацій терористами і іншими антисоціальними екстремістськими організаціями, як для агітації, так для збору, переказу грошових коштів, і координації своїх акцій. Проблема загальносвітової протидії загрозам інформаційної безпеки поглиблюється у зв'язку з тим, що тероризм повністю перейшов у сферу міжнародних відносин. Відповідно, шляхи створення ефективних систем протидії також перебувають у компетенції міжнародного права.

Важливо розвивати національні антитерористичні законодавства й водночас гармонізувати законодавчі системи всіх членів світового співтовариства з урахуванням нових форм тероризму та нових умов. На рубежі XX–XXI століть інформаційний тероризм виступає як один із найважливіших чинників міжнародних відносин. Сьогодні тероризм узято на озброєння радикально налаштованими ідеологами й політиками, а також деякими державами, котрі починають активно використовувати його для зміни картини світового устрою. Поява останнім часом нових видів злочинів, особливо, у сфері інформаційних телекомунікаційних мереж представляють реальну загрозу економічній безпеці держави і настійно вимагають адекватних заходів по боротьбі з ними. Все це обумовлює актуальність дипломної

роботи і визначає її спрямованість. Теоретична розробка і практичне вирішення проблем протидії злочинності у сфері інформаційних телекомунікаційних мереж можлива на основі використання світового досвіду, аналізу функціонування інформаційних телекомунікаційних мереж з урахуванням особливостей соціально-національної та економічної ситуації в Республіці Білорусь, а також адаптацією феномена економічної безпеки до національних інтересів білоруського суспільства. Енергетична галузь України в цілому, [1-5], як і електроенергетика зокрема потребують переоснащення новітніми технологіями, а розробникам ІТ- технологій є що запропонувати цьому сегменту. Необхідна співпраця бізнес-підрозділів та ІТ-директорів енергетичних компаній для обміну досвідом з питань впровадження інформаційних і телекомунікаційних технологій в електроенергетичній галузі, слід надати можливість відвідувачам конференції сформулювати вже накопичені питання представникам державних та регуляторних органів України. Потребують вирішення актуальні питання щодо модернізації генеруючих потужностей, інноваційні розробки в області ІТ для ефективної роботи енерго-розподільчих компаній. Слід використати наявний досвід впровадження бездротових телекомунікаційних систем в електроенергетиці.

### **Література:**

1. Баронов В.В., Калянов Г.Н., Попов Ю.Н., Титовский И.Н. Информационные технологии и управление предприятием. М.: Компания АйТи, 2004 г.
2. <http://www.crime-research.org/>;
3. История информатики и философия информационной реальности: учеб. пособие для вузов / [В.В. Тузов и др.]; под ред. Р.М. Юсупова, В.П. Котенко. - М.: Акад. Проект, 2007. - 430 с. - (Gaudeamus).
4. Кузьменко Б.В. Політологічний і кримінологічний аналіз корупції, тіньової економіки і організованої злочинності у пострадянській Україні. – Право України, 1998, №5, с. 103-105.
5. Кузьменко Б.В. Корупція та економічна злочинність у сучасній Україні: вплив на національну безпеку держави. – Право України, 1997, №7, с. 12-14.

### **Сучасні проблеми оцінки захищеності інформаційно-телекомунікаційних систем**

**Казакова Н.Ф.**

доктор технічних наук, доцент,  
завідувач кафедри комп'ютерних та інформаційно-вимірювальних технологій  
Одеської державної академії технічного регулювання та якості

**Фразе-Фразенко О.О.**

кандидат технічних наук,  
доцент кафедри комп'ютерних та інформаційно-вимірювальних технологій  
Одеської державної академії технічного регулювання та якості

**Щербина Ю.В.**

кандидат технічних наук, доцент,  
доцент кафедри комп'ютерних та інформаційно-вимірювальних технологій  
Одеської державної академії технічного регулювання та якості

Питання про необхідність захисту інформації у автоматизованих системах виникло одразу після того, як розподілені обчислювальні систем почали використовувати для її обробки. Важливість цієї проблеми постійно підвищувалась поступовим переходом до безпаперових технологій. Основна проблема полягає у тому, що область захисту дуже важко піддається формальному опису і, як наслідок, оцінка загроз даним і вибір адекватних функцій захисту може виконуватись лише експертним способом. Зважаючи на це, в Україні, з урахуванням міжнародного досвіду, накопиченого в галузі захисту, у 1999 році було розроблено і прийнято нормативний документ НД ТЗІ 2.5-004-99 під назвою "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу" [1], який регулює діяльність, пов'язану з оцінкою захищеності комп'ютерних систем від несанкціонованого доступу до інформаційних ресурсів систем, як з боку зовнішнього середовища, так і від внутрішніх загроз. У тому ж 1999 році було прийнято ще цілий пакет суміжних документів, що досі діють [2, 3, 4, 5]. З того часу комп'ютерна безпека перетворилась на самостійну галузь знань, а прискорений розвиток відкритих інформаційно-телекомунікаційних систем змусив передові країни Заходу об'єднати

свої зусилля з удосконалення способів оцінки загроз, і принципів побудови адекватних систем захисту. Результатом таких зусиль став міжнародний стандарт ISO 15408 – 1999 “Загальні критерії оцінки безпеки інформаційних технологій” (TheCommonCriteriaforInformationTechnologySecurityEvaluation), прийнятий у 1999 році. Цей документ складається із трьох частин: частина перша – “Вступ та загальна модель”, частина друга – “Функціональні вимоги безпеки” і частина третя – “Вимоги довіри до безпеки” [6, 7, 8]. Пізніше цей пакет був розширений і доповнений суміжними документами, що деталізують і пояснюють особливості його використання. Визначивши свій шлях розвитку як європейська держава, Україна повинна була приєднатись до цього напрямку і зробити свій внесок до подальшого розвитку інформаційної безпеки як науки і узгодження своєї законодавчої бази зі світовими угодами у цій галузі.

Ще однією проблемою нормативно-правового забезпечення захисту у інформаційно-телекомунікаційних системах є розробка методик та інструментальних засобів, що дають змогу виконувати достатньо точну оцінку рівня загроз та виконання вимог перелічених документів.

Слід пам’ятати, що сучасні інформаційно-телекомунікаційні системи розвиваються дуже швидко, як і мережа Internet, що служить засобом обміну даних між її суб’єктами. Звичайно, так само швидко зростає і кількість потенційних загроз в середовищі функціонування таких систем. Зважаючи на те, що прототипом українських критеріїв [1] були взяті канадські критерії, написані на рубежі 80 – 90 років минулого сторіччя, можна стверджувати, що вони не повною мірою відповідають сучасним вимогам захисту. Розбіжності, що мають місце між українськими нормативними документами і міжнародними стандартами захисту не дозволяють розробникам систем захисту використовувати оцінки і досвід зарубіжних фахівців. Треба розуміти, що такий досвід у країнах Заходу накопичується і постійно матеріалізується у вигляді додаткових до “Загальних критеріїв” методик і нормативних документів. До їх складу слід віднести насамперед “Загальну методику оцінки безпеки ІТ”, “Керівництво по проведенню сертифікації та акредитації комп’ютерної безпеки”, “Профілі захисту мережних екранів і комерційних систем” та інші.

Документи ISO/IEC мали на меті створення єдиної формальної мови для описання процесів, пов’язаних із оцінкою захищеності інформаційних технологій. Розповсюдження і використання закладених в їх основу концепцій у всіх країнах світу мало підвищити ефективність отриманих оцінок дослідження за рахунок можливості порівняння результатів роботи проведеної різними групами експертів. “Загальні критерії” забезпечують сумісність з “Федеральними критеріями США”, і фактично являють собою їх удосконалену версію. Це у першу чергу стосується концепції “профілю захисту”, що прийшла на зміну такому поняттю як “клас захисту”. Новим у “Загальних критеріях” є структура вимог до функцій захисту та їх обсяг, що став у рази більшим. Теж саме можна сказати і про новий склад вимог довіри до системи захисту. Збільшення цих обсягів пояснюється розвитком глобальних комп’ютерних мереж та розширенням спектру послуг, що надаються користувачам. Удосконалення мережних протоколів разом з позитивними сторонами приводить і до розширення спектру комп’ютерних злочинів.

Задачі що вирішуються у рамках “Загальних критеріїв” на території України регулюються документом ТЗІ 2.5-004-99. Так само як і “Єдині критерії”, він визначає функціональні вимоги до послуг безпеки (securityfunctionalrequirements) і вимоги до адекватності їх реалізації (securityassurancerequirements). Але тлумачення цих термінів та ступінь їх деталізації не у всьому співпадають. Документ ТЗІ 2.5-004-99 розділяє послуги захисту на чотири групи в залежності від типу загроз: втрати конфіденційності, втрати цілісності, втрати доступу та втрати спостережності. При цьому кількість послуг, що пропонуються у кожному із розділів відносно невелика, описується дуже формально і спосіб її реалізації не оговорується. Що ж стосується “Загальних критеріїв”, то вони розділяють функції захисту за такими признаками як “аудит”, “криптографічна підтримка”, “зв’язок”, “захист користувача”, “ідентифікація та автентифікація”, “управління безпекою”, “приватність”, “захист функцій безпеки та оцінки”, “використання ресурсів”, “доступ до об’єкту” і “довірений канал/маршрут”. ТЗІ 2.5-004-99 на перше місце ставить втрати від реалізації конкретного виду загроз. В “Єдиних критеріях” головними вважаються уразливості в системі захисту та способи їх ліквідації. В останньому випадку способи захисту визначаються на основі статистичного аналізу атак.

Спільним у “Єдиних критеріях” і НД ТЗІ 2.5-004-99 є те, що вони акцентують увагу на програмно-технічному аспекті реалізації захисту інформації, а питання управління безпекою у них відображені слабо. Зважаючи на це, наприкінці 2000 року міжнародний інститут стандартів ISO випустив новий стандарт по управлінню безпекою ISO/IEC 17799 [11] під назвою “Практичні правила управління інформаційною безпекою” (Code of Practice for Information Security Management), розроблений на базі британського стандарту BS 7799. У ньому питання, пов’язані з оцінкою механізмів безпеки організаційного рівню описані більш повно у порівнянні із тим, як це зроблено у “Єдиних критеріях”. У

2007 році був прийнятий розроблений на основі стандарту ISO/IEC 17799 стандарт ISO/IEC 27002 «Інформаційні технології — Технології безпеки — Практичні правила менеджменту інформаційної безпеки (англ. Information technology — Security techniques — Code of practice for information security management)». Цей стандарт надає кращі практичні поради щодо менеджменту інформаційної безпеки для тих, хто відповідає за створення, реалізацію або обслуговування відповідних систем.

Із сказаного випливає, що давно настав час прийняти “Єдині критерії” у якості національного стандарту, що на практиці означає необхідність спочатку узгодити з ними своє національне законодавство у тій частині, що так або інакше пов’язана з інформаційною безпекою. Спроба якось поєднати або узгодити оцінки отримані на основі власних національних і міжнародних критеріїв, так як це було зроблено у нормативних документах [12, 13] є відверто невдалою і не відповідає нагальним вимогам захисту. Наступним кроком має бути створення суміжних нормативних документів та технологій, що дозволяють практично реалізувати вимоги національних стандартів захисту інформаційних технологій.

### **Література:**

1. НД ТЗІ 1.1-003-99. Критерії оцінки захищеності в комп’ютерних системах від несанкціонованого доступу. ДСТСЗІ СБ України.
2. НД ТЗІ 1.1-003-99 Термінологія в області захисту інформації в комп’ютерних системах від несанкціонованого доступу. ДСТСЗІ СБ України.
3. НД ТЗІ 1.1-002-99 Загальні положення по захисту інформації в комп’ютерних системах від несанкціонованого доступу. ДСТСЗІ СБ України.
4. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності в комп’ютерних системах від несанкціонованого доступу. ДСТСЗІ СБ України.
5. НД ТЗІ 3.7-001-99 Методичні вказівки по створенню технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.
6. Information technology. Security techniques. Evaluation criteria for IT security. Part 1 : Introduction and general model. – ISO/IEC 15408-1.19 99.
7. Information technology. Security techniques. Evaluation criteria for IT security. Part 2 : Security functional requirements. – ISO/IEC 15408-2.1999.
8. Information technology. Security techniques. Evaluation criteria for IT security. Part 3: Security assurance requirements. – ISO/IEC 15408-3 .1999.
9. НД ТЗІ 2.6-002-2015. Порядок зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99.
10. НД ТЗІ 2.7-013-2016. Методичні вказівки з виконання зіставлення результатів оцінювання засобів захисту інформації від несанкціонованого доступу на відповідність вимогам ISO/IEC 15408 з вимогами НД ТЗІ 2.5-004-99.
11. Information technology. Security techniques. Code of practice for information security management. – ISO/IEC 17799-2005.
12. НД ТЗІ 2.6-002-2015 Порядок зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99.
13. НД ТЗІ 2.7-013-2016 Методичні вказівки з виконання зіставлення результатів оцінювання засобів захисту інформації від несанкціонованого доступу на відповідність вимогам ISO/IEC 15408 з вимогами НД ТЗІ 2.5-004-99.

### **Методи та засоби таймерного захисту інформації**

**Осадчий Є.О.**

завідуючий НДЛ Київського національного  
університету імені Тараса Шевченка,

**Горбунов О.А.**

Київський національний  
університет імені Тараса Шевченка

Життєвий цикл пристроя-трансформера (ПТ) забезпечують технології названі трансформерними (ТТ) [1, с.11]. Це можуть бути і ті технології, що надають продукту необхідні властивості для досягнення поставленої мети. У реальному, а не іграшковому світі можна не тільки відшукати ПТ і ТТ, а й побачити перспективність їх застосування в технічному прогресі. Виявилось, що здатністю до трансформації може володіти навіть найпростіший пристрій. Подальший розвиток ПТ, не залежно від

складності та сфери застосування, зажадало визнання їх певним видом винаходу. У ньому мають бути присутні всі існуючі властивості аналогів, а також нові - кожну з яких, при необхідності, може бути актуалізовано. Якщо в будь-якій технології інформаційна складова є пріоритетною, то це дає підстави також внести її в назву. В якості живого прикладу ТТ доцільно послатися на «розкручену» і перспективну в майбутньому медичну інформаційну ТТ, яка містить в своєму складі складні ПТ. У неї яскраво виражена інформаційна комунікативна складова. Ця ТТ досить добре представлена в статті Kelly Servick журналу Science від 11 December 2015: Vol. 350 no. 6266 pp. 1306-1309, DOI: 10.1126 / science.350.6266.1306. Тому, немає сенсу описувати подробиці і розкривати перспективи розвитку її складових. Розглянемо специфічну ТТ в інформаційній предметній області боротьби з кібернетичною злочинністю. Вона більш відома як ТТ «таймерного» кодування інформації [1, с.60-66]. Для нас ця ТТ цікава тим, що сама постановка завдання зажадала ряду унікальних винахідницьких рішень, перші з яких, вже змогли перевести її в практичну площину. Ми обмежимося розглядом суті найважливіших з них - тих, які стали ключовими для реалізації цієї технології. Але з початку, обґрунтуємо їх вибір.

Найближчим аналогом ТТ «таймерного» кодування можна вважати відомий прийом кінематографії (криміналістики) - функцію "стоп кадру" за часом, а потім - пошук в максимально збільшеному кадрі інформативно необхідного фрагмента. У комп'ютерному програмуванні - це операція "переривання по таймеру". Її можна використовувати для часового (таймерного) кодування інформації. Наприклад, послідовно зчитуються записи лінійного файлу і в заданий момент часу (таймерною міткою) вибирається необхідний запис (ряд записів). Тоді, по цій мітці, завжди можна знайти потрібну інформацію. Унікальність частоти таймера і генератора змістовної для користувача інформації забезпечують ефективність захисту таймерного кодування. Але, швидкодія таймерного лічильника, на існуючих комп'ютерах, дуже низька. Нам вдалося, на звичайному персональному комп'ютері (ПК), програмно змодельовати роботу таймерного кодування при обробці записів інформації розміром до 100 байт. Навіть таке обмеження дало можливість продемонструвати більш ніж 10 кратне стиснення вже архівованої інформації. Але цей експеримент також підтвердив наявність непереборних технічних обмежень для комп'ютерів Фон Неймановської архітектури. Так як таке перетворення інформації для них є малоефективним. Тому, була запропонована архітектура ПТ для майбутнього таймерного комп'ютера, першу чергу швидкодіючих, унікальних по частоті та функціонуванню еталонних лічильників часу. Вони працюють на операції зсуву, тобто в 1 системі числення (СЧ), а потім час відтворюється в зручних для користування СЧ. На їх базі були створені алгоритми які не тільки збільшують швидкість обробки інформації, але і забезпечують її нетрадиційним «таймерним» захистом. Доведено, що сьогодні, межею швидкодії таких лічильників може бути швидкість світла. Коротко покажемо прикладне значення цих рішень. Воно ґрунтується на припущенні, що будь-яка інформація, в кінцевому підсумку - число, яке може бути представлено в одній з  $k$  - тих систем числення, при  $1 \leq k \leq n$ , де  $n$  - образне (аналогове) її відображення, що є достатнім для повного її осмислення. Допускаються змішані СЧ. Число на першому рівні смислової інтерпретації є даними і в найпростішому випадку складається з послідовності «1». Основна властивість такого числа - кількість. Його можна порахувати і представити в комфортній для людини і комп'ютера  $k$ -ій СЧ. Це є інформація, що інтерпретується (змістовна) для користувача, тобто є її аналоговим (образним) уявленням для нього. На цифровому рівні йому відповідає уявлення в  $n$  - річній СЧ. На формалізованому (цифровому) рівні представлення інформації - це число, місце знаходження на носії останньої з множини 1 або її подання в  $n$  - річній СЧ. Звідси, 1 і  $n$  - річна СЧ, дві сторони одного і того ж. Будь-яку комбінаторику, як різновид інформації, теж можна привести до числа. Наприклад, комбінаторика символів алфавіту дає слово. Їх кількість, для європейських мов, звичайно є більшою кількості використовуваних символів алфавіту, на момент написання повідомлення, наступного змістовного рівня (речення). Простий їх перебір, навіть не статистично оптимізований, вимагає менше часу, ніж генерація, з використанням двійкового лічильника, речення шляхом рахування числа. Інформаційна суть цієї технології, в первинній обробці інформації представленої в пам'яті комп'ютера в вигляді унікальної тимчасової «таймерної» мітки і вона є змістом ТТ таймерного перетворення інформації. У реальності, для традиційних ПК, це може бути, наприклад, унікальне двійкове число (як фізична перешкода на носії). Воно з'являється на тлі лінійного запису в певний момент часу, якому відповідає генерована, наприклад, в результаті двійкового рахунку, аналогова інформація. Витрати часу на перетворення інформації з цифрової форми представлення в аналогову і назад для цієї технології є дотичним (несуттєвим). Важливіше забезпечити її однозначну аналогову (змістовну) інтерпретацію усіма користувачами. А це зводиться до простого процесу знаходження однозначної відповідності числа в різних СЧ і остання ( $n$ -на) з них є найповнішою для смислової інтерпретації одержувачем. Таке відповідність найпростіше здійснити через «1» СЧ коли одна і та ж особа передає і отримує інформацію і володіє надійною асоціативною пам'яттю. Для того, щоб розпізнати інформацію, йому достатньо лише

отримати часовий сигнал про її появу. Звідси справедливе твердження. Менша кількість символів в інформаційному повідомленні потенційно (при наявності бази знань) містить в собі більше інформації і навпаки. Обґрунтуємо значення СЧ і виявимо базові конструктивні елементи (БКЕ), які зможуть стати кращими для комп'ютерів майбутнього і досягнення мети передачі інформації. Існують об'єктивні технічні причини поширення комп'ютерів Фон Неймановської архітектури. Вони базуються на двійковому цифровому кодуванні. Тому, всю інформацію, в т.ч. аналогову, намагаються привести до двійкового числа. Але якби була рівноцінною ефективність обробки інформації в будь-якій СЧ, а не в 2-ій, то використовували б виключно аналогові комп'ютери, тобто обробляли б інформацію в 1/n - річній СЧ. Наведена нами концепція побудови аналогових комп'ютерів значно спрощує і прискорює всі можливі комп'ютерні операції. Не випадково, первинна ідея комп'ютера ґрунтувалась на роботі машини Тюрінга.

Відомо, що первинною базовою комп'ютерною операцією є операція зсуву. Наступна в ієрархії - операція двійкового складання і вона вже потребує більш складних технічних БКЕ комп'ютера. На технічному рівні операцію зсуву реалізують лінії затримки будь-якого виконання. Вони ідеально підходять і для реалізації лічильника часу (одиничного лічильника). Лінія затримки проста і перспективна, але нею обмежуватися недоцільно коли час розпізнавання, з її допомогою, адекватного символу в просторі пам'яті комп'ютера є нестабільним. На винахідницький рівень нам вдалося зняти це обмеження. Реальна перспектива досягнення обмеження швидкості операції зсуву швидкістю світла дозволяють сподіватися на практичну цінність і перспективність запропонованих технічних рішень. Таку можливість представляє архітектура конструкції специфічних швидкодіючих лічильників, наприклад, [2]. Їх задача - якомога швидше зафіксувати в просторі пам'яті положення «1» (таймерної мітки) що рухається в момент її відповідності розпізнається значення інформації що генерується. Вона адекватна її поданню в k-ічній СЧ, або в аналоговому вигляді, що задовольняє потреби користувача. Повнота її смислового розпізнавання залежить від алгоритму генерації. Наприклад, для текстової інформації, за змістовим навантаженням (зверху-вниз): назва (заголовок), реферат (анотація), зміст (назва розділів), абзаци, речення, слова, символи. Можливі й інші інтерпретації. У кращому випадку, інформацію можна згенерувати за одну операцію зсуву (найменший до розпізнавання інтервал часу). Наприклад, коли необхідне нам повідомлення, генерується першим. У гіршому - кількість інтервалів часу, має дорівнювати кількості символів повідомлення.

#### **Література:**

1. Осадчий Є.О. Трансформерні технології побудови машин і механізмів.- К.: Науковий світ, 2004.- 167 с.
2. Патент Российской Федерации №2128878 МКИ6 Н 03К 23/00. N разрядный счетчик / Осадчий Е.А., Осадчий А.Е.(Украина).- Опубл.10.04.1999.- Бюл. №10.- 16 с.

#### **Основні правові аспекти використання інформаційних технологій у боротьбі з кіберзлочинністю в Україні: проблематика та шляхи вирішення**

**Єгоров Д.А.**

слухач магістратури за спеціальністю «Судова експертиза»,  
Національна академія внутрішніх справ

**Хахановський В.Г.**

доктор юридичних наук, професор  
професор кафедри інформаційних технологій НАВС

На сучасному етапі розвитку суспільних, культурних та економічних відносин в Україні особливої уваги потребує низка питань у сфері протидії кіберзлочинності. Злочинність у визначеній сфері зростає не лише кількісно, такі кримінальні правопорушення стають дедалі більш складними, зростає рівень їх антисоціальної спрямованості. Даний вид злочинів завдає шкоди не тільки економіці нашої держави, а й державному ладу. Поширення комп'ютерної злочинності призвело до необхідності вивчення цього явища, вироблення рекомендацій боротьби з основними напрямками кіберзлочинності.

Широке впровадження комп'ютерних технологій в усі сфери сучасного життя, поряд з простотою і легкістю доступу до глобальної мережі як персональних так і промислових пристроїв має не тільки позитивні наслідки, а й негативні, такі як зростання масштабу кіберзлочинності.

Кіберзлочинність як явище виникло виключно в процесі еволюції комп'ютерних та інформаційних технологій, а метою злочинців є персональні та корпоративні дані, які самі по собі становлять цінність



або за допомогою яких злочинці протиправним шляхом можуть заволодіти грошима, нематеріальними активами або майновими чи немайновими правами тощо. Сьогодні існує багато типів кіберзлочинів, серед яких найбільшу загрозу являють: он-лайн шахрайство, DoS-атаки, дефейс, розповсюдження шкідливих програм (Malware), кардерство, фішинг, комп'ютерне шпигунство, екстремізм у мережі (який все частіше кваліфікується як кібертероризм), особиста образа або наклеп тощо. Більшість із перелічених вище злочинів скоюються не лише на території або у віртуальному просторі однієї конкретної країни, вони можуть мати і більш глобальний міждержавний чи навіть міжнародний характер, тобто є по своїй суті трансграничними.

Актуальність розглянутих у пропонованій доповіді питань зумовлена потребами правоохоронної практики в науково-обґрунтованих рекомендаціях щодо використання інформаційних технологій для протидії трансграничній комп'ютерній злочинності на теренах нашої держави.

Злочинцям легко приховувати докази і здобути злочинним шляхом. Тому вони стали значною загрозою для критичної інфраструктури багатьох держав, адже й енергетичні системи, і фінансові установи, транспорт, медицина залежать від надійної роботи комп'ютерної техніки [1, с. 7].

Слід відзначити відповідну специфіку протидії комп'ютерній злочинності в Україні. Ця специфіка обумовлена наступними факторами [2, с. 84–89]:

- відсутністю налагодженої системи правового та організаційно-технічного забезпечення законних інтересів громадян, держави та суспільства в галузі інформаційної безпеки;
- обмеженими можливостями бюджетного фінансування робіт по створенню правової, організаційної та технічної бази інформаційної безпеки;
- недостатнім усвідомленням можливих політичних, економічних, моральних та юридичних наслідків комп'ютерних злочинів;
- слабкістю координації дій по боротьбі з комп'ютерними злочинами правоохоронних органів, органів суду, прокуратури та невідповідністю їх кадрового складу до ефективного попередження, виявлення та розслідування таких діянь;
- серйозним відставанням вітчизняної індустрії щодо розробки, впровадження засобів і технологій інформатизації та інформаційної безпеки від розвинутих країн світу.

Так, через відсутність протягом тривалого часу кримінологічно значущої інформації про комп'ютерну злочинність, протидія їй з боку правоохоронних органів не завжди носила системний характер. Тому першим етапом організаційних заходів по боротьбі з комп'ютерною злочинністю повинна бути інформаційно-аналітична робота. Перш за все, це створення системи обліку комп'ютерних злочинів, статистичної звітності, розробки порядку аналітичної діяльності органів, які здійснюють протидію таким злочинам, розробки нормативно-правових актів, що регламентують діяльність (взаємодію) спеціалізованих підрозділів з протидії правопорушенням у сфері інформаційно-телекомунікаційних технологій та розробки відповідних методик. Отримані в ході першого етапу організаційних заходів боротьби з комп'ютерною злочинністю дані повинні бути покладені в основу більш повного та всебічного аналізу таких суспільно небезпечних проявів [4]. Виходячи з трансграничності кіберзлочинності на даний час, від фахівця у сфері кібербезпеки необхідні як знання у галузі інформаційних технологій, так і володіння іноземними мовами (в першу чергу англійською) для кооперації на міжнародному рівні та для швидкого отримання інформації з іншомовних джерел.

Боротьба зі злочинністю в сучасних умовах міжнародних комп'ютерних мереж ускладнена з наступних причин:

- злочинні діяння можуть мати місце в кіберпросторі. Для виявлення та розслідування комп'ютерних злочинів, тобто будь-яких злочинів, вчинених з використанням комп'ютерної чи телекомунікаційної мережі, потрібні конкретний спеціальний досвід і знання, процедури розслідування і відповідні юридичні повноваження;
- міжнародні комп'ютерні мережі, такі як Інтернет, є відкритим середовищем, що дає користувачам можливості чинити певні дії за межами кордонів держав, у яких вони перебувають. У той же час оперативні заходи або слідчі дії правоохоронних органів повинні обмежуватися територією власної держави. Це означає, що боротьбу зі злочинністю у відкритих комп'ютерних мережах не можна здійснювати без належного міжнародного співробітництва;
- відкритість глобальних інформаційних мереж надає можливість користувачам вибирати таку юрисдикцію, яка відповідає їхнім цілям. Користувачі можуть вибирати ті країни, в яких певні діяння, здійснені в кіберпросторі, не визначаються як кримінально карані. Такі країни можуть створювати привабливі можливості для протиправних дій осіб з тих держав, де такі дії, згідно внутрішнього законодавства, підпадають під кримінальну відповідальність.

Враховуючи важливість наведених проблем, Радою Європи 23 листопада 2001 року у Будапешті прийнято Конвенцію Ради Європи про кіберзлочинність. Це один з найважливіших документів, що

регулюють правовідносини у сфері глобальної комп'ютерної мережі і доки єдиний документ такого рівня. Прийняття його - це своєрідна віха в історії боротьби з кіберзлочинністю [3]. Наша країна ратифікувала цю конвенцію 7 вересня 2005 року [5, с. 71].

Однак, оскільки жодна держава не може захистити себе, вживаючи заходів тільки на національному рівні, для комплексної протидії кіберзлочинності необхідні:

- гармонізація кримінального законодавства про кіберзлочини на міжнародному рівні;
- розробка на міжнародному рівні та імплементація в національне законодавство процесуальних стандартів, що дозволяють ефективно розслідувати злочини в глобальних інформаційних мережах, отримувати, досліджувати і представляти електронні докази з урахуванням трансграничності проблеми;
- налагоджене співробітництво правоохоронних органів при розслідуванні кіберзлочинів на оперативному рівні;
- механізм вирішення юрисдикційних питань у кіберпросторі.

Таким чином, міжнародне співробітництво є ключовим моментом у ліквідації правового вакууму, існуючого між розвитком інформаційних технологій та реагуванням на них законодавства. Процес вироблення заходів на міжнародному рівні, як свідчить досвід, сам по собі є комплексною проблемою. Однак це єдиний шлях забезпечити безпеку користувачів і держави від електронних посягань, а також ефективно розслідувати і запобігати кіберзлочинам.

### **Література:**

1. Гуцалюк М. Перший міжнародний стратегічний конгрес «E-CRIME 2002» / М. Гуцалюк // Крок. – 2002. – № 24.
2. Бутузов В.М. Злочини із застосуванням сучасних інформаційних технологій // Науково-практичний журнал “Боротьба з організованою злочинністю і корупцією” – 2003. – № 7.
3. Европейская Конвенция по киберпреступлениям от 23 ноября 2001 г. / [Електронний ресурс] – Режим доступу: <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081580>.
4. Бутузов В.М. “Особенности планирования заходов по запобіганню та протидії злочинам у сфері високих технологій” Матеріали міжвузівської науково-практичної конференції 14 грудня 2007 року: Боротьба зі злочинами у сфері комп'ютерної інформації: проблеми та шляхи їх вирішення – Донецьк: ДЮІ ЛУНВС, 2007.
5. Про ратифікацію Конвенції про кіберзлочинність: закон України від 7 верес. 2005 р. № 2824-IV // Відомості Верховної Ради України. - 2006. - № 5-6.

### **Приховані канали витоку інформації в інформаційно-телекомунікаційних системах Державної прикордонної служби України та шляхи їх ліквідації**

**Стрельбіцький М.А.**

кандидат технічних наук, доцент,  
докторант докторантури Національної академії  
Державної прикордонної служби України імені Б. Хмельницького

**Ваврічен Ол.О.А.**

старший викладач кафедри зв'язку, автоматизації та захисту інформації  
Національної академії Державної прикордонної служби України імені Б. Хмельницького

Побудова сучасних інформаційних систем тісно пов'язана з проблемою забезпечення інформаційної безпеки. Вивченню цього питання присвячена значна кількість робіт дослідників, серед яких Leonard J. LaPadula, D. Elliot Bell, Harrison M., Hoffman J., B.A. Герасименко, А.А. Грушо та інші. Разом із тим, на теперішній час розроблена та впроваджена в дію велика сукупність міжнародних та вітчизняних стандартів та нормативних документів у галузі інформаційної безпеки.

Інформаційна безпека - стан захищеності системи від загроз чотирьох основних типів: конфіденційності, цілісності, доступності та спостереженості [7]. Для опису процесу протидії зазначеним загроз розроблені математичні моделі, які формалізують засади розмежування доступу, контролю цілісності інформації, доступності даних та математично суворо визначають вимоги та умови безпечного функціонування інформаційної системи, або іншими словами, суворо обґрунтовують коректність і адекватність функціонування систем забезпечення інформаційної безпеки.

Одним із питань забезпечення конфіденційності інформації є проблема розмежування доступу до ресурсів інформаційної системи. Аналіз літератури [1–5] показав, що в даний час існує достатня

кількість підходів, що визначає доступ користувачів до тих або інших видів даних (ресурсів) інформаційної системи. При цьому основними з них є технології систем: дискреційного розмежування доступу; мандатного розмежування доступу; тематичного розмежування доступу; рольового розмежування доступу; суб'єктно-орієнтована технологія ізольованого програмного середовища.

Разом із тим, як показав аналіз вище перерахованих систем, розмежування доступу користувачів до інформації з різним ступенем секретності здійснюється на підставі раніше визначених категорій даних та рівнів доступу на конкретний момент часу або невеликий термін функціонування системи.

Існуючу систему надання доступу та допуску до матеріальних носіїв секретної інформації (МНСІ) можна віднести до дискреційної системи розмежування доступу, яка описується мандатною моделлю доступу Бела ЛаПадули [2], а саме можливістю ознайомлення з документом, гриф секретності якого не вище допуску користувача (правило заборони читання наверх). Дана модель обмежує інформаційні потоки з метою недопущення витоку інформації.

Керівний документ, який визначає ступінь конфіденційності інформації – «Звід відомостей, що становлять державну таємницю» (ЗВДТ) [6] визначає порядок присвоєння грифа секретності МНСІ, а саме відповідність інформації хоча б одному із пунктів цього документу є підставою для надання документу, виробу чи іншому матеріальному носію інформації, що містить ці відомості, грифа секретності, який відповідає ступеню секретності, установленому для них у ЗВДТ.

Проведений аналіз розділів ЗВДТ показав наявність агрегованих пунктів з різними ступенями секретності, причому в окремих розділах більше 50 %.

Під агрегованим пунктом ЗВДТ будемо розуміти пункт в якому ступінь секретності сукупності його складових відрізняється, а саме вищий від окремої складової. Існуючі моделі розмежування доступу не враховують наявність агрегованих пунктів з різними ступенями секретності.

Розглянемо можливі шляхи виникнення витоку інформації. З цією метою формалізуємо окремі поняття:

$\{O\}$  – об'єкти системи (користувачі або процеси, які виконуються від їх імені)

$\{S\}$  – суб'єкти системи (конфіденційна інформація)

$\{R\}$  – матриця доступів, рядки якої відповідають суб'єктам, а стовбці – об'єктам

Значимо, що  $\{O^A\} \cup \{O^H\} = \{O\}$ ,  $\{O^A\} \cap \{O^H\} = \emptyset$

де:  $\{O^A\}$  – агреговані об'єкти системи

$\{O^H\}$  – не агреговані об'єкти системи

Всі об'єкти та суб'єкти системи мають відповідний рівень допуску  $l \in L$ , де  $L$  – множина рівнів конфіденційності. Таким чином, суб'єкт  $S_l$  має доступ  $A(S_l, O_k)$  (де  $A$  – предикат наявності доступу) до об'єкта  $O_k$  тоді і тільки тоді, коли  $l \geq k$ , тобто при домінуванні рівня допуску суб'єкта над об'єктом та наявності допуску  $\{S_l, O_k\} \in R$ .

Перший спосіб. У відповідності до моделей розмежування доступу та вимог керівних документів існує процедура пониження ступеня конфіденційності даних (довірений суб'єкт – в термінах моделей, експерт – ЗВДТ). Таким чином, можлива ситуація з декласифікації окремих складових агрегованого об'єкту без врахування часу з подальшим наданням доступу користувачеві з відповідним рівнем допуску. При умові пониження всіх складових об'єкта та надання суб'єкту даного рівня допуску до вказаних об'єктів виникає витік інформації, так як  $O_l^A = O_{l-1}^A$ . Таким чином, можливе виникнення прихованого каналу витоку інформації при деагрегації об'єкта при дотриманні вимог політики безпеки та керівних документів.

Другий спосіб. У відповідності до визначення поняття агрегованого об'єкта системи та відповідно до вимог ЗВДТ рівень його конфіденційності повинен стати вищий при наявності на МНСІ всіх його складових. Таким чином, можлива зворотна першому способу ситуація, коли суб'єкти у відповідності до політики безпеки формують на МНСІ сукупність агрегованого об'єкта з вищим ступенем конфіденційності.

У випадку доступу суб'єкта  $S_{l-1}^m$  до МНСІ  $O_{l-1}$  на якому агрегується сукупність об'єкта  $O_l^A$  виникає прихований канал витоку інформації, так як порушується рівень доступу (рівень об'єкта переважає над рівнем суб'єкта).

З метою ліквідації зазначених прихованих каналів витоку інформації необхідно реалізувати відповідні механізми в політиці безпеки інформаційно-телекомунікаційних систем. Ліквідація першого способу прихованого витоку інформації передбачена моделлю Бела ЛаПадули [2], а саме «заборона запису вниз». Разом із тим в реальній системі реалізація цього принципу є проблемною, так як пониження рівня класифікації об'єктів передбачено керівними документами, зокрема ЗВДТ, при перевищенні терміну зберігання. Ліквідація другого способу прихованого витоку інформації при агрегації об'єкта не передбачена моделями розмежування доступу.

Вирішення наведених проблем можливе шляхом впровадження в інформаційно-телекомунікаційну систему тематичного розмежування доступу, який передбачає наявність механізму збереження історії надання доступів суб'єкта до об'єктів системи з початку реєстрації користувача та формування і підтримання тематичного класифікатора, який базується на вимогах керівних документів та особливостей функціонування прикордонного відомства.

Як було зазначено вище, проблема прихованого витоку інформації виникає тільки при розгляді агрегованих об'єктів  $\{O^A\}$ , які відповідають певній тематиці ЗВДТ.

**Висновок.** В результаті аналізу керівних документів та існуючих моделей розмежування доступу визначені можливі канали прихованого витоку інформації без порушення політики безпеки. Запропоновано спосіб попередження несанкціонованого доступу суб'єктів інформаційної системи шляхом запровадження тематичного класифікатора та функції історії доступів.

Напрямами подальших досліджень є дослідження процесу формування тематичного класифікатора в залежності від особливостей функціонування прикордонного відомства, а також визначення процедури формування функції історії доступів у випадку пониження рівня доступу суб'єкта інформаційної системи.

#### **Література:**

1. Девянин П.Н. Модели безопасности компьютерных систем / П.Н. Девянин. – М.: Издательский центр «Академия», 2005. – 144 с.
2. Bell D.E. Unified Exposition and Multics Interpretation MITRE Corporation / D.E. Bell, L.J. LaPadula // Secure Computer System: (1976). [Електрон. ресурс]. – Режимдоступресурсу: <http://csrc.nist.gov/publications/history/bell76.pdf>.
3. Biba K. Integrity Considerations for Secure Computer Systems / K. Biba // Technical Report MTR-3153, MITRE Corporation, Bedford, MA (Apr. 1977).
4. Семенов, С. Г., В. М. Зміївська, and А. В. Голубенко. "Порівняльні дослідження технологій розмежування доступу для захисту даних в комп'ютерній системі." Системи обробки інформації 3 (2015): 99-102.
5. Цирлов В.Л. Основы информационной безопасности: краткий курс . Учебное пособие. — Ростов-на-Дону: Феникс, 2008. — 253 с. — (Профессиональное образование). — ISBN 978-5-222-13164-0.
6. Служба Безпеки України Наказ 12.08.2005 № 440 Про затвердження Зводу відомостей, що становлять державну таємницю/ Зареєстровано в Міністерстві юстиції країни 17 серпня 2005 р. за № 902/11182
7. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу НД ТЗІ 2.5-004-99. Затверджено Наказом департаменту спеціальних телекомунікаційних систем та захисту інформації служби безпеки України від «28» квітня 1999 р. № 22. Із змінами згідно наказу адміністрації Держспецзв'язку від 28.12.2012 № 806

#### **Використання інформаційних систем для візуального аналізу даних в боротьбі з кіберзлочинністю**

**Дабіжа Д.В.**

ад'юнкт кафедри криміналістики та судової медицини  
Національної академії внутрішніх справ

**Хахановський В.Г.**

доктор юридичних наук, професор  
професор кафедри інформаційних технологій  
Національної академії внутрішніх справ

Новітні засоби зв'язку та системи комунікацій нівелюють кордони між країнами й націями. Цифрові технології принципово змінюють не тільки можливості зв'язку, але й технології обміну товарами, послугами, знаннями, управління виробничими, соціально-економічними й політичними процесами у

житті колективів, регіонів та країн. Разом з безліччю переваг процесу комп'ютеризації та інформатизації з'являються нові види протиправних діянь із використанням технічних засобів та Інтернету. Йдеться насамперед про кримінальні правопорушення у сфері комп'ютерної інформації – комп'ютерної злочинності або кіберзлочинності [1, с. 21; 2, с. 55; 3, с. 69, с. 110].

Загалом кіберзлочинність – це злочинність в так званому «віртуальному просторі або кіберпросторі». Кіберпростір можна визначити як модельований за допомогою комп'ютерата телекомунікаційних технологій інформаційний простір, в якому знаходяться відомості про осіб, предмети або речі, факти, події, явища і процеси, представлені в математичному, символічному або будь-якому іншому вигляді і що знаходяться в процесі руху по локальних і глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального пристрою, а також іншого носія, спеціально призначеного для їх зберігання й накопичення, обробки і передачі [3].

Одним із важливих засобів для розкриття та розслідування кримінальних правопорушень, що вчинені з використанням високих інформаційних технологій і телекомунікаційних мереж є впровадження методів алгоритмізації та програмування в діяльність органів поліції.

Зазвичай під алгоритмом розуміються набір інструкцій, які описують порядок точно визначених дій виконавця, щоб досягти результату розв'язання задачі за скінченну кількість дій; система правил виконання дискретного процесу, яка досягає поставленої мети за скінченний час.

У криміналістиці поняття алгоритму формувалось завдяки результатам широкого використання знань, запозичених з різних наук. Разом з цим особливість алгоритму, який використовується у криміналістиці, на відміну алгоритмів, які застосовуються в математиці, полягає у відсутності чіткості і недвозначності у визначенні наслідків того чи іншого рішення, що зумовлено специфікою криміналістичної діяльності та неможливістю в усіх випадках побудувати «жорсткі» (чітко визначені) алгоритми. Насамперед це пов'язано із завданнями, які вирішує криміналістика.

Так, під час проведення окремих слідчих (розшукових) дій слідчий стикається з широким колом найрізноманітніших ситуацій, що вимагають від нього правильного (адекватного) сприйняття, оцінки та вирішення їх шляхом здійснення низки послідовних дій. З цього питання М.П. Яблоков підкреслює: у розслідуванні можна виявити масу однотипних ситуацій і відповідних їм дій слідчого, які можуть бути використані для створення алгоритму розслідування в типових слідчих ситуаціях [4, с. 70].

Одночасно треба враховувати, що різноманітність, оригінальність та нестандартність конкретних ситуацій суттєво ускладнюють їх типізацію. Крім того, не можна окреслити всі без винятку ситуації та запропонувати до них відповідні алгоритми дій слідчого, тобто ідеально (стовідсотково) формалізувати розв'язання завдань розслідування [5, с. 102–108]. В. В. Бірюков також наголошує на тому, що головна проблема алгоритмізації розслідування знаходиться саме в найрізноманітніших слідчих ситуаціях [6, с. 195].

Діяльність з алгоритмізації завжди передуює процесу програмування з подальшою візуалізацією. Так, Є. П. Іщенко слушно наголошував, що комп'ютеризація надасть максимальну віддачу лише у тандемі з алгоритмізацією розслідування [6, с. 4].

Практика вирішення криміналістичних завдань з використанням математичних методів та ЕОМ свідчить, що коли досліджуваний об'єкт структурно недостатньо складний, а його утворювальні елементи легко формалізуються, то змістовний опис такого виду дозволяє перейти до побудови математичної моделі та математичного формулювання завдання дослідження. Але, як зазначає В. Г. Хахановський, у слідчо-криміналістичній сфері такі ситуації трапляються досить рідко, тому, як правило, математичному моделюванню має передувати побудова формалізованої схеми об'єкта та процесу його дослідження. Щодо кібернетичного моделювання та вирішення слідчо-криміналістичних завдань з використанням ЕОМ, то формалізація об'єкта його дослідження у таких випадках є обов'язковою процедурою [8, с. 152].

Програмування розслідування кримінальних правопорушень є методом раціоналізації і оптимізації його планування, зміст якого складають комп'ютерні програми, спрямовані на визначення наявної ситуації, з'ясування завдань розслідування і вибір засобів для їх досягнення [9, с. 145–146].

Однією з переваг програмної алгоритмізації є можливість графічного, схематичного (візуального) представлення взаємовідносин, обігу (руху) товарів, подій і діяльності, що стосуються явищ або подій про кримінальні правопорушення, які аналізуються. Представлення за допомогою конкретних символів і засад окремих етапів або цілісності аналізу, що проводиться, у вирішальний спосіб полегшує однакову інтерпретацію, а також розуміння істини аналізу і представлених висновків та пропозицій для подальших дій з розкриття кримінальних правопорушень, що вчинені з використанням високих інформаційних технологій і телекомунікаційних мереж.

Говорячи про передові методи алгоритмізації та аналізу, не можна не згадати про програму «I2», яку вважають світовим лідером серед програмних засобів для візуального аналізу даних в процесі розслідування кримінальних правопорушень і використовують аналітики та слідчі всього світу.

Також, існують й інші візуалізаційні аналітичні системи, які використовуються правоохоронними органами зарубіжних держав. Так, система CrimeView Server здійснює аналіз певних ділянок місцевості (зон) з максимальним рівнем вуличної злочинності, зміни маршрутів патрулювання у виявлені зони. Система My Neighborhood Map System призначена для візуалізації повідомлень про злочини, що надходять, і звітів поліції. Складається з наступних компонентів: 911 Incident Responses Map; Police Reports Map; Monthly Crime Statistics Map. Система CrimeDC забезпечує надання громадянам даних про вчинені кримінальні правопорушення в районі їх проживання, у тому числі статистичні дані [10, с. 134, 135].

Значна частина таких систем має досить високу ціну та пропонує не інтеграцію з діючими інформаційними системами та обліками, а повний перехід на них як на нові незалежні системи.

Разом із дослідженнями іноземних колег за 45 років, що минули з початку інформатизації в МВС України, накопичено чималий досвід використання інформаційних систем і технологій у процесі запобігання кримінальним правопорушенням, їх розкритті та розслідуванні.

Так, сьогодні однією з перспективних є інтелектуальна система аналізу Realtime intelligence crime analytics system (RICAS), що функціонує з серпня 2014 року в ГУНП України в Харківській області. Цей програмний комплекс розроблявся впродовж 2012–2014 років співробітниками Управління інформаційного забезпечення ГУ НПУ в Харківській області спільно з місцевими ІТ-компаніями.

RICAS – це унікальна інтелектуальна система кримінального аналізу даних, яка об'єднала в єдиному просторі відображення основні і найбільш передові методи і методики кримінального аналізу та аналітичного пошуку в реальному часі, що дозволяє значно підвищити ефективність і результативність розкриття кримінальних правопорушень «по гарячих слідах» і нерозкритих раніше кримінальних правопорушень. Ця система є надбудовою до існуючої ІПІС та відкриває можливості застосування математичних інструментів технологій Data, Mining, Visual mining та OLAP.

Підбиваючи підсумок, слід наголосити на тому, що саме впровадження інформаційних систем для візуального аналізу даних на державному рівні сприятиме розвитку та вдосконаленню сучасних криміналістичних методів алгоритмізації, аналізу криміногенної ситуації та підвищенню ефективності боротьби з кіберзлочинністю.

### **Література:**

1. Документування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку при проведенні дослідчої перевірки : наук.-прак. посіб. / В. М. Бутузов, Л. П. Скалозуб, К. В. Тітуніна, В. П. Шеломенцев. – Севастополь : ЧП «Тимченко», 2010. – 245 с.
2. Організаційно-правові та тактичні основи протидії злочинності у сфері високих інформаційних технологій : навч. посіб. / [В. М. Бутузов, В. Д. Гавловський, Л. П. Скалозуб та ін.] ; за ред. Б. В. Романюка; Є. Д. Скулиша. – К. : 2011. – 404 с.
3. Бутузов В. М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : монографія / В. М. Бутузов. – К. : КИТ, 2010. – 408 с.
4. Яблоков Н.П. Совершенствование методических основ расследования преступлений / Н.П. Яблоков // Советское государство и право. - М.: Наука, 1976. – № 2. - С. 67–72.
5. Журавель В.А. Ситуаційний підхід до формування окремих криміналістичних методик розслідування злочинів / В.А. Журавель // Теорія та практика судової експертизи і криміналістики. – Х. : Право, 2008. – Вип. 8. – С.102– 108.
6. Бирюков В.В. Алгоритмизация расследования. Задачи и проблемы / В.В. Бирюков // Вісник Луганського інституту внутрішніх справ МВС України: Науково-теоретичний журнал. – Луганськ : Луганська академія внутрішніх справ МВС України, 2004. - Випуск 1. – С. 192–197.
7. Ищенко Е.П. Компьютер и криминалистический алгоритм : взаимная оптимизация / Е.П. Ищенко // Вестник криминалистики. – Вып.2 (4). – М.: Спарк, 2002. – С. 4–7
8. Хахановський В. Г. Проблеми теорії і практики криміналістичної інформатики : монографія / В. Г. Хахановський. – К. : Вид. Дім «Аванпост-Прим», 2010. – 382 с.
9. Зорин Г.А. Криминалистическая методология (Фундаментальная криминалистика XXI века) / Г.А. Зорин. - Мн. : Амалфея, 2000. – 608 с.
10. Узлов Д. Ю. Применение интеллектуальной системы криминального анализа в реальном времени (RICAS) для аналитического сопровождения оперативно-розыскной деятельности и досудебного расследования / Д. Ю. Узлов, В. М. Струков, А. Б. Григорович, А. И. Петрусенко, С. Н. Доскаленко // Право і Безпека. – 2015. – № 2. – С. 132–139.

**Act of the forensic medicine: main features of the storage and access to the evident database. The main ways of protecting electronic versions of the medical documents in Ukraine and Poland**

**Larysa Kupriianova**

PhD in Medicine;

Associate Professor of the Department of Criminalistics  
and Judicial Expertology in  
the Kharkiv National University of Internal Affairs

**Daryna Kupriianova**

Student on the Faculty of Law in

The National University of Opole, Opole, Poland

It is known among all of people that the results of the expertise in sphere of forensic medicine can be used like evidences in the court during the trial for cases from the criminal and administrative law. Moreover, all results and conclusions of the forensic medical expertise, which will be provide by an expert of the forensic medicine is an evidence of the same value, as evidences provided by policemen [1, p. 39-77]. This condition is respected and followed by judges of all instances, regardless where the trials situated are. However, it is known among the specialists, that in different countries of the European Union, such is in Poland, for example, we can see absolutely different and more effective procedure and law in the sphere of storing and providing of the results of forensic medical expertise [3, p. 112-157].

Let us propose you to consider the process of storing and proving the results of forensic medical expertise for trial in Ukraine and in Poland.

We have to note also, that, despite of the fact of existence of different type of responsibilities and duties, people, who work as a forensic medical experts, are just a civil workers, they still do not have enough rights, according to Ukrainian law, for example, to be able to protect medical documents and information about results of developments or searching from the ciber crimes. They do not have enough knowledge for this, actually [2, p. 56-92].

If we speak about Ukraine in the sphere of protecting of private information about details of medical examinations, tests, a wide variety types of developments and conclusion of all, that we underlined above, we can speak just so, that all databases, even the most important and private is downloaded to the usual computer with access to the Internet. All archives of the Ukrainian clinics and hospitals, and, even documents, which more or less are important for the trial, are not protected from the ciber crimes. Moreover, we can speak that this information is particularly not private, according to the Ukrainian law. In the archives of the hospitals or clinics, nobody will check how many copies you will do from this or that document, even if this document is one of the most important evidence for trial. I addition, policemen are not check such transferring of information, too. And, what is more important, such irresponsible behavior in the sphere of private medical results of expertise can provide finally to so tragically consequences, like ciber crimes as well.

If we speak about Poland, so here we can see diametrically different situation with all types of medical documents. Here, according to the criminal law, and law in the sphere of administrative process, it is prosecuted to provide the results of such expertise, to give an access for anybody, who are not a person who takes part in this case in the trial; and, what is the most important fact here, there is a prosecution of using of medical information like an evidence in no cases in trial, even if they are got legally from the hospital [4, p. 54-72]. Moreover, the chief medical officer and the chief of the archive have a personal responsibility for this documents and access for them. And all they duties and responsibilities are written in the criminal law mainly [5, p. 14-51].

Because of the fact, as a conclusion for this article, authors think that it is incredibly important to improve the law and knowledge of the ciber police in the sphere of such crimes. The most acute problem now for the cyber police, is to stop all possibilities of illegal using of medical information without difference or is it important results of expertise for trial, or it is just privet examination's result. In addition, we have to provide protecting of the medical information from the illegal access to it, by working out and active using of the effective protecting programs, to reduce number of possibilities of using medical information illegally by ciber criminals.

**Literature:**

1. Зелинский А. Ф. Криминология: курс лекций / А. Ф.Зелинский. – Х.: Прапор, 1996. – 260 с.
2. Литвак О.М. Держава і злочинність: монографія / О. М. Литвак. – К.: Атіка, 2004. – 304 с.
3. Polish criminal Law: par.2 art.54. - 209 str.
4. L. Gardocki - Prawo karne; wyd. 16. – Str. 54-72.
5. Marek: Prawo karne; wyd. 10. – Str. 14-51.

**Разработка метода управления рисками разработки программного обеспечения**

**Коваленко А.В.**

кандидат технических наук, доцент  
доцент кафедры программирования и защиты информации  
Кировоградского национального технического университета,

**Смирнов А.А.**

доктор технических наук, профессор  
профессор кафедры программирования и защиты информации  
Кировоградского национального технического университета,

**Коваленко А.С.**

ассистент кафедры программирования и защиты информации  
Кировоградского национального технического университета,

Киберпреступность, в данное время, это быстрорастущая угроза для многих отраслей в мировой экономике и промышленности. Угрозы могут классифицироваться, как случайные или преднамеренные. Случайными угрозами являются такие угрозы, которые возникают без предварительного умысла. Примерами реализованных случайных угроз являются: эксплуатация неисправного оборудования, неквалифицированный ремонт компьютерной техники, неправильное срабатывание системы, грубые просчеты в работе, а так же ошибки в разработке программном обеспечении. Проведенные исследования, а также анализ литературы [1, с. 24; 2, с. 19] показали, что управление риском разработки программного обеспечения (ПО) состоит в заблаговременном выявлении связанных с риском финансовых, технических, психологических, и др. опасностей, и принятии мер по снижению риска путем целенаправленного изменения этих факторов с учетом эффективности принимаемых мер. Управление риском разработки ПО включает систему мероприятий, осуществляемых как до проявления негативного события, так и после его реализации. Однако, как показали исследования, превентивный анализ и учет большинства возможных эксплуатационных ошибок позволит снизить финансовые и др. затраты в жизненном цикле разработки ПО.

Цель работы состоит в том, чтобы показать, что в основу метода управления рисками разработки ПО можно положить полумарковскую модель принятия решений для управляемого марковского процесса в непрерывном времени, что существенно уменьшит риски опасностей, в том числе случайных угроз.

Под термином "управление риском" понимают разработку и обоснование оптимальных программ деятельности, призванных эффективно реализовать решения в области обеспечения безопасности. При этом главным элементом такой деятельности является процесс оптимального распределения ограниченных ресурсов с учетом характерных эксплуатационных, экономических и социальных факторов [2, с. 39].

Рассматриваемую задачу управления рисками разработки ПО при определенных ограничениях на мероприятия по тестированию качества и безопасности, сформулируем в виде полумарковской модели принятия решений для управляемого марковского процесса в непрерывном времени и дисконтированными доходами (с коэффициентом  $0 < \alpha < 1$  в нормальных условиях процесса создания ПО) или расходами (в условиях с отклонениями от плана, связанными с пренебрежением невыявления уязвимостей (ошибок) безопасности). При этом данный вид эксплуатационных рисков отождествляются с последовательно соединенными независимыми элементами, восстанавливаемыми за конечное время.

Оптимальную нерандомизированную стационарную стратегию управления определим с помощью псевдобулевых методов бивалентного программирования, находя все решения системы ограничений. Эти решения определяются на основе алгоритма пересечения решений отдельных неравенств-ограничений, предложенного в работе [3, с. 97] для нахождения базисных решений системы линейных неравенств с булевыми переменными.

В таких условиях сформулируем основную задачу. Пусть каждому состоянию  $i \in S$ , где  $S = \{0, 1, 2, \dots, N\}$  рассматриваемой системы управления рисками разработки ПО поставлено в соответствие конечное множество  $R_i$  решений, элементы которого обозначим как



$r = 1, 2, \dots, r_i$ . Если система находится в состоянии  $i \in S$  и принимается решение  $r = R_i$ , то ее дальнейшее поведение определяется вероятностным законом

$$Y_{ij}^r(t) = P_{ij}^{(r)} F_{ij}^{(r)}(t), \quad j \in S, \quad (1)$$

где  $P_{ij}^{(r)}$  – вероятность перехода системы из состояния  $i$  в состояние  $j$ ;  $F_{ij}^{(r)}(t)$  – функция распределения времени пребывания системы в состоянии  $i$  при принятии решения  $r$  и при условии, что следующий переход произойдет в состояние  $j$ .

При выполнении ряда условий, в каждом состоянии  $i \in S$  существует  $r_i$  решений из конечного множества  $R_i$ . Выбор некоторого решения  $r$  из этого множества  $R_i$  в состоянии  $i \in S$  означает задание величин  $Y_{ij}^r(t)$ ,  $P_{ij}^{(r)}$ ,  $F_{ij}^{(r)}(t)$ ,  $k_i^{(r)}$ ,  $j \in S$ .

При условии непрерывности во времени исследуемого процесса будем пользоваться переоценкой экспоненциального вида с нормой  $\alpha$ , то есть если в некоторый момент времени затраты составляют какую-то единичную величину, то через время  $t$  эти затраты уже будут  $e^{-\alpha t}$  единичных величин. Тогда если  $k_i$  – расход за единицу времени, то суммарный расход за время  $t$  имеет вид

$$\int_0^t k_i e^{-\alpha \tau} d\tau = \frac{k_i}{\alpha} (1 - e^{-\alpha t}). \quad (2)$$

Обозначим  $i_n$  состояние системы после  $n$ -го перехода,  $u_n$  – принятое решение, а  $\tau_n$  – время пребывания в этом состоянии ( $n = 0, 1, 2, \dots$ ),  $i_0$  – начальное состояние. Допустимую стратегию  $\beta$  для системы управления разработкой ПО определим как последовательность  $\{\beta_0, \beta_1, \beta_2, \dots\}$ , где  $\beta_n(\bullet / z_n)$  – вероятностная мера, сосредоточенная на функции ограничения  $U(S)$  на принятые решения (управления), определяемые системой неравенств

$$\sum_{j \in S} c_{rj} x_{rj} \leq b_r, \quad r \in R = UR_j, \quad j \in S, \quad (3)$$

и зависящая от истории управляемой системы к моменту  $n$ -го перехода  $z_n = (i_0, u_0, \tau_0, \dots, i_{n-1}, u_{n-1}, \tau_{n-1}, i_n)$ . Мера  $\beta_n(\bullet / z_n)$  задает рандомизированное правило выбора решения  $u_n$  на основе информации  $z_n$ . Такую стратегию  $\beta$  можно назвать рандомизированной. Стратегия  $\beta$  является марковской, если  $\beta_n(\bullet / z_n) = \beta_n(\bullet / i_n)$ , где  $n = 0, 1, 2, \dots$ . Если стратегия  $\beta$  – марковская стационарная, то управляемый процесс является полумарковским.

Обозначим через  $g_i(t, \alpha, \beta)$  суммарный расход системы, управляемой в соответствии со стратегией  $\beta$ , с нормой переоценки  $\alpha$ , за время  $t$  жизненного цикла разработки ПО. Обязательным условием является то, что процесс начинается в момент  $t = 0$  из состояния  $i$ . Через  $v_i(t, \alpha, \beta) = g_i(t, \alpha, \beta)/t$  обозначим суммарный средний расход системы за время  $t$  при тех же условиях.

Если затраты  $c_{rj}$  позволяют выполнить каждое из ограничений (3), то реализованная на основании (3) система определяет в пространстве  $\mathfrak{R}^d$ ,  $d = \dim R$ , некоторое конечное множество дискретных точек. Тогда существует нерандомизированная стационарная стратегия  $\beta^*$ , называемая  $\beta$  – оптимальной, которая минимизирует суммарный средний расход  $v(\alpha, \beta)$  при произвольной стратегии  $\beta$  и норме переоценки  $\alpha(\alpha > 0)$  [4, с. 128]. При этом  $v(\alpha, \beta)$  есть  $(N + 1) \times 1$ - мерный вектор  $(v_0(\alpha, \beta), v_1(\alpha, \beta), \dots, v_N(\alpha, \beta))$ , где  $v_i(\alpha, \beta) = \lim_{t \rightarrow \infty} v_i(t, \alpha, \beta)$ ,  $i \in S$ . Необходимо

найти  $\alpha$  – оптимальную нерандомизированную марковскую стационарную стратегию  $\beta^*$ , которая минимизирует суммарный средний расход  $v(\alpha, \beta)$  при произвольном начальном распределении процесса  $y = (y_0, y_1, \dots, y_N)$ ,  $\sum_{i \in S} y_i = 1$ ,  $y_i \geq 0$ ,  $i \in S$ .

Не уменьшая общности, в качестве начального распределения возьмем вектор  $y = (1, 0, \dots, 0)$ , т.е. начальное состояние системы. На основе полумарковской модели принятия решений данную задачу приведем к эквивалентной задаче бивалентного программирования с использованием псевдобулевых методов.

Таким образом, в работе усовершенствован метод управления рисками разработки ПО. В основу данного метода была положена полумарковская модель принятия решений для управляемого марковского процесса в непрерывном времени. Отличительной особенностью предложенного метода является использование псевдобулевых методов бивалентного программирования с нелинейной целевой функцией и линейными ограничениями для определения оптимальной стратегии устранения эксплуатационных ошибок. Данный метод актуален при управлении рисками безопасности ПО и соответственно дает возможность сократить случаи случайных угроз при использовании ПО.

Дальнейшие исследования должны быть направлены на оптимизационную стратегию полумарковской модели принятия решений.

#### **Литература:**

1. Безкоровайный М.М. Кибербезопасность подходы к определению понятия // Вопросы кибербезопасности. 2014. № 1 (2). С. 22–27.
2. Хохлов Н.В. Управление риском: Учебн. пособ. для ВУЗов / Н.В. Хохлов. – М: ЮНИТИ-ДАНА, 2001. – 241с.
3. Зоркальцев В.И. Системы линейных неравенств / В.И. Зоркальцев, М.А. Киселева// И: Иркутск, 2007. – 128 с.
4. Вентцель Е.С.: Теория случайных процессов и ее инженерные приложения / Е.С. Вентцель// М.: Академия, 2003, 325 с.

#### **Оцінка технологій радіо доступу з метою реалізації в телекомунікаційній мережі**

**Волинець Д.О.**

старший викладач кафедри зв'язку,  
автоматизації та захисту інформації  
Національної академії Державної прикордонної служби України

**Чесановський І.І.**

кандидат технічних наук, доцент,  
начальник кафедри зв'язку,  
автоматизації та захисту інформації  
Національної академії Державної прикордонної служби України

Організація системи забезпечення інформаційної безпеки на об'єкті інформаційної діяльності це складова частина загальної системи інформаційного захисту органу державної влади, правоохоронної структури, підприємства (організації) будь-якої форми власності. Одним із першочергових завдань є забезпечення надійної охорони контрольованої зони. Це питання в основному вирішується організаційними та інженерними засобами.

Між тим в умовах значного зростання використання мобільних радіотерміналів і мережевого радіообладнання для функціонування телекомунікаційної складової відомчих інформаційно-телекомунікаційних систем, постає питання організації бездротових каналів насамперед в ланці «мобільне робоче місце – серверне обладнання».

Виходячи з цього, постає питання вибору стандарту для організації радіодоступу, оскільки зростаюча мобільність автоматизованих робочих місць не може бути задоволена лише проводовими або автономними рішеннями. Окремим аспектом впровадження сучасних технологій доступу до інформаційних ресурсів в системі автоматизації різних напрямів діяльності є підвищенні вимоги до

безпеки передачі даних, особливо на рівні доступу користувацьких терміналів до мережі, оскільки, як показує практика, це найвразливіша ділянка глобальних, розподілених інформаційних мереж.

Таким чином, вибір технології організації радіодоступу має ґрунтуватись на аналізі цілого комплексу показників технічного, якісного і безпекового характеру.

На сьогоднішній день, на ринку телекомунікаційного обладнання присутня ціла низка технологій радіодоступу, які можуть розглядатись як перспективні для впровадження в телекомунікаційній системі. В табл. 1 приведені основні характеристики найбільш поширених та найбільш перспективних технологій організації бездротових мереж та з'єднань.

З приведених даних можна зробити висновок, що кожна технологія має свої особливості, що визначають її переваги або недоліки в застосуванні.

Для об'єктивної оцінки цих переваг і недоліків різних технологій, з метою проведення їх порівняльної оцінки, необхідно ввести певний комплексний показник ефективності  $K_{ef}$ , що враховує всі можливі співвідношення в окремих характеристиках. Загальний вираз для даного коефіцієнта може бути записаний в наступному вигляді:

$$K_{ef,k} = \prod_i X_{i,k}, \quad (1)$$

де  $X_i$  - нормована по необхідному значенню  $i$ -та характеристика  $k$ -го стандарту, що визначається з наступного виразу:

$$X_{i,k} = \begin{cases} \frac{X_i^{(k)}}{X_{i,max}}, & \frac{X_i^{(k)}}{X_{i,max}} \leq 1, \\ 1, & \frac{X_i^{(k)}}{X_{i,max}} > 1, \end{cases} \quad (2)$$

де  $X_{i,max}$  - необхідне граничне значення  $i$ -ї характеристики для застосування в конкретній підсистемі;  $X_i^{(k)}$  - значення  $i$ -ї характеристики  $k$ -го стандарту.

Дослідження технологій проводилися за найбільш вагомими, на нашу думку, характеристиками для використання на об'єктах інформаційної діяльності. Під час розрахунку «вплив» характеристик на забезпечення оперативно-службової діяльності прийнято за одиницю.

Порівнявши технології за запропонованим комплексним показником (рис.1) ми бачимо, що ефективнішою є технологія Wi-Fi (IEEE 802.11). Між тим, за характеристикою «дальність дії» (рис. 2) після 200 метрів значення показника ефективності для технології Wi-Fi значно зменшується.

Таблиця 1 – Характеристики основних сучасних стандартів радіодоступу

Характеристик и/стандарт	Технологія радіодоступу				
	WMAN (міські бездротові мережі)	WLAN (локальні бездротові мережі)	WPAN (персональні бездротові мережі)		
Стандарти	WiMAX (Mobile WMAN) (IEEE 802.16)	Wi-Fi (IEEE 802.11)	Bluetooth (IEEE 802.15.1)	UWB (IEEE 802.15.4a/b)	Zig-Bee (IEEE 802.15.4)
Максимальна пропускна спроможність	до 1 Гбіт/с (WMAN), до 100 Мбіт/с (Mobile WMAN)	150 Мбіт/с	3 Мбіт/с	48 0 кбіт/с	250 Кбіт/с

Діапазон частот	1,5-11 ГГц (WMAN), 2,3-13,6 ГГц (Mobile WMAN)	2,4-2,5 ГГц, 5 ГГц,	2,4- 2,48 ГГц	3,1 - 10,6 ГГц	868 МГц
Дальність, м	25000 (WMAN), 5000 (Mobile WMAN)	150	10- 100	10	10-75
Максимальна кількість елементів мережі	до 1000	до 100	до 7	до 128	до 255
Алгоритм захисту інформації	56-бітові ключі	128-бітові ключі	128- бітові ключі	DR M	128-бітові ключі
Необхідність використання ліцензованих діапазонів	так	ні	Ні	ні	ні

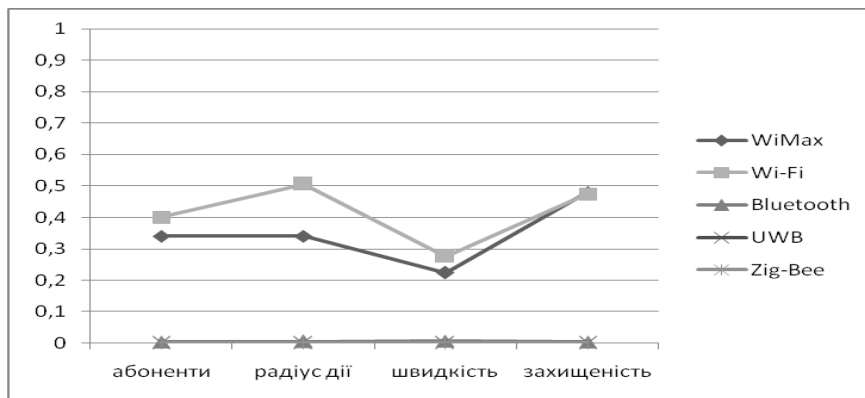


Рисунок 1- Середні значення комплексного показника ефективності для основних технологій бездротового доступу

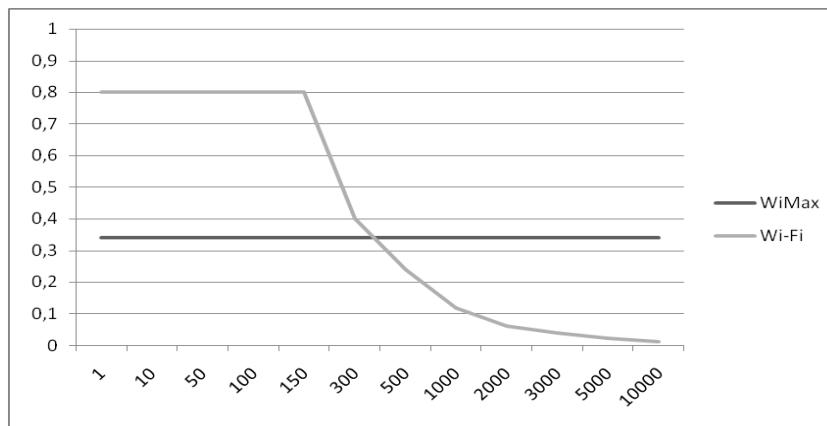


Рисунок 2 - Залежність комплексного показника ефективності від дальності дії технологій бездротового доступу для стандартів WiMax та Wi-Fi

Таким чином за результатами порівнянь стандартів бездротової організації телекомунікаційних мереж слід вважати, що за основними характеристиками (кількість абонентів, радіус дії, швидкість передачі даних та захищеність) із існуючих на сьогодні технологій (при умові територіального обмеження підрозділу до 200-400 метрів) найбільш актуальною є технологія Wi-Fi (IEEE 802.11).

Разом з тим дана технологія має низку недоліків, які не гарантують захист інформації, що передається і, тому, постає питання дослідження шляхів підвищення безпеки даних, у відомих локальних обчислювальних мережах.

**Література:**

1. IEEE Standard for Information technology. 802.11-2012. Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements [Текст] . – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. – 2012. – Р. 1-2793.
2. Довгий С.О., Воробієнко П.П., Гуляєв К.Д. Сучасні телекомунікації: Мережі, технології, безпека, економіка, регулювання. - Видання друге (доповнене).- /За загальною редакцією Довгого С.О.-К.: «Азимут-Україна».-2013.-608с.
3. Макаренко А.Ю., Парфенова А.О., Могильний С.Б. Бездротові технології передачі даних Wi-Fi, Bluetooth та ZigBee - Вісник Національного технічного університету України "КПІ" Серія – Радіотехніка. Радіоапаратобудування.-2010.-№41, с -171.

**Методика оцінки рівня кібербезпеки в Україні**

**Кудінов В.А.**

кандидат фізико-математичних наук, доцент,  
завідувач кафедри інформаційних технологій  
Національної академії внутрішніх справ

Серед основних напрямів державної інформаційної політики в Україні є створення інформаційних систем і мереж інформації, розвиток електронного урядування, постійне оновлення, збагачення та зберігання національних інформаційних ресурсів [1]. Тому останнього часу в Україні спостерігається інтенсивне впровадження сучасних інформаційних технологій практично у всі сфери життєдіяльності держави, набуває подальшого розвитку інформаційне суспільство. Але водночас переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній безпеці: поряд із інцидентами природного (ненавмисного) походження зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб [2]. Це вимагає невідкладного створення національної системи кібербезпеки як складової системи забезпечення національної безпеки України, метою якої є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [2].

Під кібербезпекою держави будемо розуміти стан захищеності кіберпростору в цілому або окремих об'єктів його інфраструктури та засобів їх взаємодії від ризику стороннього кібернетичного впливу. Оцінка рівня кібербезпеки в Україні відноситься до класу багатокритеріальних завдань. Для її вирішення в умовах невизначеності, а також для аналізу та прогнозування ситуацій з великою кількістю значимих факторів найбільш раціональними і визначальними є експертні методи. Останнім часом значного поширення серед відомих методів експертного оцінювання, що дозволяють безпосередньо використовувати судження та інтуїцію експертів у будь-якій формалізованій структурі [3] для вирішення завдань з соціальним, політичним або воєнним змістом, отримав метод анкетування.

Зазначений метод запропоновано використовувати для одержання числової характеристики комплексного показника оцінки рівня кібербезпеки держави (індексу кіберпотужності G), що дозволить прийняти рішення про його відповідність заданим вимогам. Методика передбачає виконання п'яти кроків: 1) визначення предметної галузі експертизи та формування завдання групам експертів на її проведення; 2) формування структури бази знань з предметної галузі експертизи; 3) проведення розрахунку компетентності сформованої групи експертів в ході вирішення мети дослідження; 4) визначення індексу кіберпотужності; 5) документування та аналіз результатів експертизи.

Індекс кіберпотужності вважатимемо динамічною кількісно-якісною характеристикою, яка вказує на здатність держави забезпечити власну кібербезпеку та підтримувати безпечне функціонування об'єктів їх інформаційної і кіберінфраструктури в умовах кіберзагроз. Його визначення здійснюється на підставі виявлення відхилень від штатного режиму функціонування інформаційних ресурсів, інформаційно-телекомунікаційних систем і мереж, а також програмних і апаратних засобів шляхом аналізу чотирьох основних категорій, кожна з яких включає низку узагальнених індикаторів та показників, а саме:

- 1) наявності нормативно-правової бази (ставлення керівництва держави до питань забезпечення кібербезпеки; стан розвитку політики кіберзахисту);
- 2) стану соціально-економічного розвитку держави (рівень освіти, науки та техніки; рівень розвитку інноваційного середовища);
- 3) наявності розгалуженої технологічної інфраструктури (якісний стан та рівень впровадження технологічної інфраструктури);

4) ступеня використання інформаційно-комунікаційних технологій та інформаційно-телекомунікаційних систем у розвитку інформаційного суспільства (використання інформаційно-комунікаційних технологій у корпоративних мережах та інтелектуальних транспортних системах; використання ресурсів мережі Інтернет для розміщення пропозицій щодо надання пропозицій і послуг, замовлення товарів і послуг).

Слід відмітити, що існує низка ознак стороннього кібернетичного впливу, що пов'язані з відхиленнями від штатного режиму функціонування інформаційних ресурсів, інформаційно-телекомунікаційних систем і мереж, а також програмних і апаратних засобів, зокрема: 1) виведення з ладу окремих компонентів радіоелектронних систем; 2) змінювання алгоритмів функціонування програмного забезпечення систем управління в інформаційно-телекомунікаційних системах і мережах; 3) несанкціоновані зміни у файлах (їх розмірів та останньої дати модифікації); 4) порушення безпеки інформаційного обміну, протоколів передачі даних вхідного або вихідного трафіку, а також прав доступу користувачів до інформаційних ресурсів; 5) уповільнення завантаження та роботи комп'ютера; 6) зменшення обсягів вільної оперативної пам'яті; 7) виконання неконтрольованих процесів тощо.

На підставі розробленої анкети експерта для оцінювання рівня критичності кібербезпеки з урахуванням значень відповідних показників та їхніх вагових коефіцієнтів можуть бути обчислені за спеціальними формулами значення індикаторів, категорій та індексу кіберпотужності  $G$ .

Прийняття рішення щодо здатності держави протистояти атакам у кіберпросторі буде здійснюватися на підставі наступного правила:

1) якщо  $90 \leq G \leq 100$ , то рівень захищеності держави від ризику стороннього кібервпливу вважається достатньо високим для підтримки безпечного функціонування об'єктів її інформаційної і кіберінфраструктури;

2) якщо  $45 \leq G < 90$ , то рівень захищеності держави від ризику стороннього кібервпливу вважається допустимим для підтримки безпечного функціонування об'єктів її інформаційної і кіберінфраструктури;

3) якщо  $G < 45$ , то рівень захищеності держави від ризику стороннього кібервпливу вважається недостатнім для підтримки безпечного функціонування об'єктів її інформаційної і кіберінфраструктури.

В останньому випадку відповідним органам держави необхідно буде розробити належні заходи щодо підвищення результативності власних систем кібернетичної безпеки.

Таким чином, запропонована методика надає можливість одержати числову характеристику комплексного показника оцінки рівня кібербезпеки держави, значення якого свідчить про необхідність розробки належних заходів щодо підвищення результативності власних систем кібернетичної безпеки.

#### **Література:**

1. Про внесення змін до Закону України «Про інформацію» // Відомості Верховної Ради України. – 2011. – № 32. – ст. 313.
2. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15 березня 2016 року № 96/2016.
3. Бешелев С.Д. Экспертные оценки / С.Д. Бешелев, Ф.Г. Гурвич. – М.: «Наука», 1973. – 263 с.

#### **Правове забезпечення захисту інформації пов'язаної із охороною державного кордону**

**Кушнір І.П.**

кандидат юридичних наук

старший викладач кафедри теорії та історії держави і права  
та приватно-правових дисциплін Національної академії Державної прикордонної  
служби України імені Б. Хмельницького

«Хто володіє інформацією – той володіє світом», цей відомий вислів В. Черчілля, набуває дедалі більшої актуальності в сучасних умовах з розвитком інформаційних систем й технологій. Тому, державна політика забезпечення інформаційної безпеки України є невід'ємною складовою державної політики національної безпеки України [1, с.11]. Зокрема, це стосується інформації, яка пов'язана із забезпеченням недоторканності державного кордону та охорони суверенних прав України в її виключній (морській) економічній зоні. Державна прикордонна служба України (далі – ДПСУ) виконує

завдання з охорони державного кордону [2, ст. 1], а отже і забезпечує отримання, обмін, збереження та захист інформації у цій сфері.

Стратегія розвитку Державної прикордонної служби України, метою якої є забезпечення ефективної реалізації політики у сфері безпеки державного кордону, а також охорони суверенних прав України в її виключній (морській) економічній зоні, ставить перед органами охорони державного кордону подвійні завдання. З одного боку це має бути захист інформації, з іншого – забезпечення відкритості та прозорості діяльності ДПСУ [3].

Для забезпечення захисту інформації передбачається модернізації системи зв'язку, інформатизації та захисту інформації:

- організація каналів передачі даних за допомогою засобів проводового та безпроводового доступу до телекомунікаційних мереж, а також супутникового зв'язку;
- заміна обладнання автоматичних телефонних станцій на сучасне цифрове обладнання IP-телефонії з надійною системою адміністрування, контролю та безпеки;
- оснащення органів охорони державного кордону сучасними короткохвильовими радіозасобами, спеціальними комплексними інформаційно-телекомунікаційними апаратними, у тому числі на броньованій базі, а кораблів Морської охорони ДПСУ – сучасними цифровими короткохвильовими і ультракороткохвильовими радіозасобами, засобами супутникового зв'язку та обладнанням криптографічного захисту;
- модернізація системи ультракороткохвильового радіозв'язку, програмно-технічних комплексів різного призначення та підсистем з функціями оброблення інформації про осіб, які перетинають державний кордон, їх паспортних документів з використанням електронних носіїв інформації, у тому числі з функцією біометричного контролю;
- удосконалення складових частин інтегрованої інформаційно-телекомунікаційної системи "Гарт" та модернізація інтегрованої міжвідомчої інформаційно-телекомунікаційної системи "Аркан" щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон;
- розгортання в органах охорони державного кордону мобільних автоматизованих робочих місць з доступом до баз даних, сучасної системи відеоспостереження, спеціальної телекомунікаційної системи;
- запровадження системи електронного документообігу з використанням електронного цифрового підпису, сучасних комплексів криптографічного захисту інформації, новітніх засобів спеціального зв'язку на рухомих об'єктах та механізмів кібербезпеки в інформаційно-телекомунікаційних системах [3].

Ведення інформаційно-аналітичної діяльності в інтересах забезпечення захисту державного кордону України є однією із функцій ДПСУ [2, п. 5, ст. 2], що полягає у збиранні, аналітичній обробці, фіксації, зберіганні, пошуку і поширенні, та забезпеченні захисту інформації. Виконання такого завдання обумовлює наявність відповідних повноважень посадових осіб ДПСУ:

Голова ДПСУ забезпечує в межах повноважень, передбачених законом, реалізацію державної політики стосовно державної таємниці, захисту інформації з обмеженим доступом, контроль за їх збереженням в Адміністрації ДПСУ [4, п. 12];

Начальник органу охорони державного кордону здійснює контроль за дотриманням режимно-секретних заходів та веденням секретного діловодства в структурних підрозділах, а в разі виявлення порушень і вимог технічного захисту інформації та режиму секретності забороняє обробку інформації з обмеженим доступом [5, п.10.15].

Порядок обліку, зберігання, використання та знищення документів, справ, видань, магнітних та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави визначає Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію (далі – Інструкція). Згідно з якою, керівники організацій (в тому числі і посадові особи ДПСУ) несуть відповідальність за забезпечення правильного ведення обліку, зберігання та використання документів з грифом "Для службового користування".

Ведення обліку, зберігання, розмноження та використання документів з грифом "Для службового користування", а також контроль за дотриманням вимог Інструкції покладається на управління справами, загальні відділи, канцелярії організацій [6, п. 6].

Запобігання розголошенню відомостей, що містяться в документах з грифом "Для службового користування", та випадкам втрат таких документів покладається на режимно-секретні підрозділи організацій [6, п. 7].

Отже, захисту інформації пов'язаної із охороною державного кордону отримав належне правове закріплення та залежить від виконання посадовими особами своїх обов'язків.

### Література:

1. Інформаційна безпека особистості, суспільства, держави: Підручник. – К.: Видавничо-поліграфічний центр “Київський університет”, 2008. – 274 с.
2. Про Державну прикордонну службу України : Закон України від 3 квітня 2003 року // Відомості Верховної Ради України. – 2003. – № 27. – Ст. 208.
3. Про схвалення Стратегії розвитку Державної прикордонної служби України : розпорядження Кабінету Міністрів України від 23 листопада 2015 р. № 1189-р // Урядовий кур’єр. – 2015 – № 220.
4. Положення про Адміністрацію Державної прикордонної служби України : постанова Кабінету Міністрів України від 16 жовтня 2014 р. № 533 // Урядовий кур’єр. – 2014 – № 195.
5. Положення про орган охорони державного кордону Державної прикордонної служби України : наказ Адміністрації Державної прикордонної служби України від 15 лютого 2005 р. № 116 // Офіційний вісник України – 2005. – № 11 – с. 27.
6. Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію : постанова Кабінету Міністрів України від 27 листопада 1998 р. № 1893 // Офіційний вісник України. – 1998 – № 48.

### Дослідження методів динамічного аналізу віртуальних соціальних мереж з точки зору інформаційної безпеки

Мелешко Є.В.

кандидат технічних наук, доцент  
доцент кафедри програмування та захисту інформації  
Кіровоградського національного технічного університету

Важливим завданням аналізу соціальних мереж є прогноз формування зв'язків між акторами та співтовариствами. У більшості додатків для аналізу соціальних мереж зв'язки вважаються динамічними і можуть змінюватися з часом. Дослідження динаміки розвитку соціальних мереж дозволяє прогнозувати реакцію учасників соціальної мережі на здійснюваний на них інформаційно-психологічний вплив.

У процес прогнозування зв'язків можуть бути залучені як структура мережі, так і інформація про особливості різних вершин. Візуалізація допомагає природним чином звести разом різну інформацію про мережу і зробити її доступнішою для розуміння. Важливим є створення алгоритмів, що поєднують в собі методи аналізу і методи візуалізації, щоб поліпшити розуміння структури і динаміки мережі.

Динамічні методи аналізу дозволяють дослідити можливість досягнення консенсусу в середині соціальної мережі. Основним поняттям динамічних методів є *граф довіри*. Цей граф може описуватися квадратною матрицею [1, с. 265]:

$$T \in R_{n \times n}, T_{ij} > 0, \sum_{j=1}^n T_{ij} = 1, \quad (1)$$

де  $T$  – матриця суміжності зваженого орієнтованого графу з невід’ємними вагами на ребрах; ребро від  $i$  до  $j$  є, якщо  $i$ -тий актор довіряє  $j$ -тому, вага ребра – сила зв'язку. Ваги нормовані так, що сума ваг вихідних ребер рівна 1; елемент  $T_{ij}$  описує, як актор  $i$  оцінює судження (думку, погляди) актора  $j$  при формуванні свого судження на наступному кроці.

Для динамічного аналізу соціальних мереж найбільш часто використовуються теорія графів та теорія ігор. Окремо варто виділити теорію мережних ігор (або ігор формування мереж) – розділ теорії ігор, що акцентує увагу на формуванні мережних структур – стійких зв'язків між гравцями – в умовах розбіжності інтересів і/або різної інформованості останніх [2, с. 21].

Ігри на соціальних мережах – ігри, в яких вершинами являються агенти – учасники соціальної мережі, а зважені дуги відображають ступень їх "довіри" один до одного або впливу один на одного. Також в даній моделі існують гравці, що здатні впливати на агентів з врахуванням їх довіри один до одного, вони здатні здійснювати цілеспрямований вплив на агентів.

Дослідження ігор на соціальних мережах включає наступні загальні етапи [2, с. 28]:

- 1) опис мережі та дослідження її динаміки;
- 2) опис множини гравців, їх вподобань, інформованості, множин припустимих стратегій і контрольованих ними параметрів;
- 3) зведення гри на мережі до тої чи іншої відомої теоретико-ігрової моделі (гра в нормальній формі,



кооперативна гра тощо).

4) застосування класичного теоретико-ігрового аналізу до поставленої задачі.

Неконтрольований вплив гравців з деструктивними цілями на користувачів соціальної мережі може призвести до виникнення загроз інформаційній безпеці окремої особистості, спільноти або держави.

Інша задача динамічного аналізу – прогнозування формування зв'язків. Дана задача полягає у визначенні, чи будуть дві конкретні вершини з'єднані одна з одною через деякий проміжок часу. Для її вирішення застосовують автоматичне моделювання процесу розвитку соціальної мережі з використанням таких характеристик мережі як кількість спільних сусідів, геодезична відстань, впливовість вершин тощо.

З погляду інформаційної безпеки держави, динамічні методи аналізу соціальних мереж корисні тим, що дозволяють прогнозувати формування та динаміку поглядів акторів під час інформаційно-психологічних впливів та інформаційно-психологічного керування.

### **Література:**

1. Строк Ф.В. Консенсус в социальных сетях: динамический подход / Ф.В. Строк // Доклады Всероссийской научной конференции «Анализ изображений, сетей и текстов» – АИСТ'2012. Екатеринбург, 16-18 марта 2012 г. – С. 264–272.

2. Губанов Д.А. Социальные сети: модели информационного влияния, управления и противоборства. / Д.А. Губанов, Д.А. Новиков, А.Г. Чхартишвили. – М.: Физматлит, 2010.

3. Батура Т.В. Методы анализа компьютерных социальных сетей / Т.В. Батура // Вестник Новосибирского государственного университета. Серия: Информационные технологии. – 2012. – Т. 10, № 4. – С. 13–28.

4. Горбулін В.П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія / В. П. Горбулін, О. Г. Додонов, Д. В. Ланде. – К.: Інтертехнологія, 2009. – 164 с.

5. Davern M. Social Networks and Economic Sociology: A Proposed Research Agenda for a More Complete Social Science / M. Davern // The American Journal of Economics and Sociology. – 1997. – Vol. 56, No. 3. – P. 287-302.

6. Hanneman R. A. Introduction to Social Network Methods (free introductory textbook on social network analysis). / R. A. Hanneman, M.D. Riddle – 2005. [Електронний ресурс] Режим доступу: <http://faculty.ucr.edu/~hanneman/>

### **Деякі особливості розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку**

**Миколенко О.М.**

кандидат юридичних наук, доцент,  
доцент кафедри кримінального права, кримінального  
процесу та криміналістики  
Одеського національного університету імені І.І. Мечникова

Розвиток сучасних інформаційних технологій, удосконалення виробництва і розширення сфери застосування новітньої кібернетичної техніки дали можливість зародження специфічного, складного виду злочинних діянь, де комп'ютерне оснащення та електронна інформація є об'єктом протиправного посягання. Поряд з позитивними здобутками, інформатизація супроводжується побічним, негативним явищем криміногенного характеру, до якого відносять злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

На сучасному етапі технологізації суспільства: обробки та обміну інформацією за допомогою міжнародної глобальної мережі INTERNET, відбуваються негативні процеси – перехід від простої поодинокі комп'ютерної злочинності до організованої – складної. На жаль, спостерігається динаміка злиття новоявленої злочинності з міжнародним криміналітетом, що несе у собі відповідну загрозу суспільству в цілому. Слід зазначити, що така транскордонність ускладнює можливості розкриття та розслідування цієї категорії злочинів працівниками правоохоронних органів різних держав.

До переліку негативних чинників розповсюдження цієї категорії злочинів та низького рівня їх розкриття можна віднести:

1. Низький рівень контролю за тиражуванням та розповсюдженням програмної комп'ютерної продукції.

2. Високу латентність злочинів. Лише 10 – 15 % комп'ютерних злочинів стають відомими правоохоронним органам.

3. Недостатність теоретичних знань і практичних навичок розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, інформаційних технологій практичними працівниками правоохоронних органів, неможливість доведення до суду кримінальних проваджень цієї категорії.

Зупинимо свою увагу саме на останньому чиннику. Слід зазначити, що досудове розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку та збирання доказів по цим справам, істотно відрізняються від розслідувань інших “традиційних” злочинів, або зазвичай буває більш складним. За цими кримінальними справами найчастіше допускаються помилки, що пояснюється відсутністю належного рівня теоретичної та практичної підготовки оперативних працівників і слідчих. Таке розслідування не вимагає спеціальної технічної підготовки слідчого або прокурора, і в більшості випадків залежить від грамотної та досвідченої роботи експертів.

Результати аналізу практичної діяльності правоохоронних органів по розслідуванню злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку свідчать про те, що дослідження комп'ютерної техніки доцільно проводити в умовах криміналістичної лабораторії, де цю роботу виконують фахівці з необхідною професійною підготовкою. Адже докази, що пов'язані з комп'ютерними злочинами, які були вилучені з місця події, можуть бути легко змінені, як в результаті помилок при їх вилученні, так і в процесі самого дослідження [1, с. 81-85]. Таким чином, незважаючи на де-юре, відсутність законодавчої вимоги про обов'язкове призначення експертизи в цих провадженнях, де-факто, без призначення і проведення експертизи не можна говорити про ефективне розслідування таких справ.

Також окремою проблемою є процес представлення доказів в судовому процесі, який вимагає спеціальних знань і відповідної підготовки. Тут не можна недооцінювати роль експертизи, яка може дати кваліфіковану відповідь на поставлені питання. Однак експертиза вимагає якогось часу не тільки на її проведення, а й на пошук відповідних фахівців, а при вилученні комп'ютерної техніки часто важливим фактором, що дозволяє зберегти необхідну доказову інформацію, є раптовість та оперативність. Саме тому вилучення комп'ютерів і інформації доводиться проводити тими силами, які є в наявності, тобто слідчими або оперативними підрозділами. І в цьому випадку саме слідчий не застрахований від помилок, обумовлених недостатністю знань, що пізніше використовується захистом в суді.

Отже, поставлена проблема має два аспекти: загальні помилки, які допускаються працівниками правоохоронних органів при розслідуванні комп'ютерних злочинів, і технічні аспекти, пов'язані із захистом інформації, яка встановлюється на комп'ютерах їх безпосередніми користувачами.

Не менш складною є і робота прокурора у суді: обвинувачення у справах по комп'ютерних злочинах має будуватися так, щоб судді, присяжні та сторони провадження, які мало знаються на комп'ютерах і комп'ютерних програмах, змогли зрозуміти складні технічні моменти та процеси, дослідити докази по справі. Слабкі знання специфіки технічних проблем суддею або присяжними можуть бути навіть небезпечними для кримінального провадження. Як приклад, можна навести судовий розгляд відомої справи Роберта Т. Моріса про запровадження ним програми-хробака (вірус Моріса) до мережі Інтернет у 1988 року [2]. Вірус Моріса інфікував 6 200 комп'ютерів. І незважаючи на те, що ця програма не завдала прямих матеріальних збитків (не були викрадені чи пошкоджені дані), комп'ютерні центри і звичайні користувачі зазнали збитків за час виявлення цієї програми і час, який був потрібен на перевірку та відновлення працездатності системи. Під час обвинувального процесу, обвинувачуваний підтвердив впровадження програми-хробака, але заявив, що це було зроблено необережно. У результаті Роберта Т. Моріса було засуджено умовно. І таких випадків, коли умовне засудження назначалося за комп'ютерні злочини, які принесли багатомільйонні збитки, чимало.

Отже, підводячи підсумок, наполягаємо на обов'язковій участі спеціаліста при провадженні слідчих (розшукових) дій при розслідуванні злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Крім того, вважаємо за необхідне постійну участь фахівця у стадіях судового провадження та здійснення ним, так би мовити, технічного “супроводу” кримінального провадження, адже слабкі знання специфіки технічних проблем суддею або присяжними можуть нашкодити провадженню, зокрема, зрадлива інтерпретація доказів може призвести до хибного висновку, і як результат - неправосудного судового рішення.

**Література:**

1. Моїсєєв О.М. Залучення спеціаліста до розслідування комп'ютерних злочинів / О.М. Моїсєєв // Правові основи захисту комп'ютерної інформації від протиправних посягань: Матеріали міжвузівської науково-практичної конференції (м. Донецьк, 22 грудня 2000 р.). – Донецький інститут внутрішніх справ, 2001. – С. 81 – 85.
2. Атака на INTERNET [Електронний ресурс]. – Режим доступу: <http://www.sources.ru/security/attack2/09-04.html>. – Назва з екрану.

**Перспективы использования пористого кремния в качестве датчиков систем  
с контролем доступа**

**Мирошниченко А.І.**

преподаватель ассистент

кафедры общетехнической и фундаментальной подготовки

Одесской государственной академии технического регулирования и качества

**Лещенко О.І.**

доцент кафедры компьютерных и информационно

измерительных технологий

Одесской государственной академии технического регулирования и качества

С ростом современных технологий все более остро стоит вопрос защиты, как персональных данных, так и защиты оборудования от несанкционированного вскрытия и доступа. Помимо защиты с помощью специальных программ, которые имеют возможность блокировать и, или, фиксировать несанкционированные доступы в систему, используются также разнообразные датчики. Основное требование к таким датчикам – это дешевизна (особенно если они одноразового использования), простота в изготовлении, широкий спектр электрических и люминесцентных свойств. Наиболее пригодным материалом для этих целей может быть пористый кремний, который представляет собой сложную структуру нанокристаллитов.

Пористый кремний изготавливается путем анодного травления монокристаллического в растворах плавиковой кислоты. Одно из достоинств этого материала является то, что свойства получаемого в результате образца сильно зависят от многочисленных факторов – кристаллографического направления подложки, уровня легирования, а также типа легирования, концентрации плавиковой кислоты, плотности тока анодирования, времени травления, последующей термообработке, уровня освещенности во время травления. Управляя этими факторами можно получить образец с заданными параметрами, наиболее подходящими для решения поставленной задачи. Однако, несмотря на многочисленные опыты, до сих пор нет полной картины образования пористого кремния. В частности, мало исследованы свойства пористого кремния, изготовленного на подложках с кристаллографической ориентацией (110). Эти исследования необходимы, так, как получив полную картину образования данного материала, и, научившись управлять процессом изготовления, можно получить в распоряжение дешевые датчики, имеющие широкий спектр применения.

Исследовались фотолюминесцентные свойства пористого кремния, полученного на подложке на подложках КДБ-10, с удельным сопротивлением 10 Ом·см, с кристаллографической ориентацией (110). Травление производилось в растворе плавиковой кислоты, в ячейке с горизонтальным расположением электродов, где анодом служила платиновая сетка, а катодом – поверхность самой пластины кремния. В качестве переменного параметра было выбрано время травления, которое изменялось от 5 до 30 минут. Фотолюминесценция возбуждалась газовым лазером с длиной волны 330 нм, средней излучательной мощностью около 3 мВт, длительностью импульса 10 нс. Спектры записывались непосредственно на компьютер с помощью специальной программы. Результаты представлены на рисунке 1.

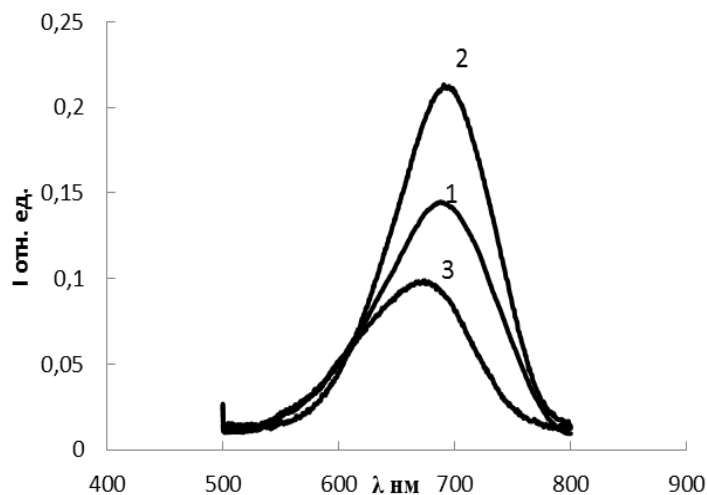


Рис. 1 – Спектры фотолюминесценции. 1 – для образца, изготовленного при времени тока анодирования 5 мин., 2 - 15 мин., 3 - 30 мин.

Как видно из рисунка все спектры имеют гауссоподобную форму. Также из спектров видно, что максимумы излучения всех образцов сдвинуты в более коротковолновую область спектра, по сравнению с монокристаллическим кремнием, чей максимум излучения находится в инфракрасной области (длина волны порядка 1,1 мкм). Этот сдвиг обуславливается тем, что при травлении кремния в растворе происходит образование нано-кластеров, размерами порядка нескольких нанометров, что в свою очередь приводит к изменению ширины запрещенной зоны полупроводника [1, 2].

Анализ технологии получения пористого кремния и получаемых при этом его характеристик показал, что фоточувствительность зависит от времени травления. Помимо этого, происходит сдвиг максимума поглощения в более коротковолновую область по мере увеличения времени травления. Подобная зависимость позволит создавать датчик, способный эффективно реагировать на излучение от ультрафиолетовой до инфракрасной области спектра, что в совокупности с дешевой и относительной простотой процесса изготовления, делает пористый кремний одним из наиболее перспективных материалов в этой области.

#### Литература:

1. С. П. Зимин Электрофизика пористого кремния и структур на его основе. Диссертация на соискание д. физ. – мат. наук. – Ярославль, 2003. – 305 с.
2. N. J. Pulsford, G. L. J. A. Rikken, Y. A. R. R. Kessener, E. J. Lous, A. H. J. Venhuisen. J. Luminecs, 57, 181 (1993)

#### Модель построения киберзащищенного информационного пространства ЦОД: математический аспект

**Шестак Я.В.**  
аспирант,  
Ogbu JamesOnyigwang

**Оксиюк А.Г.**  
доктор технических наук, профессор  
Киевского национального университета имени Тараса Шевченко, г. Киев

Актуальным вопросом современного информационного пространства центров обработки данных (далее ЦОД) выступает построение эффективной защиты от кибератак.

ЦОД – это централизованная комплексная система, которая является отказоустойчивой и обеспечивает качественное обслуживание бизнес-процессов проходящих в ее рамках, с высоким уровнем предоставляемых услуг [1]. Основным фундаментальным условием надежной работоспособности современного ЦОД является его безопасность. Чем выше уровень предоставляемой безопасности всех информационных ресурсов, хранящихся в системе и находящихся в обороте, тем выше степень гарантированного обеспечения требуемого качества сервиса.

Главными приоритетным и требованиями, применяемыми к ЦОДам, нашего времени, выступают целостность хранимой информации, ее доступность и конфиденциальность [2]. В рамках финансовых учреждений, нарушение функционирования ЦОД может привести к необратимым финансовым и политическим процессам, что, во многих случаях, является недопустимым явлением.

Цель обеспечения киберзащищенного информационного пространства сводится к минимизации информационных потерь в ЦОДе, за счет уменьшения рисков и снижения уровня возможных внешних и внутренних воздействий.

По структурному составу ЦОД, к главным объектам, требующим качественной защиты, следует отнести: информацию, которая хранится и обрабатывается в системе; программное обеспечение, установленное в рамках ЦОД; элементы системы, оборудование центра [3].

С математической точки зрения модель центра обработки данных представляет собой граф в виде:

$$\text{ЦОД} = (M_{\text{ву}} \cup M_{\text{хд}} \cup M_{\text{кс}}) \quad (1)$$

где ЦОД – центр обработки данных;

$M_{\text{ву}}$  – множество вычислительных узлов ЦОД;

$M_{\text{хд}}$  – множество хранилищ данных;

$M_{\text{кс}}$  – множество коммутационных элементов сети обмена и физических каналов передачи данных.

Модель ресурсного запроса описывается выражением типа:

$$PЗ = M_{\text{вм}} \cup M_{\text{мз}}, M_{\text{вк}} \quad (2)$$

где PЗ – ресурсный запрос;

$M_{\text{вм}}$  – множество виртуальных машин, используемых приложениями;

$M_{\text{мз}}$  – множество элементов;

$M_{\text{вк}}$  – множество виртуальных каналов передачи данных между виртуальными машинами и элементами запроса.

Назначение ресурсного запроса формируется в виде:

$$A: PЗ \rightarrow \text{ЦОД} = \{M_{\text{вм}} \rightarrow M_{\text{ву}}, M_{\text{мз}} \rightarrow M_{\text{хд}}, M_{\text{вк}} \rightarrow M_{\text{кс}}\} \quad (3)$$

При этом, для актуальной работы, необходимым является выполнение следующих условий:

Каждый вычислительный узел обязан иметь производительность и общую суммарную память, которая соответствует суммарной составляющей всех виртуальных машин относящихся к нему;

Каждый виртуальный канал может быть отображен на физический канал при условии, что общее количество виртуальных каналов отображенных на физический канал, меньше номинальной пропускной способности канала передачи данных;

Каждый виртуальный канал может проходить через коммутационный элемент, при условии, что количество виртуальных каналов, проходящих через коммутационный элемент, меньше чем общая пропускная способность этого элемента (байт/с);

Каждый элемент общего информационного пространства может быть размещен в хранилище данных, при условии, что каждый элемент, а также его тип совпадают с типом хранилища данных и общее количество всех хранимых элементов не превышает объема всей памяти.

С целью минимизации информационных потерь в ЦОДе, за счет уменьшения рисков и снижения уровня возможных внешних и внутренних воздействий, предлагается использовать механизмы оптимизации размещения виртуальных машин на физических серверах, т.е. применить принцип минимального заполнения серверов:

$$y_i = \begin{cases} 1 - \text{а сервере имеется одна виртуальная машина;} \\ 0 - \text{сервер не задействован} \end{cases} \quad \min \sum_{i=1}^n y_i \quad (4)$$

Практическая реализация данного подхода позволяет минимизировать уровень как внешних так и внутренних воздействий, а также снизить затраты на содержание общего парка серверов ЦОД, в случае идентичных технических характеристик.

**Література:**

1. Оценка защищенно информационных процессов в территориальных ОВД: модели исследования: монография / под ред. С.В. Скрыля. – Воронеж: Воронежский институт МВД России, 2010. – 217 с.
2. Вдовин П.М., Костенко В.А. Алгоритм распределения ресурсов в центрах обработки данных с раздельными планами ровщиками для различных типов ресурсов // Известия РАН. Теория и системы управления, 2014. – № 6. – 56-68 с.
3. Теленик С.Ф. Генетичні алгоритми вирішення задач управління ресурсами і навантаженням центрів оброблення даних / С.Ф. Теленик, О.І. Ролік, М.М. Букасов, С.А. Андросов // Автоматика. Автоматизація. Електротехнічні комплекси та системи. – 2010. – №1 (25). – 106–120 с.

**Принципи формування вимог до систем безпеки мереж 5G**

**Одарченко Р.С.**

кандидат технічних наук, доцент,  
заступник директора навчально-наукового  
інституту Аеронавігації Національного авіаційного університету, м. Київ

**Гнатюк С.О.**

доцент кафедри безпеки інформаційних технологій  
Національного авіаційного університету, м. Київ

В розвинутих країнах, зокрема, в США, Європі та країнах Азії вже є доволі багато операторів, які надають послуги за допомогою мереж LTE [1], а вже до 2020 року планується запуск перших мереж 5G у комерційну експлуатацію [2-3].

При цьому кожен користувач будь-якої мережі прагне забезпечити конфіденційність передаваних даних та унеможливити спроби мережових атак на мобільні пристрої. До того ж набирає популярності концепція Інтернету речей IoT [4], що висуває ще більші вимоги до захисту інформаційної інфраструктури.

Безпека є одним з основних проблемних місць комунікаційної мережі в даний час. Розгортання жодної мережі не може відбутися без забезпечення гарантованої безпеки для всіх зацікавлених сторін, наприклад, кінцевих користувачів, постачальників послуг, віртуальних операторів, провайдерів інфраструктури. Таким чином, метою даної роботи є виявлення недоліків систем захисту мереж попередніх поколінь та формування вимог до безпеки майбутніх 5G мереж в цілому та їх окремих компонентів.

Розглянемо проблемні місця в мережах LTE [5].

Перша очевидна загроза - атаки DoS (Denial of Service) на мережу. Ємність радіоканалу в LTE передбачається велика, але все ж вона має обмеження. Мережеві ресурси базової станції діляться між абонентами, і хоча є обмеження для монополізації смуги окремим користувачем, проте атака на відмову в обслуговуванні мережі цілком можлива. Зникнення RNC призвело до того, що доступ до ядра мережі LTE можливий безпосередньо з базової станції.

Інша загроза – вірусні атаки. Хоча таким атакам схильні пристрої, а не мережа, технологія LTE збільшує швидкість поширення шкідливих програм, оскільки сам цей стандарт є високошвидкісним. До того ж плата за користування послугами четвертого покоління навряд чи буде залежати від обсягу трафіку - тарифи будуть або безлімітними, або з обмеженням по смугі пропускання. Тому користувачі не зможуть швидко помітити трафік, породжуваний шкідливими програмами і вбудованими в них сканерами вразливостей. А значить, у розробників вірусів буде більше можливостей для монетизації своїх мобільних розробок: від стеження за конкретною людиною до злодійства одноразових паролів в системах дистанційного банківського обслуговування.

Третя небезпека – атаки на додаткові сервіси. Власне, LTE розроблялося не тільки для забезпечення доступу до Інтернету мобільних користувачів, а скоріше як платформа для впровадження нових послуг: відео, ігрових та багатьох інших. Ці сервіси також можуть бути уразливі для найрізноманітніших атак - як з Інтернету, так і з мобільної мережі. Цілком можливо, що, атакувавши один із сервісів, зловмисники зможуть впровадити в клієнтські пристрої небезпечні програми.

Загроза користувачам LTE може виходити і від сервісів подвійного призначення. Мобільні оператори мають так багато цінної інформації про абонентів, що рано чи пізно захочуть її монетизувати. Типовим прикладом є LBS-сервіси. З одного боку, їх можна використовувати,

наприклад, для контролю за переміщенням вантажів, для визначення місцезнаходження дітей і для оповіщення про надзвичайні ситуації, але з іншого - їх же можна використовувати для незаконного стеження. З поширенням інтелектуальних пристроїв число потенційно небезпечних сервісів буде тільки зростати. Злом такого сервісу дозволить зловмисникам отримати доступ до цінної інформації провайдера і побудувати нові схеми злочинів і незаконного отримання грошей.

Ми привели далеко не повний перелік нових загроз, пов'язаних з появою LTE. Є також проблеми і з самим стандартом. Дуже гостро стоїть завдання взаємодії з недовіреними (не LTE) мережами. Якщо трафік між користувальницьким устаткуванням і eNB шифрується (ця вимога стандарту) і загроза порушення конфіденційності стає неактуальною, то, наприклад, взаємодія eNB з радіоконтроллер мережі 3G за замовчуванням ніяк не захищений, а отже, це пролом для можливих атак з боку зловмисників. Як і відсутність обов'язкової аутентифікації між ядром мережі і eNB, цю опцію оператор зв'язку може як використовувати, так і не задіяти в принципі, щоб знизити свої витрати з розгортання мережі LTE.

Але, не дивлячись на всі переваги і на деякі недоліки в системах безпеки, аналітики в усьому світі розуміють, що на зміну LTE за оцінками експертів після 2020 року мають прийти мережі 5-го покоління – 5G. Вони повинні будуть враховувати всі недоліки мереж попередніх поколінь.

Основний вплив на те, як ми повинні підходити до формування вимог до систем безпеки та конфіденційності в мережах 5G, створюють наступні чинники:

- Нові моделі довіри ;
- Безпека для нових моделей надання послуг;
- Розширений перелік загроз;
- Збільшення недоторканності приватного життя.

Цей перелік не є вичерпним та висуває певні вимоги до принципово нових систем безпеки. Зокрема, в стільникових мережах нового покоління повинні бути забезпечені наступні частини загальної структури системи безпеки. Це, насамперед:

- Забезпечення безпеки;
- Управління ідентифікацією;
- Безпека радіомережі 5G;
- Гнучка і масштабована архітектура безпеки;
- Енергоефективна безпека;
- Хмарна безпека.

#### **Висновки**

Розглянутий розвиток стільникових мереж зв'язку як в Україні, так і в світі надав змогу обґрунтувати необхідність дослідження стільникових мереж п'ятого покоління, окреслити їх основні переваги. Також були проаналізовані системи безпеки стільникових мереж.

В результаті проведених досліджень стало зрозумілим, що мережі 5G відіграватимуть в майбутньому поки що найбільш значущу роль в формуванні електронного суспільства, критичної інфраструктури тощо. Тому дуже актуальними і важливими є питання, пов'язані із забезпеченням інформаційної безпеки в майбутніх мережах 5G. Основні рушійні сили розвитку 5G, згруповані в чотири основні характеристики створюють визначальний вплив на підходи щодо формування вимог до систем безпеки та конфіденційності в мережах 5G. Тому були сформульовані ключові напрямки удосконалення систем безпеки стільникових мереж (управління ідентифікацією, безпека радіомережі, підвищення енергоефективності, гнучка і масштабована архітектура, безпека хмарних сервісів тощо), що дозволило обґрунтувати необхідність проведення подальших досліджень, пов'язаних із оптимізацією захисту мереж 5G.

#### **Література:**

1. [Електронний ресурс] – електронні текстові дані – режим допуску: [http://www.gsacom.com/downloads/pdf/GSA\\_Evolution\\_to\\_LTE\\_report\\_060514.php4](http://www.gsacom.com/downloads/pdf/GSA_Evolution_to_LTE_report_060514.php4)
2. 4G America's recommendation on 5G Requirements and Solutions, October 2014, p. 40;
3. Understanding 5G [Електронний ресурс]– електронні текстові дані – режим доступу: <http://www.arnitsu.com>
4. Белоцерковский А.Е. Интернет вещей – это будущее, которое уже наступило [Електронний ресурс]– електронні текстові дані – режим доступу: <http://www.therunet.com/interviews/5015-internet-veschey-eto-buduschee-kotoroe-uzhe-nastupilo>
5. Скорость и безопасность в LTE [Електронний ресурс]– електронні текстові дані – режим доступу: <http://www.osp.ru/nets/2012/06/13032673/>

*Одеський державний університет внутрішніх справ*  
*«Кибербезпека в Україні: правові та організаційні питання»*  
**Дослідження методів класифікації захищених операційних систем за варіантами їх використання**

**Зерко А.Л.**

аспірант факультету інформаційних технологій,  
Київський Національний  
Університет ім. Тараса Шевченка

**Оксіюк О.Г.**

доктор технічних наук, професор,  
завідувач кафедри кібербезпеки та захисту інформації  
Київський Національний  
Університет ім. Тараса Шевченка

На даний момент часу у світі інформаційних технологій існує певна кількість механізмів захисту для операційних систем. У цих механізмів навіть є відповідні рівні (додатки, модифікації). Кожен з цих механізмів, можливо налаштувати на свій лад, якщо є така можливість, проте тут, також, існують рамки.

Сама захищеність операційної системи, можна сказати складається саме з цих механізмів та їх налаштувань. І при конфігуруванні механізмів захисту кінцевий результат залежить від рівня знань, майстерності та вмінь адміністратора, який проводить настрійку.

А що, як розглядати захищену операційну систему, не як вже готовий набір механізмів захисту, а визначити та налаштовувати механізми захисту саме під потреби користувача та вимоги зберігання інформації? Для цього необхідно провести аналіз варіантів класифікації захищених операційних систем за їх використанням.

**Мета.** Розробити класифікацію захищених операційних систем за варіантами використання.

**Актуальність.** Класифікація допоможе більш чітко визначати необхідні механізми та їх налаштування для захисту операційних систем. Також дозволить зменшити навантаження та складність в управлінні операційними системами за рахунок правильного підбору механізмів захисту.

**Основний виклад інформації.** Класифікація операційних систем (ОС) не така проста, як здається на перший погляд. Для точної класифікації необхідно розбити ОС на деякі групи за варіантами їх використання.

Найголовнішим критерієм для класифікації ОС є середовище використання. Отже будемо розрізняти два види ОС за середовищем використання:

1. ЗОС для робочих станцій, що використовуються в внутрішній локальній мережі (інтернет)
2. ЗОС для використання в зовнішній мережі (Інтернет).

Далі необхідно розділити ОС за класом комп'ютера:

1. ЗОС для робочої станції, яка керує ресурсами окремого комп'ютера;
2. ЗОС серверні, які мають виконувати завдання управління мережевими ресурсами, забезпечувати доступність мережевих ресурсів, цілісність та достовірність даних.

Необхідно враховувати також варіант використання ЗОС для вирішення завдань забезпечення безпеки для локального комп'ютеру, який не призначений для підключення до зовнішніх мереж. Такий варіант використання ЗОС призводить до полегшення розгляду багатьох питань, але слід враховувати, що такі робочі станції, скоріш за все використовуються для обробки важливої інформації. І загрози спроб несанкціонованого доступу при прямому доступі обслуговуючого персоналу є досить серйозними.

Також врахуємо варіанти використання ЗОС на робочих станціях у внутрішній мережі, коли в ній присутні сервери та, коли їх не має. Адже у варіанті, коли в мережі є сервер, або декілька серверів, - то механізми захисту в ЗОС на робочій станції будуть відрізнятися від набору та налаштувань механізмів в ЗОС на робочих станціях у внутрішній мережі без серверів.

Отже можемо узагальнити результат аналізу в табличному виді:

№	Клас використання ЗОС
1.	ЗОС для використання на ізольованому комп'ютері без виходу до жодної з мереж
2.	ЗОС для використання на робочій станції у внутрішній мережі Інтранет
3.	ЗОС для використання на робочій станції у зовнішній мережі Інтернет
4.	ЗОС для використання на сервері у мережі Інтранет
5.	ЗОС для використання на сервері у мережі Інтернет



Висновок. Варіанти використання ЗОС для мереж різних типів призводить до необхідності врахування зовнішнього оточення при проведенні аналізу питань захисту інформації, розробки вимог до механізмів захисту інформації в середовищі захищеної ОС.

Таким чином в залежності від варіанту використання та класифікації системи для ОС необхідний свій рівень захисту та відповідний набір компонент захисту даних – для формування ядра захисту інформації.

#### **Література:**

1. Державна служба спеціального зв'язку та захисту інформації України.  
<http://www.dstszi.gov.ua/dstszi/control/uk/index>.
2. Компанія «АТМНІС», [https://atmnis.com/files/user\\_files/BBOS.pdf](https://atmnis.com/files/user_files/BBOS.pdf)
3. Компанія «Майлінукс», <http://mylinux.ua/press-release5>
4. Компанія ТОВ НДІ «Автопром», <http://avtoprom.kiev.ua/rproduct2.html>
5. Нестеров С. А. Інформаційна безпека та захист інформації: Учеб. посібник.- СПб.: Видавництво політехн. ун-ту, 2009. - 126 с.
6. Макаренко С. І. Інформаційна безпека: навчальний посібник для студентів вузів.- Ставрополь: СФ МДГУ ім. М. А. Шолохова, 2009. - 372 с.

#### **Особливості використання криптозахищених автоматичних ідентифікаційних судових станцій**

**Коновець В.І.**

провідний науковий співробітник;  
Науково-дослідного центру ЗС України «Державний океанаріум», м.Одеса

**Симоненков В.М.**

старший науковий співробітник;  
Науково-дослідного центру ЗС України «Державний океанаріум», м.Одеса

**Черниш І.А.**

старший науковий співробітник,  
Науково-дослідного центру ЗС України «Державний океанаріум», м.Одеса

Оцінка досвіду бойових дій у локальних збройних конфліктах свідчить про необхідність удосконалення систем управління, оперативного радіообміну тактичною, зокрема навігаційною, інформацією та візуалізації тактичної обстановки.

Одним із шляхів підвищення стійкості управління є впровадження “blue force” AIC – криптозахищених (encryption) автоматичних ідентифікаційних судових станцій (EAIS).

Функціональність EAIS визначається відповідними стандартами, в тому числі й у військово-морській сфері.

Одним з основних в цій сфері є стандарт НАТО STANAG 4668/4669 – WARSHIP-AIS (W-AIS), який задає функціональність AIS для військового використання.

Використання технологій EAIS забезпечує автоматичний обмін захищеними даними між кораблями і береговими станціями з використанням алгоритмів шифрування Blowfish та/або AIS з ключем шифрування до 448 (128) біт. При цьому, шифрована інформація, яка широкомовно передається по каналу передачі даних, буде доступна тільки тим елементам мережі, які спільно використовують той же ключ шифрування та “бачать” дані і спеціальні повідомлення AIS один одного.

Основні режими роботи EAIS:

1. Mode = Normal

Станція виконує всі функції звичайного AIC класу А транспондера. Вихідні повідомлення транслюються у відкритому форматі на стандартних частотах AIS відповідно до МСЭ М.1371-5. Транспондер приймає і оброблює спеціальні EAIS повідомлення.

2. Mode = Silent (Receive-only)

Радіопередачі повністю відключені. Транспондер приймає і оброблює спеціальні EAIS повідомлення, а також стандартні повідомлення AIC МСЭ М.1371-5, за виключенням команд полінга та переводу у визначений режим роботи. Цей режим встановлюється, як правило, при включенні живлення.

### 3. Mode = Protected

EAIS приймає і оброблює усі незашифровані передачі від комерційних суден, оснащених AIS в зоні дії, а також шифровані повідомлення EAIS. Передача інформації здійснюється тільки шифрованими повідомленнями EAIS 6&8 або 25&26. Обмін шифрованими повідомленнями можливий на виділеному каналі УКХ.

Застосування додаткового “захищеного режиму” роботи в W-AIS забезпечує використання зашифрованої передачі даних і обміну цільовою (навігаційною) інформацією в групі, передачу цілей через бортові модулі, а також підвищує ситуативну поінформованість і рішення C2.

З іншого боку, на ринку EAIS доступні без суттєвих обмежень, включаючи також модифіковані по відношенню до стандартних, наприклад, з можливістю передачі по відкритим каналам AIS викривленої позиції судна, а по закритим – фактичної. Оскільки усі передачі в EAIS ведуться повідомленнями 6&8 або 25&26, то актуальним також становиться завдання виявлення і моніторингу активності EAIS станцій в зоні відповідальності країни. В доповіді розглядаються можливі підходи рішення цього завдання.

## **Дослід США щодо застосування оперативної техніки у протидії злочинності**

**Пеньков С.В.**

кандидат юридичних наук  
здобувач кафедри оперативно-розшукової діяльності  
та розкриття злочинів факультету № 2  
Харківського національного університету внутрішніх справ

У рамках реформування правоохоронної системи України все гостріше постає питання її адекватного технічного оснащення, а також ефективної організації застосування відповідних технічних засобів. Певну допомогу у вирішенні цього завдання може надати досвід США, які мають одну з найбільш сучасно-оснащених правоохоронних систем світу. У цьому сенсі корисним представляється розглянути окремі аспекти застосування оперативної техніки в цій країні.

Передусім потрібно зауважити, що поліцейські відомства США, які мають право на проведення усього комплексу оперативно-розшукових заходів, мають на озброєнні і достатньо повний арсенал оперативної техніки, що дозволяє їм самостійно, без залучення сторонніх підрозділів, провадити відповідні заходи. Зокрема це стосується таких органів як ФБР та Адміністрація по контролю за дотриманням законодавства про наркотики [1, с. 232]. Причому, у ФБР використанням оперативної техніки опікуються SOG (Special Operation Group) і ТТА (Technically Trained Agents) [2, с. 96], а в Адміністрації по контролю за дотриманням законодавства про наркотики – відділи технічних операцій (Technical Operations Unit) [3, 6632.2(K)].

У країнах Європейського союзу та США більшість заходів із застосуванням техніки потребують судового санкціонування. Проте існують і виключення, зокрема це стосується використання GPS-трекерів [4]. Така ситуація постійно викликає суспільне невдоволення, що тягне за собою судові тяжби громадськості із державними органами.

Варто також звернути увагу, що оперативна техніка є інструментом порушення приватності. Причому, судова практика показує, що оперативні підрозділи у випадку неналежного врегулювання певних правовідносин намагаються якнайбільше застосовувати оперативну техніку у розрізі такої неврегульованості. Таку ситуацію можна охарактеризувати як проведення «технічних заходів на грані закону».

В цьому сенсі слід згадати накопичення правоохоронними органами США інформації про пересування автомобільного транспорту [5], застосування спеціальних радарів для спостереження за переміщенням осіб у приміщеннях [6], GPS-трекерів [7] та проміжних базових станцій, як правило, стінгреїв (Stingrays, виробник Florida-based Harris Corporation), – спеціальних пристроїв для спостереження за стільниковими телефонами, які імітують роботу базової станції, що уможливорює встановлення місцезнаходження абонента спостереження та одержання деталізованих даних про його виклики. Так, лише у Нью-Йорку за період 02.01.2008-21.05.2015 рр. поліцією було 1016 разів застосовано стінгреї [8]. На придбання означених комплексів, їх обслуговування та навчання персоналу поліція витрачає сотні тисяч доларів [9].

Правозахисники відзначають, що для використання проміжних базових станцій у США застосовувалася більш спрощена процедура одержання судового дозволу (pen register order), аніж потрібне зазвичай для таких випадків одержання ордеру (warrant). Така ситуація обумовлена

відсутністю чітких приписів щодо порядку використання стінгреїв. Враховуючи це суди нерідко виносять протилежні рішення щодо допустимості одержаних з їх використанням доказів [10].

Цікавим видається досвід США щодо здійснення комп'ютерної розвідки. Прикладами відповідних засобів оперативної техніки, застосовуваних США у рамках комп'ютерної розвідки, є спеціальні програми, які сприяють збиранню та аналізу інформації про правопорушників в мережі. Особливо велика кількість відповідних застосувань розробляється для протидії обігу дитячої порнографії та протидії терористичній активності. Останнім часом правоохоронні органи також все частіше звертають увагу на спеціалізоване програмне забезпечення для аналізу даних з комп'ютерних соціальних мереж. Так, наприклад програма Dunami від виробника PATHAR застосовується ФБР та призначена для аналізу даних з Twitter, Facebook, Instagram з метою виявлення центрів впливу і ознак прояву радикалізму [11].

З метою впровадження спеціального програмного забезпечення для оперативних потреб у США можуть створюватися венчурні фірми, як от In-Q-Tel, а для використання таких програмних та апаратно-програмних комплексів організовано роботу окремих підрозділів. У цьому сенсі слід згадати спеціальний підрозділ ФБР з проведення віддалених операцій (Remote Operations Unit), який займається розробкою та придбанням спеціалізованих інструментів, призначених для стеження за фігурантами розслідувань [12]. Маються на увазі так звані «мережні технології розслідування» [13], тобто засоби, використовувані для роботи в комп'ютерних мережах. До компетенції цього підрозділу належить й експлуатація так званих вразливостей нульового дня («zero-day» exploits).

Слід відмітити, що саме цей підрозділ відповідає за проведення високотехнологічних оперативно-технічних заходів. Він функціонує у структурі Управління оперативних технологій (Operational Technology Division), яке у свою чергу не лише здійснює забезпечення оперативно-технічних заходів, але й спеціалізується на дослідженні цифрових доказів.

Україні також може стати у нагоді досвід США, де серйозна увага приділяється засвоєнню правоохоронцями знань і навичок використання оперативної техніки, про що свідчить серед іншого існування окремого відділу оперативної техніки у структурі Навчального центру федеральних правоохоронних органів. Цей підрозділ проектує, розробляє та здійснює проведення програм навчання, які належать до попередження, виявлення, розслідування кримінальних правопорушень за допомогою електронної апаратури спостереження, різних засобів оперативної техніки, збиранню цифрових доказів за допомогою комп'ютерної експертизи, цифровій фотографії [1, с. 285].

Описані технічні засоби та організаційні аспекти їх застосування можуть бути використані в Україні під час реформування правоохоронної системи. Для здешевлення відповідних ініціатив пропонується використовувати потенціал науково-дослідних підрозділів у структурі відповідних відомств.

### **Література:**

1. Полиция зарубежных стран: система организации и опыт профессиональной подготовки кадров: учебное пособие / С.В. Асямов, Д.М. Миразов, А.А. Таджикиев, А.С. Якубов. – Т. : Издательство «Fan va texnologiya», 2010. – 452 с.
2. Макнамара Д. Секреты компьютерного шпионажа: Тактика и контрмеры / Д. Макнамара ; пер с англ.; под ред. С. М. Молявко. – М. : БИНОМ. Лаборатория знаний, 2004. – 536 с.
3. Drug Enforcement Administration (DEA) Agents Manual (rev. 2002) (639 pp).
4. Angel Amaya vs. USA, 2012 (Iowa Dist. Ct. 2012) [Електронний ресурс] / No. CR 11-4065-MWB. – Режим доступу: [http://www.wired.com/images\\_blogs/threatlevel/2012/04/Amaya-ruling.pdf](http://www.wired.com/images_blogs/threatlevel/2012/04/Amaya-ruling.pdf).
5. Millions of cars tracked across US in 'massive' real-time DEA spy program [Електронний ресурс]. – Режим доступу: <http://www.theguardian.com/world/2015/jan/27/millions-of-cars-tracked-across-us-in-massive-real-time-spying-program>.
6. Heath Br. New police radars can 'see' inside homes [Електронний ресурс] / Brad Heath. – Режим доступу: <http://www.usatoday.com/story/news/2015/01/19/police-radar-see-through-walls/22007615/>.
7. Antoine Jones vs. USA, 2011 (Supreme Court of the United States. 2011) [Електронний ресурс] / No. 10-1259. – Режим доступу: [http://www.supremecourt.gov/oral\\_arguments/argument\\_transcripts/10-1259.pdf](http://www.supremecourt.gov/oral_arguments/argument_transcripts/10-1259.pdf).
8. NYPD Has Used Stingrays More Than 1,000 Times Since 2008 [Електронний ресурс]. – Режим доступу : <http://www.nyclu.org/news/nypd-has-used-stingrays-more-1000-times-2008>.
9. NYPD stingray purchase records [Електронний ресурс]. – Режим доступу: [http://www.nyclu.org/files/NYSpolice\\_stingray\\_purchaserecords.pdf](http://www.nyclu.org/files/NYSpolice_stingray_purchaserecords.pdf).
10. Впервые за всю историю суд не принял доказательства, полученные с помощью Stingray [Електронний ресурс]. – Режим доступу: <http://www.securitylab.ru/news/483103.php>.

11. ЦРУ инвестирует в технологии сбора и анализа данных пользователей соцсетей [Електронний ресурс]. – Режим доступу: <http://www.securitylab.ru/news/481259.php>.
12. O'Neill P. H. Former Tor developer created malware for the FBI to hack Tor users [Електронний ресурс] / Patrick Howell O'Neill // The Daily Dot. – Apr 27, 2016. – Режим доступу: <http://www.dailydot.com/politics/government-contractor-tor-malware/>.
13. Nakashima E. Meet the woman in charge of the FBI's most controversial high-tech tools [Електронний ресурс] / Ellen Nakashima // The Washington Post. – Dec. 8, 2015. – Режим доступу: [https://www.washingtonpost.com/world/national-security/meet-the-woman-in-charge-of-the-fbis-most-contentious-high-tech-tools/2015/12/08/15adb35e-9860-11e5-8917-653b65c809eb\\_story.html](https://www.washingtonpost.com/world/national-security/meet-the-woman-in-charge-of-the-fbis-most-contentious-high-tech-tools/2015/12/08/15adb35e-9860-11e5-8917-653b65c809eb_story.html).

### **Інформаційно-пошукові системи в діяльності поліцейських**

**Косаревська О.В.**

кандидат педагогічних наук, доцент,  
доцент кафедри кібербезпеки та інформаційного забезпечення ОДУВС

На сьогодні в умовах стрімкого зростання інформаційних потоків у суспільстві постають питання налагодження та вдосконалення державного управління інформаційною сферою та її складовими і, зокрема, управління інформаційними ресурсами національної поліції України.

У сучасний період розбудови в Україні правової держави та прагнення її інтеграції до Європейського Союзу на перший план висуваються проблеми утвердження пріоритету людини в економічній, політичній і духовній сферах, які значною мірою пов'язані з узгодженням державного управління та правовим регулюванням суспільних відносин в інформаційній сфері. Конституція проголосила Україну суверенною і незалежною, демократичною, соціальною та правовою державою. Саме така держава повинна ставити науку і техніку, інформацію на службу всьому суспільству і кожній окремій людині, спрямовувати їх використання на гармонійний, усебічний розвиток кожної особистості [1, с.6].

У сучасному світі інформаційні ресурси стають рушійною силою процесів розвитку. Включення до сфери ринкових відносин інформаційних ресурсів, розвиток міжнародного співробітництва, широке впровадження відомчих (в тому числі й Національна поліція України), державних, міждержавних і глобальних інформаційно-телекомунікаційних систем, що містять інформаційні ресурси, які поступово охоплюють усі сфери суспільного життя, вимагають завчасного вирішення низки організаційно-правових, матеріальних, фінансових, технічних проблем щодо управління інформаційними ресурсами [1, с. 378].

Інформаційні ресурси є одним з основних елементів інформаційного забезпечення управління національної поліції України. Вдосконалення управління інформаційними ресурсами надасть змогу покращити як інформаційне забезпечення, так і управління системи правоохоронних органів України в цілому [2, с.274].

Питаннями дослідження інформаційних пошукових систем в діяльності правоохоронних органів досліджували В.В. Бірюков, Р.С. Белкін, А.І. Вінберг, Е.П. Іщенко, Є.Д. Лук'янчиков, В.Г. Хахановський, М.Я. Швець тощо. Разом із тим, проблеми об'єктивної та достовірної інформації, особливо в умовах прийнятого Кримінального процесуального кодексу України та впровадження ЄРДР, далеко не вичерпні та потребують удосконалення.

Інформаційні пошукові системи в діяльності правоохоронних органів України посідає дуже важливе місце. В. Афанасьєв справедливо зазначає, що керуюча и керована системи не можуть існувати без інформації [3, с. 19]. Саме інформаційно-аналітична робота дає можливість ефективно забезпечити всі види управлінської діяльності, організувати якісний зв'язок, який виникає між різними ланками системи управління, а також вирішувати поточні проблеми у процесі здійснення правоохоронної діяльності відділами та підрозділами національної поліції України. Інформаційно-аналітичне забезпечення правоохоронних органів України сучасними дослідниками визначається як комплекс організаційних, правових, технологічних засобів, які забезпечують процес збирання, отримання, обробки, поширення, аналізу та використання інформаційних ресурсів, необхідних для виконання визначених законом завдань та функцій цих органів [4, с. 351].

Використання комп'ютерних інформаційних систем і технологій у правоохоронній сфері вимагає: удосконалення форм і методів керування системами інформаційного забезпечення, подальшої централізації та інтеграції комп'ютерних банків даних, упровадження новітніх комп'ютерних інформаційних технологій для ведення кримінологічних обліків, розбудови та широкого використання

ефективних та потужних комп'ютерних мереж, застосування спеціалізованих засобів захисту та безпеки інформації, налагодження ефективного взаємо обміну кримінологічною інформацією на міждержавному рівні [5].

Таким чином, найбільш оптимальні шляхи вирішення завдань сучасного інформаційного забезпечення правоохоронних органів України мають бути досягнуті за рахунок: упровадження єдиної політики інформаційного забезпечення; створення багатоцільових інформаційних підсистем діяльності правоохоронних органів; удосконалення організаційно-кадрового забезпечення інформаційних підрозділів та їх переоснащення сучасною потужною комп'ютерною технікою з впровадженням сучасних інформаційних технологій. Для вирішення цих завдань необхідна не тільки фінансова підтримка, але й централізована нормативна база, яка спроможна забезпечити регламентацію діяльності інформаційно-аналітичних підрозділів національної поліції України.

#### **Література:**

1. Катеринчук І.П. Актуальні проблеми інформаційного забезпечення правоохоронних органів України / І.П. Катеринчук // Форум права. - 2011. - № 2. - С. 376-380.
2. Арістова І.В. Державна інформаційна політика та її реалізація в діяльності органів внутрішніх справ України: організаційно-правові засади: Дис... докт. юрид. наук: 12.00.07. - Харків, 2002. - 445с.
3. Афанасьев В. Г. Социальная информация / В. Г. Афанасьев. - М. : Наука, 1994. - 201 с.
4. Плішкін В. М. Теорія управління органами внутрішніх справ: підручник / В. М. Плішкін. - К. : Нац. акад. внутр. справ України, 1999. - 702 с.
5. Вишня В. Б. Застосування сучасних інформаційних технологій в діяльності ОВС / В. Б. Вишня, О. В. Вишня, В. О. Мирошніченко // Вісн. Запор. юрид. ін-ту ДЦУВС. - 2008. - № 3. - С. 233-238.
6. Арістова І.В. Організаційно-правові засади управління інформаційними ресурсами органів внутрішніх справ України Дис. к.ю.н: 12.00.07. - Запоріжжя, 2005. - 245с.

#### **Інформаційні технології забезпечення безпеки електронного бізнесу**

**Орлик О.В.**

кандидат економічних наук, доцент  
зав. кафедри інформаційних систем в економіці  
Одеського національного економічного університету

В сучасних умовах найбільшу значимість і поширеність має технологія Інтернет, яка надала підприємствам безмежні можливості в області передачі, розповсюдження та розсилки інформації, дозволила виконувати фінансово-банківські операції, операції з купівлі-продажу товарів, незважаючи на відстані і кордони. Разом з тим, крім позитивного ефекту, деякі особливості даної технології, які допомогли їй поширитися по всьому світу, в той же час створюють сприятливі можливості для багатьох видів злочинної діяльності.

Результатом забезпечення економічної безпеки підприємства є стабільність його функціонування, ефективність фінансово-економічної діяльності, особиста безпека персоналу. Незважаючи на те, що Інтернет забезпечує доступ виробників до максимальної кількості споживачів, дає можливість освоїти велику кількість нових ринків, паралельно виникають питання забезпечення безпеки. З урахуванням цього діяльність із забезпечення економічної безпеки підприємства включає в себе чотири основних напрямки: інформаційне забезпечення комерційної діяльності підприємства в ринкових умовах; захист інтелектуальної власності (в тому числі комерційної таємниці); захист матеріальних і фінансових цінностей; захист персоналу [1, с.90]. За оцінками експертів, витрати на створення системи безпеки підприємства і його оптимальне функціонування можуть досягати 25% витрат на весь процес виробництва [2].

З поширенням мережі Інтернет швидкість і обсяг інформації різко зросли. Кордони сучасного офісу значно розширилися завдяки бездротовим технологіям.

Активне підключення споживачів до мережі Інтернет викликало розвиток електронного бізнесу. Сфери застосування електронного бізнесу різноманітні: електронна торгівля, банківські операції, страхові операції, купівля-продаж різних продуктів, операції на фондовій біржі, IP-телефонія тощо [3]. Банки пропонують послуги управління рахунком і платежі в режимі реального часу. Цілодобово працюють Інтернет-магазини. Інтернет став простим і зручним засобом зв'язку між підприємствами

(business-to-business, B2B), між підприємцями і споживачами (business-to-consumer, B2C), між споживачами (consumer-to-consumer, C2C) та реалізації інших видів електронної комерції.

Перевагами використання підприємствами електронної комерції можна назвати наступні: низька собівартість передачі даних; простота розгортання додатків і управління ними; альтернативний додатковий спосіб ведення бізнесу; недорога рекламна площа; можливість цілодобового доступу; можливість ідентифікувати покупця; розширення ринків збуту товарів та послуг; зростаюча кількість потенційних клієнтів; зменшення часу на отримання відомостей про товар чи послугу; зменшення витрат часу на придбання необхідного товару; інформацію про товар можна представляти в Інтернеті у різному вигляді (текст, графіка, відео, тощо); мінімізація витрат на персонал та оренду приміщень.

Завдяки інформаційним технологіям різко підвищився рівень економічних можливостей у різних галузях виробничої діяльності. Але на сьогодні ситуація з електронним бізнесом залишається досить складною. Це відбувається через невелику ділову активність населення країни, а також через проблеми, пов'язані з організацією безпеки електронного бізнесу, захистом від кіберзлочинності.

З розвитком комп'ютерної техніки та використанням комп'ютерних мереж постає проблема захисту джерел інформації. Будь-яке несанкціоноване вторгнення може призвести до втрати важливої інформації, її секретності, і як наслідок – використання цієї інформації в будь-яких корисливих цілях.

Як вважають експерти, витік 20% комерційної інформації в шістдесяті випадках зі ста призводить до банкрутства підприємства [4].

Швидкий розвиток інформаційних систем загального та спеціального призначення викликає необхідність вдосконалення методів і способів користування – з одного боку, з іншого – методів і засобів захисту від несанкціонованого доступу до інформації.

Підприємства повинні захищати свої активи від випадкового чи злочинного внутрішнього та зовнішнього неправильного використання. Інформація клієнта також повинна бути захищена. Приймаючи рішення про організацію електронного бізнесу, підприємству необхідно бути готовим до того, що використання пластикових карт клієнтами в якості основного платіжного інструменту може спровокувати спроби різного роду комп'ютерних злочинів.

Основні види шахрайських дій зловмисників: придбання товарів і послуг за реквізитами вкрадених пластикових кредитних карток; злам баз даних, що містять інформацію з пластикових карт (відомості про власників пластикових карт, які здійснюють покупки в електронних магазинах); організація шахрайських електронних магазинів [1, с.92].

Виділяють декілька складових елементів захисту електронного бізнесу:

- інженерно-технічний захист інформації призначений для пасивної і активної протидії за допомогою комплексів технічних засобів;
- програмно-математичний захист інформації призначений для захисту цінної інформації, що обробляється і зберігається в комп'ютерах, локальних мережах і різних інформаційних системах;
- організаційний захист інформації містить заходи, що спонукають персонал дотримуватися правил захисту цінної інформації підприємства. Ці заходи складають 50-60% в структурі більшості систем захисту інформації. Це пов'язано з низкою факторів, а також з тим, що важливою стороною організаційного захисту інформації є підбір, розстановка і навчання персоналу, який буде здійснювати на практиці принципи і методи захисту [4].

Зміст складових елементів захисту, методи і засоби захисту повинні регулярно змінюватись з метою запобігання їх розкриття.

При цьому впроваджуються наступні механізми безпеки: шифрування, електронний цифровий підпис, контроль доступу, забезпечення цілісності даних, забезпечення аутентифікації [3].

Шифрування служить завданням дотримання конфіденційності інформації, що передається. Шифрування передбачає оборотне перетворення інформації з метою приховування від неавторизованих осіб, з наданням в той же час доступу до даної інформації авторизованим користувачам, які мають певний аутентичний ключ.

Електронний цифровий підпис (ЕЦП) призначений для захисту електронного документа від підробки. Особливість ЕЦП полягає у тому, що він ґрунтується на алгоритмах криптографічного захисту інформації і накладається за допомогою особистого ключа – спеціального коду, відомого тільки особі, яка підписала документ. Дійсність ЕЦП перевіряється за допомогою відкритого ключа – коду перевірки. Цей код робить неможливим підробку ЕЦП автора електронного документа, але надає можливість перевірити його справжність.

Контроль доступу – функція системи, що забезпечує технологію безпеки, яка дозволяє або забороняє доступ до певних типів даних, засновується на ідентифікації суб'єкта, якому потрібен

доступ, і об'єкта даних, що є метою доступу. Доступ до захищеної інформації повинен бути обмежений, щоб тільки особи, які мають право доступу, могли отримувати цю інформацію.

Комп'ютерні програми і в багатьох випадках чужорідні комп'ютери за допомогою локальної мережі, Інтернету, бездротових технологій можуть отримати секретну інформацію, яка їм не призначена. Тому, складність механізмів контролю доступу повинна бути в паритеті з цінністю інформації, тобто чим більш важливою або цінною є інформація, тим складнішими повинні бути механізми контролю доступу до неї.

Цілісність даних означає, що дані не були змінені при виконанні будь-яких операцій над ними, будь то передача, зберігання і відображення.

Забезпечення аутентифікація передбачає проведення процедури перевірки автентичності іншої сторони: перевірка справжності користувача шляхом порівняння введеного їм пароля з паролем, збереженим в базі даних користувачів; підтвердження справжності електронного листа шляхом перевірки цифрового підпису листа з відкритим ключем відправника тощо.

Основними заходами протидії комп'ютерним злочинам також є: контроль роботи розробників комп'ютерних систем, захист від несанкціонованого доступу до системи, профілактика від комп'ютерних вірусів, ретельність підбору персоналу, виключення випадків ведення особливо важких робіт тільки однією людиною, охорона об'єктів безпеки, установка резервних систем електроживлення, оснащення приміщень кодовими замками і сигналізацією тощо. Основними характеристиками кожного заходу є вартість захисту та економічний ефект використання.

Отже, з розвитком комп'ютерних інформаційних технологій загострилася проблема комп'ютерних злочинів, які можуть завдати підприємству як фінансових, так і інформаційних втрат. Головне в організації бізнесу – не тільки грамотно використовувати наявну інформацію, але і забезпечити її якісний захист всіма доступними засобами.

#### **Література:**

1. Дробышева, В.Г. Роль и место информационных технологий в системе экономической безопасности государства [Текст] / В.Г. Дробышева, А.П. Черноиванов // Социально-экономические явления и процессы. – 2011. – №3-4. – С. 87-93.
2. Козивкин, В. В. Экономическая безопасность промышленного предприятия [Электронный ресурс] / В.В. Козивкин. – Режим доступа \www/ URL: [http://secandsafe.ru/pravovaya\\_baza/blogi/ekonomicheskaya\\_bezopasnost/ekonomicheskaya\\_bezopasnost\\_pro\\_myshlennogo\\_predpriyatiya](http://secandsafe.ru/pravovaya_baza/blogi/ekonomicheskaya_bezopasnost/ekonomicheskaya_bezopasnost_pro_myshlennogo_predpriyatiya). – Заголовок з екрана, доступ вільний, 08.10.2016.
3. Будянский, П. С. Роль информационных технологий в современной экономике [Электронный ресурс] / П.С. Будянский. – Режим доступа \www/ URL: <http://economyar.narod.ru/budjnskii.pdf>. – Заголовок з екрана, доступ вільний, 08.10.2016.
4. Павлов, А. П. Информационные технологии экономической безопасности бизнеса [Электронный ресурс] / А.П. Павлов, А. В. Колосов // Мир науки. Научный Интернет журнал. – 2013. – Вып. 1. – Режим доступа \www/ URL: <http://mir-nauki.com/PDF/02EMN113.pdf>. – Заголовок з екрана, доступ вільний, 08.10.2016.

#### **Подстройки коэффициентов модели управления как методика процедуры адаптации**

**Балтовский А.А.**

доктор технических наук доцент, профессор кафедры кибербезопасности и информационного обеспечения Одесского государственного университета внутренних дел

**Сифоров А.И.,**

кандидат технических наук доцент,  
начальник учебно-методического отдела Одесского государственного университета внутренних дел

Условия функционирования реальных адаптивных автоматизированных систем управления (ААСУ) таковы, что характеристики задающих и возмущающих воздействий либо известны недостаточно, либо существенно изменяются во времени, что сказывается на их качественных показателях. Избежать этого возможно путем использования адаптивной подстройки коэффициентов моделей управляемых объектов [1,2].

Пусть в качестве модели управления используется полином вида

$$y_M = k_0 + \sum_{i=1}^n k_i x_i + \sum_{i=1}^n \sum_{j=1}^n k_{ij} x_i x_j,$$

или

$$y_M = \sum_{i=1}^n \sum_{j=1}^n k_{ij} x_i x_j, \quad (x_0 = 0),$$

т.е. полная квадратичная модель [1-3].

Предлагаемой методикой предполагается перевод модели  $y_M$  в каноническую форму

$$Y_M^k = A_0 + \sum_{i=1}^n A_i U_i^2,$$

где  $U_i$  - новые пересчитанные переменные.

Такое преобразование позволяет уменьшить число параметров модели до  $n + 1$ . После этого преобразования осуществляется процесс подстройки коэффициентов  $A_i (i = 1, 2, \dots, n)$  модели  $Y_M^k$ .

Задача приведения уравнения  $y_M$  к каноническому виду состоит в переходе к новой системе координат (обозначим их  $t_1, t_2, \dots, t_n$ ) и в последующем повороте координатных осей этой системы так, что линейные члены взаимодействия исчезают.

Методика перехода от исходного уравнения  $y_M$  к канонической форме  $Y_M^k$  заключается в следующем [1-3]:

1. На первом этапе уравнение  $y_M$  преобразуется к квадратичной форме вида

$$y_M = \beta_0 + \sum_{i=1}^n \sum_{j=1}^n k_{ij} t_i t_j. \text{ Осуществляется эта процедура путем замены } x_i = t_i + \alpha_i.$$

2. Затем выражение для  $x_i$  из предыдущего выражения подставляется в исходное выражение и коэффициенты при  $t_i$  приравниваются к нулю. Т.о. образуется система  $n$  уравнений с  $n$  независимыми  $\alpha_i$ . Решая указанную систему, определяем  $\alpha_i$  и рассчитываем свободный член. В векторной форме уравнение квадратичной формы принимает вид  $Y_M = \beta_0 + T^T B T$ , где  $T$  - вектор переменных  $t_i$ ;

$T^T$  - аппроксимированный вектор  $T$ ;  $B$  - симметрическая матрица коэффициентов  $k_{ij}$ .

Скорость сходимости одношагового алгоритма адаптации будет наивысшей в том случае, когда векторы входных воздействий ортогональны т.е. когда  $X_i X_j = 0$ , где  $i, j = 1, 2, \dots, n$  ( $n$  - количество учитываемых независимых входных переменных) при  $i \neq j$ . Это свойство предлагается использовать в алгоритме управления технологическим объектом. Алгоритм вначале задает нулевые оценки параметров модели  $k_{i0}$ . При этом считается также, что известны контролируемые входные переменные, которые являются составными элементами модели. На первом шаге алгоритма

$$x_i = (x_{i_{\max}} + x_{i_{\min}}) / 2,$$

где  $x_{i_{\max}}, x_{i_{\min}}$  - предельно допустимые значения данной переменной (берутся обычно из регламента).

Значение второй управляющей переменной  $x_2$  определяется из условия  $\sum_{i=1}^n k_{i0} x_{i1} = y_3$ , где  $y_3$

- заданное значение выходной переменной.

Определенные таким образом управляющие воздействия реализуются на объекте управления [3].

На последующих двух шагах алгоритма, при тех же оценках коэффициентов и при известных контролируемых переменных, управляющие воздействия рассчитываются из условий



$$\sum_{i=1}^n k_{i0} x_{in} = y_3,$$

$$\sum_{i=1}^n k_{in-1} x_{in} = 0,$$

где  $n-1$ ,  $n$  характеризуют соответственно  $n-1$  и  $n$  - шаги работы алгоритма, а затем рассчитанные управляющие воздействия снова реализуются на объекте.

На четвертом шаге после получения значения выходной величины  $y_i$  - реакции объекта на вектор входных переменных  $x_i$  - уточняются параметры модели по формуле

$$\bar{K}_1 = \bar{K}_0 + ((y_1 - y_3) / (y + \bar{x}_1^T \bar{x}_T)) \bar{x}_1,$$

а значение управляющих воздействий находятся из условий

$$\sum_{i=1}^n k_{i0} x_{i4} = y_3, \sum_{i=1}^n k_{i3} x_{i4} = 0.$$

### Литература:

1. Виттих В.А. Адаптивная дискретизация с использованием метода наименьших квадратов / Виттих В.А. ; Автометрия, Ин-т математики. — К. : Ин-т математики, 2006. — 111 с. — (Математика та её применение) (Труды / Ин-т математики НАН Украины ; т. 4). — Библиогр.: с. 97—106 (93 назв.).
2. Виттих В.А. Адаптивная дискретизация с использованием экспоненциальных функций: учеб. [для студ. высш.учеб. завед.] / В.А. Виттих, В.П. Сабилло ; М-во образования и науки СССР, Ин-т инновац. технологий. — М: Растр-9, 1974. — 375 с. : ил., табл., портр. — Библиогр.: с. 358—362. — ISBN 978-966-2004-01-4.
3. Егоров С.В. Моделирование и оптимизация в АСУТП: учеб. [для студ. высш.учеб. завед.] / С.В. Егоров, Д.А. Мирахметов ; М-во образования и науки СССР, Ин-т инновац. технологий. — М : Растр-9, 1987. — 200 с. : ил., табл., портр. — Библиогр.: с. 240—251. — ISBN 987-376-2003-01-4.

### Визначення проявів корупційних правопорушень в інформаційній сфері

**Підвашецька Л.В.**

слухач 2-го курсу магістратури  
факультету №2 ОДУВС

**Форос Г.В.**

кандидат юридичних наук, доцент  
професор кафедри кібербезпеки та  
інформаційного забезпечення ОДУВС

Корупція є однією з найгостріших соціальних проблем сучасності. Деякі дослідники вважають, що корупція стала головною політичною проблемою кінця ХХ століття і на сьогодні вона є одним з основних чинників, що створюють реальну загрозу як національній безпеці, так і демократичному розвитку кожної держави. Будучи багатоаспектним явищем в Україні, причинність корупційних проявів поділяють на дві групи. Перша включає всебічні причини корупції в Україні (відсутність належної законодавчої бази для більш ефективної протидії корупції, неналежне виконання запобіжних функцій інститутами держави, впливовість суб'єктів корупційних правопорушень, які наділені ефективною системою захисту від соціального контролю, низький рівень заробітної плати державних службовців порівняно з заробітною платою у приватному секторі, трансформації явища корупції з соціальної аномалії на норму функціонування державної влади та вирішення життєвих проблем для значної кількості населення). Другу групу складають ті, які власне відносяться до існування та поширення корупції безпосередньо в інформаційній сфері [1].

Питанням вивчення з проблематики поширення та боротьби з корупційними правопорушеннями займалися такі вітчизняні науковці, як: В. Б. Авер'янов, О. Ф. Андрійко, Ю. П. Битяк, В. М. Гаращук, Р.

А. Калюжний, так і зарубіжні, серед яких: Д. М. Бахрах, Б. В. Волженкіна, О. Гределанда, М. В. Костеннікова, А. В. Куракіна, С. Коткіна, Р. Клітгарда та ін. Однак, майже повністю відсутні дослідження щодо прояву корупції в інформаційній сфері, досі не визначеним є поняття «корупційних правопорушень в інформаційній сфері», ознаки, які відмежовують цей вид правопорушення від інших.

Корупція внашій державі «торкнулась» майже всіх сфер суспільства, втому числі й інформаційної, що своєю чергу може призвести до руйнування та унеможливлення реалізації задекларованих прав на можливість вільного одержання, використання, поширення та зберігання відомостей, необхідних їм для реалізації своїх прав, свобод ізаконних інтересів, здійснення завдань і функцій [2].

Вважаючи за доцільне розглядати дану проблематику з позиції інформаційної сфери як сфери інформаційної діяльності, яка динамічно інтегрує між собою всі ключові складові цієї сфери, такі як: її суб'єкти (фізичні, юридичні особи), їх діяльність (інформаційні дії, процеси) та об'єкти цієї діяльності (інформація, засоби зв'язку та інформатизація), слід підкреслити той факт, що даному виду правопорушень притаманна своя форма суспільних відносин, об'єктом яких є «інформація» як ресурс й «інформаційна інфраструктура» [3]. Дана концепція знайшла своє відображення в основі законодавства про інформацію, а саме в Законі України «Про інформацію» [4], який хоча і не містить дефініції інформаційної сфери як такої, проте визначає основні види інформаційної діяльності.

Розглядаючи проблему визначення корупційного правопорушення в інформаційній сфері А.І. Алексєєв в своїх дослідженнях зазначає той факт, що «неможливо чітко інтерпретувати даний вид правопорушення з правової точки зору» [5]. Суб'єктами таких діянь виступають як особи, уповноважені на виконання функцій держави або місцевого самоврядування, так і особи, які прирівняні до них (наприклад нотаріуси), посадові особи юридичних осіб.

На жаль, сучасні дослідження свідчать, що значна частина громадян України не оцінює корупцію негативно і вважає за можливе вирішення особистих питань за допомогою дачі хабарів, використання службових можливостей родичів, друзів, які, перебувають на державній службі. Тим самим, С.В. Невмержицький у своїх дослідженнях виокремив, що «українцям не вигідна цивілізована європейська модель корупції, в якій рівень корупційних проявів досить низький, оскільки корупція сприймається в суспільстві як явна аномалія, порушення закону, який поважає і дотримується громадськість» [6]. Так, обмеженість або повна відсутність повноцінного доступу до нових технологій, інформації, сучасних систем зв'язку, збору, обробки та передачі інформації може призвести до негативних наслідків, внаслідок якої буде порушення задекларованих демократичних прав та свобод людини та громадянина у гарантованій законом доступі до інформаційно-комунікаційних технологій сучасності.

Таким чином, корупційні правопорушення в інформаційній сфері на сьогодні є одним із розповсюджених та негативних проявів, яка полягає в активних діях особи, а саме в незаконному використанні та розповсюдженні інформації, що стала відома особі у зв'язку із виконанням нею службових обов'язків. Для подолання зростання негативного впливу на безпеку в інформаційному просторі слід впровадити стійкий механізм боротьби із корупційними проявами в мережі Інтернет та вдосконалити нормативно-правову базу в протидії корупції в інформаційно-комунікаційній сфері.

### **Література:**

1. Олійник О. Захист інформації в умовах інформаційного суспільства / О. Олійник // Право України. - 2005. - № 10. - 100-101 с.
2. Проблеми протидії правопорушенням в інформаційній сфері: реалії та перспективи // [Електронний ресурс]. – Режим доступу: <http://www.viche.info/journal/3151/>
3. Юридична характеристика в інформаційній сфері // [Електронний ресурс]. – Режим доступу: <http://radnuk.info/pidrychnuku/admin-pravo/493-stetsenko/21418-2012-06-23-10-57-06.html>
4. Про інформацію: Закон України від 02.10.1992 № 2657-ХІІ // [Електронний ресурс]. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/2657-12>
5. Монахов В.Н. СМИ и Интернет: проблемы правового регулирования / Отв. ред. М. В. Горбаневский. – М.: ЭКОПРИНТ, 2003. – 320 с.
6. Невмержицький С. В. Корупція в Україні: причини, наслідки, механізми протидії / С. В. Невмержицький. - К., 2008. - 10 с.

**Щур К.В.**

слухач 2-го курсу магістратури  
факультету №2 ОДУВС

**Форос Г.В.**

кандидат юридичних наук, доцент  
професор кафедри кібербезпеки та  
інформаційного забезпечення ОДУВС

Незважаючи на прийняті в національних законодавствах заходи щодо протидії кіберзлочинності у ряді країн, у тому числі і в Україні, її «уніфікований» склад до цього часу чітко не визначений, оскільки як можливості технічних засобів, програмного забезпечення, засобів телекомунікацій, так і кримінальні хитрування самих кіберзлочинців, безперервно зростають з розвитком науково-технічного прогресу і відсталістю правових норм протидії [1, с. 30].

Проаналізувавши українські статистичні дані можна зробити висновок про те, що збиток, який завдає кіберзлочинність, сьогодні значно перевищує розмір збитків від традиційних видів злочинів. Кількість протиправних посягань на інформаційні ресурси держави зростає [2]. І якщо враховувати щоденне збільшення обсягів інформації, яка обробляється державними структурами, виникає необхідність їх захисту від протизаконних дій.

За даними PricewaterhouseCoopers кіберзлочинність стала одним з найпоширеніших економічних злочинів в Україні, а збитки від онлайн-злочинів і махінацій на сьогодні вже перевищили збитки від традиційних форм злочинності в Україні.

Специфіка даного виду злочинності полягає у:

- відносній комфортності, тобто готування та скоєння злочину здійснюється, практично не відходячи від «робочого місця»;
- доступності – у зв'язку з тенденцією постійного зниження цін на комп'ютерну техніку;
- географії скоєння злочинів, яка є досить широкою, але враховуючи те, що основна кількість комп'ютерів розташована у великих населених пунктах, то саме на них і припадає «левова частка» злочинності;
- віддаленості об'єкту злочинних посягань – він може знаходитись за тисячі кілометрів від місця скоєння злочину;
- складності виявлення, фіксації і вилучення криміналістично-значущої інформації (слідової картини злочину) при виконанні слідчих дій для використання її в якості речового доказу і т. ін.

На сьогоднішній день українці являються постійними користувачами мережі Інтернет. З кожним роком злочинів в Інтернеті збільшується приблизно на 25-30%. В Україні вже були прецеденти, коли групи хакерів зупиняли діяльність сайтів держави і намагалися зламати бази даних. Тому влада вже сьогодні повинна подбати про кібербезпеку.

Одною з головних проблем ІТ-безпеки в Україні являється відсутність скоординованого підрахунку а також і оцінки хакерських атак. В результаті країна не знає, як зламують її ресурси, хто це робить і звідки.

Розслідуванням злочинів з використанням комп'ютерних технологій проводить команда реагування на надзвичайні комп'ютерні події України CERT-UA, що займається, серед іншого, реагуванням на кібератаки проти державних ресурсів. Метою діяльності CERT-UA є забезпечення захисту державних інформаційних ресурсів та інформаційних і телекомунікаційних систем від несанкціонованого доступу, неправомірного використання, а також порушень їх конфіденційності, цілісності та доступності. Кожен раз, коли хто-небудь атакує офіційні web-сторінки держустанов, CERT-UA проводить розслідування.

Також слід відзначити що раніше українські хакери писали віруси для злому і розкрадання даних в західних країнах, то тепер у зв'язку з посиленням боротьби американського і європейських урядів з комп'ютерними злочинами їх увага переключилася на Україну.

Наша країна з її низьким рівнем обізнаності про загрози використання комп'ютерів і низьким рівнем інформаційної безпеки стає для них багатим джерелом. Розкрадання коштів в системах інтернет банкінгу, даних кредитних карт, шахрайство в інформаційних мережах і інсайдерські витоки інформації стають повсякденними явищами.

За оцінками експертів, в останні місяці в управлінні з боротьби з кіберзлочинністю фіксується значна кількість випадків крадіжки грошей через клієнт-банк.

Однак подібні факти замовчуються, повідомлень в ЗМІ про них практично немає. У ряді випадків є ситуації, коли такі шахрайські схеми реалізуються організованими групами, у які входять представники банків та силових структур.

Українською проблемою є як недостатня кількість державних експертів в області комп'ютерно-технічної експертизи, так і складності з введенням в правове поле досліджень фахівців комерційних організацій. Середній термін проведення комп'ютерно-технічних експертиз становить від півроку і вище через високу завантаженість профільних державних установ. Для проведення розслідування таких злочинів необхідні кваліфіковані фахівці, що володіють не тільки технічними навичками, але й знаннями в галузі права.

Боротися з подібними проблемами можна за допомогою інтеграційного підходу. Тому уряди багатьох країн йдуть сьогодні шляхом створення на державному рівні комплексних систем інформаційної безпеки шляхом об'єднання зусиль державних органів, представників бізнес-співтовариств і громадських організацій.

Таким чином, стрімкий розвиток інформаційних технологій є причиною прогресу кіберзлочинності. Вже сьогодні шкода, завдана віртуальними злочинцями в Україні, оцінюється в десятки мільйонів гривень. Країна прагне до світового лідерства за кількістю кіберзагроз. Крім того, збільшилась кількість загроз для користувачів мобільних технологій.

Підводячи підсумок можна сказати, що проблема профілактики і стимулювання кіберзлочинності в Україні – це комплексна проблема. На сьогоднішній день закони повинні відповідати вимогам, що пред'являються сучасним рівнем розвитку технологій. Пріоритетним напрямком є також організація взаємодії і координація зусиль правоохоронних органів, спецслужб, судової системи, забезпечення їх необхідною матеріально-технічною базою. Сьогодні жодна держава не в змозі протистояти кіберзлочинності самотійно. Нагальною є необхідність активізації міжнародної співпраці в цій сфері.

#### **Література:**

1. Карпов Н., Вертузаев М. К вопросу о борьбе с компьютерными преступлениями в Украине // Закон и жизнь. – 2004. – № 7.

2. Глава СБУ назвал основные угрозы нацбезопасности [Електронний ресурс]. — Режим доступу: [http://lb.ua/news/2012/03/23/142428\\_glava\\_sbu\\_nazval\\_osnovnie\\_ugrozi.html](http://lb.ua/news/2012/03/23/142428_glava_sbu_nazval_osnovnie_ugrozi.html).

#### **Деякі аспекти щодо проблем запобігання та протидії кіберзлочинності**

**Бадюк М.О.**

слухач 2-го курсу магістратури  
факультету №2 ОДУВС

**Форос Г.В.**

кандидат юридичних наук, доцент  
професор кафедри кібербезпеки та  
інформаційного забезпечення ОДУВС

Розвиток науково-технічного прогресу, пов'язаний з впровадженням сучасних інформаційних технологій, призвів до появи нових видів злочинів, зокрема, до незаконного втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж, викрадення, привласнення, вимагання комп'ютерної інформації, які узагальнені у небезпечному антисоціальному явищі, що отримало назву «кіберзлочинність»[1].

Українське ж законодавство у сфері захисту інформації, на думку Ю. Омельченка, вимагає дуже серйозного доопрацювання. «Потенційно існує ймовірність того, що кіберзлочинність буде виштовхуватися з Європи, то вона буде перебиратися в Україну. Та й уже цей процес відбувається», - зазначив експерт [2, с.10].

Підкіберзлочинністю слід розуміти сукупність злочинів, що вчинюються у віртуальному просторі за допомогою комп'ютерних систем або шляхом використання комп'ютерних мереж та інших засобів доступу до віртуального простору, в межах комп'ютерних мереж, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних [3, с.332].

Основною проблемою боротьби зі злочинністю в мережі Інтернет є транснаціональність самої мережі і відсутність механізмів контролю, необхідних для правозастосування. Мережа Інтернет створювалася технологічно як структура без ієрархії і без якогось «ядра», зруйнувавши які можна було б паралізувати її роботу і навряд чи хтось міг уявити масштаби розвитку проекту, спочатку не

призначеного для широкої аудиторії. Основною метою створення цієї мережі була стійкість до атак ззовні, і навряд чи хтось міг передбачити подальший масштаб її розвитку, її економічну та соціальну роль в майбутньому. Саме відсутність розроблених механізмів контролю мережі зсередини укупі з її доступністю і легкістю використання стало однією з глобальних проблем інформаційного співтовариства: децентралізована структура мережі, відсутність національних кордонів в кіберпросторі зумовили можливості для росту злочинності та на роки відклали розроблення механізмів правового та соціального контролю в сфері використання інформаційних мереж для вчинення злочинів [4].

Слід відмітити відповідну специфіку протидії кіберзлочинності в багатьох країнах, у тому числі й в Україні. Ця специфіка обумовлена наступними факторами:

- відсутністю налагодженої системи правового та організаційно-технічного забезпечення законних інтересів громадян, держави та суспільства в галузі інформаційної безпеки;
- обмеженими можливостями бюджетного фінансування робіт по створенню правової, організаційної та технічної бази інформаційної безпеки;
- недостатнім усвідомленням можливих політичних, економічних, моральних та юридичних наслідків комп'ютерних злочинів;
- слабкістю координації дій по боротьбі з комп'ютерними злочинами правоохоронних органів, органів суду, прокуратури та невідповідністю їх кадрового складу до ефективного попередження, виявлення та розслідування таких діянь;
- серйозним відставанням вітчизняної індустрії розробки, впровадження засобів і технологій інформатизації та інформаційної безпеки від розвинутих країн світу [5].

Боротьба зі злочинністю в сучасних умовах міжнародних комп'ютерних мереж ускладнена з наступних причин:

- злочинні діяння можуть мати місце в кіберпросторі. Для виявлення та розслідування комп'ютерних злочинів вчинених з використанням комп'ютерної мережі, потрібні конкретний спеціальний досвід і знання, процедури розслідування і відповідні юридичні повноваження;
- міжнародні комп'ютерні мережі, такі як Інтернет, є відкритим середовищем, що дає користувачам можливості чинити певні дії за межами кордонів держав, у яких вони перебувають. Це означає, що боротьбу зі злочинністю у відкритих комп'ютерних мережах не можна здійснювати без належного міжнародного співробітництва;
- відкритість глобальних інформаційних мереж надає можливість користувачам вибирати таку юрисдикцію, яка відповідає їхнім цілям. Користувачі можуть вибирати ті країни, в яких певні діяння, здійснені в кіберпросторі, не визначаються як кримінальнокарані. Такі країни можуть створювати привабливі можливості для протиправних дій осіб з тих держав, де такі дії, згідно внутрішнього законодавства, підпадають під кримінальну відповідальність.

Необхідний постійний розвиток внутрішньодержавної правової бази у сфері обігу комп'ютерної інформації, яка повинна відповідати вимогам сучасності та бути адаптованою до норм міжнародного права. Особливої уваги потрібно приділяти удосконаленню та узгодженню кримінального та кримінально-процесуального законодавства, пов'язаного з кваліфікацією, виявленням та розслідуванням кіберзлочинів. Слід також вирішити правові питання з приводу розголошення провайдерами інформації про користувачів на запит правоохоронних органів та можливості використання такої інформації як доказу [3, с. 340].

Отже, враховуючи вищезазначене, а також спираючись на вітчизняний та міжнародний досвід, вважаємо за потрібне визначити найбільш доцільні, на погляд, шляхи вирішення проблемних питань боротьби з комп'ютерними злочинами в Україні:

- приведення національного законодавства у відповідність до вимог Конвенції ООН проти транснаціональної організованої злочинності та Конвенції Ради Європи про кіберзлочинність, подальше вдосконалення нормативно-правової бази, яка регулює боротьбу з комп'ютерною злочинністю (розширення можливостей правоохоронних органів з урахуванням транснаціонального характеру комп'ютерної злочинності, розроблення ефективного механізму взаємодії національних правоохоронних органів з компетентними органами інших країн);
- утворення спеціалізованого підрозділу, виключною компетенцією якого стала б боротьба з комп'ютерною злочинністю, що за умови надання цьому підрозділу відповідних повноважень та залучення відповідних кадрових і матеріально-технічних ресурсів сприятиме підвищенню ефективності роботи правоохоронної системи України у цій сфері;
- налагодження, на відповідній правовій основі, ефективної взаємодії з міжбанківськими інституціями, телекомунікаційними компаніями, зацікавленими центральними державними органами та правоохоронними органами інших країн з метою документування злочинних груп з міжнародними зв'язками.

**Література:**

1. Шакірова З.Х. Кіберзлочинність як масштабна проблема [Електронний ресурс] / З.Х. Шакірова // Сучасні наукові дослідження та інновації. – 2013. – Режим доступу: <http://web.snauka.ru/issues/2013/08/25764>.
2. Прохоренко В. Кіберзлочинність для України стає актуальним поняттям – НБУ. - // Економічна правда від 26 лютого, 2013 року.
3. Голіна В.В., Головін Б.М. Кримінологія: Загальна та Особлива частини // Навчальний посібник. - Х.: Право, 2014. - 513 с.
4. Савчук Н.В. Кіберзлочинність: зміст та методи боротьби / Н.В. Савчук // Теоретичні та прикладні питання економіки: зб. наук. праць. – К.: Видавничо-поліграфічний центр «Київський університет», 2009, 338-342с.
5. Бутузов В.М. Злочини із застосуванням сучасних інформаційних технологій // Науково-практичний журнал «Боротьба з організованою злочинністю і корупцією» - 2003. - № 7. - С. 84-89.

**Інформаційні технології в поліцейській діяльності**

**Деркач В.А.**

завідувач відділення технічних засобів навчання  
навчально-методичного відділу ОДУВС

**Деркач І.І.**

слухач магістратури факультету №2  
ННІЗДН ОДУВС

Діяльність органів внутрішніх справ значною мірою пов'язана з отриманням та використанням відомостей обмеженого доступу, розголошення яких може спричинити порушення конституційних прав громадян, а також зниження ефективності роботи правоохоронних органів щодо попередження, розкриття та розслідування злочинів, тому потрібно розглянути поняття інформаційне забезпечення – це комплекс методів, заходів, засобів різного характеру, які забезпечують створення та функціонування інформаційних технологій, а також їх ефективне використання для вирішення покладених на них завдань. З даного поняття випливає, що інформаційна технологія – це цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування [9].

У процесі здійснення своєї діяльності співробітники національної поліції України отримують інформацію про режим і характер роботи підприємств, розташованих на території, що обслуговується, відомості, що стосуються особистого життя громадян, а також іншу інформацію (наприклад, службового характеру). Дана інформація, а також відомості про окремі методи, прийоми і результати роботи органів внутрішніх справ складають службову таємницю. Розголошення таких відомостей порушує нормальну їх діяльність і значно знижує її ефективність.

Велика увага сьогодні приділяється нормативно-правовому забезпеченню інформаційної безпеки. Базові засади закладаються Конституцією України (ст. 17, 19, 31, 32, 34, 50, 57 та 64) [1], Закон України «Про інформацію» закладає правові основи інформаційної діяльності [2].

Крім цього ціла низка законодавчих актів регулює відносини у інформаційній сфері. Це, зокрема, Закони України «Про телекомунікації», «Про Національну програму інформатизації», «Про захист інформації в інформаційно-телекомунікаційних системах», а у Кримінальний кодекс України було введено розділ XVI, в якому визначалася відповідальність за злочини в інформаційній сфері.

Цілий ряд нормативно-правових актів, які безпосередньо стосуються питань інформаційної безпеки прийнято Міністерством внутрішніх справ України та Національною поліцією України. Серед цих документів особливу увагу необхідно звернути на:

- Доручення МВС України від 19.03.2015 № 13155/Ав «Про заходи із протидії витоку службової інформації» [3];
- Доручення МВС України від 24.04.2015 № 19130/Ав «Про недопущення витоку інформації, що утворюється в службовій діяльності» [4];
- Наказ Національної поліції України від 07.12.2015 № 176 «Про запобігання негативним наслідкам використання інтернет-ресурсів російських провайдерів» [5];

Саме в цих документах встановлено вимоги до парольного захисту, розглянуто питання застосування у службовій діяльності поштових серверів та роботи з електронною поштою [3].

На сьогодні існує багато загроз при роботі з інформацією на сучасному комп'ютерному обладнанні. Треба зазначити, що значна кількість проблем виникає саме з вини користувача. На сьогодні, на жаль, саме користувачі є винні у більшості випадків у тому, що важлива інформація може бути втрачена, спотворена або викрадена. Нехтуючи простими правилами користувачі ставлять під загрозу не тільки персональну, а і службову інформацію.

Тому в цілому, система інформаційного забезпечення національної поліції України – це сукупність взаємопов'язаних та взаємодіючих організаційних елементів та технічних засобів, яка здійснює інформаційне забезпечення національної поліції України [4].

Основною метою системи інформаційного забезпечення національної поліції України є всебічна інформаційна підтримка діяльності правоохоронних органів у боротьбі зі злочинністю на основі комплексу організаційних, нормативно-правових, технічних, програмних та інших заходів.

Вжиті Міністерством заходи щодо створення Інтегрованої інформаційно-пошукової системи (далі - ІПС ) стали передумовою для впровадження Єдиної комп'ютерної інформаційної системи правоохоронних органів (СБУ, Держприкордонслужба, Держмитслужба, ДПА та Генпрокуратура України) з питань боротьби зі злочинністю, створення якої передбачено Указом Президента України від 11.01.2006 р. № 80/2006 та розпорядженням Кабінету Міністрів України від 19.09.2007 р. № 754-р «Про схвалення Концепції Державної програми інформаційно-телекомунікаційного забезпечення правоохоронних органів, діяльність яких пов'язана з боротьбою із злочинністю».

Необхідно також відмітити, що зазначена система містить у собі наступні бази даних: «Факт», «Злочин», «Доставлені», «Контур», «Особа», «Розшук», «Адміністративне правопорушення», «Корупційне правопорушення», «Мігрант», «Угон», «Річ», «Втрачені документи», «Кримінальна зброя», «Зареєстрована зброя», «Електронний рапорт».

До складу ІПС входять такі підсистеми «Особа», «Розшук», «Пізнання», «Номерні речі», «Антикваріат», «Кримінальна зброя», «Автомобілотранспорт», «Арсенал», «АПРА», «Втрачені паспорти», а також Система централізованого управління нарядами патрульної служби (далі – система «ЦУНАМІ») [6, с. 243, 245].

Система «ЦУНАМІ» являє собою комплекс апаратних та програмних засобів, а також персоналу, призначений для управління силами й засобами органів національної поліції України. Дана система забезпечує користувачів необхідними інформаційними, технічними та аналітичними ресурсами для виконання функціональних обов'язків та прийняття ефективних управлінських рішень. Система фіксує, зберігає та робить доступними для аналізу та контролю повідомлення до правоохоронних органів і результати реагування на них [8, с. 126].

Впровадження системи «ЦУНАМІ» обумовила процес організації діяльності, управління силами й засобами національної поліції України для ефективного реагування на повідомлення про злочини та події, оптимізувала роботу нарядів патрульної служби, задіяних для охорони громадського порядку в системі єдиної дислокації, слідчо-оперативних груп чергових частин, скоротила час реагування на повідомлення громадян про злочини та події, попередженню правопорушень й затримання злочинців по «гарячих слідах», здійснює оперативний контроль за своєчасністю і якістю реагування нарядами патрульної служби на злочини та правопорушення, дотриманню законності під час виконання службових обов'язків працівниками національної поліції України [8, с. 129].

Реалізація проекту «ЦУНАМІ» в інших регіонах України забезпечить подальший стабільний соціально-економічний розвиток міста, підвищить захист життя, здоров'я, власності громадян від протиправних посягань та ефективність контролю за об'єктами інфраструктури країни.

#### **Література:**

1. Конституція України від 28 червня 1996 р. // Відомості Верховної Ради України. - 1996. - №30. -ст.141.
2. Закон України «Про інформацію» від 02.10.1992 р.
3. Доручення МВС України від 19.03.2015 № 13155/Ав «Про заходи із протидії витоку службової інформації».
4. Доручення МВС України від 24.04.2015 № 19130/Ав «Про недопущення витоку інформації, що утворюється в службовій діяльності».
5. Наказ Національної поліції України від 07.12.2015 № 176 «Про запобігання негативним наслідкам використання інтернет-ресурсів російських провайдерів».
6. Комп'ютерні технології у діяльності органів внутрішніх справ України (Загальна частина): Посібник / Хахановський В.Г., Кудінов В.А., Грищенко О.І. – К.: КНУВС, 2006. – 368 с.

7. Системна інформатизація правоохоронної діяльності: європейські нормативно-правові акти та підходи до упорядкування суспільних інформаційних відносин у зв'язку з автоматизованою обробкою даних у правоохоронній діяльності: Посібник. Книга 2 / Упорядники: М.Швець, В.Брижко, Б.Романюк, В.Цимбалюк; За ред. члена-кореспондента АПрН України М.Швеця та к.ю.н. Б.Романюка. – К.: НДЦПІ АПрН України, 2006 р. – 509 с.
8. Хахановський В.Г. Проблеми теорії і практики криміналістичної інформатики, монографія, – К.: Вид.Дім „Аванпост-Прим”, 2010. – 382 с.
9. Катеринчук І.П. Актуальні проблеми інформаційного забезпечення правоохоронних органів України / І. П. Катеринчук // Форум права. - 2011. - № 2. - С. 376-380.

### **Сутність та роль кібербезпеки в сучасному суспільстві**

**Храпкіна В.В.**

доктор економічних наук, професор,  
Київський університет ринкових відносин

**Храпкін О.М.**

студент Національного авіаційного університету

Сучасний розвиток суспільства спонукає до широкого використання комп'ютерних систем і телекомунікаційних мереж, що істотно підвищує ефективність обміну інформацією. Водночас переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці. Поряд із інцидентами природного походження зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб.

Поширюються випадки незаконного збирання, зберігання, використання, знищення, поширення, персональних даних, незаконних фінансових операцій, крадіжок та шахрайства у мережі Інтернет. Кіберзлочинність стає транснаціональною та здатна завдати значної шкоди інтересам особи, суспільства і держави. Означене свідчить про необхідність дослідження сутності поняття «кібербезпека», впорядкування внутрішнього нормативно-правового поля, вирішення комплексу проблем, пов'язаних із розбудовою національної системи кібербезпеки.

Незважаючи на широкий інтерес до зазначеного безпекового напрямку, наукові дослідження досі є поодинокими й часто несистемними. Аналіз наукових джерел вказує на відсутність сталого поняття кібербезпеки.

Досліджуючи питання кібербезпеки, слід відзначити, що це поняття відносно нове. Воно з'явилося на початку 90-х років у Сполучених Штатах Америки і за майже два десятиріччя охопило всі країни світу. Не зважаючи на це, науковці і практики не мають єдиної думки щодо цього поняття.

Так, В.Н. Фурашев, Г.В. Новицький визначають кібербезпеку як стан здібності людини, суспільства і держави щодо запобігання та уникнення спрямованого, в першу чергу – несвідомого, негативного впливу (управління) інформації [1, с. 2].

На думку О.А.Баранова, кібербезпека – це такий стан захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через: неповноту, невчасність та невірність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації [3].

Шеломенцев В.П. під кібернетичною безпекою пропонує розуміти стан захищеності життєво важливих інтересів і громадянина, суспільства і держави від зовнішніх та внутрішніх загроз, пов'язаних з використанням ресурсів кіберпростору (іншими словами ресурсами інформаційно-телекомунікаційних систем), за якого в державі забезпечуються сталий розвиток інформаційного суспільства [4].

Кібербезпеку можна визначити також як стан захищеності кіберпростору держави в цілому або окремих об'єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і/або національним інтересам [5].

Впорядкування проблем кібербезпеки в межах нормативно-правового поля можна вважати лише частково успішними. Позитивним є той факт, що в 2016 році була прийнята Стратегія кібербезпеки України [6], яка визначає пріоритети та напрями забезпечення кібербезпеки України. До цього ж



моменту єдиним реальним документом кібербезпекового характеру була ратифікована Україною Конвенція про кіберзлочинність [7]. Однак вона, по-перше, присвячена доволі вузькому сегменту кіберзагроз (кіберзлочинам у сфері комп'ютерної інформації), а по-друге, по суті, є регіональним документом, який до того ж не сприймається значною кількістю геополітичних гравців [8].

У Стратегії кібербезпеки України кібербезпеку визначено як стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, що досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів [6].

Таким чином, поняття кібербезпека являє собою стан захищеності життєво важливих інтересів громадянина, суспільства і держави від зовнішніх та внутрішніх загроз, пов'язаних з використанням ресурсів інформаційно-телекомунікаційних систем, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз.

### **Література:**

1. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності // Інформація і право. – 2012. – № 2. – С. 162-169.
2. Новицький Г.В. Теоретико-правові основи забезпечення національної безпеки України / Г.В. Новицький. – К. : Інтертехнологія, 2008. – 496 с.
3. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека» //Правова інформатика. – 2014. - № 2(42). – 54-62 с
4. Шеломенцев В.П. Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 20112. - №2. – 299-309 с.
5. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с.
6. Конвенція про кіберзлочинність // Офіційний вісник України. – 2007. – № 65; 10 вересня. – 107 с.
7. Стратегія кібербезпеки України // [Електронний ресурс] – Режим доступу: <http://www.president.gov.ua/documents/962016-19836>
8. Черноног О.О. Напрями підвищення ефективності забезпечення кібербезпеки інформаційних технологій в системі публічного управління // Електронний ресурс] – Режим доступу: <http://mino.esrae.ru/178-1484>

### **Проблеми боротьби з кіберзлочинністю у сучасних умовах становлення України**

**Черняк Н.П.**

кандидат юридичних наук, доцент  
доцент кафедри кримінального процесу,  
Дніпропетровського державного університету внутрішніх справ

Сучасний світ практично неможливо уявити без нових інформаційних технологій, в основі яких лежить широке використання комп'ютерної техніки та новітніх засобів комунікацій. Сьогодні комп'ютери впроваджуються в різноманітні галузі людської діяльності. Усі найважливіші функції сучасного суспільства, так чи інакше, пов'язані з комп'ютерами, комп'ютерними мережами і комп'ютерною інформацією. Останнім часом в Україні значно зросла кількість Інтернет користувачів, адже підключення до глобальної мережі стало доступним та зручним. Слід зазначити, що персональний комп'ютер та мобільний телефон з підключенням до Інтернету сприймається як належне та необхідне. Популярність Інтернету не випадкова, адже він забезпечує цілодобовий доступ до величезної кількості інформації, швидку передачу даних, можливість проведення банківських, торгових, біржових операцій, переказ коштів і багато іншого. Інтернет – це чудовий засіб для зв'язку та спілкування. Для багатьох людей він став цілим світом, віртуальним світом. Як і в реальному світі, так і в віртуальному, де панує комп'ютерна інформація, трапляються злочини, кіберзлочини [1].

Злочинність в кіберпросторі - одна з найгостріших проблем, з якою зіткнулося міжнародне співтовариство протягом останніх десятиліть у зв'язку з розвитком інформаційних технологій.

Це, насамперед, зумовлено прискореним розвитком науки й технологій у сфері комп'ютеризації, а також постійним і стрімким розширенням сфери застосування комп'ютерної техніки.

Боротьба з кіберзлочинністю неможлива без глибокого розуміння і правових проблем регулювання інформаційних мереж. Проаналізувавши дану проблематику і думки багатьох вчених та науковців, виділимо деякі з них.

По-перше, відсутність механізмів контролю. Слід зазначити, що основна проблема боротьби зі злочинністю в мережі Інтернет полягає в транснаціональності самої мережі і у відсутності механізмів контролю, необхідних для правозастосування. Основною метою створення цієї мережі була стійкість до атак ззовні, і навряд чи хтось міг передбачити подальший масштаб її розвитку та її соціальну та економічну роль у майбутньому. Саме відсутність розроблених механізмів контролю мережі зсередини укупі з її доступністю і легкістю використання стало однією з глобальних проблем інформаційного співтовариства: децентралізована структура мережі і відсутність національних кордонів у кіберпросторі зумовили можливості для зростання злочинності та на роки відклали розробку механізмів соціального та правового контролю у сфері використання інформаційних мереж для вчинення злочинів [2]. Слід наголосити на тому, що в останні роки інформаційні мережі розвиваються занадто швидко, щоб існуючі механізми контролю встигали реагувати на нові проблеми.

По-друге, кількість користувачів мережі. Із збільшенням числа користувачів зростають, такі фактори ризику, а саме: збільшується залежність суспільства від інформаційних технологій, що, у свою чергу, обумовлює його вразливість до різного роду інформаційних зазіхань; збільшується можливість використання мережі для вчинення злочинів, а також росте потенційна можливість стати жертвою використання інформаційних технологій в злочинних цілях. При цьому вчинення злочину не вимагає великих зусиль і витрат - достатньо мати комп'ютер, програмне забезпечення та підключення до інформаційної мережі.

По-третє, автоматизація та швидкість використання. Комп'ютерні дані можуть бути передані з однієї точки світу в іншу за кілька секунд. Більше того, практично будь-яка передача даних у мережі зазвичай включає декілька країн, оскільки, коли інформація розбивається на частини і йде по найбільш зручним та доступним каналам. Контролювати передачу даних, з урахуванням їх обсягу та кількості користувачів, дуже важко, якщо не неможливо. Злочинець, потерпілий, сервер з необхідною інформацією можуть перебувати в різних країнах і на різних континентах, що вимагає співпраці правоохоронних органів декількох країн при розслідуванні злочину [2].

По-четверте, недостатня кількість державних експертів в області комп'ютерно-технічної експертизи та складнощі з введенням в правове поле досліджень фахівців комерційних організацій. Типовий термін проведення комп'ютерно-технічних експертиз становить від півроку і вище через високу завантаженість профільних державних установ.

На думку Ю. Омельченка українське законодавство у сфері захисту інформації вимагає дуже серйозного доопрацювання. «Потенційно існує ймовірність того, що кіберзлочинність буде виштовхуватися з Європи, то вона буде перебиратися в Україну. Та й уже цей процес відбувається», - зазначає експерт [3, с.10].

Однак, оскільки жодна держава не може захистити себе, вживаючи заходів тільки на національному рівні, для комплексної протидії кіберзлочинності необхідні:

- гармонізація кримінального законодавства про кіберзлочини на міжнародному рівні;
- розробка на міжнародному рівні та імплементація в національне законодавство процесуальних стандартів, що дозволяють ефективно розслідувати злочини в глобальних інформаційних мережах, отримувати, досліджувати і представляти електронні докази з урахуванням транскордонної проблеми;
- налагоджене співробітництво при розслідуванні кіберзлочинів органів досудового розслідування з оперативними підрозділами;
- механізм вирішення юрисдикційних питань у кіберпросторі.

Отже, ефективний контроль негативних явищ у кіберпросторі вимагає набагато більш інтенсивного міжнародного співробітництва, ніж існуючі заходи по боротьбі з будь-якими іншими формами транснаціональної злочинності. Міжнародне співробітництво є ключовим моментом у ліквідації правового вакууму, існуючого між розвитком інформаційних технологій та реагуванням на них законодавства. Процес вироблення заходів на міжнародному рівні, як показує досвід, сам по собі є комплексною проблемою. Однак, слід погодитись з думкою багатьох науковців, що це єдиний шлях забезпечити безпеку користувачів і держави від електронних посягань, а також ефективно розслідувати і переслідувати кіберзлочини.

#### **Література:**

1. Довбиш Н. Кіберзлочинність в Україні [Електронний ресурс]. – Режим доступу: <http://www.science-community.org/ru/node/16132>

2. Кіберзлочинність: проблеми боротьби і прогнози [Електронний ресурс]. – Режим доступу: [http://anticyber.com.ua/article\\_detail.php?id=140](http://anticyber.com.ua/article_detail.php?id=140)

3. Прохоренко В. Кіберзлочинність для України стає актуальним поняттям – НБУ. - // Економічна правда від 26 лютого, 2013 року.- 10 с.

### **Криптографічні методи захисту інформації: види та вимоги до них**

**Гладковський Е.О.**

слухач 2-го курсу магістратури факультету № 1  
Одеського державного університету внутрішніх справ

**Ісмайлов К.Ю.**

кандидат юридичних наук,  
завідувач кафедри кібербезпеки та інформаційного забезпечення  
Одеського державного університету внутрішніх справ

Збереження інформації в таємниці турбує людей ще з стародавніх часів, коли з появою писемності з'явилася і небезпека прочитання її небажаними особами. З розвитком новітніх комп'ютерних технологій та формування інформаційного суспільства, глобалізації всесвітньої мережі Інтернет, набуває ще більшого значення проблема захисту персональних даних фізичних, юридичних осіб, а також державних установ.

В даний час більшість засобів захисту інформації базується на використанні криптографічних шифрів і процедур шифрування-розшифрування. Ці процеси відбуваються в рамках певної криптосистеми, яка диктує правила і визначає параметри шифрування і дешифрування.

Вивченню методу криптографічного шифрування присвячені праці таких науковців: В.В. Ященко, І.Н. Войцехівська, О.В. Гомонай, О.В. Вербіцький, В.О. Хорошко, М.С. Шелест, Ю.Є. Яремчук та ін.

Перш ніж переходити до детального розгляду криптографічного захисту інформації, необхідно розглянути, що саме входить в це поняття, отже: криптографічний захист - це вид захисту, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо [1].

Доцент Адигеев М.Г., розглядає криптографію, як науку про способи перетворення інформації з метою її захисту від незаконних користувачів [2, с. 4].

Професор Войцехівська І.Н. надає найбільш розгорнуте поняття криптографія (від грец. *κρυπτός* - таємний, прихований та *γράφω* - пишу) - спеціальна історична дисципліна про шифрування (та розшифровування) записів за спец. технологіями з метою зробити їх зміст зрозумілим тільки для обмеженого кола осіб [3].

Проаналізувавши сучасні засоби криптографічного захисту інформації можна здійснити таку видову класифікацію:

- засоби, які реалізують криптографічні алгоритми перетворення інформації;
- засоби, системи та комплекси захисту від нав'язування неправдивої інформації, що використовують криптографічні алгоритми перетворення інформації;
- засоби, системи і комплекси, призначені для виготовлення та розподілу ключів для засобів криптографічного захисту інформації;
- системи та комплекси, що входять до складу комплексів захисту інформації від несанкціонованого доступу, та використовують криптографічні алгоритми перетворення інформації [4].

Отже, метою застосування криптографічних методів є захист інформаційної системи від цілеспрямованих руйнівних впливів (атак) з боку противника. Способи захисту істотно залежать від ситуації: по-перше від якого роду загрози необхідно захищатися; по-друге якими можливостями володіє противник.

Шифрування дозволяє захистити інформацію шляхом її перетворення в незрозумілий текст (шифр-текст) з можливістю подальшого розшифрування (дешифрування). Зашифровувати можна і звичайні тексти, і комп'ютерні файли. Так, шифрування поділяється на симетричне та асиметричне [3].

В симетричному шифруванні використовується один таємний ключ і для шифрування, і для дешифрування. В асиметричному шифруванні для шифрування використовується загальнодоступний ключ, а для дешифрування – інший, таємний, який генерується за допомогою генераторів псевдовипадкових чисел.

Асиметричне шифрування ще називають шифруванням із відкритим ключем. Недоліком симетричного шифрування є необхідність передачі ключа особі, якій адресований текст, що спричиняє загрозу його розкриття та дешифрування інформації зловмисниками.

Перевагою симетричного шифрування є його більша швидкість, ніж асиметричного, бо під час асиметричного шифрування використовують довші ключі, що збільшує час шифрування. Спосіб кодування тексту під час шифрування заснований на алгоритмі, а закодований текст можна дешифрувати лише за допомогою ключа. Для надсилання повідомлень різним адресатам може бути використаний один алгоритм із різними ключами.

Секретність визначається ключем, а не алгоритмом, оскільки більшість алгоритмів є відомими широкому колу фахівців. Унаслідок підвищення продуктивності комп'ютерної техніки зростає імовірність добирання ключів шляхом перебору комбінацій, тому доводиться використовувати дедалі довші ключі, а це збільшує час на шифрування, що в свою чергу негативно відображається на оперативності передачі даних.

Для сучасних криптографічних систем захисту інформації є загальні вимоги, а саме:

- зашифроване повідомлення повинно піддаватися читанню тільки при наявності ключа;
- кількість операцій, необхідних для визначення ключа шифрування за фрагментом шифрованого повідомлення і відповідного йому відкритого тексту, повинна бути не менша загальної кількості можливих ключів;
- кількість операцій, необхідних для розшифровування інформації шляхом перебору всіх можливих ключів, повинна мати строгу нижню оцінку і виходити за межі можливостей сучасних комп'ютерів (з урахуванням можливості використання мережних обчислень та прогнозу зростання потужності обчислювальних засобів);
- знання алгоритму шифрування не повинно впливати на надійність криптографічного захисту;
- незначна зміна ключа повинна приводити до істотної зміни вигляду зашифрованого повідомлення;
- структурні елементи алгоритму шифрування повинні бути незмінними;
- довжина шифрованого тексту повинна бути близькою довжині вихідного тексту;
- не повинно бути простих і легко встановлюваних залежностей між ключами, послідовно використовуваними в процесі шифрування;
- алгоритм повинен допускати як програмну, так і апаратну реалізацію, при цьому зміна довжини ключа не повинна вести до якісного погіршення алгоритму шифрування [5, с. 54].

Отже розглянувши поняття, види та характеристики криптографічного методу захисту інформації можна дійти висновків

- що доцільним є використання асиметричних методів шифрування даних. Хоча несиметрична криптографія є досить повільною у порівнянні зі швидкими і перевіреними часом і практикою симетричних алгоритмів, все ж таки використання несиметричної криптографії радикально спрощує процедуру розподілу ключів між учасниками інформаційних відносин.
- є ряд недоліків, які притаманні криптографічним системам, а саме: якщо інформація була криптографічно зашифрована, то у випадку збоїв у жорсткому диску, така інформація буде втрачена, оскільки практично не буде підлягати відновленню та розшифруванню
- для кращого захисту слід використовувати криптографічно стійку функцію зміни станів отже, можна зробити висновок, що в додатках, що пред'являють підвищені вимоги до безпеки конфіденційної інформації, не слід використовувати шифратори «з довільним доступом», так як принцип їх побудови суперечить даним вимогам
- для шифрування з метою передачі інформації в інформаційних мережах доцільно застосовувати асиметричні методи, а для шифрування з метою зберігання інформації – симетричні.

### **Література:**

1. Про Положення про порядок здійснення криптографічного захисту інформації в Україні: Указ Президента України від 22.05.1998 № 505/98. [Електронний ресурс]. – Режим доступу: <http://zakon3.rada.gov.ua/laws/show/505/98>.
2. Адигеев М.Г. Введение в криптографию. Часть 1. Основные понятия, задачи и методы криптографии. - Ростов-на-Дону: Ростовский гос. ун-т, 2002. - 35 с.
3. Войцехівська І.Н. Криптографія // Енциклопедія історії України: Т. 5: Кон - Кю / Редкол.: В.А. Смолій (голова) та ін. НАН України. Інститут історії України. - К.: В-во «Наукова думка», 2008. - 568 с. [Електронний ресурс]. - Режим доступу: <http://www.history.org.ua/?termin=Kriptografiya>.
4. Горобцов В.О. Криптографічний захист інформації. Юридический словарь / В. О. Горобцов // [zakony.com.ua](http://zakony.com.ua) від 11.02.2014 [Електронний ресурс]. – Режим доступу: <http://www.zakony.com.ua>.

5. Хорошко В.О., Азаров О.Д., Шелест М.С., Яремчук Ю.Є. Основи комп'ютерної стеганографії. Навчальний посібник. - Вінниця: ВДТУ, 2003. - 143 с.

### **Слідчий огляд в справах про комп'ютерні злочини**

**Білоусов А.С.**

кандидат юридичних наук, доцент,  
доцент кафедри кримінального процесу та криміналістики  
Інституту права ім. В. Сташиса Класичного приватного університету  
м. Запоріжжя

Слідчий огляд є, як правило, невідкладною слідчою дією, що полягає у безпосередньому сприйнятті, дослідженні, оцінці й фіксації слідчим обстановки місця події, слідів та об'єктів, які мають відношення для справи, їх ознак, властивостей, станів та взаємозв'язків, з метою з'ясування сутності події, що сталася, механізму злочину та його обставин, які мають значення для встановлення істини по справі. Слідчий огляд являє собою цілеспрямовану діяльність процесуальної особи, що має бути належним чином організована і спланована. Планування й організація слідчої діяльності виступають як тактичні прийоми [1, с.151].

Загальні та окремі тактичні вимоги щодо проведення слідчого огляду наповнюються істотними особливостями в разі огляду комп'ютерних об'єктів. Основна складність в разі розслідування злочинів, що вчинені з використанням комп'ютерних об'єктів, полягає в тому, що дії з огляду на властивості комп'ютерних об'єктів не охоплюються традиційним розумінням слідчого огляду. Відмінною особливістю огляду таких комп'ютерних об'єктів як системні блоки електронно-обчислювальних машин, комп'ютерні програми, інформація, що міститься на магнітних носіях тощо є те, що їх не можна оглянути і сприйняти безпосередньо всіма учасниками огляду, як це передбачено завданнями проведення слідчого огляду. Для сприйняття властивостей окремих комп'ютерних об'єктів потрібно здійснити доступ до них шляхом використання спеціальних технічних пристроїв з відповідним програмним забезпеченням. При цьому слідчий в присутності понятих не просто спостерігає за комп'ютерним об'єктом, а повинен сам або за допомогою спеціаліста ввести в автоматизовану систему певні команди, і лише після цього буде отримана інформація, яка й розкриє та зробить доступною для сприйняття властивість комп'ютерних об'єктів.

Підготовка до огляду місця події з наявними на ньому комп'ютерними об'єктами поділяється на два етапи. Перший етап охоплює підготовку слідчого до виїзду на місце події і розпочинається відразу після отримання ним інформації про подію з ознаками комп'ютерного злочину. Вже на цьому етапі варто звернутися по допомогу до спеціаліста в галузі комп'ютерної техніки, бажано, щоб цей же спеціаліст надавав би допомогу під час огляду. Не зайвою буде допомога і оперативних сил та засобів.

До виїзду на місце події треба уточнити місце знаходження засобів електронно-обчислювальної техніки, комп'ютерної інформації, що використовувалися під час вчинення злочину, або на яких збереглися сліди злочину і віддати розпорядження відповідним посадовим особам підприємства, установи щодо забезпечення охорони місця події, звернувши особливу увагу на охорону комп'ютерних об'єктів та вжиття можливих заходів щодо запобігання внесення змін в обстановку й знищення слідів. Визначивши місце, де знаходяться засоби комп'ютерної техніки та носії комп'ютерної інформації, варто встановити їх власника чи користувачів, уточнити місце їх перебування на час планованого проведення огляду і з'ясувати можливість процесуального вилучення в разі потреби комп'ютерної техніки та носіїв такої інформації. Також не зайвим буде з'ясувати питання щодо режиму роботи об'єкта, де буде проводитися слідча дія, кількісний та персональний склад осіб, допущених до операційної системи, а в разі встановлення на ділянках з обробки інформації режиму обмеженого доступу до неї, підібрати понятих та інших учасників слідчої дії з урахуванням цих обставин.

Після прибуття на місце події слідчий повинен визначитися з конкретним місцем проведення слідчої дії, обсягами роботи, яку належить виконати, достатністю задіяних для цього сил і засобів. Особливістю огляду за справами про комп'ютерні злочини є те, що відразу після прибуття до місця події слідчий повинен здійснити заходи щодо недопущення до засобів обчислювальної техніки, які є на місці події всіх осіб, що працюють на об'єкті. Щоправда, на тих об'єктах, де безперервна робота обчислювальної техніки забезпечує роботу всього технологічного процесу або його окремих складових, заборонити здійснення операцій по керуванню комп'ютерними процесами не можна. І тому, слідчий до початку огляду повинен зафіксувати технічні параметри комп'ютерної техніки на кожному робочому місці та попередити виконавців про невтручання в інформаційні процеси, якщо це не пов'язано з

технологічними питаннями виробництва. Для цього доцільно визначити, яка програма з керування технологічним процесом виконується на конкретній ЕОМ, вивчити зображення на екрані дисплею і за можливості детально описати його. З цією метою можна здійснити фотографування або відеозапис зображення. Останній спосіб фіксації надає реальну можливість дати найбільше правильну оцінку подіям, що відбуваються, на підставі детального аналізу інформації, яка виведена на екран монітора, супутньої світлової індикації та інших проявів, що мають значення для оцінки ситуації.

Пошук слідів на місці події варто розпочинати відразу не з такої її категорії, як інформаційні сліди, а з виявлення, фіксації та вилучення слідів рук, що залишилися на дверних ручках, шафах, шухлядах та інших місцях, де злочинці за звичне залишають сліди в разі вчинення „традиційних” злочинів. Після цього виявляють і вилучають сліди із технічних пристроїв – дисководів, вмикачів живлення, з корпусу комп’ютера, клавіш клавіатури та маніпуляторів, роз’ємів портів і мережних плат, а також з кнопок керування і поверхні друкуючих пристроїв. Це пов’язане з тим, що в подальшому з використанням цього обладнання буде здійснюватися доступ до інформаційної бази комп’ютерної мережі чи системи слідчим або спеціалістом за його дорученням і на цих об’єктах можуть бути знищені сліди злочинця, а натомість залишені сліди учасників слідчої дії.

З огляду на технічні особливості запуску, зупинення та функціонування комп’ютерної техніки не слід дозволяти підозрюваній особі під час проведення огляду торкатися до комп’ютера чи комп’ютерного обладнання. Проте, окремі науковці цілком слушно вказують, що в окремих випадках бажано, щоб підозрюваний був присутній при огляді його комп’ютера, оскільки саме він може надати найважливішу інформацію про особливості функціонування комп’ютерної системи: паролі, коди доступу; перелік інстальованих комп’ютерних програм; місце знаходження окремої інформації на машинному носії (окремих директорій, у тому числі прихованих). Однак його необхідно примати на відстані від комп’ютерного обладнання та джерела електричного струму, щоб запобігти можливим спробам зміни або знищення інформації – комп’ютерних доказів [2, с.186].

До джерел інформації, що має криміналістичне значення, можна віднести різноманітні предмети і документи, зокрема пристрої обчислювальної техніки, комп’ютерні носії інформації, окремі файли, що зберігаються в них та інші комп’ютерні об’єкти. Їх огляд здійснюють у тих випадках, якщо ці предмети, або електронні документи, що містяться в них, стосуються прямо або можуть стосуватися побічно події злочину. Наслідки протиправних дій можуть мати вираз в зміні певних характеристик даних параметрів та документів, що й утворює специфічні сліди злочину. Пошук і виявлення подібних слідів, а також дослідження документів, що зберігаються на нетрадиційних носіях, їх вилучення і огляд мають особливості, що змушують з особливою ретельністю підходити до провадження з огляду місця події.

До програми огляду комп’ютерних об’єктів в ході огляду місця події окрім звичайних дій, що пов’язані з оглядом, доцільно включати також окремі специфічні дії, до яких можна віднести:

- вивчення реальної конфігурації обчислювальної системи, топології внутрішніх комп’ютерних мереж і використаної схеми підключення до глобальної мережі;
- огляд кабельних ліній зв’язку з метою виявлення можливих каналів витоку інформації і несанкціонованих власником чи користувачем системи фізичних підключень;
- отримання даних щодо провайдера, через якого здійснено підключення до глобальної мережі;
- визначення технічних параметрів пристроїв і характеристик технічних каналів зв’язку, що входять в обчислювальний комплекс, та властивостей встановленого програмного забезпечення;
- дослідження системних журналів, аналіз можливих подій з несанкціонованої зміни системних паролів доступу або реєстрації нових користувачів;
- пошук програм, що здійснюють перехоплення вхідних даних і програм віддаленого керування обчислювальною системою;
- вивчення файлових систем для виявлення файлів з незвичними ознаками [3, с. 271-272].

При безпосередньому огляді засобів комп’ютерної техніки треба зафіксувати їх розташування в приміщенні, вказати в протоколі призначення технічного засобу, його назву, серійний номер, комплектацію, наявність і тип дисководів, мережних карт, рознімань тощо, наявність і тип підключених периферійних пристроїв, наявність з’єднання з локальною обчислювальною системою або мережами телекомунікацій і стан пристроїв. Також повинні бути зазначені в протоколі наявність і стан всіх позначок на технічному засобі, пломб, спеціальних знаків і наліпок, інвентарних номерів, контрольних маркерів, що нанесені на корпус і поверхню пристроїв комп’ютерів, наявність забруднень, механічних пошкоджень та їх локалізацію.

Оглядаючи комп’ютер як окремих об’єкт, варто знати, що дослідженню підлягає насамперед його інформаційна база та так звана „архітектура” комп’ютера. Адже кожен комп’ютер має відповідне математичне забезпечення програм, які на ньому виконуються. Розробники програмного забезпечення

заздалегідь передбачають можливість виникнення потреби встановлення дій, що були виконані оператором. Це дає змогу з точністю до секунди встановити час увімкнення комп'ютера в будь-який час доби, встановити факт користування поштовими програмами і методи доступу до них, визначити коло кореспондентів, з якими спілкувалися за допомогою цього комп'ютера, дізнатися зміст листування до того ж як текстових повідомлень, так графічного матеріалу та зображень.

Конкретне місце порушення правил експлуатації ЕОМ можна визначити під час огляду автоматизованих робочих місць користувачів комп'ютерної системи або мережі всіх підключених до них ЕОМ. Такий огляд треба проводити за участю спеціаліста, який допоможе з'ясувати дислокацію комп'ютера, робота на якому призвела до шкідливих наслідків в наслідок злочинного порушення правил його експлуатації. До того ж треба розрізнити місце порушення правил і місце настання шкідливих наслідків. Вони не завжди збігаються територіально, а особливо коли порушують правила експлуатації комп'ютерних мереж, в яких персональні ЕОМ інколи розташовані на достатньо значній відстані [4, с. 730-731].

Під час огляду варто звернути увагу не лише на наявність (відсутність) фізичних пошкоджень комп'ютерної техніки, але й на стан вікон, дверей та пристроїв для їх замикання. Сліди пошкоджень можуть бути виявлені за допомогою спеціальних засобів упізнання користувача персонального комп'ютера.

За результатами огляду місця події часто виникає потреба здійснення вилучення окремих слідів та інших об'єктів, що мають значення доказів для їх долучення до справи та можливого в подальшому поглибленого дослідження шляхом проведення слідчого огляду або призначення судово-експертних досліджень. На особливу увагу заслуговує вилучення тих об'єктів, які ми відносимо до комп'ютерних. Властивості цих об'єктів потребують їх врахування як при прийнятті рішення щодо потреби вилучення, так і у визначенні способу вилучення, відповідного процесуального оформлення факту та умов зберігання вилучених об'єктів.

#### **Література:**

1. Салтевський М.В. Криміналістика. Методика і тактика. – Харків: Консум, 2001. – 527 с.
2. Біленчук П.Д., Романюк Б. В., Цимбалюк В. С. та ін. Комп'ютерна злочинність. Навч. посібник. – К.: Атіка, 2002. – 240 с.
3. Осипенко А. Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: Монография. – М.: Норма, 2004. – 432 с.
4. Ищенко Е. П., Топорков А. А. Криминалистика: Учебник / Под ред. Е. П. Ищенко. – М.: Юридическая фирма "КОНТРАКТ": ИНФРА-М, 2005. – 748 с.

#### **Аналіз окремих вразливостей технології ss7 в мережах мобільного зв'язку**

**Власенко І.М.**

курсант групи Ф-4-13-4 факультету № 4  
Харківського національного університету внутрішніх справ

Вразливості мереж мобільного зв'язку на основі технології SS7 надають можливості зловмисникам проводити атаки, що можуть спричинити витік конфіденційних даних або порушення доступності абонентів і елементів мережі в інтересах третіх осіб.

Особливості цих атак полягають у застосуванні досить простого обладнання для їх проведення. Для цього достатньо створити вузол на базі звичайного комп'ютера під керуванням операційної системи сімейства Linux, з встановленим SDK для формування пакетів SS7. Відповідне програмне забезпечення є загальнодоступним в Інтернеті. Формування повідомлень сигналізації SS7 і відправка їх в мережу здійснюється засобами загальнодоступних стеків протоколу SS7.

Атакуючим може бути особа або група осіб, які спроможні побудувати вузол, що імітує роботу оператора мобільного зв'язку. Доступ до мережі може бути одержано, наприклад, з використанням інсайдерської діяльності фахівців, які обслуговують мережі мобільного зв'язку.

Технічному фахівцеві для здійснення деяких атак досить скористатися легітимним набором функцій існуючого обладнання мережі зв'язку. Залишається також і можливість проникнути в мережу оператора через зламані пристрої GGSN або Femtocell.

Цілями атакуючого можуть бути різні схеми шахрайства, отримання конфіденційної інформації про абонента, порушення доступності окремих абонентів або всієї мережі. Атаки можуть виконуватися на замовлення, в інтересах третіх осіб.

Зловмисник, який успішно здійснив одну атаку з використанням команд сигнальної мережі SS7 стосовно з'ясування місцезнаходження абонента, з легкістю може провести весь спектр інших атак за допомогою тих самих команд.

Основними наслідками атак, які можуть бути реалізовані у рамках описаного методу можуть бути розкриття ідентифікатора IMSI, визначення місця розташування абонента, порушення його доступності, перехоплення вхідних SMS-повідомлень, зміна профілю абонента в VLR, підслуховування вихідних дзвінків.

На основі вищевказаного можна зробити висновок, що для безпечного використання стільникового зв'язку необхідно доопрацювати прогалини в протоколі сигнальної мережі SS7. Крім того, потрібно вести постійні роботи з виявлення та недопущення проникнення в мережу стільникового зв'язку сторонніх осіб з метою здійснення несанкціонованих дій з інформацією абонентів.

### **Інформаційно-аналітичне забезпечення оперативного пошуку ознак злочинів, пов'язаних з торгівлею людьми**

**Мельнікова О.О.**

викладач кафедри  
кібербезпеки та інформаційного забезпечення  
Одеського державного університету внутрішніх справ

**Мишко В.В.**

кандидат юридичних наук  
доцент кафедри ОРД факультету № 1  
Одеського державного університету внутрішніх справ

З початку нового тисячоліття феномен торгівлі «живим товаром» набув значної гостроти та актуальності, суспільство вимагало більш рішучих дій у боротьбі з цією проблемою як на національному, так і на міжнародному рівнях.

Департамент боротьби зі злочинами, пов'язаними з торгівлею людьми (далі - ДБЗПТЛ), Національної поліції України є структурним підрозділом Національної поліції України, який функціонує у складі кримінальної поліції та відповідно до законодавства України забезпечує реалізацію державної політики у сфері протидії торгівлі людьми, запобігання вчиненню, виявлення, припинення та розкриття кримінальних правопорушень, пов'язаних з нелегальною міграцією, а також правопорушень у сфері суспільної моралі.

ДБЗПТЛ відповідно до покладених на нього завдань організовує та здійснює оперативно-розшукову діяльність, спрямовану на виявлення та припинення кримінальних правопорушень, пов'язаних з торгівлею людьми, нелегальною міграцією, а також правопорушень у сфері суспільної моралі, та комплексне використання джерел оперативної інформації, можливостей оперативних підрозділів та застосування оперативно-технічних засобів під час провадження в оперативно-розшукових справах. Відповідно до законодавства України користується базами (банками) даних Національної поліції України та МВС, а також інших державних органів, надає пропозиції щодо створення нових та вдосконалення діючих автоматизованих інформаційних систем; забезпечує своєчасне поповнення та належне використання оперативно-пошукових обліків.

У Департаменті боротьби зі злочинами, пов'язаними з торгівлею людьми, Національної поліції України за сприяння Міжнародної організації з міграції (МОМ) та фінансування Державного департаменту США запроваджені системи кримінального аналізу та аналізу ризиків, сумісні зі стандартами ЄС. Аналогічну систему вже було успішно запроваджено у Державній прикордонній службі України (ДПСУ), і представники ДПСУ входять до числа експертів, залучених до розробки систем кримінального аналізу та аналізу ризиків у Департаменті боротьби зі злочинами, пов'язаними з торгівлею людьми, Національної поліції України. Все це обумовлює необхідність дослідження інформаційно-аналітичного забезпечення діяльності оперативних підрозділів та надання рекомендацій щодо шляхів удосконалення інформаційно-аналітичної діяльності ДБЗПТЛ.

Питанням організаційно-аналітичного забезпечення приділялася увага в науковій літературі, зокрема С. Албулом, А. Іпакьяном, О. Воробйовим, Б. Заботіним, С. Тельшевським, В. Лукашевим, Н. Михайлюком, В. Іллічовим, В. Самойловим. Водночас у системі організаційно - аналітичного забезпечення оперативного пошуку ознак злочинів, пов'язаних з торгівлею людьми є ряд проблем, що позначаються на якості управління, шляхи до розв'язання яких – в удосконаленні організаційно-



аналітичного забезпечення підрозділів ДБЗПТЛ.

В сучасній теорії оперативно-розшукової діяльності до організації протидії злочинам відносять вивчення, аналіз та оцінку оперативної обстановки, інформаційно-аналітичне забезпечення, планування оперативно-розшукової діяльності, взаємодію в оперативно-розшуковій діяльності, фінансове забезпечення оперативно-розшукової діяльності, контроль та нагляд за оперативно-розшуковою діяльністю. У свою чергу, організація оперативно-розшукової діяльності оперативних підрозділів Національної поліції, зокрема щодо здійснення оперативного пошуку ознак злочинів, пов'язаних з торгівлею людьми, нерозривно пов'язана з інформацією, яка виступає і як предмет, і як знаряддя, і як результат цієї діяльності. Як слушно зазначають науковці, саме завдяки інформаційним процесам система здатна здійснювати доцільну взаємодію з навколишніми умовами, координувати та субординувати відносини власних компонентів, спрямовувати їх рух, рівно як і рух себе самої як цілого, до задалегідь запрограмованої мети [9, с. 43].

Термінологічно, у літературі використовуються такі поняття, як «інформаційно-аналітичного забезпечення», «інформаційно-аналітичної роботи». При цьому, автори наукових праць не дають розгорнутих визначення цих понять. У зв'язку з цим, досить часто у літературі поняття «інформаційно-аналітичного забезпечення» підмінює поняття «інформаційного забезпечення» та використовується у його значенні. За нашим переконанням, ці поняття не можна ототожнювати у зв'язку з тим, що вони є різними за своєю сутністю та співвідносяться між собою як загальне і часткове. Для розуміння сутності інформаційно-аналітичної роботи та інформаційно-аналітичного забезпечення необхідно звернутися до самих понять аналізу, аналітики. Так, у тлумачному словнику В.І. Даля під «аналітикою» розуміється «спосіб вирішення питання від дії або явища до причин»[2].

У свою чергу, С.І. Ожегов під «аналізом» визначав «метод наукового дослідження шляхом розгляду окремих сторін, властивостей, складових частин чого-небудь» [5, с. 231]. Інформаційне ж забезпечення є діяльністю, що гарантує створення інформаційної основи для такого аналізу. Таким чином, очевидно, що інформаційно-аналітичне забезпечення є поняттям більш ширшим та важливішим для управління складними соціальними системами [6, с. 112].

Інформаційно-аналітичне забезпечення – це сукупність технологій, методів збору та обробки інформації, що характеризує об'єкт управлінського впливу (соціальні, політичні, економічні та інші процеси), специфічних прийомів їхньої діагностики, аналізу та синтезу, а також оцінки наслідків прийняття різних варіантів політичних рішень. Систему інформаційного-аналітичного забезпечення управління можна визначити як взаємозалежну та відповідним чином сформовану сукупність організаційних, організаційно-правових, інформаційних, методичних, програмно-технологічних компонентів, що забезпечує необхідну якість прийнятих управлінських рішень за рахунок раціонального використання інформаційних ресурсів та інформаційних технологій. З поєднанням принципів проблемної орієнтації та програмно-цільової установки як відносно тематики інформаційного забезпечення, так і відносно вибіркової підготовки інформації та доведення її до керівників відповідно до їх місця в системі управління та основних функціональних обов'язків[8, с. 5].

Систему інформаційного-аналітичного забезпечення можна визначити як взаємозалежну та відповідним чином сформовану сукупність організаційних, організаційно-правових, інформаційних, методичних, програмно-технологічних компонентів, що забезпечує необхідну якість прийнятих управлінських рішень за рахунок раціонального використання інформаційних ресурсів та інформаційних технологій. З поєднанням принципів проблемної орієнтації та програмно-цільової установки як відносно тематики інформаційного забезпечення, так і відносно вибіркової підготовки інформації та доведення її до керівників відповідно до їх місця в системі управління та основних функціональних обов'язків. Управлінські структури як суб'єкти системи інформаційного-аналітичного забезпечення постійно взаємодіють із інформаційним середовищем, регулюють рух інформації, аналізують тенденції й на цій основі розробляють рекомендації для прийняття управлінських рішень, удосконалювання оптимального управлінського впливу для досягнення цілей керування. Відповідно, однією з головних цілей інформаційно-аналітичного забезпечення оперативного пошуку ознак злочинів, пов'язаних з торгівлею людьми є виявлення загальних властивостей і ознак цих злочинів, на підставі яких здійснюється прогнозування оперативно-тактичної ситуації, що дозволяє визначити найбільш оптимальні управлінські рішення.

Інформаційно-аналітичне забезпечення є важливою складовою організаційної діяльності, що формує стадії визначення проблем системи управління та їх аналіз; підготовки та прийняття управлінського рішення; контролю за його виконанням та оцінки ефективності [3, с. 61]. Вона є більш важливою та необхідною для управління великими та складними системами. Необхідно відмітити, що аналітична робота не може здійснюватися окремо від інформаційної [4, с. 96-97]. В процесі аналізу інформації постійно виникають нові обставини та необхідність додаткового отримання інформації.

Інформація є основою, фундаментом для аналітики. Саме тому, досліджуючи організаційні аспекти оперативного пошуку ознак злочинів, пов'язаних з торгівлею людьми, ми аналізуємо саме інформаційно-аналітичне забезпечення та його місце у цій діяльності.

Головною категорією інформаційно-аналітичного забезпечення є інформація, за відсутності якої неможливо правильно і цілеспрямовано реалізовувати управлінський процес. Чинний Закон України «Про інформацію» у ст. 1 визначає такою документальні або публічно оголошені відомості про події та явища, які відбуваються в суспільстві, державі й навколишньому природному середовищі [7]. В теорії оперативно-розшукової діяльності сформульовані різні підходи до визначення категорії оперативно-розшукової інформації. Зокрема, до неї відносять: будь-які відомості, що враховуються на різних стадіях управління; фактичну інформацію, а саме відомості, що характеризують оперативно-тактичну обстановку, психологічні риси підозрюваних злочинців, поточні профілактичні та оперативно-розшукові заходи, види і способи здійснення злочинів, прикмети злочинців, про обставини, що мають значення при плануванні й здійсненні оперативно-розшукових заходів та негласних слідчих (розшукових) дій, проведенні оперативно-аналітичної роботи, а також надання сприяння у кримінальному провадженні [1, с. 37-43]; сукупність первинних та вихідних даних про осіб, причетних до підготовки злочинів, стану оперативно-розшукових сил і засобів, а також умов, у яких відбувається діяльність поліції у боротьбі зі злочинністю; на законних підставах отримані оперативними підрозділами відомості із застосуванням гласних та негласних заходів, сил та засобів, що мають значення для встановлення обставин вчинення злочину і викриття винних осіб шляхом використання їх органами досудового розслідування; інформація, яка характеризує оперативну обстановку в певному районі чи на території всієї країни, і містить відомості, отримані в ході спеціальних заходів по боротьбі зі злочинністю.

Що стосується аналітичної інформації, то вона представляє собою відомості, отримані з перевірених, співвіднесених фактів, які викладені таким чином, щоб відповідати вирішенню конкретного завдання. Аналітична інформація повинна відповідати наступним якісним характеристикам: – цінність (корисність) – ступінь сприяння досягненню мети замовника інформації; – точність – припустимий рівень викривлення інформації; – достовірність – властивість інформації відображати реально існуючі об'єкти з необхідною точністю; – повнота – необхідний обсяг відомостей для прийняття виваженого та ефективного рішення; – оперативність – іншими словами, актуальність, відповідність інформації поточному моменту; – коректність – однозначність сприйняття інформації всіма споживачами. Аналітична інформація поділяється на первинну та на вивідну (вторинну). Під первинною аналітичною інформацією маються на увазі відомості про окремі події, кількість та якість певних предметів, дії політичних акторів тощо. Як правило дана комбінація різноманітних відомостей є слабо структурованою. Єдине, що їх об'єднує – це характеристика певного явища та мета – розв'язання якого-небудь завдання. Вивідна аналітична інформація представляє собою результат логічного аналізу та узагальнення первинних аналітичних даних з боку безпосередніх учасників подій або зовнішніх спостерігачів (аналітиків, консультантів тощо). Вона дозволяє приймати зважене рішення суб'єкту будь-якої діяльності, орієнтуватися у конкретних моментах ситуації та прогнозувати подальший розвиток подій.

Як зазначалося раніше, інформаційно-аналітичне забезпечення є важливим і необхідним елементом організації оперативного пошуку ознак злочинів, пов'язаних з торгівлею людьми. Значимість оптимально організованого інформаційно-аналітичного забезпечення полягає в тому, що воно сприяє прийняттю найбільш доцільних управлінських рішень на всіх рівнях, що є однією з головних умов підвищення ефективності діяльності оперативних підрозділів органів внутрішніх справ.

### **Література:**

1. Албул С.В. Критерії оцінювання інформації, здобутої штатними негласними працівниками // Бюлетень з обміну досвідом роботи МВС України: науково-практичне видання. – Київ: МВС України, 2010. – № 184 (4)/2010. – С. 37-43.
2. Даль В. И. Толковый словарь живого великорусского языка [ Текст ] : в 4 т. / [ вступ. ст. А. М. Бабкина ]. – М. : ГИС, 1955. – ( Набрано и напеч. со 2-го изд., 1880–1882 гг. ) Т. 1 : А – З. – LXXXVIII, – 669 с. – Тит. л. изд. 1980 г.
3. Інформаційно-аналітичне забезпечення оперативно-розшукової діяльності [ Текст ] : [ монографія ] / [ В. А. Буржинський, М. Г. Вербенський, В. С. Гуславський та ін. ]. – Луганськ : РВВ ЛДУВС, 2009. – 110 с.
4. Мякота Є.В. Інформаційно-аналітична робота як елемент забезпечення протидії відмиванню коштів / Є.В. Мякота // Теоретичні та практичні засади протидії злочинам у бюджетній сфері: зб.

матеріалів міжвід. семінар-наради та науково-практичного семінару. – К.: ДДСБЕЗ МВС України, 2013. – С. 96-97.

5. Ожегов С.И. Толковый словарь русского языка / С.И. Ожегов, Н. Ю. Шведова. – [ 4-е изд., доп. ]. – М. : Азбуковник, 1999. – 324 с.

6. Плішкін В.М. Теорія управління органами внутрішніх справ: Підручник / За ред. канд. юрид. наук Ю.Ф. Кравченка. – К.: Національна академія внутрішніх справ України, 1999. – 702 с.

7. Про інформацію [Електронний ресурс] : закон України від 02. 10. 1992 р. № 2657-ХІІ із змін., внес. згідно із Законами України та Рішеннями Конституційного Суду : за станом на 09. 05. 2011 р. № 2938-17. – Електрон. дан. (1 файл ). – Режим доступу : <http://zakon1.rada.gov.ua>. – Назва з екрана.

8. Телешун С. О. Інформаційно-аналітична діяльність в державному управлінні: навч.-метод. матеріали / С. О. Телешун, І. В. Рейтерович. – К. :НАДУ, 2013. – 36 с.

9. Яковец Е. Н. Основы информационно-аналитического обеспечения оперативно-розыскной деятельности: [учебное пособие ] : [Текст] / Е.Н. Яковец. – М. : Щит-М, 2009. – 266 с.

### **DDoS-атаки: їх вплив на безпеку інформації, способи захисту**

**Беляєва Є.Г.**

курсант 1-го курсу

факультету № 4 (кіберполіції)

Харківського національного університету внутрішніх справ

**Рвачов О.М.**

старший викладач кафедри кібербезпеки

факультету № 4 (кіберполіції)

Харківського національного університету внутрішніх справ

Проблема DDoS-атак в Україні не нова і постійно є актуальною у зв'язку з великою кількістю злочинів, пов'язаних з блокуванням інформації в Інтернеті. Реалізація такої атаки на сервера компанії призводить до збитків цієї компанії. В Україні дані діяння розглядають як кримінальний злочин, що веде до кримінальної відповідальності, виходячи зі ст. 361, 362 ККУ [1]. Як показує статистика, кількість, а також потужність DDoS-атак стрімко зростає. За даними KasperskyLabу 2015 році Україна увійшла в топ-15 країн за кількістю DDoS-атак [2].

Що ж таке DDoS-атака?

DDoS-атака або розподілена атака на відмову в обслуговуванні ((Distributed) Denial-of-serviceattack) – напад на комп'ютерну систему або мережевий вузол з наміром зробити комп'ютерні ресурси недоступними для користувачів, для яких комп'ютерна система була призначена [3].

Для чого потрібен DDoS?

Перша задача DDoS-атак – політика.

Друга задача DDoS – комерційна конкуренція: платіжні системи (Chronopay vs Assist, Paypal), інтернет-банкінг (Альфа-банк, ВТБ, Ощадбанк), інтернет-магазини (Rozetka, 3.5 тисячі магазинів на платформі InSales), хостинг-провайдери (MiroHost, Zenon), розважальні ресурси, засоби масової інформації.

Третє завдання – це помста.

Одним із найпоширеніших методів нападу є насичення атакованого комп'ютера або мережевого устаткування великою кількістю зовнішніх запитів (часто безглузвих або невірних сформульованих). Таким чином атаковане устаткування не може відповісти користувачам або відповідає настільки повільно, що стає фактично недоступним.

Відмова сервісу здійснюється:

– примусом атакованого обладнання до зупинки роботи програмного забезпечення/устаткування або витрат наявних ресурсів, внаслідок чого устаткування не може продовжувати роботу;

– заняттям комунікаційних каналів між користувачами і атакованим обладнанням, внаслідок чого якість повідомлення перестає відповідати встановленим вимогам [4].

Основні види DDoS-атак:

– ICMP-флуд (Smurf-атака);

– UDP-флуд;

– SYN-флуд;

– HTTP флуд;

- посилена відображена DDoS-атака;
- Slow HTTP Post;
- Slow HTTP headers;
- фальшиві Googlebots.

Крім основних видів існує ще безліч інших типів атак і часто здається, що можливості зловмисників безмежні – це твердження вірне, якщо нічого не робити. Для будь-якої компанії, що працює на просторах Інтернету, необхідно захищатися від DDoS-атак. Завжди потрібно пам'ятати, що атака може принести більше збитків, ніж вкладені фінансові кошти на її запобігання.

DDoS-атаки діляться на 3 типи:

1. Атаки на канал.
2. Атаки на рівні протоколів.
3. Атаки на рівні додатків (7 lvl) [5].

Жертвами DDoS-атак за останній рік стало безліч комерційних компаній, онлайн-сервіси яких критичні для бізнесу – серед них Інтернет-крамниці, ЗМІ та фінансові установи. Атаки типу DDoS набирають популярність і вже стали звичним явищем для інтернет-бізнесу.

В Україні існують проблеми ідентифікації комп'ютерних злочинів. У ККУ немає чіткого визначення, що ж таке DDoS-атака. Також ці злочини мають високу латентність, що заважає визначити реальну кількість злочинів, пов'язаних з блокуванням інформації.

Існує проблема пошуку і залучення до відповідальності злочинців цієї сфери, оскільки існує багато складнощів з юридичної та технічної точки зору. За статистикою в Єдиному державному реєстрі судових рішень за період з 2010 по жовтень 2016 рр. в Україні було винесено 1299 судових вироків щодо злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж, а також мереж електрозв'язку, з яких 95 вироків відносяться до блокування інформації, і з них винесених вироків 48 [6].

Пропонується кілька способів виявлення і протидії DDoS-атак:

1. Ввести логування дій користувача в Інтернеті і зберігати про це інформацію протягом 6 місяців.
2. Створити асоціацію служб кібербезпеки у всіх зацікавлених країнах, з метою спільного взаємодії щодо виявлення та запобігання DDoS-атак. Створити при цих центрах ГШР (групи швидкого реагування) з розширеними повноваженнями (вилучення обладнання при підозрілої активності та проведення затримання), які будуть оперативно виїжджати на місце злочину.
3. Створити лабораторії з вивчення DDoS-атак та протидії їм.
4. Необхідно розробити нові технології, які замінять VPN (віртуальні приватні мережі), так як при їх використанні вихідний і вхідний трафік складно піддається розшифровці.

Підсумовуючи сказане, приходимо до висновку, що захист від DDoS-атак має важливе значення.

Головною проблемою даного виду злочину є його тяжкодоведність, так як в нашому законодавстві немає чіткого визначення самого поняття DDoS-атак.

Для боротьби з даним видом злочину необхідно посилити підготовку фахівців, які зможуть чітко виявляти подібні атаки та протиправні дії осіб, які їх вчиняють.

#### **Література:**

1. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III, в редакції від 08.10.2016 // Законодавство України [Електронний ресурс] – Режим доступу: <http://zakon.rada.gov.ua/laws/show/2341-14>.
2. Украина вошла в ТОП-15 стран с наибольшим числом жертв DDoS-атак // Українська правда: економічна правда. – 7 червня 2015 [Електронний ресурс] – Режим доступу: <http://www.epravda.com.ua/rus/news/2015/06/7/545689/>.
3. DDOS-атака: определение и терминология [Електронний ресурс] – Режим доступу: <http://allta.com.ua/ddos-ataka-opredelenie-i-terminologiya>.
4. DoS-атака [Електронний ресурс] – Режим доступу: <http://nado.znate.ru/DoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0>.
5. DDoS як актуальна проблема безпеки для бізнесу // IT-українською [Електронний ресурс] – Режим доступу: <http://it-ua.info/news/2015/03/19/ddos-yak-aktualna-problema-bezpeki-dlya-bznesu.html>.
6. Єдиний державний реєстр судових рішень [Електронний ресурс] – Режим доступу: <http://www.reyestr.court.gov.ua>.

**Рижков Е.В.**

кандидат юридичних наук, доцент  
завідувач кафедри інформатики та інформаційних технологій  
Дніпропетровського державного університету внутрішніх справ

**Тітов О.О.**

курсант 4-го курсу  
факультету підготовки фахівців для органів досудового розслідування  
Дніпропетровського державного університету внутрішніх справ

Метою даної роботи є дослідження одного з варіантів пошуку інформації, яка становить оперативний інтерес для співробітників Національної поліції.

У зв'язку з тим, що підрозділи Національної поліції стикаються з проблемою скоєння злочинів особами, інформація про яких відсутня в облікових та інформаційно-пошукових системах, виникає необхідність у альтернативних джерелах інформації та способах її отримання. Якщо роздивлятися такі джерела, як бази даних різних установ, в тому числі банків, адресних служб, звідки інформацію можна отримати тільки після відповідного запиту, то це в певній мірі стримує оперативність роботи поліції. Загальновідомо, що інформацію можна отримати “за-зв'язками” або “по-знайомству” від службових осіб відповідних організацій, оминаючи тим самим офіційність звернення, але постає питання законності. Тому, альтернативою цього є цілком законний та швидкий спосіб отримання інформації відкритих джерелах мережі Інтернет.

До відкритих джерел відносяться: Соціальні мережі («Вконтакте»[1], «Однокласники»[2], «МойМир»[3], «Facebook» [4], «Instagram» [5], «Фотострана»[6]), телефонні довідники («nomer.org» [7]), мобільні додатки («Truecaller»[8] та ін.), державні реєстри, сервіси які потребують реєстрації та на яких потрібно вказувати достовірні персональні дані.

Для пошуку інформації, яка може становити оперативний інтерес, необхідно мати початкові дані. Маючи хоча б якусь початкову інформацію, можна починати пошук.

Кількість людей, зареєстрованих в соціальних мережах, дедалі зростає. Хтось має один акаунт, хтось двата більше. Зазвичай люди у своїх облікових записах зазначають особисті дані частково або повністю (прізвище, ім'я, по-батькові, дата народження, сімейний стан та інше), електронні адреси. Деякі вказують й номери телефонів. Також публікують фотографії та відео фотографії власні, своїх родичів та зв'язків.

Аби пошук був успішним, потрібно вишукувати логічний ланцюг. Для цього, можна взяти за приклад- пошук інформації, за даними державних реєстрів, соціальних мереж, інформаційних сервісів.

Першочерговим етапом є встановлення того, чи користується особа, яка нас цікавить, соціальними мережами.

Є особа, є прізвище, ім'я та по-батькові. Спочатку робиться пошук у соціальних мережах «Вконтакте» та «Однокласники». Люди частіше за все мають акаунти у соціальних мережах. Старі акаунти або нові, не має різниці. Головне що вони містять необхідну інформацію. А саме: коло родичів, друзів, знайомих, інших зв'язків та контактів; персональні анкетні дані- дату народження, місце проживання, сімейний стан тощо; інтереси особи, шкідливі звички, спосіб життя, ким є особа за професією; спільноти за колом інтересів. Також публікуються особисті фото, фото родичів та зв'язків. Зображення, які розміщують на сторінках соціальних мереж можна прив'язати до певної місцевості та конкретного місця на карті, за допомогою прив'язки за місцем знаходження[9, с. 35-36].

Постійний моніторинг сторінок соціальних мереж дозволяє спостерігати за змінами у житті тієї особи, інформацію про яку ми шукаємо.

На допомогу у знаходженні інформації приходять сервіси у вигляді так званих «Телефонних довідників», яскравим прикладом якого є сервіс «nomer.org». У цьому сервісі зазначається така інформація, як: прізвище, ім'я, по-батькові особи; день, місяць та рік народження; контактний номер стаціонарного телефону та місце реєстрації. Цей сервіс можна характеризувати як своєрідну базу даних, тільки з відкритим доступом для всіх користувачів інтернету.

Однак для найбільш ефективного пошуку інформації потрібна взаємодія з усіма соціальними мережами та сервісами [10].

Один із можливих алгоритмів пошуку може бути таким. Маючи попередню інформацію, мило через шукаємо дані про особу в кожній соціальній мережі або інформаційному сервісі. В багатьох випадках результатом цього етапу є інформація, яку вказала особа.

Наступним етапом пошуку є встановлення зв'язків особи. Шукаємо батьків, братів або сестер, дружину або чоловіка чи інших близьких родичів. Це дає розширення площини пошуку інформації та її уточнення. Також корисними можуть бути друзі, просто знайомі або товариші.

Коли зв'язки встановлені, проводиться аналіз цих осіб та здійснюється пошук інформації, яка цікавить, на їх сторінках або використовуються їх дані для пошуку інформації на інших інформаційних сервісах.

Важливе місце пошуку займають знайдені фотознімки та відео. Їх аналіз може дати певний масив інформації. Якщо їх проаналізувати, можна визначити осіб, які зображені на фото, а також місце, де зроблено ці фотознімки.

За можливості співставляємо отримані фото особи, яка нас цікавить, із спеціалізованими базами фото- та відеоінформації відомих інформаційних продуктів, наприклад, «АРГУС». Ця автоматизована інформаційна система обробляла масив фото та відео даних, через співставлення їх із потоковим відео зображень людей. Завдяки повній інтеграції системи «АРГУС» з автоматизованими обліками інформаційних баз даних користувач отримував вичерпну відповідь на запит відносно особи, яка підлягала ідентифікації [11].

Після цього за можливості користуємося інформаційно-аналітичними продуктами з метою пошуку додаткових зв'язків та отримання інших корисних висновків [12]. На завершальному етапі, як варіант, звертаємося до сервісу «nomer.org», за допомогою якого можна знайти можливе місце проживання або реєстрації осіб та контактний номер телефону.

Вибір алгоритму пошуку інформації – це абсолютно творчий процес, який базується на технічних навичках та аналітичних здібностях. Яскравим прикладом цього є позитивний досвід діяльності працівників відділу організаційно-аналітичної роботи та контролю Управління організаційно-аналітичного забезпечення та оперативного реагування Головного управління Національної поліції у Дніпропетровській області в рамках моніторингу відкритих джерел інформації, з метою профілактики та спеціальної превенції наркозлочинам, а також виявлення факторів, які сприяють їх вчиненню. Працівниками були встановлені конкретні Інтернет-ресурси (psylab.cc, bigbro.biz, 777rc.biz, Labrc.net та інші) та потенційне коло осіб, які займаються діяльністю, пов'язаною із продажем наркотичних засобів, психотропних речовин, їх аналогів та прекурсорів.

Вказаний спосіб пошуку інформації в мережі Інтернет є ефективним у зв'язці з пошуком оперативної інформації заобліковими та інформаційно-пошуковими системами, в тому числі ІПС. Так само, за відсутності необхідної інформації в облікових та інформаційно-пошукових системах, альтернативою є пошук даних саме у відкритих джерелах та сервісах мережі Інтернет. У будь-якому разі, він повинен бути врахований в процесі підготовки кадрів для нової кіберполіції України [13].

### **Література:**

1. Соціальна мережа «Вконтакте» [Електронний ресурс]. – Режим доступу: <https://vk.com>
2. Соціальна мережа «Одноклассники» [Електронний ресурс]. – Режим доступу: <https://ok.ru>
3. Соціальна мережа «МойМир» [Електронний ресурс]. – Режим доступу: <https://my.mail.ru>
4. Соціальна мережа «Facebook» [Електронний ресурс]. – Режим доступу: <https://www.facebook.com>
5. Соціальна мережа «Instagram» [Електронний ресурс]. – Режим доступу: <https://www.instagram.com>
6. Соціальна мережа «Фотострана» [Електронний ресурс]. – Режим доступу: <https://fotostrana.ru>
7. Телефонний довідник «nomer.org» [Електронний ресурс]. – Режим доступу: <http://nomerorg.com>
8. Мобільний додаток «Truecaller» [Електронний ресурс]. – Режим доступу: <https://www.truecaller.com>
9. Використання сучасних інформаційних технологій працівниками органів внутрішніх справ при проведенні негласних слідчих (розшукових) дій : навч. посіб. / Д.О. Максимус, О.О. Юхно. – Харків : НікаНова, 2013. – 102 с.
10. Шавиркін Б. В. Деякі особливості розслідування кіберзлочинів / Б.В. Шавиркін // Боротьба з інтернет-злочинністю : матеріали міжнар. наук.-практ. конф. (Донецьк, 12–13 черв. 2013 р.). – Донецьк : Донец. юрид. ін-т, 2013. – С. 124–128.
11. Гуславский В.С., Задорожный Ю.А., Розовский Б.Г. Информационно-аналитическое обеспечение раскрытия и расследования преступлений : Монография - Изд-во «Элтон – 2», 2008. – 136 с.
12. Рижков Е.В. Информационно-аналитическое обеспечение раскрытия серийных злодеяний как складовая оценка та анализу оперативной обстановки / Е.В. Рижков, М.Ю. Литвинов // Оперативная обстановка, її

аналіз та оцінка у сфері діяльності підрозділів карного розшуку ОВС України: Спеціальний випуск Вісника ЛДУВС ім. Е.О. Дідоренка, - 2011. – № 2, у двох частинах, частина 2. – С. 12-26.

13. Рижков Е.В. Підготовка кадрів для оперативних підрозділів по боротьбі з комп'ютерною злочинністю // Компьютерная преступность и кибертерроризм: Сборник научных статей / Под ред. Голубева В.А., Ахтырской Н.Н. – Запорожье: Центр исследования компьютерной преступности, 2004. – Вып.2. – С. 164 – 167; Рижков Е.В. Про вдосконалення боротьби зі злочинами в інформаційній сфері // Компьютерная преступность и кибертерроризм: Сборник научных статей / Под ред. Голубева В.А., Рыжкова Э.В. – Запорожье: Центр исследования компьютерной преступности, 2005. – Вып. 3. – С. 240 – 242; Рыжков Э.В. Кадровое обеспечение борьбы с компьютерной преступностью в Украине // Международное сотрудничество в борьбе с компьютерной преступностью: проблемы и пути их решения: Матеріали міжнародної науково-практичної конференції (18-19 травня 2006 р.). – Донецьк: ДЮІ ЛДУВС, 2007. – С. 276 – 279; Рижков Е.В. Консультативное обеспечение борьбы с компьютерной преступностью // матеріали регіонального науково-практичного семінару (м. Донецьк, 12 грудня 2008 року). – Донецьк: Донецький юридичний інститут ЛДУВС ім. Е.О. Дідоренка, 2009 – С. 100-101; Рижков Е.В. Науково-методичне та кадрове забезпечення підготовки кадрів по боротьбі з кіберзлочинністю / Е.В. Рижков // Протидія злочинності у сфері інтелектуальної власності та комп'ютерних технологій органами внутрішніх справ: стан, проблеми та шляхи вирішення : матеріали всеукраїнської науково-практичної конференції (Донецьк, 2 листопада 2010 року). / Донецький юрид. ін.-т ЛДУВС ім. Е.О. Дідоренка. – Донецьк: ДЮІ ЛДУВС, 2010. – С. 68-72; Рижков Е.В. Підготовка кадрів для оперативних підрозділів по боротьбі з комп'ютерною злочинністю // Протидія злочинам, які вчиняються з використанням комп'ютерних мереж [Текст] : тези доповідей Міжнародної науково-практичної конференції (м. Севастополь, 1-2 жовтня 2010 року) / Державний вищий навчальний заклад «Українська академія банківської справи Національного банку України». – Суми : ДВНЗ «УАБС НБУ», 2010. – С. 114-117; Рижков Е.В. Подготовка кадров по борьбе с киберпреступностью: проблемы и перспективы / Е.В. Рижков// Актуальні питання підготовки фахівців із розслідування кіберзлочинів : зб. матеріалів круглого столу (Київ, 25 листопада 2011 р.)/ К. : Наук.-вид. відділ НА СБ України, 2012. – 107-109; Рижков Е.В. Совершенствование подготовки кадров по борьбе с киберпреступностью / Е.В. Рижков // Протидія злочинності у сфері інтелектуальної власності та комп'ютерних технологій органами внутрішніх справ: стан, проблеми та шляхи вирішення : матеріали всеукраїнської науково-практичної конференції (Донецьк, 9 грудня 2011 року). / Донецький юрид. ін.-т МВС України. – Донецьк: ДЮІ МВС України, 2012. – С. 126-128; Рижков Е.В. Досвід підготовки кадрів для оперативних підрозділів по боротьбі з кіберзлочинністю в Донецькому юридичному інституті МВС України / Рижков Е.В. // Боротьба з інтернет-злочинністю : матеріали міжнар. наук.-практ. конф. (м. Донецьк, 12-13 червня 2013 р.). – Донецьк : ДЮІ МВС України, 2013. - С. 193-196.

#### СЕКЦІЯ 4

### ПІДГОТОВКА ПЕРСОНАЛУ ДЛЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ В УКРАЇНІ

#### Деякі питання системи фахової підготовки працівників кіберполіції у вищих навчальних закладах МВС України

**Пекарський С.П.**

кандидат юридичних наук  
доцент кафедри спеціальних дисциплін  
та адміністративної діяльності  
Донецького юридичного інституту МВС України

В умовах структурних та системних змін діалектики забезпечення правоохоронної функції у минулому році розпочався процес атестації працівників підрозділів Національної поліції [1], які безпосередньо протидіють злочинності. Також розпочато реформування підрозділів кримінальної поліції, органів досудового розслідування та підрозділів превентивної діяльності [2]. Предметом даного дослідження є система підготовки фахівців для підрозділів кіберполіції у вищих навчальних закладах МВС України.

Розглядаючи дане питання нам необхідно дати визначення кіберполіції. Отже кіберполіція – це структурний підрозділ Національної поліції України (у складі кримінальної поліції), що спеціалізується на попередженні, виявленні та розкритті кримінальних правопорушень, механізмів підготовки, вчинення або приховування яких, передбачає використання електронно-обчислювальних машин (комп'ютерів), телекомунікаційних та комп'ютерних інтернет-мереж і систем [3].

Виходячи з визначення слід вказати, що в умовах реформування правоохоронної системи України ми стали свідками перетворення колишньої моделі підрозділів боротьби з кіберзлочинністю у новітній орган правозахисного призначення, який за своїми технічними та професійними можливостями матиме змогу миттєвого реагування на кіберзагрози, а також, у відповідності до кращих європейських та світових стандартів проводитиме міжнародну співпрацю по знешкодженню транснаціональних злочинних угруповань у даній сфері. Своєю чергою Департамент кіберполіції Національної поліції України (у складі кримінальної поліції) є міжрегіональним територіальним органом Національної поліції України і відповідно до законодавства України забезпечує реалізацію державної політики у сфері протидії кіберзлочинності, здійснює інформаційно-аналітичне забезпечення керівництва Національної поліції України та органів державної влади про стан вирішення питань, віднесених до його компетенції [4].

На нашу думку провідну роль у процесі підготовки фахівців для підрозділів кіберполіції повинні відігравати вищі навчальні заклади зі специфічними умовами навчання [5] системи МВС України. Саме тому вважаємо, що навчальний план підготовки фахівців для підрозділів кіберполіції ступеня бакалавра за спеціальністю «Право» повинен мати термін навчання 4 роки та передбачати здобуття особою теоретичних знань, практичних умінь та навичок, достатніх для якісного виконання обов'язків з протидії злочинності в першу чергу за оперативно-розшуковою спеціалізацією кримінальної поліції. Освітньо-професійна програма в начальних закладах зі специфічними умовами навчання [5], які перебувають в сфері управління МВС, повинна передбачати опанування ряду специфічних дисциплін, вивчення яких є обов'язковим для подальшої професійної діяльності співробітника кіберполіції. Навчальний план для кіберполіції повинен включати загальноюридичні і спеціальні технічні дисципліни. У загальному розумінні майбутні кіберполіцейські повинні оволодіти знаннями, виробити уміння та навички щодо протидії:

- злочинам проти інформаційної безпеки;
- on-line шахрайству і фінансовим злочинам;
- протиправному контенту.

Тобто виявляти ознаки даних злочинних дій, осіб, які їх готують, вчинюють, надавати вірну юридичну кваліфікацію, документувати злочинну діяльність як гласно так і не гласно, здійснюючи комплекс оперативно-розшукових заходів [6] чи негласних слідчих (розшукових) дій [7, с. 246] за допомогою технічних навиків та умінь роботи з електронно-обчислювальними машинами (комп'ютерами), телекомунікаційними та комп'ютерними інтернет-мережами і системами.

Орієнтиром для розробки навчального плану для підготовки здобувачів за державним замовленням для підрозділів кіберполіції є «Типовий навчальний план підготовки здобувачів ступеня вищої освіти



бакалавра галузь знань «Право» (08) за спеціальністю «Право» (081) терміном на 4 роки», який затверджений Міністром внутрішніх справ України А.Б. Аваковим 25.06.2015 [8]. Структура плану містить нормативну частину, яка складається з: циклу дисциплін гуманітарної і соціально-економічної підготовки, циклу дисциплін природничо-наукової (фундаментальної) підготовки, циклу дисциплін професійної та практичної підготовки. Окрім того даний план дає можливість в розділі 2.2. «Дисципліни професійної та практичної підготовки за вибором курсанта (кіберполіція)» запланувати навчальні дисципліни, які відповідають вимогам фахової підготовки працівників підрозділів кіберполіції. Загальною умовою даного структурування навчальних дисциплін по семестрам є обов'язковість попереднього вивчення «Режиму секретності» кримінального права, як загальної так і особливої частин та кримінальне процесуальне право. Також попередньо необхідно вивчити загальну теорію оперативно-розшукової діяльності, зокрема пропонуємо: «Організаційно-правові засади діяльності підрозділів кримінальної поліції», 6 семестр, обсягом 3 кредити ECTS, загальним обсягом 90 годин, форма контролю - залік; «Оперативно-розшукова діяльність (загальна частина)», 5-6 семестр, обсягом 6 кредитів ECTS, загальним обсягом 180 годин, форма контролю - екзамен; «Оперативно-розшукова діяльність (особлива частина)», 7 семестр, обсягом 4 кредити ECTS, загальним обсягом 120 годин, форма контролю - екзамен; «Негласні слідчі (розшукові) дії + Модуль «Конфіденційне співробітництво», 7 семестр, обсягом 3 кр. ECTS, загальним обсягом 90 год., форма контролю - залік;

Дана пропозиція обумовлена тим, що майбутні працівники підрозділів кіберполіції при вивченні навчальних дисциплін за напрямом підготовки повинні оперувати теоретичними категоріями кримінального права, кримінального процесуального права та теорії оперативно-розшукової діяльності. Окрім того є нагальною необхідністю залучати до навчального процесу з технічних дисциплін не тільки викладачів вищого навчального закладу системи МВС України, але і фахівців ІСІТАР, банківської сфери та ІТ-структур. Своєю чергою викладання юридичних дисциплін та спеціальних технічних дисциплін вимагає від викладача не лише вербальний виклад теоретичного та практичного матеріалу, а творчий підхід викладача з використанням новітніх педагогічних методик та мультимедійних технологій з освоєння навчального матеріалу у спеціально обладнаних комп'ютерних класах.

Прикладом цього є планування та організація навчального процесу на курсах підготовки кіберполіцейських та курсах підвищення кваліфікації співробітників кіберполіції. Курси підготовки кіберполіцейських тривали чотири місяці. Своєю чергою курси підвищення кваліфікації розпочалися 04.10.2016 у м. Харкові у Національному університеті внутрішніх справ. Протягом двох тижнів слухачі повинні опанувати 98 навчальних годин технічних та загальних дисциплін [9].

Підводячи підсумок зазначаємо, що нами була розглянута система підготовки фахівців для підрозділів кіберполіції. Організація даної підготовки повинна відповідати вимогам Закону України «Про вищу освіту», Закону України «Про Національну поліцію», Закону України «Про оперативно-розшукову діяльність» іншим нормативно-правовим актам МОН та МВС України щодо організації освітнього процесу у вищих навчальних закладах системи МВС України.

#### **Література:**

1. Про Національну поліцію : Закон України від 02 липня 2015 р. № 580-VIII // Відомості Верховної Ради України. – 2015. – № 40-41. – с. 379.
3. Структура Національної поліції [Електронний ресурс] – Режим доступу: <http://www.npu.gov.ua/uk/publish/article/1795723>
4. У Харкові випустили перших кіберполіцейських [Електронний ресурс] – Режим доступу: <https://www.npu.gov.ua/uk/publish/article/1962519>
5. Департамент кіберполіції [Електронний ресурс] – Режим доступу: <https://www.npu.gov.ua/uk/publish/article/1816252>
6. Про вищу освіту : Закон України від 01 липня 2014 р. № 1556-VII // Відомості Верховної Ради України. – 2014. – № 37-38. – с. 2004.
7. Про оперативно-розшукову діяльність : Закон України від 18 лютого 1992 р. № 2135 (зі змінами та доповненнями) // Відомості Верховної Ради України. – 1992. – № 22. – с. 303
8. Кримінальний процесуальний кодекс України. Науково-практичний коментар / За заг. ред. проф. В.Г. Гончаренка, В.Т. Нора, М.С. Шумила. – К. : Юстініан, 2012. – с. 1224 .
9. Типовий навчальний план підготовки здобувачів ступеня вищої освіти бакалавра галузь знань «Право» (08) за спеціальністю «Право» (081): затверджений Міністром внутрішніх справ України А.Б. Аваковим 25.06.2015
10. У Харкові розпочались навчання для співробітників кіберполіції (фото) [Електронний ресурс] – Режим доступу: <https://www.npu.gov.ua/uk/publish/article/2015978>

**Санакосв Д.Б.**

кандидат юридичних наук, доцент  
доцент кафедри оперативно-розшукової діяльності та спеціальної техніки  
Дніпропетровського державного університету внутрішніх справ

Стрімкий розвиток кіберзлочинності потребує постійного удосконалення існуючих, та напрацювання нових заходів протидії, зокрема – здійснення контролю доступу до розповсюдження неправомірного web-контенту спецпідрозділами ДКП та його міжрегіональними підрозділами.

У цій статті предметом аналізу є питання фільтрації інформаційного наповнення web-сайтів, задачі якої обмежуються заборонаю доступу до певних сайтів та застосування схем, що його ускладнюють з метою: 1) убезпечення громадян від таких злочинів чи правопорушень від збитків, що завдаються їм постійним перебуванням шкідливої інформації у Інтернеті (зокрема, дитяча сексуальна експлуатація); 2) обмеження вільного використання певних висловів; 3) введення заборони на доступ до інформаційного наповнення політичного змісту; 4) захист економічних інтересів, що стосується переважно мультимедійного контенту, що розповсюджується без дозволу власників авторських прав із використанням різних прикладних програм, наприклад голосового зв'язку через IP-протокол (VOIP).

Там, де держава жорстко контролює контент звичайних ЗМІ, водяться й суворі обмеження, щодо законодавчої заборони розміщення у web-мережі певних відомостей, блокування доступу до окремих сайтів та контроль доступу користувачів. Країни з жорстким контролем розташовуються, переважно, у Східній та Центральній Азії, на Близькому Сході та Північній Африці [1]. Вказані держави виявляють найбільшу активність щодо обмеження доступу до інтерактивної інформації, проте у низці інших країн заборонено доступ до сайтів певного змісту, наприклад із дитячою порнографією чи web-сторінок зі шкідливим програмним забезпеченням. Принаймні, питання про введення заборон там розглядається, до того ж із використанням технологій, які застосовуються для обмеження свободи слова в Інтернеті [2, с. 207-212].

*1. Технологія фільтрації.* Для фільтрації web-контенту пропонуються два різних підходи. Перший – провайдер надає доступ до Інтернету лише користувачам, які, за діючим законодавством, повинні (або їм рекомендовано) застосовувати механізми фільтрації; другий – інфраструктура фільтрації встановлюється у пунктах стратегічного призначення, які слугують з'єднувальною ланкою між національними мережами та міжнародною магістральною мережею як різновид віртуального кордону. Другому підходу надають перевагу країни з уже розгорнутою телекомунікаційною мережею чи з існуючим державним наглядом та контролем, де від початку необхідність застосування фільтрації web-контенту так чи інакше була очевидною (наприклад, китайська система «Great Firewall» («Золотий щит»).

*1.1. Блокування за IP-адресою.* Метод передбачає введення заборони на доступ до певних IP-адрес, включених до списку заборонених. Це – найбільш проста та примітивна у використанні технологія. Вона не вимагає значних капіталовкладень у спеціалізоване обладнання (адже її функції обмежуються перевіркою заголовків TCP/IP) та практично не впливає на продуктивність мережі.

*1.2. Блокування за доменом.* Первинна форма методики блокування трансформувалась у метод блокування із використанням не IP-адреси, а імені домену як критерію фільтрації. Цей підхід підвищив вибірковість фільтрації, але не вплинув на законослухняні домени, що користуються послугами одного й того ж хостинг-провайдера та списками заборонених IP-адрес. Однією з країн, що надають перевагу саме цьому методу, є Німеччина, де прийнято закон [3], за яким передбачено можливість інтернет-провайдерів блокувати DNS-запити, що стосуються імен доменів, включених правоохоронними органами до спеціального списку, що постійно поновлюється із тим, щоб блокувати доступ до сайтів із дитячою порнографією у максимально стислі терміни після їх ідентифікації. Такі країни як Австралія, Великобританія та Норвегія, також застосовують блокування за DNS. У випадках, коли користувач запитує IP-адресу, віднесену до «чорного списку» імен доменів, DNS-сервер повертає адресу на статичну web-сторінку з попередженням про те, щоб сторона запиту звернула увагу на інформаційне наповнення сторінки, яка її цікавить [4]. Із технічної точки зору, уникнути такого блокування досить просто: достатньо лише змінити конфігурацію комп'ютера так, щоб він звертався до DNS-сервера іншої країни (наприклад, до OpenDNS) [5].

*1.3. Блокування за URL.* Більш ефективним методом блокування є перевірка повної адреси запитуваного ресурсу у мережі (URL) та надання доступу чи відмова у ньому на підставі більш складних правил. Це дозволяє блокувати доступ лише до певних частин web-сайту. З технічної точки зору такий метод фільтрації, як правило, здійснюється шляхом встановлення проксі-серверу, який може бути і

прозорим, і не прозорим, але обов'язковим для застосування. Проксі-сервер блокує всі спроби отримати web-контент, оминаючи його. Оскільки такий сервер стає єдиним джерелом web-контенту для всіх користувачів, можна легко створити правила, що контролюватимуть режим його роботи залежно від запитованого домену, сторінки, чи навіть параметрів інформації. Наприклад, можна блокувати інтерактивні запити, в яких містяться ключові слова з «чорного списку» та виконуються через Google або іншу пошукову систему, оскільки умови пошуку будуть відображатися як параметри «get» («Надіслати») в URL, що надає доступ до отриманих результатів. Ця технологія використовується окремими країнами для масивної фільтрації web-контенту, зокрема із застосуванням програм SmartFilter і Fortinet Fortiguard від компанії McAfee [6].

*1.4. Блокування за ключовими словами або пакетна фільтрація.* При її використанні блокується більший об'єм контенту, аніж це потрібно. Так, може блокуватися доступ до навчальних матеріалів із репродуктивної біології, адже інформаційне наповнення із цих тем зазвичай містить слова, що асоціюються із порнографією. Таку інформацію, як правило, використовують у поєднанні з «білими списками» доменів, що викликають довіру, де обмеження за ключовими словами не здійснюється. Проте цей метод потребує занадто багато ресурсів, через що аналіз інформаційного трафіку стає економічно та технічно недоцільним. Водночас, на ринку комп'ютерних технологій є значна кількість різноманітних комерційних рішень з кодування інформації для нейтралізації механізмів контролю, зокрема Tor і FreeNet, які здатні приховати певні дії користувача так, щоб доступною була лише інформація про з'єднання з вузлом, що належить цим мережам, проте конкретних відомостей про отриманий контент у контролюючих підрозділів не буде [2, с. 209].

*1.5. Зміна результатів пошуку.* Як варіант, замість (чи окрім) механізмів блокування доступу до інформації можна прописати команду видаляти протизаконний чи небажаний контент із результатів пошуку в Інтернеті. Як правило, такі відомості також фільтрують за допомогою деяких зазначених нами методів, а мета видалення такого контенту полягає у тому, щоб приховати сам факт існування будь-якої цензури.

*2. Прозорість та інформація кінцевого користувача.* Слід розрізняти не лише методи перевірки контенту, але й країни, які намагаються забезпечити прозорість механізмів фільтрації та контролю, які повідомляють користувачеві про те, що запитований ресурс є забороненим, або пропонують змінити критерії фільтрації, та країни, де маршрути запиту чи параметри фільтрації змінюються без пояснень.

Протилежний підхід спостерігається у таких країнах як Саудівська Аравія, де, незважаючи на застосування фільтрації до значного за обсягами контенту, користувачу, окрім повідомлення про причини блокування інформації, пропонуються механізми звернення до державних органів для перегляду правил заборон. У будь-якому випадку, повного «чорного списку» ресурсів, що підлягають фільтрації, не існує ані у відкритому, ані в обмеженому доступі для спецпідрозділів ДКП, через що систему часто зламують із конкретною метою, наприклад для фільтрації сексуальних знімків неповнолітніх, або для інших потреб, окрім прямої [2, с. 209].

Отже, за останні кілька років органи державної влади різних країн суттєво активізували діяльність, спрямовану на фільтрацію web-контенту. Ймовірно, найближчим часом ця тенденція зберігатиметься, незважаючи на те, що механізми фільтрації може обійти користувач, який має навіть мінімальні знання. Фільтрація контенту стала останнім часом однією з основних тем, що активно обговорюються особами та організаціями, які виступають за більш жорстке регулювання Інтернету, і правозахисними організаціями, які отримали підтримку, наприклад, Піратської партії Швеції, яка виступає за збереження Інтернету у його первинному стані. Саме тому вітчизняні спеціалізовані підрозділи по боротьбі з кіберзлочинністю та торгівлею людьми мають враховувати ці тенденції та напрацьовувати досвід зарубіжних країн з метою протидії цим злочинам, передусім поширенню дитячої порнографії мережею Інтернет.

### **Література:**

1. R.Deibert. Access Denied: The Practice and Policy of Global Internet Filtering: MIT Press, 2008: [Електронний ресурс]. – Режим доступу : <http://opennet.net/accessdenied>; Оновлений список країн, які вважаються «ворогами Інтернету» : [Електронний ресурс]. – Режим доступу : <http://www.rsf.org>
2. Санакоєв Д.Б. Протидія порнографії в Інтернет підрозділами з боротьби з кіберзлочинністю та торгівлею людьми / Д.Б. Санакоєв // Право і безпека. – 2011. – № 2 (39). – 207-212 с.
3. GesetzesbeschlussdesDeutschenBundestages: [Електронний ресурс]. – Режим доступу : [http://www.doerre.com/jugendschutz/20090619\\_br\\_sperrgesetz.pdf](http://www.doerre.com/jugendschutz/20090619_br_sperrgesetz.pdf)
4. Наприклад : [Електронний ресурс]. – Режим доступу : <http://kid.telenor.net/>
5. Наприклад : [Електронний ресурс]. – Режим доступу : <http://www.opendns.com>
6. Наприклад: [Електронний ресурс]. – Режим доступу : <http://www.bartec.kiev.ua/index.php/mcafee/188-mcafee-smartfilter>

**Соловйов О. Ю.**

викладачка кафедри фундаментальних наук  
Військової академії  
м. Одеса, Україна

**Казакова Н.Ф.**

доктор технічних наук, доцент,  
завідувач кафедри комп'ютерних та інформаційно-вимірювальних технологій  
Одеської державної академії технічного регулювання та якості

Інформаційна безпека держави сьогодні, як самостійний напрям сучасних технологій, без тієї перебільшення переживає своє друге народження. Особливість нинішнього етапу розвитку не тільки інформаційних, але й практично всіх технологій характеризується надзвичайно високим ступенем їх інтеграції до усіх сфер людської діяльності та зумовленої цією обставиною взаємозалежністю і потенційною вразливістю, техногенної небезпекою.

Метою забезпечення інформаційної безпеки держави є створення нормальних умов функціонування конкретного органу державного управління та їх сукупностей, а також проведення моніторингу стану інформаційної безпеки для розроблення оптимальної моделі функціонування системи забезпечення інформаційної безпеки [1, с. 2].

Відповідно, характерними рисами сьогодення виступають не тільки економічні і політичні проблеми, які переживає Україна, але й значне зростання деструктивного впливу кібернетичних злочинів на всі сфери людської діяльності. Завдяки транснаціональним, транскордонним можливостям, які надає віртуальний простір, створений внаслідок функціонування електронних комунікацій з використанням Інтернет та інших глобальних мереж передачі даних, злочинність в цій сфері набула міжнародних масштабів.

Кібернетична та інформаційна безпека у відповідності до [3, с.8] є одними з основних факторів при оцінці стану національної безпеки.

Боротьба з кіберзлочинністю вимагає комплексного підходу, що найбільш повно відображено в Рішенні РНБОУ від 27 січня 2016 року «Про Стратегію кібербезпеки України» [4, с. 3]. Учасниками цього процесу визначені Міністерство оборони України, ДССЗІ України (Держспецзв'язку), Служба безпеки України, Національна поліція України та інші.

З метою створення передумов для своєчасного реагування на сучасні виклики в сфері кібербезпеки та підґрунтя для наступного формування підрозділів із забезпечення кібербезпеки та кіберзахисту доцільною є організація державними органами виконавчої влади у своїх базових вищих навчальних закладах навчання з питань інформаційної безпеки, кібербезпеки та захисту інформації в кіберпросторі, що також є невід'ємною складовою національної програми співробітництва Україна – НАТО [5, с. 95]. У цьому сенсі логічним є впровадження нових уніфікованих курсів підвищення кваліфікації і введенням відповідних дисциплін з однаковим підходом до викладання матеріалу. Тобто програми навчання повинні бути сформовані за узгодженими єдиними стандартами за участю всіх зацікавлених держструктур (Служба безпеки України, Служба зовнішньої розвідки України, Держспецзв'язку, Національна поліція України, Міністерство оборони України та інші), але з урахуванням основних завдань, законодавчо покладених на них, для кожної програми [6, с. 7] та стандартів НАТО. Вищевикладене надасть змогу досягти системного, єдиного підходу у створенні належної гнучкої державної системи протидії кіберзлочинності по відношенню до критичної інформаційної інфраструктури, що є однією із найважливіших складових частин стійкої структури національної системи кібербезпеки [7, с. 12].

З метою забезпечення захисту державних інформаційних ресурсів повинні бути застосовані і контрзаходи. Серед таких контрзаходів найважливішим є навчання персоналу, який буде утворювати локальний підрозділ реагування на надзвичайні події у кіберпросторі в національній мережі реагування на комп'ютерні надзвичайні події [8, с. 4].

Очевидним в такому випадку є те, що при навчанні та підвищенні кваліфікації відповідних фахівців слід приділити особливу увагу вивченню наступних питань:

- вивчення теоретичних та практичних питань автоматизованої обробки інформації та основ побудови інформаційно-комунікаційних мереж;
- вивчення теоретичних та практичних питань захисту інформації, зокрема методів виявлення каналів витоку інформації та блокування загроз інформаційній безпеці;

- вивчення принципів класифікації автоматизованих систем і утворення стандартних функціональних профілів захищеності оброблюваної інформації від несанкціонованого доступу;
- вивчення світового досвіду протидії кіберзлочинності та характерних методів здійснення кібератак;
- вивчення англійської мови на рівні не нижче B2 (Upper-intermediate);
- вивчення законодавства України у сфері електронних комунікацій, захисту інформації, інформаційної та кібербезпеки, міжнародних нормативно-правових актів з цих питань, а також технічної літератури.

З метою отримання найбільш ефективних результатів необхідно залучати для проведення теоретичного та практичного навчання та наступної перевірки знань провідних фахівців, які мають практичний досвід у галузі кібербезпеки.

Означені вище заходи нададуть змогу досягти дотримання системного підходу у забезпеченні кібербезпеки в автоматизованих системах державного та військового управління, об'єктів критичної інформаційної інфраструктури [9, с. 11].

### **Література:**

1. Система забезпечення інформаційної безпеки [Електронний ресурс] / Портал : pidruchniki. — Режим доступу \www/ URL: [http://pidruchniki.com/12631113/politologiya/sistema\\_zabezpechennya\\_informatsiynoyi\\_bezpeki#36](http://pidruchniki.com/12631113/politologiya/sistema_zabezpechennya_informatsiynoyi_bezpeki#36). — Заголовок з екрану, доступ вільний, 18.07.2014.
2. Казакова, Н. Ф. Передумови щодо організації міграції даних як методу підвищення рівня їх безпеки [Текст] / Н. Ф. Казакова // Інформаційна безпека. — 2014. — № 4(16). — С. 115-120. — ISSN 2224-9613.
3. Концептуальні засади розвитку системи забезпечення національної безпеки України [Електронний ресурс] / Портал : Національний інститут стратегічних досліджень. — Режим доступу \www/ URL: <http://www.niss.gov.ua/articles/1873>. — Заголовок з екрану, доступ вільний, 05.10.2016.
4. Стратегія кібербезпеки України : Указ Президента України від 15 березня 2016 року №96/2016 [Електронний ресурс] / Портал : rada.gov.ua. — Режим доступу \www/ URL: <http://zakon5.rada.gov.ua/laws/show/96/2016>. — Заголовок з екрану, доступ вільний, 05.10.2016.
5. Річна національна програма співробітництва Україна – НАТО на 2016 рік : Указ Президента України від 12 лютого 2016 року №45/2016 [Електронний ресурс] / Портал : president.gov.ua. — Режим доступу \www/ URL: <http://www.president.gov.ua/documents/452016-19779>. — Заголовок з екрану, доступ вільний, 05.10.2016.
6. План заходів на 2016 рік з реалізації Стратегії кібербезпеки України : розпорядження КМ України від 24 червня 2016 № 440-р [Електронний ресурс] / Портал : rada.gov.ua. — Режим доступу \www/ URL: <http://zakon2.rada.gov.ua/laws/show/440-2016-%D1%80>. — Заголовок з екрану, доступ вільний, 05.10.2016.
7. Концепція розвитку сектору безпеки і оборони України : Указ Президента України від 14 березня 2016 року № 92/2016 [Електронний ресурс] / Портал : president.gov.ua. — Режим доступу \www/ URL: <http://www.president.gov.ua/documents/922016-19832>. — Заголовок з екрану, доступ вільний, 10.10.2016.
8. Типове положення про службу захисту інформації в автоматизованій системі: НД ТЗІ 1.4-001-2000. — [Чинний від 2000-12-15]. — К. : ДСТСЗІ СБ України, 2000. — 30с.
9. Стратегія національної безпеки України : Указ Президента України від 26 травня 2015 року №287/2015 [Електронний ресурс] / Портал : president.gov.ua. — Режим доступу \www/ URL: <http://www.president.gov.ua/documents/962016-19836>. — Заголовок з екрану, доступ вільний, 10.10.2016.

### **Боротьба зі шкідливим програмним забезпеченням в сучасному кіберсередовищі**

**Барган С.С.**

студент факультету права  
Донецького юридичного інституту МВС України

**Делія Ю.В.**

кандидат юридичних наук, доцент,  
доцент кафедри загально-правових дисциплін  
Донецького юридичного інституту МВС України

Зловмисне програмне забезпечення або шкідливі програми — це програмне забезпечення, яке перешкоджає роботі комп'ютера чи серверу, збирає конфіденційну інформацію або отримує доступ до приватних комп'ютерних систем. До такого програмного забезпечення відносяться віруси, хробаки,

троянські програми, руткіти, шпійонське програмне забезпечення, рекламне програмне забезпечення, фальшиві антивіруси.

Дослідженню даної тематики відводиться значна увага міжнародних організацій (ITU, ISO, IETF), державних установ у багатьох країнах світу, виробників засобів захисту, провайдерів, організацій, а також вчених, зокрема, П. Грегорі, К. Малін, В. Гавловський, В. Лукашева, А. Молдовяна, Ю. Монахова та інших.

Одним із основних чинників збільшення чисельності та розповсюдження шкідливого програмного забезпечення (далі - ШПЗ) є грошова вигода, при умовах, що ризики ведення такої підривної діяльності мінімальні, через недосконалість українського законодавства, неефективність контролювання та захисту кіберсередовища. Також ШПЗ використовується і з метою незаконного збору розвідувальних даних спецслужбами різних держав – програми надають можливість отримувати доступ до конфіденційної інформації, в тому числі й персональної. Останнім часом виявляються програми, які на протязі кількох років незаконно збирали різну інформацію з комп'ютерів урядових, дипломатичних, військових та наукових установ і організацій на території різних країн світу, які взагалі підривають державний суверенітет [1, с. 126].

Варто зазначити, що вплив ШПЗ спрямований не лише на конфіденційну інформацію або інформацію з обмеженим доступом, але і на комп'ютери звичайних користувачів. Дана ситуація пов'язана з тим чинником, що в основній масі випадків зараження відбувається автоматизованим шляхом, через розповсюдження програм-вірусів у електронних ресурсах масового користування: файлообмінники, соціальні мережі, порно сайти та інші.

Враховуючи стрімкий розвиток технологій та кібернетики у світі, необхідно розробити чіткий концептуальний підхід щодо протидії розповсюдженню ШПЗ, яке є однією із основних кіберзагроз не лише для держави, а й для типового користувача ЕОМ [3, с. 47].

Сьогодні, в теорії та практиці інформаційної безпеки склалися два принципово різних напрямки реалізації способів протидії шкідливим програмам: перша заснована на концепції структурно-незалежних механізмів захисту інформації, і передбачає незалежність інформаційних процесів і процесів протидії таким програмам, а друга - заснована на концепції структурно-залежних механізмів захисту інформації [4, с. 7].

Відповідно до першого напрямку, засоби протидії шкідливим програмам проектуються і розробляються незалежно один від одного, причому засоби протидії шкідливим програмам надаються до вже розробленого програмного забезпечення. Особливістю механізму протидії в цьому випадку є те, що функції виявлення шкідливих програм реалізуються шляхом періодичного контролю цілісності обчислювального середовища захищених інформаційних систем з метою реєстрації несанкціонованих змін, викликаних шкідливими програмами.

Згідно з другим напрямом реалізується дворівнева система ідентифікації впливів шкідливих програм: ідентифікація факту впливу і ідентифікація наслідків впливу, шляхом порівняння поточних результатів виконання функцій обробки інформації та функцій контролю, отриманих в динаміці функціонування ПЗ [2, с. 213-214].

При цьому безпека інформаційних систем та мереж повинна розглядатися не лише з точки зору технологій, а також враховувати такі елементи, як попередження ризиків, управління ризиками та підвищення поінформованості користувачів, оскільки передбачити небезпечні наслідки легше, ніж боротися з ними. Тому на рівні органів державної влади необхідно забезпечити:

- розроблення законодавчих вимог щодо організації процесу захисту від ШПЗ, а також посилення відповідальності за навмисне виробництво та розповсюдження ШПЗ;

- координацію взаємодії між державним реагуванням на інциденти інформаційної безпеки та командами реагування провайдерів та інших приватних установ;

- залучення до розроблення захисту мережі приватних установ, оскільки саме вони в основному і є власниками більшості комп'ютерних систем;

- організацію науково-практичних досліджень з питань розроблення та вдосконалення механізмів протидії розповсюдженню ШПЗ.

- офіційну класифікацію ШПЗ, що допоможе уніфікувати діяльність пов'язану з боротьбою з ним;

- обов'язкове впровадження захисних механізмів у свої продукти виробниками апаратного та програмного забезпечення;

- налаштування та технічну підтримку програмного забезпечення, призначеного для захисту інформації, його виробниками;

- встановлення засобів антивірусного та мережевого захисту, протидії СПАМу операторами (провайдерами) послуг зв'язку.

Також слід звернути увагу на комп'ютерну грамотність типових користувачів мережі та комп'ютерних систем, з метою її підвищення, шляхом впровадження спеціальних курсів з кібербезпеки у навчальних закладах та установах, які працюють у ІТ сфері, пропагування необхідності користування антивірусними програмами, запровадити систему заохочень для осіб, котрі знайдуть ШПЗ у мережі і нададуть інформацію у відповідні структури. Окрім цього, всім користувачам необхідно працювати під обліковим записом з обмеженими правами та захищеним паролем, перевіряти антивірусним програмним забезпеченням перед кожним використанням всі носії інформації; перевіряти антивірусом всі файли, отримані електронною поштою або в соціальних мережах, проводити резервне копіювання даних, що зберігаються на комп'ютері.

Отже, незважаючи на збільшення різноманітності шляхів проникнення шкідливих кодів та вірусів до комп'ютерних систем та мереж або мобільних засобів комунікацій, ефективної протидії шкідливому програмному забезпеченню до сих пір не створено. Тому на сьогоднішній день необхідно забезпечувати захист не лише від відомого ШПЗ, а й вміти блокувати нові, нині невідомі, канали загроз, з метою підвищення ступеня захищеності кіберсередовища від впливу ШПЗ на глобальному рівні шляхом координації зусиль органів державної влади, приватного сектору та типових користувачів комп'ютерних систем.

### **Література:**

1. Гавловський Д. До питання протидії використанню шкідливого програмного забезпечення / Д. Гавловський // Боротьба з організованою злочинністю і корупцією (теорія і практика), 2014. – № 1. – С. 125-130.
2. Киселев В. В. Противодействие вредоносным программам: способы и средства / В. В. Киселев, В. А. Ярош // Вестник Воронежского института МВД России, 2007. – № 2. – С. 213-218.
3. Копитін Ю. В. Аналіз ризиків впливу шкідливого програмного забезпечення на безпеку даних в сучасному кіберсередовищі / Ю. В. Копитін // Вост.-Европ. журн. передових технологій, – 2013. – № 2/2. – С. 45-51.
4. Лозинский Д.Н. Информационная безопасность. Проблема нового тысячелетия / Д.Н. Лозинский, Е.В. Плещач // Системы безопасности, 2002. – № 4(46). – С. 13

### **Використання тренінгових технологій у підготовці персоналу для боротьби з кіберзлочинністю**

**Доценко В.В.**

кандидат психологічних наук, доцент,  
доцент кафедри педагогіки та психології  
Харківського національного університету внутрішніх справ

Одним із негативних аспектів впровадження інформаційних технологій в економічну і соціальну сфери життєдіяльності людини є поява нового різновиду протиправної поведінки – злочинів у сфері використання комп'ютерних технологій. Для боротьби з такою специфічною формою злочинності необхідні належним чином підготовлені фахівці, які володіють спеціальними знаннями і здатні застосовувати їх для розкриття комп'ютерних злочинів.

Більшість авторів (К. Беяков, В. Бутузов, В. Голубев, Д. Дубов, С. Кльоцкін, В. Мілашев, М. Литвинов, В. Мохор, В. Орлов, В. Хахановський та інші) відзначають, що проблема підготовки персоналу для боротьби зі злочинами в галузі інформаційних технологій та кіберзлочинності вивчена недостатньо і потребує ґрунтовних досліджень. На нашу думку, правоохоронцям, які протидіють кіберзлочинності крім обов'язкової технічної підготовки, володіння навичками роботи з комп'ютером і загальним орієнтуванням в інформаційному просторі необхідна професійно-психологічна підготовка з використанням інтерактивних методів навчання. Одним з таких методів є соціально-психологічний тренінг, який дозволяє ефективно вирішувати завдання, пов'язані з розвитком навичок спілкування, міжособистісного сприйняття, управління власними психічними станами, самопізнанням, особистісним зростанням тощо.

Так, для правоохоронців діяльність яких пов'язана з профілактикою та розкриттям кіберзлочинів ми пропонуємо тренінг «Конструктивне спілкування». Метою даного тренінгу є розвиток у фахівців з організації інформаційної безпеки комунікативних знань і навичок, що допоможуть їм співпрацювати і взаємодіяти з різними верствами населення через засоби масової інформації і консультативні зустрічі з представниками громадськості; розширення уявлень щодо ефектів міжособистісного сприйняття і

способів маніпулювання в процесі спілкування; знайомство з ризиками пов'язаними з методами соціальної інженерії.

Протягом тренінгу учасники відпрацьовують наступні теми:

1. Навички міжособистісного спілкування як основа ефективної діяльності правоохоронця.
2. Оцінка достовірності інформації, що повідомляється невербальними засобами комунікації.
3. Основи конструктивного спілкування в конфлікті.
4. Маніпуляції у спілкуванні: розпізнавання, нейтралізація.
5. Соціальна інженерія в інформаційних технологіях.

Остання тема є особливо актуальною для фахівців з організації інформаційної безпеки оскільки розкриває соціальну інженерію, як метод маніпулювання людиною або групою людей з метою злову систем безпеки і викрадення важливої інформації. Цитуючи американського криптографа, письменника і фахівця з комп'ютерної безпеки Б. Шнайєра «Лише атаки дилетантів націлені на машини; атаки професіоналів націлені на людей» [1] учасники тренінгу знайомляться з механізмами навмисного впливу на психічні особливості людини (ціннісні орієнтації, норми поведінки, життєві цілі, рівень знань тощо) для отримання необхідної інформації. Наприклад, соціоінженер – це зловмисник (шахрай), який здійснює атаку на людину, яка є частиною системи «людина-комп'ютер» і руйнує найдосконаліші і дорогі системи захисту інформаційних технологій.

Представлений тренінг включає в себе традиційні методи: вправи, рольові ігри, дискусії, які застосовуються в рамках методів групового рішення проблем, моделювання ситуацій, психогімнастика, методи зворотного зв'язку і рефлексії тощо. Реалізація тренінгу розвитку навичок конструктивного спілкування фахівців з організації інформаційної безпеки в процесі професійної підготовки буде сприяти їх особистісному і професійному розвитку.

#### **Література:**

1. Шнайєр Б. Матеріал из Викицитатника/ Б. Шнайєр. [Електронний ресурс]. – Режим доступу : <https://ru.wikiquote.org>

#### **Питання встановлення закономірностей, що лежать в основі утворення криміналістично значущої інформації**

**Калюга К.В.**

кандидат юридичний наук,  
заступник завідувача кафедри кримінального процесу та криміналістики  
Інституту права ім. В. Сташиса Класичного приватного університету,  
докторант кафедри,  
майор міліції у відставці, журналіст

У криміналістиці детально розроблено питання, що належать до технологічної сторони огляду, і є лише окремі вказівки щодо необхідності встановлення суб'єктивного боку події, що розслідується. Гносеологічні ж основи проведення огляду не здобули необхідного наукового висвітлення. Якоюсь мірою це результат обмеженого тлумачення процесів пізнання на досудовому етапі розслідування.

Тут ми покажемо механізм встановлення закономірностей, що лежать в основі утворення криміналістично значущої інформації.

Розкрити механізм слідоутворення – значить пізнати процес взаємодії матеріальних об'єктів, вирішити ретроспективну задачу, тобто за відображеннями теперішнього змодельовати минулу подію. Основу ретроспективного моделювання складає закована в слідах-відображеннях інформація. Для її добування, тобто вміння читати сліди, необхідно знати код. Таким кодом є механізм слідоутворення й знати його необхідно як слідчому, так і іншим учасникам досудового розслідування.

Слідоутворення виникає в процесі контакту об'єктів, які приведені в дію їх власною енергією (причина руху) або повідомленою їм з інших джерел. Від того, як рухаються взаємодіючі об'єкти та які їхні властивості, залежить вид, форма та характер відображення. Відповідно, форма руху та властивості слідоутворюючого та слідоприймаючого об'єктів займають центральне місце в механізмі слідоутворення.

Характер змін залежить від природи та стану об'єктів, які вступали у взаємодію і від способу взаємодії. Якщо будь-яка зміна стану (механічна деформація, хімічна реакція, інше) характеризується двосторонньою залежністю від обох взаємодіючих тіл, то для відображення суттєвою є одностороння



залежність одного предмета від іншого (відображуваного). В гносеологічному аспекті ця залежність виходить з принципу первинності об'єкта та вторинності його відображення.

Таким чином, відображення – це такий взаємозв'язок між двома матеріальними процесами, при якому особливості першого процесу відтворюються в відповідних особливостях другого.

Так, уточнюючи дещо спрощену тезу Р. С. Белкіна про те, що стосовно процесу доказування зміни в матеріальному середовищі, як наслідок відображення в цьому середовищі події, є інформація про цю подію, у свою чергу зауважимо, що *зміни в матеріальному середовищі, що пов'язані зі злочинною подією* – це насамперед *відображення* й воно, як певна об'єктивна властивість (ознака), що закладена у відображуючому об'єкті внаслідок його взаємодії з іншими об'єктами може бути й не затребувана споживачем і не стати власне інформацією. Тому у своїх міркуваннях виходимо з того, що властивості цього відображуючого об'єкта є *фактом*, який існує *поза та незалежно* від свідомості людини. Факт, що лежить в основі інформації, у науковій літературі зветься "*базовим фактом*", або прихованою, *потенційною інформацією*. Він завжди подається на певному носії, яким може бути будь-яке матеріальне тіло. А міра зв'язку цих фактів із подією, до якої вони відносяться, яка знаходиться у прямій залежності від кількісного та якісного змісту цих змін, є змістом цієї потенційної інформації. Інформація виникає та існує в момент діалектичної взаємодії об'єктивних даних і суб'єктивних методів. Інформація не є статичним об'єктом – вона динамічно змінюється та існує тільки в момент взаємодії даних і методів. Увесь інший час вона перебуває в стані даних. Таким чином, інформація існує тільки в момент проходження інформаційного процесу.

У криміналістичному аспекті *слідосприймаючий* (відображуючий) об'єкт зміною свого зовнішнього вигляду (ознак) і внутрішнього стану (властивостей) відтворює ознаки й властивості *слідоутворюючого* (відображуваного) об'єкта, тобто є *носієм інформації*. Звідси сліди злочину, що інтерпретуються в широкому розумінні слова як різноманітні зміни в оточенні, що виникли внаслідок дій злочинця, будуть у нашому випадку носіями потенційної інформації, оскільки зміст змін і їхні зв'язки – сутність інформації. Вони (сліди) відображуються в конкретних матеріальних (знакових) формах і мають, як справедливо зауважив Д. О. Турчин, *знаковий зміст*.

Сприйняття інформації можна розглядати як процес, який має щонайменше два рівні. Перший – це сприйняття фізичних явищ, які виступають у ролі носіїв інформації. Другий – декодування сприйнятих сигналів і формування на цій основі концептуальної моделі, тобто певної "розумової (мисленої) картини" сприйнятого (власне інформації). Тобто інформація виступає у вигляді синтезу відомостей, що сприймаються, відповідним чином опрацьовуються свідомістю людини та видобуваються з її пам'яті.

Так, слідчий у процесі розслідування злочину, на рівні свідомості сприймає певний матеріальний слід (слідовий знак), переробляє (декодує) його на основі власних знань і досвіду в систему певних значень, тобто створює у свідомості образне поняття, або "образну картину" (інформаційну модель) події, явища. Тобто знак, як відображення потенційної інформації, набуває для суб'єкта форму образу-сигналу, стає для нього активною або власною інформацією, і розглядається як єдиний мисленевий процес.

Виходячи з викладеного, інформація в самому загальному вигляді є одним із видів (властивостей) здійснення процесу відображення, котрий, у свою чергу, є матеріальною базою можливості протікання інформаційних процесів.

Означене дозволяє виділити дві визначаючі й взаємодіючі сторони інформації: *зміст повідомлення*, який уже існує в зовнішньому оточенні, і *споживача* (суб'єкта), навіть потенційного. Кожному предмету притаманна певна кількість властивостей і, відповідно, такий самий потенціал інформації. У залежності від того, з ким або із чим цей предмет вступає у взаємодію, виявляється різна інформаційна цінність цього потенціалу, що залежить не від його кількості (притаманній предмету потенційній інформації), а від того, хто (або що) цією інформацією користується. Треба погодитися з думкою В. М. Тростникова про те, що "... только соединяясь с потребителем, сообщение "выделяет,, информацию, само по себе оно никакой информационной субстанции не содержит. Одно и то же сообщение одному потребителю может давать много информации, а другому мало (В. Г. Лукашевич)".

На нашу думку, неправомірно розглядати інформацію безвідносно до процесу сприймання повідомлення. Інформація потрібна споживачу в якості вихідного матеріалу для вироблювання алгоритму прийняття рішення та для успішної дії в процесі реалізації функцій, зазначених соціальною роллю, яку він обрав у суспільстві. Тому, поки дані не організовані (упорядковані) відповідним чином і не використовуються для якої-небудь мети, вони не є інформацією. Дані стають інформацією лише тоді, коли споживач усвідомлює їхнє змістовне значення. Тому вважаємо обґрунтованою тезу Ю. А. Шерковіна про те, що "информация – это то, что вносит изменение в наше сознание и чувства и переживается нами психически либо в виде выработки и принятия решения, либо в виде тех или иных

емоцій". Ми солідарні з твердженням Р. С. Белкіна та О. І. Вінберга про те, що "інформація завжди існує не взагалі, а для когось і як така вона виникає тільки з появою її користувача". Спираючись на цю методологічну посилку, можна дійти до *головного висновку* – в об'єктивній реальності не існує інформації взагалі. Її поява зумовлюється двома моментами: *відображенням* – об'єктивною передумовою появи будь-яких змін в оточуючому середовищі та *активної пізнавальної діяльності суб'єкта* – споживача інформації. В цьому аспекті можна погодитись з думкою М.І. Хлинцова про те, що інформація – це виділена нашою свідомістю, під час вирішення конкретної задачі, частина відомостей стосовно об'єкта дослідження, яка може сприяти вирішенню цієї задачі.

Ступінь відповідності інформації базовому факту (точність відображення факту в інформації) залежить від рівня знань суб'єкта пізнання і в цілому підпорядковується закономірностям, які описав свого часу відомий вітчизняний психолог С. Л. Рубінштейн: "Осознание вещи или явления как объекта связано с переходом от ощущения, служащего только сигналом для действия, для реакции, к восприятию как образу предмета (или явления)". Досягнення високого ступеню відповідності – складна задача. Це пояснюється багатьма причинами, по-перше, низкою об'єктивних умов, які можуть не дати можливість виявити сутність базового факту, і вона залишиться не повністю відображеною. По-друге, суб'єктивними якостями особи, що здійснює пізнання, - його компетентністю у певній галузі та мірою свободи поведінки з процедурними засобами, якими він оперує під час роботи з інформаційними сигналами.

Таким чином, цілком закономірно, розглядаючи злочин як інформаційну модель події, що відбулася, а процедуру розслідування злочину розглядати як інформаційний процес судово-слідчого пізнання, що включає у себе одержання, зберігання, передачу та використання інформації.

Одним із завдань, яке потрібно вирішити на місці події, є встановлення особи, що вчинила злочин. Установленню повинен підлягати симбіоз властивостей людини (як особистості, як учасника злочинної події і процесу її відображення, як носія найрізноманітнішої інформації, що має значення в кримінальному провадженні). В основу зазначеної діяльності покладено принцип відображення, тобто аксіома взаємодії злочинця з навколишнім середовищем. У процесі такої взаємодії відбувається відображення особистісних даних на матеріальних об'єктах місця події, і навпаки – матеріальні об'єкти місця події відбиваються на тілі й одязі злочинця.

Таким чином, досліджуючи слідоутворюючі й слідоприймаючі об'єкти на місці події, можна одержати імовірнісну інформацію про особу, що вчинила злочин.

### **Підготовка майбутніх інженерів-педагогів до забезпечення безпеки інформаційних систем в освітньому середовищі**

**Малихін В.А.**

асистент кафедри комп'ютерних технологій  
в управлінні та навчанні й інформатики  
Бердянського державного педагогічного університету

Потенційні можливості розвитку сучасного суспільства все більш визначаються рівнем та ефективністю інформаційно- комунікаційних систем. У Доктрині інформаційної безпеки України підкреслено, що за сучасних умов інформаційна складова набуває дедалі більшої ваги і стає однією із найважливіших елементів забезпечення національної безпеки. [1] Інформатизація освіти вимагає сучасних підходів до підготовки фахівця в цій галузі здатного забезпечити інформаційну безпеку систем, творчо вирішувати професійні завдання, пов'язані із захистом інформації. У зв'язку із цим набуває актуальності проблема формування у студентів педагогічних спеціальностей здатності до забезпечення безпеки інформаційних систем в освітньому середовищі, як складової їх професійної компетентності.

Питанню інформаційних систем в освітньому середовищі на сьогоднішній день приділено достатньо уваги. В контексті підготовки фахівців у вищих навчальних закладах, інформаційне освітнє середовище досліджувалося у працях Ю. Атаманчука, Є. Гільман, Н. Гладченкової, Д. Дзигуа. Зміст і організацію інформаційного середовища в підвищенні кваліфікації викладачів вищого навчального закладу досліджувала І. Задорожня.

Проблема освітнього середовища як об'єкта проектування та засобу набуття компетентностей фахівцями досліджувалася такими вітчизняними науковцями як В. Артеменко, М. Глибовець, Д. Гломозда, В. Гриценко, М. Жук, А. Карпа, А. Колгатин, О. Кузьмінська, Т. Мазурок, Г. Маклаков, Н. Морзе, О. Полотай, С. Титенко, Ю. Триус, В.Хоменко тощо.

Розробкою питань інформаційної безпеки займаються як вітчизняні та зарубіжні науковці, зокрема, О. Онищенко, В. Гавловський, В. Горовий, В. Цимбалюк, В. Петрик, М. Присяжнюк та ін.

Питання ж безпеки інформаційних систем в освітньому середовищі висвітленов наукових дослідженнях недостатньо.

Аналіз наукових та фахових джерел, тенденцій розвитку інформаційного суспільства, міжнародного досвіду щодо формування професійної компетентності в сфері безпеки інформаційних систем, практики інженерно-педагогічної освіти в Україні та нормативних документів дозволив обґрунтувати доцільність формування професійної компетентності в сфері безпеки інформаційних систем у студентів інженерно-педагогічних спеціальностей комп'ютерного профілю. Встановлено, що її формування має бути обов'язковою частиною професійної підготовки майбутніх інженерів педагогів, як в педагогічному, так і інженерному аспектах, що в кінцевому рахунку має бути спрямоване на вирішення завдань підготовки висококваліфікованих, конкурентоспроможних фахівців з чітким системним мисленням і стійким морально-ціннісним світоглядом, здатних передавати свій досвід і знання.

У теорії безпеки інформаційних систем існує декілька підходів до визначення сутності поняття «Безпека інформаційних систем». Зокрема, В.Пирогов сутність цього поняття визначає як захищеність інформації та інфраструктури що її утримає від випадкових або навмисних впливів природного або штучного характеру, які можуть порушити доступність, цілісність або конфіденційність інформації. [3] У зарубіжних джерелах поняття «Безпека інформаційних систем» розглядається: як захист інформації та інформаційних систем від несанкціонованого доступу, використання, розкриття, порушення, модифікації або знищення в цілях забезпечення конфіденційності, цілісності та доступності (НФСО, 2010) [4]; як забезпечення доступу до точної та повної інформації (цілісність) тільки авторизованим користувачам (конфіденційність) за запитом (доступність).» (ISACA, 2008) [5].

Згідно з даними європейських Узгоджених Критеріїв Оцінки Безпеки Інформаційних Технологій (Information Technology Security Evaluation Criteria, ITSEC), безпека інформаційної системи включає в себе наступні складові:

- 1) конфіденційність - інформацією в системі можуть оперувати лише користувачі з відповідними повноваженнями;
- 2) цілісність - наявна в системі інформація не має пошкоджень, є повною та достатньою;
- 3) доступність - при володінні відповідними правами користувач системи повинен безперешкодно отримати необхідну інформацію в стислі терміни.

Для того, щоб забезпечувати реалізацію наступних складових, сучасні інформаційні системи повинні включати в себе відповідні підсистеми, які реалізують прийняту політику безпеки. Політика безпеки в залежності від цілей і умов функціонування системи може визначати права доступу суб'єктів до ресурсів, регламентувати порядок аудиту дій користувачів в системі, захисту мережевих комунікацій, формулювати способи відновлення системи після випадкових збоїв і т.ін. Для реалізації прийнятої політики безпеки існують правові, організаційно-адміністративні та інженерно-технічні заходи захисту інформації.

Вже зараз Україна - високо інформатизована держава. Так, 2015 році регулярно Інтернетом користувалися понад 58% жителів країни. Смартфонами з сенсорними екранами (тачскрінами) вже володіють 26% жителів України. Про це свідчать дані дослідження Київського міжнародного інституту соціології (КМІС). При цьому зростання інформатизації сприяє зростанню і розвитку кіберзлочинності. За даними антивірусних компаній близько 43% користувачів Інтернету в Україні стикалися з кібератаками на їх системи.

Стан підготовки фахівців знаходиться на рівні який не відповідає тому рівню загроз інформаційної безпеки, який існує зараз в світі. Вітчизняні експерти сходяться на думці, що для поліпшення ситуації в цій сфері необхідно працювати відразу в декількох напрямках: реформувати програми підготовки у ВНЗ, створювати можливість отримання реального досвіду в даній сфері для початківців фахівців і шукати можливості утримання вже готових професіоналів в нашій країні.

Професійна компетентність у галузі безпеки інформаційних систем, на відміну від формування сукупності професійних компетентностей, передбачених освітньо-професійними програмами підготовки фахівців для системи професійно-технічної освіти, забезпечує новий вид професійних компетентностей – здатність аналізувати мережеві трафіки, роботу засобів виявлення вторгнення; вміння виявляти і знищувати комп'ютерні віруси; працювати з нормативними правовими актами; володіти та використовувати методи і засоби вияву загроз безпеки автоматизованими системами, забезпечення конфіденційності; формувати вимоги до захисту інформації; здійснення розрахунків та інструментального контролю за показниками технічного захисту інформації; володіння методами аналізу і формалізації інформаційних процесів об'єктів і зв'язків між ними та ін.

Згідно самооцінки студентами власного рівня знань із безпеки інформаційних систем яким вони володіють на сьогоднішній день – 4% респондентів визначили свій рівень як високий, 47% – як середній та 49% оцінив свій рівень як низький. Це, на нашу думку, свідчить про недостатню увагу до проблеми формування відповідних знань в галузі безпеки інформаційних систем студентів комп'ютерного профілю, що вимагає перегляду змісту підготовки інженерів – педагогів з урахуванням нагальних потреб суспільства з вирішення питань безпеки інформаційних систем.

Аналізуючи навчальні плани спеціальності «Професійне навчання. Комп'ютерні технології» А. Ашерова, В.Шеховцова [2] виділяють дві групи дисциплін: дисципліни, що формують системотехнічні знання і системно-аналітичні вміння, і дисципліни, що формують комп'ютерні знання і вміння. Навчальний процес з дисциплін, що формує системотехнічні знання і системно-аналітичні вміння, спрямований на формування знань видів систем, їх структури, організації функціонування, методів і засобів проектування цих систем і дослідження їх якості. Навчальний процес з комп'ютерних дисциплін спрямований на формування знань про засоби і методи розробки інформаційних і програмних продуктів, інформаційних технологій і комп'ютерних систем.

На наш погляд, підготовка інженерів-педагогів до забезпечення безпеки інформаційних систем повинна передбачати реалізацію наступних завдань: аналіз змісту комп'ютерних дисциплін та системотехнічних дисциплін з позицій їх можливостей у формуванні знань і вмінь із забезпечення безпеки інформаційних систем; розробка структурно-функціональної моделі підготовки майбутніх інженерів-педагогів комп'ютерного профілю до забезпечення безпеки інформаційних систем; виокремлення ключових понять і формування учбового матеріалу.

У подальшому наші зусилля будуть спрямовані на розробку концептуальної моделі з формування професійної компетентності інженера-педагога в галузі безпеки інформаційних систем, що безперечно знайде своє відображення і на процесі становлення професіоналізму майбутнього інженера-педагога в цілому.

#### **Література:**

1. Указ Президента України № 514/2009 від 08.07.2009 «Про Доктрину інформаційної безпеки України» – Режим доступу: <http://zakon4.rada.gov.ua/laws/show/2780-12>
2. Ашеров А. Т. Метод определения структуры и содержания учебного материала, формирующего проектную культуру будущих инженеров-педагогов в процессе системотехнической подготовки / А. Т. Ашеров, В. И. Шеховцова // Теорія і практика упр. соц. системами: філос., психологія, педагогіка, соціол.. - 2009. - № 1. - С. 45-54. - Библиогр.: 15 назв. – рус
3. Информационные системы и базы данных: организация и проектирование. Учебная литература для вузов / В. Ю. Пирогов. – БХВ-Петербург, 2009. - 528 с.
4. Committee on National Security Systems: National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, 26 April 2010 [Electronic Resource]. – Mode of access : URL : [http://www.ncsc.gov/publications/policy/docs/CNSSI\\_4009.pdf](http://www.ncsc.gov/publications/policy/docs/CNSSI_4009.pdf)
5. ISACA. (2008). Glossary of terms, 2008. [Electronic Resource]. – Mode of access : URL : <http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf>

#### **Формування системи ціннісних орієнтацій майбутніх правоохоронців**

**Кислинська Д.М.**

аспірант

Харківського національного університету внутрішніх справ

**Мілорадова Н.Е.**

кандидат психологічних наук, доцент,

професор кафедри педагогіки та психології

Харківського національного університету внутрішніх справ

В умовах системного реформування, модернізації та покращення ефективності професійної діяльності працівників правоохоронної системи суттєвого значення набуває професійна підготовка висококваліфікованого персоналу для органів і підрозділів поліції. Характерною ознакою будь-яких трансформацій, як у суспільстві так і у державних системах, є дестабілізація, руйнація системи цінностей, збільшення чинників професійного і соціального стресу, розбіжність між запитами і наявними умовами життєдіяльності тощо. Вчені наголошують, що чим більш динамічними є соціально-

економічні перетворення в суспільстві, тим сильніше змінюються ціннісні орієнтації, тим більш суперечливим і менш прогнозованим стає процес їх формування [1, с. 5].

Усі зазначені ознаки вимагають нового підходу до процесу професійного становлення особистості правоохоронця та обумовлюють нагальну потребу у формуванні системи ціннісних орієнтацій і переконань майбутніх правоохоронців, що буде визначальною мірою впливати на якість розв'язання ними професійних завдань і організацію стратегій власного життя.

Ціннісні орієнтації – це найважливіші елементи структури особистості, що формуються в процесі засвоєння соціального досвіду і проявляються у цілях, ідеалах, переконаннях, уявленнях особистості. Закріплена життєвим досвідом індивіда система ціннісних орієнтацій утворює змістовну сторону спрямованості особистості і є важливим фактором регуляції соціальних взаємовідносин людей і поведінки індивіда [4]. Як стверджує низка вчених (Ф.Є. Василюк, Д.О. Леонтьєв, С.Л. Рубінштейн, М.С. Яницький), система розвинених ціннісних орієнтацій – це ознака зрілості особистості, показник міри її соціальності і того, що можна очікувати від індивіда.

Теоретичний аналіз досліджень проблеми ціннісних орієнтацій особистості дозволив виокремити чотири їх основні функції:

1) визначення мети – цінності орієнтують людину серед об'єктів навколишнього світу, тобто не тільки регулюють, а й направляють дії [3]; визначають життєву перспективу, «вектор» розвитку особистості і виконують одночасно функції усвідомлення картини майбутнього, регулювання поведінки і визначення її мети [5];

2) мотивування – цінності є вибірковою системою спрямованості інтересів і потреб особистості, джерелом мотивів, тим самим, є найважливішим психологічним органом саморозвитку і особистісного зростання, визначаючи одночасно його напрямок і способи його здійснення [2];

3) оцінювання – викликають певне емоційне ставлення особистості до різних сторін і явищ життя на основі особистого досвіду, що виражається у визначенні значимості об'єкта, усвідомлення особистістю свого ставлення до суспільства, до самого себе, до навколишньої дійсності [1, с. 2];

4) саморегуляція активності людини – ціннісні орієнтації функціонують не лише як способи раціоналізації поведінки, а і як підсвідомі структури, що визначають спрямованість волі, уваги та інтелекту [2]. Ціннісні орієнтації забезпечують саморегуляцію діяльності людини, яка полягає в його здатності свідомо вирішувати поставлені перед ним завдання [2, с. 5].

Відповідно до цього можемо стверджувати, що усвідомлені цінності суб'єктивно готові до реалізації шляхом їх використання в соціально орієнтованій діяльності, що здійснюється за допомогою спеціальних умінь, прийомів і навичок. Оскільки ціннісні орієнтації формуються у процесі соціального розвитку індивіда, у ході виконання ним соціальних ролей, їх розвитку буде сприяти спрямований соціальний вплив таким інститутам як сім'я, школа, вищий навчальний заклад, а в умовах сьогодення не слід виключати і вагомий вплив, ЗМІ, реклами та інтернету.

Вищий навчальний заклад здійснює істотний вплив на формування ціннісних орієнтацій сучасної молоді виконуючи функцію трансляції цінностей і залучачи особистість до цінностей соціуму, культури, майбутньої професії допомагає їй присвоїти їх.

У майбутніх правоохоронців формування системи ціннісних орієнтацій відбувається поетапно і співвідноситься з періодами навчання у виші. Нами було виокремлено наступні етапи:

Перший етап – переоцінка цінностей і переконань, якими керувалась особистість до цього, співпадає з першим курсом навчання. Відбувається адаптація майбутніх правоохоронців до нових умов життя, навчання і несення служби. Курсанти виробляють навички та уміння необхідні для навчання у відомчому навчальному закладі зі статутним розпорядком дня, знайомляться з реаліями майбутньої професії.

Другий етап – інтеріоризація, присвоєння цінностей – другий курс навчання. Маючи певний досвід навчання у виші МВС другокурсники уже більш впевнено несуть службу, їх характер загартувався, поведінка стала більш відповідальною і самостійною.

Третій етап – особистісні зміни на основі нових ціннісних орієнтацій – третій курс навчання. Спостерігаються значні та якісні зміни у поглядах, переконаннях і поведінці третьоккурсників. Формується більшість професійно-важливих рис характеру, вмінь і навичок, розвивається впевненість у власних силах і можливостях, творчий пошук, організаторські здібності тощо.

Четвертий етап – діяльність щодо вибудовування власної ієрархії цінностей – четвертий курс навчання. Курсанти демонструють певний рівень соціальної зрілості особистості, стійкі мотиви і готовність до професійної діяльності.

Умовами формування ціннісних орієнтацій у майбутніх правоохоронців визначено наступні: розуміння причин і умов за яких об'єктивні цінності курсантів стають суб'єктивно значимими, стійкими життєвими орієнтирами особистості, її ціннісними орієнтаціями; підготовка науково-

педагогічного складу до процесу формування ціннісних орієнтацій у майбутніх правоохоронців; усвідомлення курсантами цінностей соціуму, культури і майбутньої професійної діяльності; соціально орієнтована діяльність курсантів.

Ефективними засобами організації процесу формування системи ціннісних орієнтацій майбутніх правоохоронців на етапі професійної підготовки виступають: надання інформації про майбутню професію, що дозволить сформувати адекватний тип мотивації до правоохоронної діяльності; активізація діяльності з використанням інтерактивних методів навчання; розвиток творчого підходу у вирішенні складних професійних завдань; засвоєння змісту основних видів професійної діяльності; отримання спеціальних знань, умінь та навичок; розвиток професійно-важливих якостей; включення механізмів особистісного розвитку: самопізнання, рефлексія; створення підтримуючого середовища.

Таким чином, саме пошук шляхів формування ціннісних орієнтацій майбутніх правоохоронців допоможе процесу становлення нової формації фахівців правоохоронців, здатних після здобуття освіти ефективно виконувати професійні завдання.

### **Література:**

1. Журавлева Н.А. Динамика ценностных ориентаций личности в условиях социально-экономических изменений: Дис... к-та психол. наук: 19.00.05. – социальная психология – М. : РАН, 2002. – 228 с.
2. Здравомыслов А.Г. Потребности, интересы, ценности / А.Г. Здравомыслов. – М. : Политиздат, 1986. – 222 с.
3. Наумова Н.Ф. Социологические и психологические аспекты целенаправленного поведения / Н.Ф. Наумова. – М.: Наука, 1996. – 200 с.
4. Психологічний тлумачний словник найсучасніших термінів / під керівництвом В. Б. Шапаря. – Х.: Прапор, 2009. – 672 с.
5. Яницкий М. С. Ценностные ориентации личности как динамическая система / М. С. Яницкий – Кемерово: Кузбассвузиздат, 2000. – 204 с.

### **Тренінг розвитку професійних настановлень у підготовці фахівців для боротьби з кіберзлочинністю**

**Мілорадова Н.Е.**

кандидат психологічних наук, доцент,  
професор кафедри педагогіки та психології Харківського національного  
університету внутрішніх справ

В умовах затяжної економічної, політичної кризи та активних соціальних змін, що призвели до певного послаблення соціально-психологічних механізмів регуляції суспільства, в тому числі і соціальної групи правоохоронців, знаходять своє поширення такі негативні явища як корупція, деформація правосвідомості, зокрема, професійної, домінування матеріальних цінностей над моральними, що у більшості випадків є неприпустимим. Все це неминуче відбивається на професійних настановленнях майбутніх правоохоронців, в результаті чого змінюються їх система цінностей та мотивація до роботи, поширюються вищезгадані негативні соціальні явища в їх колах.

На думку Г.Ю. Маклакова, найбільше значення у процесі підготовки фахівців у сфері інформаційної безпеки має формування високих моральних якостей. За його словами, ІТ-фахівець – це той самий «хакер», лише з високими морально-етичними життєвими нормами, який виконує суспільно корисні функції [2]. Тому, набуває актуальності розробка і впровадження в процес фахової підготовки правоохоронців інноваційних методів навчання спрямованих на формування їх системи ціннісних орієнтацій і настановлень.

Нами розроблений і впроваджений у процес фахової підготовки курсантів ХНУВС тренінг розвитку професійних настановлень майбутніх правоохоронців [1].

Зазначений тренінг спрямований на формування професійного образу «Я» та розвиток необхідних професійних когніцій, емоційних відношень і моделей поведінки. Це реалізується поетапним освоєнням системи навичок цілепокладання та кар'єрного планування, засвоєнням навичок емоційної саморегуляції, впевненої поведінки, формуванням вміння використовувати різні моделі поведінки та професійні ролі залежно від ситуації тощо.

Сфера змін – когнітивна, емоційна і поведінкова сфери особистості правоохоронців на етапі фахової підготовки.

Основними завданнями тренінгу є:

1. Розвиток навичок особистої ефективності у сфері самопрезентаційної поведінки майбутніх правоохоронців як представників публічної і комунікативної професії.
2. Мотивування учасників тренінгу до розвитку знань, умінь і навичок з метою підвищення ефективності професійної діяльності. Формування системи навичок цілепокладання та кар'єрного планування. Засвоєння поняття професійної ролі, усвідомлення того, що професія правоохоронця вимагає виконання певної професійної ролі, завдяки якій полегшується процес адаптації та досягнення професійного успіху.
3. Оволодіння способами регуляції емоційних станів, розвиток вольової сфери особистості, готовності до діяльності в екстремальних умовах професійної діяльності правоохоронця.
4. Навчання стратегіям ефективної поведінки в складних, конфліктних ситуаціях професійної діяльності.

Тренінг розвитку структурних компонентів професійних настановлень правоохоронців на етапі фахової підготовки створює основу спрямованого психологічного впливу на особистість, дозволяє формувати і розвивати новий рівень усвідомлення професійного середовища і себе в ньому, певні настановлення, ціннісні орієнтації, емоційне відношення та виявляти і змінювати поведінкові стереотипи, деструктивні форми поведінки тощо.

#### Література:

1. Мілорадова Н.Е. Тренінг розвитку професійних настановлень майбутніх правоохоронців / Н.Е. Мілорадова, Е.В. Шеховцова, О.І. Федоренко, В.В. Доценко, : навчально-методичний посібник – Харків: Харківський національний університет внутрішніх справ, 2015. – 120 с.
2. Орлов О.В. Державне управління підготовкою фахівців у сфері кібербезпеки / О.В. Орлов // Державне будівництво [Електронний ресурс]. – Режим доступу : <http://kbuara.kharkov.ua>.

#### Особливості підготовки фахівців у сфері публічного управління

**Муляр Т.С.**

кандидат економічних наук, доцент,  
доцент кафедри менеджменту  
організацій і адміністрування ім. М. П. Поліщука  
Житомирського національного агроєкологічного університету

Зміни є невід'ємною складовою розвитку будь-якої організації, а також всіх сфер суспільного життя особливо в умовах сучасного динамічного та мінливого середовища. Вони викликають заміну традиційних механізмів управління на ринкові: “наказувати і контролювати” на “мотивувати та отримувати результат”. В умовах сьогодення процеси змін потребують застосування нових підходів до управління: заміни традиційних способів управління, що базувалися на застосуванні чітких бюрократичних процедур, на такі, що зорієнтовані на надання якісних публічних послуг. Запровадження ринкового стилю управління, децентралізація, зосередження уваги на результатах роботи, а не на процедурах вплинули на появу нової форми управління у державному секторі.

Так, модель публічного адміністрування (“бюрократична модель”) трансформувалася у модель публічного управління (“ринкова модель”). Її поява була спричинена потребою підвищення продуктивності роботи державних установ. Підвищити дієвість управління можна шляхом підвищення ефективності використання людських ресурсів. У центрі уваги перебуває людина [1]. А тому, діяльність публічного управління має бути спрямована на надання якісних публічних послуг, а не на виконання робіт згідно з інструкціями та правилами.

Термін “публічне управління” (англ. *public management*), вперше використаний англійським державним службовцем Десмондом Кілінгом у 1972 р. – “Публічне управління – це пошук у найкращий спосіб використання ресурсів задля досягнення пріоритетних цілей державної політики” [2, с. 15].

Основне завдання менеджера у публічній чи у приватній сфері – мінімальними витратами ресурсів, часу і зусиль досягнути ефективності діяльності. Перед публічним управлінцем стоїть інше завдання – раціонально використати наявну інфраструктуру для надання публічних благ та задоволення суспільного інтересу. Ця відмінність і спричиняє особливість підготовки фахівців у сфері публічного управління.

Таким чином, публічне управління суттєво відрізняється від менеджменту за своєю місією і цілями. Менеджмент орієнтується на задоволення людських потреб з метою отримання прибутку. Публічне управління орієнтується на надання послуг суспільству при раціональному використанні ресурсів в процесі здійснення державної політики.

В публічному управлінні має забезпечуватись реалізація принципів верховенства права і законності, контроль з боку суспільства за діями державних органів, органів місцевого самоврядування, їх посадових службових осіб.

В умовах сьогодення професіоналізм публічних службовців стає запорукою його ефективності. А тому, підготовка майбутніх фахівців для органів публічної влади та місцевого самоврядування виходить із цілей і завдань, які стоять перед системою управлінських органів, і враховує основні напрямки і практичний досвід адміністративних реформ, які було здійснено протягом останнього десятиліття у багатьох країнах світу.

З метою формування дієвого кадрового потенціалу для регіональних органів влади в Житомирському національному агроекологічному університеті організована система підготовки кадрів для органів публічного управління. Вона відповідає вимогам, зокрема: суспільно-політичним, соціально-економічним, правовим, екологічним, ментальним.

До основних видів професійної діяльності публічних управлінців можна віднести як організаційно-розпорядчу діяльність, так і інформаційно-методичну, комунікативну, проектну та допоміжно-технологічну, тобто суто виконавську діяльність у будь-яких організаціях, що функціонують в публічному секторі.

Головне завдання навчального закладу – забезпечити рівень теоретичної підготовки випускників, що вступатимуть на публічну службу відповідно до вимог публічних органів до рівня його практичної підготовки. Це зумовлює забезпечити комплексний підхід в реалізації освітнього процесу, підвищенню його якості й орієнтованості на пріоритети практичного застосування одержаних знань.

Отже, підготовка кадрів у сфері публічного управління виходять з усвідомлення нової ролі держави та реалій сьогодення.

#### **Література:**

1. *Mary P. Follett. Creating Democracy, Transforming Management*, Tonn, Joan C., New Haven: Yale University Press, 2003. 366 p.
2. *Keeling D. Management in Government* / D. Keeling (1972), London: Allen & Unwin.
3. Енциклопедичний словник з державного управління / уклад.: Ю. П. Сурмін, В. Д. Бакуменко, А. М. Михненко та ін.; за ред. Ю. В. Ковбасюка, В. П. Трошинського, Ю. П. Сурміна. - К. : НАДУ, 2010. – 820с.

#### **Особливості підготовки фахівців для підрозділів боротьби з кіберзлочинністю**

**Черновол В.С.**

курсант факультету № 4

Харківського національного університету внутрішніх справ

**Онищенко Ю.М.**

кандидат наук з державного управління,

доцент кафедри кібербезпеки факультету № 4

Харківського національного університету внутрішніх справ

Стрімкий розвиток інформаційних технологій досить сильно трансформує світ. Разом з тим відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок досліджень, ідей та інновацій, стимулює відповідальну та ефективну роботу влади, але і створює загрози для безпеки держави, суспільства та окремих користувачів. Отже, питання забезпечення належної кібербезпеки наразі є відкритим.

Згідно Конвенції про кіберзлочинність, ратифікованої Законом України від 7 вересня 2005 року № 2824-IV першочерговим заходом для захисту суспільства від кіберзлочинності є створення відповідного законодавства і налагодження міжнародного співробітництва в даній галузі [1].

На основі Конвенції був виданий Указ Президента України від 26 травня 2015 року № 287 «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»», яким затверджено Стратегію кібербезпеки України.



Відповідно до Розділу 3 Стратегії кібербезпеки України на Національну поліцію України, у сфері забезпечення кібербезпеки, в установленому порядку, покладаються наступні завдання:

- забезпечення захисту прав і свобод людини та громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі;
- запобігання, виявлення, припинення та розкриття кіберзлочинів;
- підвищення поінформованості громадян про безпеку в кіберпросторі [2].

Для забезпечення виконання вищевикладених завдань в системі МВС України було створено Департамент кіберполіції як міжрегіональний територіальний орган Національної поліції України.

Відповідно до Положення про Департамент кіберполіції Національної поліції України, затвердженого наказом Національної поліції від 10 листопада 2015 року № 85 кіберполіція України приймає участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, учинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Кіберполіція сприяє в порядку, передбаченому чинним законодавством, іншим підрозділам Національної поліції України у попередженні, виявленні та припиненні кримінальних правопорушень [3].

Враховуючи швидкий розвиток даної сфери діяльності поліції та необхідність виконання вищезазначених завдань постала необхідність у комплексній підготовці висококваліфікованих фахівців у сфері боротьби з кіберзлочинністю.

Наразі існує дві незалежні системи підготовки фахівців – це здобуття ступеня вищої освіти «бакалавр» зі спеціалізації «боротьба з кіберзлочинністю» та перепідготовка фахівців з вищою технічною чи/або юридичною освітою у рамках реформування поліції.

В системі академічної освіти, з 2013 року відбувається підготовка фахівців для підрозділів боротьби з кіберзлочинністю на базі факультету № 4 Харківського національного університету внутрішніх справ, який з 1997 року готував фахівців з питань інформаційних технологій для Міністерства внутрішніх справ України.

Відповідно до ст. 50 Закону України «Про вищу освіту» освітній процес у вищих навчальних закладах здійснюється за такими формами: навчальні заняття; самостійна робота; практична підготовка; контрольні заходи. Основними видами навчальних занять у вищих навчальних закладах є: лекція; лабораторне, практичне, семінарське, індивідуальне заняття; консультація.

Згідно з Наказом МВС України від 15.10.2015 № 1251 «Про проведення конкурсу на заміщення вакантних посад старших інспекторів, інспекторів і спеціальних агентів інформаційних технологій міжрегіонального територіального органу Департаменту кіберполіції Національної поліції» на базі Харківського національного університету внутрішніх справ з березня по липень 2016 року відбувалась підготовка працівників кіберполіції. Освітній процес складався з навчальних занять, що містили в собі лекційний матеріал, практичне відпрацювання теорії та дискусію. Відповідною формою контролю були квізи та екзамени, матеріали яких були розроблені у відповідності до вимог ОБСЕ.

Виходячи з вищевикладеного, для найбільш ефективної підготовки фахівців по боротьбі з кіберзлочинністю в системі академічної вищої освіти доцільно поєднати традиційні форми навчання та інноваційні засоби ведення занять.

Таким чином, для підготовки висококваліфікованих фахівців з боротьби з кіберзлочинністю необхідно збільшити кількість комп'ютерних класів, ввести в навчальну програму практичні заняття для закріплення теоретичного матеріалу в режимі on-line, а також залучати до навчального процесу працівників практичних підрозділів боротьби з кіберзлочинністю, проводити, так звані, бінарні заняття.

#### **Література:**

1. Конвенція про кіберзлочинність: Закон України: [станом на 07 вересня 2005 р.]. – Режим доступу: [http://zakon3.rada.gov.ua/laws/show/994\\_575](http://zakon3.rada.gov.ua/laws/show/994_575).
2. Стратегія кібербезпеки України: Указ Президента України № 96/2016: [станом на 15 березня 2016 р.]. - Режим доступу: <http://zakon2.rada.gov.ua/laws/show/96/2016>.
3. Положення про Департамент кіберполіції Національної поліції України: Наказ Національної поліції України від 10.11.2015 № 85. - Режим доступу: [https://www.npu.gov.ua/uk/publish/printable\\_article/1816252](https://www.npu.gov.ua/uk/publish/printable_article/1816252).
4. Про вищу освіту: Закон України: [станом на 09 серп. 2016 р.]. – Режим доступу: <http://zakon3.rada.gov.ua/laws/show/1556-18>.
5. «Про проведення конкурсу на заміщення вакантних посад старших інспекторів, інспекторів і спеціальних агентів інформаційних технологій міжрегіонального територіального органу

## Аналітична обробка інформації у діяльності поліції Харкова

**Світличний В.А.**

кандидат технічних наук,  
викладач кафедри кібербезпеки  
Харківського національного університету внутрішніх справ

Фахівцями Управління інформаційного забезпечення Харківського обласного головного управління національної поліції України (ГУНП) спільно з місцевими ІТ – компаніями розроблений інноваційний комплекс аналітичної обробки інформації різноманітних банків даних з відображенням на детальній інтерактивній карті як самих об'єктів так і результатів їх аналізу. Комплекс має робочу назву «RICAS» (Real – time Intelligence Crime Analytics System) і на сьогоднішній день знаходиться на етапі тестового впровадження.

Унікальний інтелектуальний комплекс RICAS об'єднав в єдиному просторі відображення основні і найбільш передові методи і методики кримінального аналізу і аналітичного пошуку в реальному часі, що дозволяє значно підвищити ефективність і результативність розкриття злочинів за гарячими слідами і нерозкритих раніше злочинів

Застосування RICAS дає можливість:

- збереження відеоданих на серверах, їх перегляд та аналіз у разі необхідності;
- безпосереднього доступу до кожної відеокамери на детальній інтерактивній карті області;
- відображення на цій карті об'єктів та осіб, які можуть впливати на розвиток ситуації.

Аналітична робота в системі виконується в автоматизованому режимі: на першому етапі по запиті, що поступивши в систему, за допомогою розроблених алгоритмів автоматичний здійснюється пошук, результати якого відображаються в текстовій формі і на географічній карті, на іншому етапі оператором в ручному режимі здійснюється візуальний аналіз отриманих даних і приймається остаточне рішення або системі задаються додаткові аналітичні запити, наприклад вивчення поведінкового профілю, темпоральний та семантичний аналіз, тощо.

Як відомо, найбільш постійним і точним з точки зору психології злочинця являється його поведінковий профіль. Він відображає багато параметрів діяльності злочинця — звичний спосіб скоєння злочину, місця здійснення і інші дрібні залежності, які в сукупності відповідають одному профілю. Наявність тих або інших поведінкових ознак, з певною долею вірогідності може свідчити про те, що цей суб'єкт може бути причетний до події. З цього принципу формується так званий груповий поведінковий аналіз. Безумовно, поведінковий профіль злочинця ніяк не може існувати без впливу на інших суб'єктів. Тому, в кримінальній практиці часто помітні збіги за тими або іншими поведінковими параметрами у різних суб'єктів, що коли-небудь брали участь в єдиних подіях. Аналіз групового поведінкового профілю дозволяє визначати подільників, спільників, без явних зв'язків між собою. Відображення хронології подій, що сталися, і тимчасове розмежування дозволяє оперативно виявляти приховані просторово-часові закономірності між різними подіями. Інтелектуальний семантичний аналіз комплексу RICAS, включає потужне ядро по роботі з семантикою. Аналіз неструктурованих даних відбувається в режимі реального часу. Семантичне ядро системи дозволяє будувати складні пошукові запити, що включають всілякі динамічні і статичні компоненти, — обмеження за часом, методу скоєння злочину, дислокації і так далі. Усі функції виконуються миттєво і дозволяють максимально швидко візуалізувати інформацію і виконувати аналітичну роботу.

В процесі тестування комплексу підтверджується його гнучкість та спроможність інтегрування будь-яких даних, з можливістю часового та просторового аналізу їх зв'язків між собою. Розроблений комплекс не обмежується Харковом та областю, а з легкістю масштабується до рівня країни і навіть більше.

У основі комплексу знаходяться основні і найбільш передові методи і методики кримінального аналізу і аналітичного пошуку в реальному часі, що дозволяє значно підвищити ефективність і результативність розкриття злочинів за гарячими слідами і нерозкритих раніше злочинів.

Однією із складових частин комплексу RICAS є зовнішній Інтернет – сервіс взаємодії правоохоронних органів з громадськістю – проект [Police.kh.ua](http://Police.kh.ua), який на даний час користується популярністю в мережі Інтернет.

Проведені тестові випробування впродовж 3-х місяців підтверджують можливості комплексу щодо реагування на кримінальні та інші події. В результаті роботи команди з 3 аналітиків протягом цього часу було надано 152 аналітичних довідки з відомостями про осіб, можливо причетних до вчинення злочинів, більшу половину з яких підтверджено в ході перевірочних та оперативних заходів, зазначених осіб викрито у вчиненні злочинів.

На теперішній годину комплекс тестується на обчислювальних потужностях ГУНП в Харківській області. Для його розгортання в робочий режим необхідне створення сучасного дата-центру на базі ГУНП в Харківській області, створення ситуаційно - аналітичного центру та організація підготовки відповідних фахівців для роботи в ньому.

Комплекс RICAS працює в реальному часі і дозволяє розкривати злочини на основі аналізу баз даних, накопичених поліцією/міліцією за останні 20 років. Системі доступні дані про більш ніж 5 мільйонів подій, що сталися на Харківщині, починаючи з 1995 року. За 4,5 місяця, які в Харкові тестували систему, вона допомогла розкрити близько 300 злочинів

Для опрацювання зазначених пропозицій доцільним вбачається створення рішенням обласної ради спільної робочої групи, до якої увійшли б представники ГУНП в Харківській області, зокрема Управління інформаційного забезпечення, а також представники зацікавлених департаментів і служб Харківської обласної державної адміністрації та Харківської обласної ради.

### **Підготовка персоналу для боротьби з кіберзлочинністю на вузівському рівні**

**Пасько О.М.**

кандидат юридичних наук, доцент  
доцент кафедри психології та педагогіки  
факультету № 3 ОДУВС

На сучасному етапі державотворення змінюються способи вчинення злочину, особливо це обумовлюється високим рівнем впровадження сучасних інформаційних технологій, використовуючи які правопорушники здійснюють протиправні діяння. Тому поліцейські, а саме персонал для боротьби з кіберзлочинністю повинні бути готовими не лише розслідувати дані злочини, але й вміти попереджати.

Важливим аспектом професіогенезу працівника поліції є отримання освіти у ВНЗ МВС України. Вузівська підготовка складається із трьох етапів: вступ до ВНЗ МВС України, навчання у ВНЗ МВС України та закінчення навчання.

Відбір кандидатів на навчання здійснюється підрозділами кадрового забезпечення органів і підрозділів внутрішніх справ та внутрішніх військ спільно з постійно діючими комісіями з питань профорієнтації кандидатів та відбірковими комісіями ВНЗ МВС відповідно до вимог Закону України «Про національну поліцію» [1], Наказу МВС України від 15.04.2016 № 315 «Про затвердження Порядку добору, направлення та зарахування кандидатів на навчання до вищих навчальних закладів із специфічними умовами навчання, які здійснюють підготовку кадрів для Міністерства внутрішніх справ, поліцейських та військовослужбовців Національної гвардії України» [2] та ін.

Конкурсний відбір кандидатів на навчання до ВНЗ МВС здійснюється за результатами зовнішнього незалежного тестування, підтвердженого сертифікатами Українського центру оцінювання якості освіти, а також психологічного обстеження, оцінки рівня фізичної підготовки вступників до ВНЗ та співбесіди щодо готовності до проходження служби в органах внутрішніх справ.

Згідно Наказу МВС України від 15.04.2016 № 315 «Про затвердження Порядку добору, направлення та зарахування кандидатів на навчання до вищих навчальних закладів із специфічними умовами навчання, які здійснюють підготовку кадрів для Міністерства внутрішніх справ, поліцейських та військовослужбовців Національної гвардії України» [2] ВНЗ МВС розробляють правила прийому на навчання на підставі Умов прийому до вищих навчальних закладів України і погоджують їх з Департаментом кадрового забезпечення МВС і МОН України. Терміни проведення конкурсу сертифікатів зовнішнього незалежного оцінювання, перелік та форми проведення вступних екзаменів до ВНЗ ВС установлюються МВС за погодженням з МОН України.

#### **Навчання у ВНЗ**

**1. Навчальна підготовка.** Базис навчання у ВНЗ безумовно зосереджений на самому процесі навчання, який складається із наступних напрямків форм організації навчального процесу: навчальний (лекційні заняття, семінарські, практичні заняття та ділові ігри), виховний, практичний та самостійна підготовка.

*Лекційні заняття.* Вони встановлюють базис теоретичного матеріалу, який спрямовує курсантів у необхідний напрямок вивчення теми та подальшого самостійного опрацювання.

*Семінарські, практичні заняття та ділові ігри.*

Семінарські, практичні заняття. Закріплення теоретичного матеріалу і його перевірка здійснюється під час семінарських та практичних занять. Під час яких ми більше уваги звертаємо на організацію попередньої самостійної роботи курсантів з вивчення нового матеріалу. Методика проведення занять науково-педагогічним складом базується на трьох складових: бесіда з навчальних питань, дискусії з навчальних питань, обговорення реферативних повідомлень. Їх основа пов'язана із поглибленням, розширенням, деталізацією знань, отриманих на лекції в узагальненій формі, і сприяння виробленню навичок професійної діяльності. Вони розвивають наукове мислення і мову, дозволяють перевірити знання курсантів і виступають як засоби оперативного зворотного зв'язку.

*Ділові ігри.* Вони є формою відтворення наочного і соціального змісту майбутньої професійної діяльності фахівця, моделюваннями таких систем та ситуацій, які характерні для правоохоронної діяльності. За допомогою знакових засобів (мова, графіки, таблиці, документи) в діловій грі відтворюється професійна обстановка, схожа по основних сутнісних характеристиках з реальною. Разом з тим в діловій грі відтворюються лише типові, узагальнені ситуації в стислому масштабі часу.

Зазвичай процес організації навчання у ВНЗ спрямований на надання великого годинного навантаження на лекційні заняття, годин для семінарських, практичних занять та ділових ігор не достатньо не тільки для закріплення матеріалу, але і подальшого їх збереження у пам'яті. Тому слід збільшувати кількість такого навантаження з метою детального закріплення знань та розвиток вмінь та здатності їх використовувати. Також дієвим є проведення занять з елементами тренінгу та запрошення працівників практичних органів на лекційні та семінарські заняття.

*Консультації.*

Під час консультації науково-педагогічний склад допомагає курсантам самостійно вивчати та вирішувати навчальні проблеми, вибирати ефективні методи роботи, орієнтує їх на головні питання курсу навчання, які необхідно пропрацювати найбільш глибоко, та надає відповіді на окремі питання або пояснення певних теоретичних положень чи аспектів їх практичного застосування.

**2. Виховна діяльність** здійснюється в під впливом спеціальних підготовлених і планомірних виховних дій, мета яких спрямована на очікування змін в особистості. Блоки дисциплін, достатньо повно представлених в навчальних планах спеціальності, дають можливість отримання етичного, естетичного, фізичного, правового, цивільного, економічного, розумового, екологічного, трудового та ін. виховання.

**3. Практична діяльність.** Вона обумовлюється безпосереднім закріпленням отриманих знань у процесі практичного відтворення.

**4. Самостійна робота.** Навчити курсантів самостійно вчитися – це одна з головних завдань науково-педагогічних працівників ОДУВС. Успішність самостійного навчання багато в чому буде залежати і від ступеня попереднього оволодіння ними методикою роботи над навчальними матеріалами. Особливо це важливо за умов розвитку суспільних відносин і різноманітних прийомів та засобів у скоєнні злочинів, і відповідно, об'єм необхідних знань для фахівців органів досудового слідства різко та швидко збільшується, і не завжди можна робити головну ставку на засвоєння необхідної суми фактів. Тому їм важливо вміти самостійно поповнювати свої знання і не тільки, щоб орієнтуватися в стрімкому потоці нормативно-законодавчих змін, але й вміти їх використовувати для узагальнення конкретних функціональних обов'язків.

Відповідно, самостійна робота є важливою і невід'ємною складовою частиною організації навчального процесу та основним засобом оволодіння навчальним матеріалом у час, вільний від навчальних занять. На виконання спроможності курсантів до самостійної роботи науково-педагогічному складу необхідно підпорядкувати всі заходи організації та проведення навчально-виховного процесу, який необхідно будувати так, щоб він навчав їх творчому та науковому підходу до вивчення будь-якого навчального чи проблемного питання в ході самостійної роботи.

Отже, розвиток та формування різновидів готовності курсантів ВНЗ спрямований у послідовній взаємозалежності навчальної, виховної, практичної та самостійної роботи. Оскільки завдання вищої освіти не тільки спрямоване на оснащення знань, умінь та навичок, але й на здатність їх виконувати по завершенню навчання. Слід зазначити, що у більшості випадків у ВНЗ відповідно до навчальних планів домінують лекційні заняття і менша кількість семінарських та практичних. Ми вважаємо це основними недоліком при розвитку компетентної особи, оскільки знання необхідно постійно закріплювати практичними зайняттями з метою їх усвідомлення формування професійних вмінь та навичок.

Системний підхід при підготовці поліцейських на вузівському рівні сприятиме ефективній та якісній підготовці персоналу для боротьби з кіберзлочинністю.

**Література:**

1. Про національну поліцію [ Електронний ресурс ] : закон України від від 02.07.2015 № 580. – Електрон. дан. (1 файл). – Режим доступу : <http://zakon3.rada.gov.ua/laws/show/580-19> . – Назва з екрану.

2. Про затвердження Порядку добору, направлення та зарахування кандидатів на навчання до вищих навчальних закладів із специфічними умовами навчання, які здійснюють підготовку кадрів для Міністерства внутрішніх справ, поліцейських та військовослужбовців Національної гвардії України [Електронний ресурс] : наказ МВС України від 15.04.2016 № 315. Електрон. дан. (1 файл). – Режим доступу: <http://zakon4.rada.gov.ua/laws/show/z0668-16>. – Назва з екрану.

**Професіограма слідчого у контексті набуття ним психологічних навичок розслідування злочинів у сфері використання комп'ютерних технологій**

**Савченко В. С.**

здобувач кафедри психології ВНЗ «Університет економіки та права «КРОК»  
м. Київ, Україна

Особливість нашої перехідної епохи - це прагнення кожного наступного покоління користуватися благами і вигодами, які несе із собою нова техніка, а старше покоління побоюється її всевладдя. Тому не дивно, що і батьки, і поліція, і співробітники спеціальних служб проявляють тривогу, коли стикаються з речами, які вони не можуть зрозуміти і контролювати. А наслідки цих тривог очевидні.

В основі професіограми слідчого лежить пошукова сторона діяльності, яка реалізує прагнення до розкриття злочину і полягає в збиранні вихідної інформації для вирішення професійних завдань [3, с. 83]. Розглянемо дане твердження на яскравому прикладі розслідування правопорушень скоєних відомими хакерами Кевіном Митником та Сьюзан Сандер, яка вирішила використати факти накопичені нею за майже цілий рік, щоб викрити злочинну діяльність спільника та відвести від себе усі можливі «загрози». У неї були підстави підозрювати, що районний прокурор повідомить їй про підозру у вчиненні кримінального правопорушення по десяти пунктах, включаючи незаконне проникнення в головний офіс корпорації PacificBell та участь у змові з метою шахрайства з використанням комп'ютерної техніки.

Щоб уникнути цього, вона вирішила сама піти до слідчого Боба Рена відділу районного прокурора з метою обов'язково переключити його увагу на своїх друзів. Вона заявила слідчому, що нею рухає виключно турбота про безпеку своєї країни. Кевін знає, що у неї є надзвичайно важлива інформація, і Сьюзан не сумнівається, що він захоче її дістати[2, с.8].

Необхідно відмітити, що допит - це боротьба за істину. Сили в цій боротьбі слідчому дають різні наукові знання, в тому числі знання психології [3, с. 88]. Тому постійно необхідно приділяти велику увагу мотивації правопорушника викрити своїх спільників.

Як приклад Сьюзан привела слідчому цікавий епізод. Одного разу вона нібито провела в своїй оселі кілька днів поспіль, а коли вийшла, то повідомила Кевіну Митнику, що весь цей час скачувала на свій комп'ютер та друкувала параметри запуску міжконтинентальних балістичних ракет з ядерними боеголовками. Вона похвалилася, що відтепер знає графіки чергування персоналу, який обслуговує ці ракети в шахтах (і відповідно наділений правом проводити запуск), а також режим поточного обслуговування і характеристики резервної системи. За її словами, якщо така інформація потрапить до рук хакера (при цьому вона явно мала на увазі Митника), то він мало не з вуличного кафе зможе запустити по каналах військової зв'язку потрібну послідовність команд, підняти з шахт сотні ракет і направити їх в будь-яку точку світу.

У цьому епізоді існує можливість побачити комплекс психологічних причин кримінальних конфліктів пов'язаний насамперед з досвідом формування особистості і загальною культурою поведінки. І головне тут, на наш погляд, - невміння йти на компроміси, гіпертрофоване «почуття ворога», пов'язане з підвищеною підозрілістю, а також норми поведінки, які ведуть до неминучої необхідності відплати за завдані збитки. Традиції помсти і насиченість людської культури зразками насильницької поведінки самим фатальним чином проявляються в спілкуванні конкретних суб'єктів [1, с.159]. Сьюзан не подбав про те, щоб хоч як-небудь підтвердити цю історію, замість цього зробила акцент на тому, що їй нібито вдалося розробити алгоритм, який дозволить ввести комп'ютер в оману: змодельовати таку ситуацію або послідовність дій, коли необхідність для неї несення першого удару або удару у відповідь вже виконана. Але вся справа в тому, як стверджувала Сьюзан, що найвразливіше

місце - це національна система зв'язку. Вся діяльність Пентагону занадто залежить від надійності або ненадійності системи телефонної зв'язку Bell, і це перетворює її в зручну мішень для хакерів.

Розповівши все це слідчому, Сюзан запропонувала звільнити її від кримінального переслідування в обмін на співробітництво зі слідством та покази проти Кевіна Митника [2, с. 9].

На даному етапі треба відмітити, що існує погляд, згідно з яким кримінально-процесуальний конфлікт являє собою стадію, етап розвитку кримінального конфлікту. «В основі кожного злочину, - писав Р.С. Белкін, - лежить конфлікт правопорушника із законом, з інтересом суспільства і держави. Відновлення порушеного права починається з розкриття та розслідування злочину, в ході якого конфлікт із законом може знайти форму конфлікту зі слідчим - особою, покликаним встановити істину». Ту ж думку висловлює О.Я. Баєв: «Різновидом, формою кримінально-правового конфлікту є полегшення його в кримінально-процесуальні відносини, що виникають між державою та особою, яка вчинила злочин» [1, с. 160].

Слідчий направив Сюзан до районного прокурора. Той вирішив так само, як і слідчий: запропонував Сюзан співробітничати зі слідством і натомість пообіцяв не порушувати проти неї кримінальну справу. Мислення, що розкриває причини будь-яких явищ, називають причинно-наслідковим.

Саме такий характер носить мислення прокурора. Зрозуміло, Сюзан погодилась виступити свідком обвинувачення на суді і викласти свою версію.

Практика показує, що для розкриття даного типу злочину вміле поєднання слідчих дій з оперативно-розшуковими заходами особливо важливо. Фахівці з безпеки комп'ютерних мереж давно підозрюють цю річ, а тепер Сюзан підтвердила її з усією наочністю: найбільш ненадійний елемент в будь-якій системі - це людина [2, с. 10].

Через призму конфлікту розглядаються іноді і окремі психологічні особливості слідчі дії даного типу злочину. Так, Г.Г. Доспулов пише про «конфліктної ситуації допиту», яка виникає, коли «допитуваний відмовляється від дачі показань або дає неправдиві свідчення». З цього випливає судження, що відноситься вже до оцінки доказів: мовляв, «матеріали показань обвинуваченого (підозрюваного) складаються в ході підготовки до вчинення, вчинення злочину і приховування слідів». Ці та подібні їм судження складають своєрідну концепцію конфліктного розслідування. З ототожнення процесуального конфлікту з кримінальним (з його етапом, формою) неминуче випливає висновок про тотожність підозрюваного (або обвинуваченого) із злочинцем [1, с. 163].

Такі ототожнення несумісні з конституційним принципом презумпції невинуватості, за яким обвинувачений вважається невинним, поки його винність не буде встановленовироком суду, що набрало законної сили.

#### **Література:**

1. Кудрявцев В. Н. Избранные труды по социальным наукам: В 3 т./В. Н. Кудрявцев; Рос. акад. наук.-М.:Наука.Т.2: Криминология. Социология. Конфликтология.-2002.-282 с.
2. Д.Марков, К. Хэфнер - Хакеры. – К.: «Полиграфкнига», 1996. - 92 с.
3. Васильев В.Л. Юридическая психология: Учебник для вузов. 6-е издание. - СПб.: Питер. 2009. – 608 с.

#### **Особливості підготовки персоналу для боротьби з кіберзлочинністю в Україні**

**Кравченко В.О.**

курсант факультету підготовки фахівців  
для органів досудового розслідування  
Дніпропетровського державного університету внутрішніх справ

**Черняк Н.П.**

кандидат юридичних наук, доцент  
доцент кафедри кримінального процесу  
Дніпропетровського державного університету внутрішніх справ

Розв'язання завдань, що стоять сьогодні перед Національною поліцією України, неможливе без вдосконалення вмінь та навичок у сфері боротьби з кіберзлочинністю. Стрімке розгортання науково-технічної революції призвело до прискорення всіх соціальних процесів. У наш час багато людей, підприємств, організацій використовують найрізноманітніші технології, в тому числі й Інтернет. Вони

потрапляють в групу ризику, адже атаки шахраїв можливі з будь-якого куточку світу. Кіберзлочинність стала одним з основних викликів, що постають перед сучасним суспільством.

Кіберзлочинність (або злочин з використанням комп'ютерних технологій) – це економічний злочин, скоєний із використанням обчислювальної техніки та мережі Інтернет. Приклади кіберзлочинності: розповсюдження вірусів, незаконне завантаження інформації, фішинг та фармінг, а також викрадення особистої інформації (наприклад, реквізитів банківських рахунків). До цієї категорії відносяться тільки ті економічні злочини, в яких основним (а не допоміжним чи супутнім) інструментом скоєння злочину є комп'ютер, Інтернет або електронні носії інформації та пристрої [1].

На відміну від традиційних економічних злочинів, кіберзлочинність динамічно змінюється, постійно виникають нові ризики, і як наслідок, необхідно постійно адаптувати свої вміння та відточувати навички. У зарубіжних країнах налагоджена система співробітництва, яка допомагає виявити нові прояви кіберзлочинності та ефективно протидіяти їм. Так як Україна тільки буде власну стратегію для забезпечення охорони кіберпростору необхідно враховувати найкращий світовий досвід. На сьогодні, відбувається перетворення колишньої моделі підрозділів боротьби з кіберзлочинністю до новітнього органу правозахисного призначення, який за своїми технічними та професійними можливостями матиме змогу миттєвого реагування на кіберзагрози, а також проводитиме міжнародну співпрацю по знешкодженню транснаціональних злочинних угруповань у даній сфері.

При поверхневому огляді стратегій кібербезпеки різних країн, можна виділити об'єднуючі ключові позиції:

- побудова урядової моделі, спрямованої на забезпечення кібербезпеки;
- визначення адекватного механізму, в основному у вигляді суспільно-державного партнерства, який дозволить приватним та державним зацікавленим сторонам обговорювати та затверджувати політики, пов'язані з проблемою кібербезпеки;
- планування та визначення необхідних політик та регулюючих механізмів, чітке позначення ролей, прав та відповідальності для приватного та державного сектора у сфері протидії кіберзлочинності;
- визначення цілей та способів розвитку державних можливостей, а також необхідної законодавчої бази для участі у міжнародній боротьбі з кіберзлочинністю;
- визначення ключових інформаційних інфраструктур, у тому числі – основних активів, сервісів та взаємозалежностей;
- підвищення готовності, зменшення часу реакції на інциденти, розробка плану відновлення після збоїв та розробка механізмів захисту для ключових інформаційних інфраструктур;
- розробка системного та інтегрованого підходу до державного управління ризиками;
- визначення цілей інформаційних програм та затвердження їх у якості пріоритетних, покликаних прищепити користувачам нові моделі поведінки та моделі роботи;
- доказ необхідності нової програми освіти в якій робиться акцент на навчання ІТ-фахівців та професіоналів в області кібербезпеки;
- розвиток міжнародної співпраці [2, с. 61].

Відповідно до Положення про Департамент кіберполіції НП України, затвердженого наказом Національної поліції від 10.11.2015 № 85, як міжрегіональний територіальний орган створено Департамент кіберполіції, який є міжрегіональним територіальним органом Національної поліції України відповідно до законодавства України забезпечує реалізацію державної політики у сфері протидії кіберзлочинності, здійснює інформаційно-аналітичне забезпечення керівництва Національної поліції України та органів державної влади про стан вирішення питань, віднесених до його компетенції [3].

З метою підвищення ефективності діяльності правоохоронних органів на Конференції Ради Європи щодо співробітництва у сфері протидії кіберзлочинності (м. Страсбург, Франція) пріоритетними визнано заходи щодо підготовки, перепідготовки та підвищення кваліфікації співробітників відповідної спеціалізації для правоохоронних органів, здатних застосовувати сучасні методи оперативно-технічного документування та розкриття комп'ютерних злочинів, що потребує запровадження суттєвих новацій стосовно змісту й методів навчання [4, с. 8].

На нашу думку щоб підготувати працівників Національної поліції України для боротьби з кіберзлочинами необхідно враховувати специфіку такої підготовки. Насамперед необхідно забезпечити навчальні заклади системи МВС навчальним матеріалом, програмно-технічними засобами, які використовуються на практиці. Також працівники правоохоронних органів, які протидіють злочинам з використанням комп'ютерних технологій, повинні в досконалому знати іноземні мови, володіти технічними навичками користування комп'ютером, Інтернетом, електронними носіями інформації та пристроями. Сучасною та досить ефективною підготовкою стане взаємозв'язок між

теорією та практикою. Варто проводити спецкурси, тренінги, міжнародні конференції, досліджувати практику правоохоронної діяльності у боротьбі з кіберзлочинністю, створювати нові навчальні дисципліни, розширювати міжнародні зв'язки. Необхідно створити групу оперативного реагування на кіберзлочини. Добре підготована група оперативного реагування забезпечить виявлення злочину, оцінку ризику та можливої загрози. Важливим є також інформованість працівників про поточне та майбутнє комп'ютерне середовище.

Таким чином, можна зробити висновок, що кіберзлочинність – це реальна глобальна загроза, яка потребує від правоохоронних органів специфічних навичок та вмінь. Вона може виходити за межі конкретної юрисдикції та походити з будь-якої країни світу. Необхідною умовою підготовки фахівців для підрозділів боротьби з кіберзлочинністю насамперед є належний рівень матеріально-технічного забезпечення, вивчення та аналіз досвіду зарубіжних країн.

#### **Література:**

1. Україна. Всесвітній огляд економічних злочинів. Кіберзлочини в центрі уваги [Електронний ресурс] - режим доступу до ресурсу : // <http://www.pwc.com/ua>
2. Казакова Н. Ф. Світові тенденції боротьби з кіберзлочинністю / Н. Ф. Казакова, О. О. Йона // Вісник Східноукраїнського національного університету імені Володимира Даля. – Луганськ: СНУ ім. В. Даля, 2013. - №15 (204).– Ч.1. - 59-62 с.
3. Департамент кіберполіції Національної поліції України [Електронний ресурс] / режим доступу до ресурсу : // [www.npu.gov.ua](http://www.npu.gov.ua)
4. Черней В.В. Роль відомчої освіти та науки в забезпеченні протидії кіберзлочинності в Україні / В.В. Черней // Науковий вісник національної академії внутрішніх справ.- Київ: 2014.- № 3.- 63 с.

#### **Особливості управління в територіальних органах національної поліції**

**Підвашецька Л.В.**

слухач магістратури факультету №2  
Одеського державного університету внутрішніх справ

**Корнієнко М.В.**

кандидат юридичних наук, доцент,  
професор кафедри адміністративної діяльності  
ОВС та економічної безпеки  
Одеського державного університету внутрішніх справ

На сьогодні під час стрімкого руху нашої держави до європейських перетворень, реформування органів поліції займає одне з найважливіших місць. Зараз одним із завдань поліції є надання поліцейських послуг у сферах забезпечення публічної безпеки і порядку, охорони прав і свобод людини, а також інтересів суспільства і держави, протидія злочинності та всебічна допомога громадянам. Поліція повинна чітко і якісно працювати у кожному населеному пункті для служіння суспільству та захисту його прав.

Основною метою змін, що відбуваються на сьогоднішній день у правоохоронній структурі є забезпечення правопорядку і безпеки громадян в будь-якому місці України – від малого села до великого міста. Високий рівень довіри людей до поліції – вторинна мета, що забезпечує високу якість виконання головного завдання поліцейського [3].

У новій структурі велика роль відводиться органам управління на чолі з Центральним офісом національної поліції та Головним управлінням національної поліції в регіонах. Але найбільш важлива роль у взаємовідносинах поліції з громадянами відведена територіальним органам поліції на місцях, тому що вони безпосередньо безперервно реагують на звернення громадян. Тому ефективна структура і функціональність цих підрозділів є визначальними у питанні якісного забезпечення правоохоронної діяльності.

З цією метою система місцевих органів поліції в структурі Головних управлінь національної поліції в регіонах сформована за «кущовим» принципом, який передбачає створення відділів поліції, через які буде здійснюватися управління та організація діяльності відділень поліції (базових органів) у складі «куща». У той же час ключовими елементами територіальних органів поліції на місцях (відділів, відділень) є і поліцейські ділянки, через які в основному і здійснюється безпосередня комунікація з суспільством і населенням [2].





Основними завданнями відділень поліції, як базових органів поліції в першу чергу є: зосередження уваги дільничних офіцерів поліції на ефективній превенції та з'ясуванні потреб громадян і спільне з громадою їх вирішення. Насамперед що стосується безпеки, правової, інформаційної та моніторингової діяльності; створення груп реагування поліції, основним завданням яких є: негайний виїзд на виклик, патрулювання певної зони відповідальності з метою попередження вчинення кримінальних та адміністративних правопорушень, проведення профілактичної та роз'яснювальної роботи з громадянами, здійснення перевірочних заходів відносно осіб за якими здійснюється нагляд і т.д.; попередження і розслідування найбільш характерних для невеликих населених пунктів тяжких правопорушень; виконання інших функцій пов'язаних з питаннями забезпечення правопорядку на території обслуговування.

Відділ поліції («кущовий» орган) – утворюється з розрахунку один на 3-6 відділень поліції і крім виконання завдань, характерних для базових органів поліції, здійснює функції з розслідування складних злочинів, діяльності дорожньої поліції, ізолятора тимчасового утримання, а також – організаційно-аналітичного, кадрового, матеріально-технічного забезпечення та контролю за роботою відділень поліції [3].

Даний принцип роботи поліції вже на протязі багатьох років ефективно працює в Європейських державах.



Відповідно до розділу VIII Закону України «Про Національну поліцію», який визначає громадський контроль поліції, ч.1 статті 86 регламентує, що «З метою інформування громадськості про діяльність поліції керівник поліції та керівники територіальних органів поліції раз на рік готують та опубліковують на офіційних веб-порталах органів поліції звіт про діяльність поліції. Керівники територіальних органів поліції зобов'язані регулярно оприлюднювати статистичні та аналітичні дані про вжиті заходи щодо виявлення, запобігання та припинення порушень публічного порядку на офіційних веб-порталах органів, які вони очолюють» [1].

Також керівники територіальних органів поліції повинні не менше одного разу на два місяці проводити відкриті зустрічі з представниками органів місцевого самоврядування на рівнях областей, районів, міст та сіл з метою налагодження ефективної співпраці між поліцією та органами місцевого самоврядування і населенням, це в повній мірі впроваджує принцип роботи поліції "pablikrelations" - врахування думки громадськості. На таких зустрічах обговорюється діяльність поліції, визначаються поточні проблеми та обираються найефективніші способи їх вирішення.

Так О. М. Бандурка зазначає, що "pablikrelations" в діяльності ОВС – це функція управління, що сприяє налагодженню або підтримці взаємовигідних зв'язків між органом внутрішніх справ та громадськістю шляхом вироблення та поширення спеціальної інформації через засоби комунікації і безпосередньо серед населення для спрямованого формування бажаної громадської думки [4, с. 277].

Одним з об'єктів "pablikrelations" та головним критерієм оцінки її діяльності виступає громадська думка.

Також з метою належного контролю за діяльністю поліції, здійснюється постійне залучення представників громадськості до спільного розгляду скарг на дії чи бездіяльність поліцейських та до перевірки інформації про належне виконання покладених на них обов'язків відповідно до законів та інших нормативно-правових актів України.

Співпраця між поліцією та громадськістю насамперед спрямована на виявлення та усунення проблем, пов'язаних із здійсненням поліцейської діяльності, і сприяння застосуванню сучасних методів підготовки та виконання спільних проєктів, програм та заходів для задоволення потреб населення та покращення ефективності виконання поліцією покладених на неї завдань, підвищення результативності та ефективності здійснення такої діяльності.

Вище викладене свідчить про ознаку партнерства як виду спільної діяльності, яка полягає у рівноправності учасників спільної діяльності, що в цілому передбачає рівні права та обов'язки кожної зі сторін і взаємну відповідальність. Партнерство це ідеальний варіант стосунків рівноправних суб'єктів, які усвідомлюють власне значення своїх дій для партнера по взаємодії і свою діяльність будують так, щоб виправдати сподівання партнера і таким чином досягти спільної мети. Партнерство можливе лише за умови взаємної довіри, взаємної впевненості та взаємної діяльності, спрямованої на досягнення спільного результату.

На сьогоднішній день структурна побудова органів поліції дуже чітка і продумана вона визначає розподіл функцій і ролей керівників різних рівнів в органах Національної поліції України, які в свою чергу застосовуючи сучасні методи підготовки та виконання покладених державою прав та обов'язків спільно із населенням на партнерських стосунках реалізують спільні проєкти, програми та заходи для задоволення потреб суспільства, направлених на покращення ефективності виконання поліцією покладених на неї завдань, підвищення результативності та ефективності здійснення такої діяльності.

#### **Література:**

1. Закон України Про Національну поліцію / від 02.07.2015 року Відомості Верховної Ради України. – 2015. – № 580. – Ст. 378. із змін., внес. згідно із Законами України: станом на 18.02.2016 ВВР, 2016, № 1021 - VIII № 129. Електронний ресурс. <http://zakon3.rada.gov.ua/laws/show/580-19> – Назва з екрана.
2. Структура Национальной полиции Украины. Инфографика // [Електронний ресурс]. – Режим доступу: <http://nv.ua/ukraine/events/struktura-natsionalnoj-politsii-ukrainy-infografika-85757.html>
3. Аваков А.Б. // Поліція. Як це буде працювати: від найменших сіл і невеликих міст – до столиці // [Електронний ресурс]. – Режим доступу: [http://blogs.pravda.com.ua/authors/avakov/5631fd1e5a588/view\\_print/](http://blogs.pravda.com.ua/authors/avakov/5631fd1e5a588/view_print/)
4. Бандурка О. М. Управління в органах внутрішніх справ України : підруч. / О. М. Бандурка. - Харків : Університет внутрішніх справ, 1998. - 480 с.

**Поляков Є.В.**

кандидат юридичних наук, доцент  
доцент кафедри ОРД факультету № 1 ОДУВС

**Гонтарук Е.Л.**

курсант 414 взводу  
факультету №3 ОДУВС

Умови сьогодення ставлять суспільство перед проблемою створення єдиного інтегрованого інформаційного простору, території без меж та кордонів, де кожен житель планети зможе знайти потрібну йому інформацію, а також це основна перспективна форма спілкування між членами суспільства та державами, яка не потребує будь-яких додаткових витрат та часу. В науковому аспекті ці процеси називають одним словом – інформатизація. Однак, якими б корисними не були створені людиною блага, вони завжди можуть стати зброєю проти них же самим – саме це й сталося в випадку з інформацією. Таке поняття як кіберзлочинність, та один з його різновидів – кібертероризм, все частіше й частіше стає підставою слідчо-розшукової та оперативно-розшукової діяльності уповноважених органів, а суспільство постійно зустрічає дані поняття в ЗМІ. Враховуючи геометричну прогресію поширення злочинності пов'язаної з кіберпростором та інформацією, для нашої держави сьогодні є дуже важливим дослідження особливостей та характеристик даного виду злочинів, адже питання їх запобігання, боротьби, розкриття, а також виявлення осіб, винних у їх вчиненні потребує розробки специфічного механізму. В даній роботі увага буде приділена одному з найменш досліджуваних, однак найбільш глобальному злочину у сфері комп'ютерного простору, а саме – кібертероризму. Питання кібертероризму в Україні набуває особливої актуальності у зв'язку з ситуацією на Сході, а також поширенням антидержавних настроїв, що покликані створити атмосферу розбрату та протистояння окремих регіонів України. Лише зупинивши цю інформаційну лавину, можливо відновити конституційний лад та територіальну цілісність в країні.

Вивченням даної проблеми займалися ряд вчених та науковців, роботи яких стали джерельною базою даного дослідження. Серед них: В. В. Копійка, Є. А. Макаренко, Д. Т. Малишенко, М. Носенко, М. М. Рижигов, Е.В. Старостина та інші.

Розглядаючи таку тему як тероризм в кіберпросторі, слід зазначити, що для українського кримінального законодавства даний термін є досить новим, та відображається лише опосередковано в окремих складах злочинів, однак прямо ніде не прописаний. Зокрема це більшість злочинів, передбачених Розділом 16 КК України у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж і мереж електрозв'язку, а також як спосіб вчинення окремих складів злочинів проти основ національної безпеки України, проти громадської безпеки, проти громадського порядку та моральності та інших[1].

Вчені пропонують таке визначення кібертероризму: навмисна політично-мотивована атака проти інформацій, комп'ютерних систем, комп'ютерних програм та баз даних у вигляді насильственного вторгнення з боку міжнародних груп або секретних агентів. В свою чергу запоглядами експертів ООН, поняття «кіберзлочинність» об'єднує будь-який злочин, який можна здійснити за допомогою комп'ютерної системи або мережі та також проти комп'ютерної системи або мережі. Інтернет – головна зброя терористичних груп, яку вони використовують для зв'язку, проведення пропаганди, поширення інформацій, вірусів та інше. Особливий інтерес для терористів представляють державні інформаційні системи, об'єктами їх діяльності стають важливі елементи державної інфраструктури, наприклад, системи управління та функціонування атомних об'єктів, електростанцій, залізні дороги, аеропорти та інше [2, с. 57].

Потенційною загрозою являється те, що в якості учасників кібертерористичної діяльності розглядаються кібертерористи-одинаки, кібертерористичні організації та окремі держави. В цьому випадку кібертероризм є одним із стратегічних інструментів, які націлено на руйнування і ослаблення політичної, економічної, військової могутності країни, тим більше що кібертероризм є відносно недорогим засобом для здійснення стратегічних цілей держави[3]. Враховуючи таке різноманіття суб'єктів, їх прийнято класифікувати на такі види:

- 1) атаки з боку державних установ або на їх замовлення;
- 2) атаки з боку певних організацій або на їх замовлення;
- 3) атаки з боку фізичних осіб або на їх замовлення[4, с. 170].

На жаль, випадки кібертероризму, спрямовані на перешкоджання нормальній діяльності державних підприємств, установ та організацій в Україні зустрічаються все частіше, а наслідки їх щораз серйозніші. Так, 23 грудня 2015 року через стороннє втручання в роботу об'єктів вітчизняної енергосистеми частково без електропостачання залишилися Івано-Франківська область (загалом 80 тис. домогосподарств). Служба безпеки України повідомила про виявлення шкідливого програмного забезпечення в комп'ютерних мережах окремих обленерго («Прикарпаттяобленерго», «Київобленерго» та «Чернівціобленерго»). Було встановлено, що для атаки застосовували шкідливе програмне забезпечення «BlackEnergy». Кібератака складалася з п'яти елементів:

- зараження мереж за допомогою підроблених листів;
- захоплення управління автоматизованою системою диспетчерського управління з вимиканнями на підстанціях;
- виведення з ладу мереж безперебійного живлення, модемів, комутаторів та іншої IT-інфраструктури;
- знищення інформації на серверах і робочих станціях (утилітою «KillDisk»);
- атака на телефонні номери колл-центрів (з російських номерів) з метою відмови від обслуговування знеструмлених абонентів.

Іншим випадком є події січня 2016 року, коли ШПЗ було виявлено в комп'ютерній мережі аеропорту «Бориспіль», до якої входить і управління повітряним рухом аеропорту.[5, с. 79] Атаки подібного роду є добре спланованими та, скоріш за все, лише першими проявами інформаційних посягань на національну та громадську безпеку держави.

У світі цілком виправдано кібертероризм виносять на один щабель за рівнем суспільної небезпечності з іншими видами тероризму, який став страшним сном сучасних мегаполісів, тримаючи в постійному страху мільярди людей. Враховуючи обставини, що складаються в Україні, питання попередження та боротьби з кібертероризмом потребує невідкладних дій та провадження заходів спрямованих на моніторинг та викриття злочинних акцій у сфері транспортних телекомунікаційних мереж, електронних баз даних, інформаційних телекомунікаційних систем, оскільки наслідки такого шкідливого впливу за масштабом можуть перевершити найстрашніші катастрофи та теракти, навіть такі як атака на Башти Близнюки 11 вересня 2001, або Московське метро.

#### **Література:**

1. Кримінальний кодекс України–[Електронний ресурс]//Верховна Рада України - Закон від 05.04.2001.- № 2341-III. – Режим доступу: <http://zakon5.rada.gov.ua/laws/show/2341-14>
2. Бойченко О. В., Ончурова О. О. Кібертероризм у складі сучасних проблем національної безпеки - [Електронний ресурс]/ О. В. Бойченко, О. О. Ончурова // Фортеця права – 2010. - №2. – С. 57 – Режим доступу: [http://www.nbuv.gov.ua/old\\_jrn/e-journals/FP/2010-2/10bovpnb.pdf](http://www.nbuv.gov.ua/old_jrn/e-journals/FP/2010-2/10bovpnb.pdf)
3. Потеряхіна І. С. Роль кібертероризму в сучасних міжнародних відносинах [Електронний ресурс]- / І. С. Потеряхіна // Історичний факультет МДУ – Режим доступу: <http://istfak.org.ua/tendentsii-rozvytku-suchasnoi-sistemy-mizhnarodnykh-vidnosyn-ta-svitovoho-politychnoho-protsesu/183-protsesy-rehionalizatsii/368-rol-kiberteroryzmu-v-suchasnykh-mizhnarodnykh-vidnosynakh>
4. Ясенко О. Базиданих як об'єкткібертерористичних атак / О. Ясенко // Актуальні проблеми міжнародних відносин – 2011. – №95/2.
5. Парфило О. А., Нізовцев Ю. Ю. Актуальні питання судово-експертного дослідження шкідливих програмних засобів у межах протидії кібертероризму /О.А. Парфило, Ю.Ю. Нізовцев // Криміналістичний вісник – 2016. - № 1 (25).

#### **Кіберпростір і оперативно-розшукова діяльність**

**Шевчук О.Ю.**

кандидат юридичних наук, доцент,  
доцент кафедри СТ та ОРД ННІ №1  
Національної академії внутрішніх справ

Розвиток та розповсюдження сучасних засобів обчислювальної техніки сприяли створенню передумов для зростання злочинності, пов'язаної з неправомірним доступом до комп'ютерних мереж, несанкціонованим отриманням або зміною інформації, інших кримінальних правопорушень. Як показує практика, класичні оперативно-розшукові заходи, є недостатніми для боротьби з кіберзлочинністю,

тому правоохоронним органам необхідно пристосувати існуючі, а можливо розробити й нові оперативно-розшукові заходи, що дозволять ефективно протистояти такому типу злочинів.

Над цією проблемою працювали такі вітчизняні вчені, як І.О. Воронов, В.О. Голубєв, О.Ф. Долженков, М.Ю. Літвінов, Є.В. Рижков, С.М. Рогозін, Л.П. Скалозуб, Ю.В. Степанов, Ф.Ф. Хараберюш та інші. Різні аспекти застосування інформаційних технологій в оперативно-розшуковій діяльності (далі ОРД) розглядали науковців, зокрема: А.В. Борбат, В.В. Зорін, С.С. Овчинський, В.С. Овчинський, А.С. Овчинський, М.М. Перепелиця, В.І. Попов та інші. Було розроблене та втілене в життя таке поняття як «комп'ютерна розвідка», окреслені особливості деяких оперативно-розшукових методів, що можуть використовуватися при своєчасному виявленні «комп'ютерних злочинів». Однак комплексний підхід до проведення деяких оперативно-розшукових заходів через кіберпростір, що є базовими для ефективної боротьби з кіберзлочинністю загалом, не розглядався.

Саме поняття «кіберзлочинність» передбачає використання в процесі злочинної діяльності віртуального простору – кіберпростору. Відповідно методи боротьби з такими злочинами у межах здійснення ОРД повинні містити не лише стандартні прийоми, але й використання кіберпростору. Для того, щоб з'ясувати значення «кіберпростір» у сучасному його контексті, необхідно дослідити його етимологію. Термін «кіберпростір» є сполученням двох слів – «кібер» та «простір». Слово – «кібер» походить від грецького «kuber» та означає «над», під простором розуміють вільний великий обшир, просторинь, територію.

Узагальнивши та проаналізувавши різні думки щодо визначення терміну «кіберпростір» [1, с. 130; 2, с. 52] можна виділити інструмент, за допомогою якого виникає (існує) кіберпростір - це технічні (комп'ютерні) системи, що дозволяє надати наступне тлумачення цього терміну: кіберпростір - це інформаційне середовище (простір), яке виникає (існує) за допомогою технічних (комп'ютерних) систем при взаємодії людей між собою, взаємодії технічних (комп'ютерних) систем та управлінні людьми цими технічними (комп'ютерними) системами.

Отже, враховуючи думки різних вчених, кіберпростір має такі основні ознаки: це інформаційний простір; є комунікативним середовищем; утворюється за допомогою технічних систем. Кіберпростір також визнав появу так званої «комп'ютерної злочинності» або «кіберзлочинності». Усі комп'ютерні злочини охоплює одна ознака – використання сукупності елементів комп'ютерних технологій як засобу вчинення злочину. Під засобом вчинення злочину в кримінальному праві розуміються матеріальні об'єкти, які полегшують вчинення умисного злочину на будь-якій його стадії, засоби комп'ютерної техніки найповніше підходять під це визначення.

Більш детальний підхід до поняття «комп'ютерний злочин» дозволяє виділити спосіб його вчинення. Основними способами використання засобів інформаційних технологій для досягнення злочинної мети є: створення злочинцем комп'ютерної бази даних, що містить інформацію про злочин; використання ЕОМ і периферійних пристроїв як поліграфічної бази для проектування і виготовлення фальсифікованих (підроблених) документів, грошових знаків, кредитних карток; використання електронних засобів доступу (комп'ютерні, телекомунікаційні системи, кредитні картки) для здійснення розкрадань шляхом крадіжок і привласнення [3, с. 44]. Отже, комп'ютерні злочини вчинюються через кіберпростір. Всю сукупність злочинів, передбачених кримінальним кодексом, можна поділити на ті, які можуть бути та які не можуть бути вчинені через кіберпростір. Злочин можна вважати вчиненим через кіберпростір, коли виконується одна з наступних вимог - при здійсненні злочину засобами комп'ютерної техніки (ЗКТ) використовуються: для автоматизації злочинної діяльності; для втручання в роботу інших ЗКТ; як телекомунікаційний засіб. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку конкретизовані у Особливій частині розділу XVI Кримінального кодексу України, а саме: несанкціоноване втручання у роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК України); створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361<sup>1</sup> КК України); несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361<sup>2</sup> КК України); несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362 КК України); порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363 КК України); перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж

електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363<sup>1</sup> КК України) [4, с. 73-78].

У статті 8 Закону України «Про ОРД» для оперативних підрозділів визначені права, які можуть бути реалізовані в тому числі і в кіберпросторі [5]. На практиці оперативні працівники використовують кіберпростір при проведенні ОРД, але ці дії вони виконують спираючись більшою мірою на свій особистий досвід, без опори на розроблені теоретико-методологічні основи.

У контексті вищевикладеного треба визнати, що наші правоохоронні органи виявляють недостатню активність щодо попередження, своєчасного виявлення і припинення злочинів, які вчинюються через кіберпростір, хоча необхідно відмітити, що з кожним роком ця негативна тенденція поступово зникає. Основними причинами невисокого рівня боротьби зі злочинністю у кіберпросторі в Україні є: досить повільне формування державної політики в напрямку реальної протидії новим антисоціальним явищам або антисоціальним явищам в новому контексті; відсутність в оперативних підрозділах відповідних кваліфікованих кадрів; недостатність або відсутність в оперативних підрозділах методик попередження, своєчасного виявлення і припинення спеціалізованих злочинів; обмаль кадрових та фінансових ресурсів, які задіяні у протидії злочинним проявам в кіберпросторі; відсутність належної взаємодії з прокуратурою та судом; відсутність продуктивної міжнародної співпраці, адже багато з таких злочинів мають транснаціональний характер; недостатність технічної бази здійснення ОРД у кіберпросторі; відсутність відповідних нормативних механізмів регулювання ОРД в кіберпросторі.

З наведеного випливає, що в сучасній Україні є нагальна потреба в використанні нового інформаційного середовища (кіберпростору), через яке чиняться злочини, як і реального (традиційного) середовища для проведення ОРД. Таким чином, можна стверджувати, що зараз для суб'єктів ОРД України необхідною є розробка організаційно-тактичних основ проведення ОРД у кіберпросторі та введення в дію відповідних правових механізмів їх здійснення. |

Це надасть можливість правоохоронним органам, насамперед Національній поліції України, активізувати, поглибити та суттєво вдосконалити лінію боротьби зі злочинністю в цій сфері.

#### **Література:**

1. Бондаренко С.В. К вопросу о таксономии киберпространства /С.В. Бондаренко // Рационализм и культура на пороге третьего тысячелетия. Материалы Третьего российского философского конгресса (16 - 20 сентября 2002 г.). Том. 4. – Ростов-на-Дону: Издательство СКНЦ ВШ, 2002. – 130–131 с.
2. Гавловський В. Інформаційна безпека: захист інформації в автоматизованих системах (організаційно-правовий аспект) /В. Гавловський // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К., 2000. – 50– 53 с.
3. Пашнев Д. Виды и классификация преступлений, совершаемых с помощью компьютерных технологий // Компьютерная преступность и кибертерроризм: Сборник научных статей / Под ред. А. Голубева, Н.Н. Ахтырской. – Запорожье: Центр исследования компьютерной преступности, 2004. – Вып. 2. – 296 с.
4. Кримінальний кодекс України: Закон України від 5 квітня 2001 року № 2341-III // Відомості Верховної Ради (ВВР), 2001, № 25-26, ст. 131.
5. Про оперативно-розшукову діяльність: Закон України від 18 лютого 1992 року № 2135-XII // Відомості Верховної Ради (ВВР), 1992, № 22, ст. 303.

**Всеукраїнська науково-практична конференція  
Кібербезпека в Україні: правові та організаційні питання  
24 листопада 2017 року  
м. Одеса, Україна**

## **ЗАПРОШЕННЯ**

Інформуємо Вас, що **24 листопада 2017 року** в м. Одеса відбудеться Всеукраїнська науково-практична конференція «Кібербезпека в Україні: правові та організаційні питання».

Для участі в конференції запрошуються вчені, співробітники науково-дослідних установ, аспіранти, курсанти, студенти.

Робочі мови конференції: українська, англійська, російська.

### **ПОДАННЯ ДОКУМЕНТІВ:**

Для участі в конференції представити наступні документи:

1. Заявку у відповідності з формою;
2. Тези доповіді на одній із робочих мов, оформлені у відповідності із запропонованим зразком;

### **ПУБЛІКАЦІЯ ПРАЦЬ КОНФЕРЕНЦІЇ**

Тези доповідей, отримані Організаційним комітетом та прийняті до друку, будуть видані до початку конференції у збірнику праць конференції та вислані безкоштовно на електронні адреса учасників конференції.

### **АДРЕСА ОРГКОМІТЕТУ:**

Кафедра кібербезпеки та інформаційного забезпечення  
Одеського державного університету внутрішніх справ

вул. Успенська, 1, м. Одеса 65000, Україна

Сайт <http://oduvs.sem-dev.co.ua/kafedra-kiberbezpeki-ta-informatsijnogo-zabezpechennya/>

E-mail: [oduvs.kiber@ukr.net](mailto:oduvs.kiber@ukr.net)

### **Контактні особи:**

Ісмаїлов Карен Юрійович +38 (099) 70-600-70;

+38 (097) 70-600-90;

[0997060070@ukr.net](mailto:0997060070@ukr.net)

Форос Ганна Володимирівна +38 (067) 485-30-84

## ЗМІСТ

### ПЛЕНАРНЕ ЗАСІДАННЯ

<b>Катеринчук І.П.</b> Правоохоронні органи в боротьбі з кіберзлочинністю.....	4
<b>Албул С.В.</b> Протидія інформаційним загрозам в умовах антитерористичної операції.....	7
<b>Грохольський В.Л.</b> ..... Адміністративно-правові заходи боротьби з кіберзлочинністю в Україні	9
<b>Карчевский Н.В.</b> Киберпреступление или преступление в сфере использования информационных технологий? .....	10
<b>Гришук Р.В.</b> Інформаційна та кібернетична безпека: роль та місце в умовах гібридної війни.....	16
<b>Пядишев В.Г.</b> Місце кібертероризму в структурі кіберзлочинності та напрями боротьби з ним.....	17
<b>Лефтеров Л.В., Бабенко А.М.</b> Нормативно-правові засади використання високотехнологічних і програмних інструментів у боротьбі з кіберзлочинністю .....	19
<b>Ісмаїлов К.Ю., Мусаєва С.С.</b> Особливості забезпечення кібернетичної безпеки України в сучасних умовах розвитку кіберпростору .....	21

### СЕКЦІЯ 1

#### ПРАВОВЕ РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

<b>Головка О.М., Савінова Н.А.</b> Вплив на людську свідомість в медіапросторі як інформаційна загроза сучасності.....	24
<b>Маковій В.П., Бабенко Т.С.</b> Співвідношення публічного та приватного інтересу у межах протидії кіберзлочинності.....	26
<b>Деля Ю.В.</b> Захист інформаційної діяльності органів публічного адміністрування в Україні.....	28
<b>Бібік І.С., Бабенко А.М.</b> Вплив Інтернету як фактор вчинення неповнолітніми злочинів проти життя та здоров'я особи у регіонах України.....	30
<b>Сверба Ю.І., Березовська Н.Л.</b> Деякі питання кримінально-правової характеристики DDOS-атаки.....	33
<b>Мукоїда Р.В., Шелехов А.О.</b> Законодавство України у сфері боротьби з кіберзлочинністю.....	35



<b>Березовська Н.Л.</b> Кібербезпека як об'єкт кримінально-правової охорони.....	37
<b>Шуміло О.О., Голіна В.В.</b> Щодо актуальності імплементації міжнародних стандартів кібербезпеки до національного законодавства України.....	38
<b>Дорохіна Ю.А.</b> До проблеми розуміння кіберзлочинів проти власності.....	40
<b>Задніченко С.І.</b> Комп'ютерна програма як одна зі складових неправомірної вигоди.....	42
<b>Іващенко Ю.К., Черняк Н.П.</b> Кібербезпека в Україні: сучасний стан.....	43
<b>Калініна І.В.</b> Правова природа та доказове значення висновку експерта у кримінальних провадженнях про кіберзлочини.....	45
<b>Кришечевич О.В.</b> Кримінальна відповідальність за комп'ютерне шахрайство – один з елементів кіберзлочинності .....	47
<b>Солдатенко О.А., Гурагов А.П.</b> Психологічний аспект слідчих та співробітників оперативних підрозділів під час досудового розслідування кримінальних правопорушень.....	49
<b>Солдатенко О.А., Легкий М.І.</b> Принцип поваги до людської гідності під час кримінального процесу.....	50
<b>Солдатенко О.А., Любова Н.О.</b> Експерт як важливий учасник кримінального процесу.....	51
<b>Форос Г.В., Козуменко Є.І.</b> Спеціальний суб'єкт злочину в сфері інформаційної безпеки.....	53
<b>Форос Г.В., Никитюк В.С.</b> Щодо особливостей правового забезпечення інформаційної безпеки.....	55
<b>Теслюк І.О., Цільмак О.М.</b> Криміналістичне прогнозування як стратегічний метод при проведенні обшуку.....	56
<b>Андрусенко С.В., Горбенюк Т.А.</b> Правове регулювання забезпечення безпеки осіб залучених до проведення негласних слідчих (розшукових) дій.....	58
<b>Бараненко Р.В., Вікторов Д.І.</b> Дослідження факторів, що впливають на вчинення кіберзлочинів.....	60
<b>Делія Ю.В., Власенко А.В.</b> Протидія торгівлі людьми в мережі Інтернет.....	63
<b>Ісмайлов К.Ю., Никитюк В.О.</b> Передові юридичні доктрини в інформаційному праві в період незалежності України.....	64

**Мукоїда Р.В., Шелехов А.О.**

Використання правоохоронними органами сучасних інформаційно-аналітичних технологій у протидії тіньовій економіці в Україні.....	66
---	----

**Біба А.В., Пекарський С.П.**

Компетенція кіберполіції з протидії ввезенню, виготовленню, збуту і розповсюдженню порнографічних предметів.....	68
--	----

**Пекарський С.П., Кушнарєва К.О.**

Компетенція кіберполіції з протидії ввезенню, виготовленню, збуту або розповсюдженню творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію.....	70
--	----

**Хлевицький В.Б.**

Окремі проблеми правового забезпечення кібернетичної безпеки в Україні в умовах розвитку інформаційного суспільства.....	72
--	----

**Шелехов А.О., Корнієнко М.В.**

Використання європейського досвіду в організації роботи поліції України.....	74
--	----

**Небеська М.С.**

Сучасні проблеми кіберзлочинності: міжнародний аспект.....	77
--	----

**Небеська М.С., Свиріпа І.В.**

Актуальні питання нормативно-правового забезпечення аналітично-інформаційної системи Національної поліції України.....	79
--	----

## СЕКЦІЯ 2 АДМІНІСТРАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

**Нікітенко О.І., Журавель І.В.**

Адміністративно-правове регулювання у сфері забезпечення кібербезпеки в Україні.....	82
--	----

**Козюра В.Д., Хорошко В.О.**

Створення системи кібернетичної безпеки в Україні: деякі актуальні питання.....	83
---	----

**Манжай О.В.**

Особливості безпечної роботи з інформацією в МВС та Національній поліції України.....	85
---	----

**Делія Ю.В., Кіянчук В.М.**

Кібербезпека інтелектуальної власності у відкритій мережі інтернет.....	86
---	----

**Манжай І.А.**

Аналіз активності у деструктивних мережних співтовариствах для прогнозування сплесків протиправної діяльності.....	88
--	----

**Нашинець-Наумова А.Ю.**

Парадигмальна трансформація концепції інформаційної безпеки.....	89
--	----

**Добровольська О.О., Даніч М.А.**

Деякі психологічні особливості осіб, які вчиняють злочини у сфері високих технологій.....	91
---	----

<b>Політова А.С.</b> Термінологічна невизначеність у сфері кібербезпеки.....	92
<b>Гончаров М.В.</b> До питання кібернетичної безпеки в Україні.....	94
<b>Припутень Д.С., Кожушина О.В.</b> Сутність та зміст громадського порядку і його адміністративно-правової охорони.....	96
<b>Скачкова Т.Ю.</b> Початкові дії спеціаліста під час огляду місця події за фактом порушення працездатності комп'ютерної системи.....	97
<b>Форос Г.В., Баркар Р.І.</b> Кібертероризм як різновид тероризму.....	99
<b>Форос Г.В., Кондрашева К.С.</b> Інформаційне суспільство та кібербезпека.....	101
<b>Форос Г.В.</b> Щодо розмежування понять «кібербезпека» та «інформаційна безпека».....	102
<b>Косаревська О.В., Новіцький О.І.</b> Протидія кіберзлочинності як складова інформаційної безпеки держави.....	104
<b>Косаревська О.В., Шутило С.В.</b> Кіберзлочини у фінансово-банківській сфері: скілінг та способи його викорінення.....	106
<b>Бараненко Р.В., Гітрук О.О.</b> Кібербезпека як один із факторів забезпечення національної безпеки держави.....	108
<b>Бухонський С.О.</b> Щодо сучасного стану інформаційно-аналітичного забезпечення початкового етапу досудового розслідування та перспективи його розви.....	110
<b>Романов О.Д., Касюн О.О.</b> Кібератаки і кібертероризм: поняття та особливості реалізації атак у кіберпросторі.....	113
<b>Ігнатушко Ю.І.</b> Проблеми розслідування злочинів щодо порушення авторського права на комп'ютерні програми.....	115
<b>Ком'яга А.В.</b> Актуальні питання адміністративно-правового забезпечення кібербезпеки в Україні .....	117
<b>Бааджи Н.А.</b> Проблеми визначення поняття адміністративного розсуду.....	118
<b>Любчик В.Б., Слободянюк О.О.</b> Кіберзлочинність як злочин транснаціонального характеру .....	120
<b>Медведенко С.В., Колодніцький Р.Р.</b> Роль та місце зворотного зв'язку в процесі здійснення управлінської діяльності.....	122
<b>Мукоїда Р.В., Аносенков А.А.</b> Створення інформаційного середовища взаємодії та роботи у сфері запобігання та протидії легалізації (відмиванню) доходів.....	125

**Розовик І.В., Шевчук О.Ю.**

Кіберзлочинність в Україні: перспективи протидії.....127

**Саакян М.Б.**

Правове регулювання поширення інформації в мережі Інтернет.....128

**Нерубащенко І.Ю., Янковий М.О.**

Особа злочинця як елемент криміналістичної характеристики злочинів у сфері мобільних телекомунікацій.....131

### СЕКЦІЯ 3 ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ В БОРОТЬБІ З КІБЕРЗЛОЧИННІСТЮ

**Кузьменко Б.В.**

Використання інформаційних технологій і систем на підприємствах енергетики України.....133

**Казакова Н.Ф., Фразе-Фразенко О.О., Щербина Ю.В.**

Сучасні проблеми оцінки захищеності інформаційно-телекомунікаційних систем.....134

**Осадчий Є.О., Горбунов О.А.**

Методи та засоби таймерного захисту інформації.....136

**Хахановський В.Г., Єгоров Д.А.**

Основні правові аспекти використання інформаційних технологій у боротьбі з кіберзлочинністю в Україні: проблематика та шляхи вирішення.....138

**Стрельбіцький М.А., Ваврічен О.А.**

Приховані канали витоку інформації в інформаційно-телекомунікаційних системах Державної прикордонної служби України та шляхи їх ліквідації.....140

**Хахановський В.Г., Дабіжа Д.В.**

Використання інформаційних систем для візуального аналізу даних в боротьбі з кіберзлочинністю.....142

**Larysa Kupriianova, Daryna Kupriianova**

Act of the forensic medicine: main features of the storage an access to theevident database. The main ways of protecting electronic versions of the medical documents in Ukraine and Poland.....145

**Коваленко А.В., Смирнов А.А., Коваленко А.С.**

Разработка метода управления рисками разработки программного обеспечения.....146

**Волинець Д.О., Чесановський І.І.**

Оцінка технологій радіо доступу з метою реалізації в телекомунікаційній мережі.....148

**Кудінов В.А.**

Методика оцінки рівня кібербезпеки в Україні.....151

**Кушнір І.П.**

Правове забезпечення захисту інформації пов'язаної із охороною державного кордону.....152

**Мелешко Є.В.**

Дослідження методів динамічного аналізу віртуальних соціальних мереж з точки зору інформаційної безпеки.....154

**Миколенко О.М.**

Деякі особливості розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.....155

**Мирошниченко А.И., Лещенко О.И.**

Перспективы использования пористого кремния в качестве датчиков систем с контролем доступа .....157

**Шестак Я.В., Оксуюк А.Г.**

Модель построения киберзащищенного информационного пространства ЦОД: Математический аспект.....159

**Одарченко Р.С., Гнатюк С.О.**

Принципи формування вимог до систем безпеки мереж 5G.....160

**Зерко А.Л., Оксуюк О.Г.**

Дослідження методів класифікації захищених операційних систем за варіантами їх використання.....162

**Коновець В.І., Симоненков В.М., Черниш І.А.**

Особливості використання криптозахищених автоматичних ідентифікаційних судових станцій.....163

**Пеньков С.В.**

Дослід США щодо застосування оперативної техніки у протидії злочинності.....164

**Косаревська О.В.**

Інформаційно-пошукові системи в діяльності поліцейських.....166

**Орлик О.В.**

Інформаційні технології забезпечення безпеки електронного бізнесу.....167

**Балтовский А.А., Сифоров А.И.**

Подстройки коэффициентов модели управления как методика процедуры адаптации.....169

**Форос Г.В., Підвашецька Л.В.**

Визначення проявів корупційних правопорушень в інформаційній сфері.....171

**Форос Г.В., Щур К.В.**

Діяльність України у сфері боротьби з кіберзлочинністю.....173

**Форос Г.В., Бадюк М.О.**

Деякі аспекти щодо проблем запобігання та протидії кіберзлочинності.....174

**Деркач В.А., Деркач І.І.**

Інформаційні технології в поліцейській діяльності.....176

**Храпкіна В.В., Храпкін О.М.**

Сутність та роль кібербезпеки в сучасному суспільстві.....178

**Черняк Н.П.**

Проблеми боротьби з кіберзлочинністю у сучасних умовах становлення України.....179

**Ісмайлов К.Ю., Гладковський Е.О.**

Криптографічні методи захисту інформації: види та вимоги до них.....181

**Білоусов А.С.**

Слідчий огляд в справах про комп'ютерні злочини.....183

**Власенко І.М.**

Аналіз окремих вразливостей технології ss7 в мережах мобільного зв'язку.....185

**Мельнікова О.О., Мишко В.В.**

Інформаційно-аналітичне забезпечення оперативного пошуку ознак злочинів,  
пов'язаних з торгівлею людьми.....186

**Рвачов О.М., Беляєва Є.Г.**

DDoS-атаки: їх вплив на безпеку інформації, способи захисту.....189

#### СЕКЦІЯ 4 ПІДГОТОВКА ПЕРСОНАЛУ ДЛЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ В УКРАЇНІ

**Рижков Е.В., Тітов О.О.**

Пошукінформації яка становить оперативний інтерес, в мережі Інтернет.....191

**Пекарський С.П.**

Деякі питання системи фахової підготовки працівників кіберполіції  
у вищих навчальних закладах МВС України.....194

**Санакоєв Д.Б.**

Засоби протидії неправомірному контенту підрозділами кіберполіції України:  
міжнародний досвід.....196

**Соловйов О. Ю., Казакова Н.Ф.**

Особливості підготовки фахівців по боротьбі з кіберзлочинністю.....198

**Деля Ю.В., Барган С.С.**

Боротьба зі шкідливим програмним забезпеченням в сучасному кіберсередовищі.....199

**Доценко В.В.**

Використання тренінгових технологій у підготовці персоналу  
для боротьби з кіберзлочинністю.....201

**Калюга К.В.**

Питання встановлення закономірностей, що лежать в основі утворення криміналістично  
значущої інформації.....202

**Малихін В.А.**

Підготовка майбутніх інженерів-педагогів до забезпечення безпеки  
інформаційних систем в освітньому середовищі.....204

**Мілорадова Н.Е., Кислинська Д.М.**

Формування системи ціннісних орієнтацій майбутніх правоохоронців.....206

**Мілорадова Н.Е.**

Тренінг розвитку професійних настановлень у підготовці фахівців для боротьби з  
кіберзлочинністю .....208

**Муляр Т.М.**

Особливості підготовки фахівців у сфері публічного управління.....209

**Онищенко Ю.М., Черновол В.С.**

Особливості підготовки фахівців для підрозділів боротьби з кіберзлочинністю.....210

**Світличний В.А.**

Аналітична обробка інформації в діяльності поліції Харкова.....212

**Пасько О.М.**

Підготовка персоналу для боротьби з кіберзлочинністю на вузівському рівні.....213

**Савченко В.С.**

Професіограма слідчого в контексті набуття ним психологічних навичок  
розслідування злочинів у сфері використання комп'ютерних технологій.....215

**Кравченко В.О., Черняк Н.П.**

Особливості підготовки персоналу для боротьби з кіберзлочинністю в Україні.....216

**Корнієнко М.В., Підващеська Л.В.**

Особливості управління в територіальних органах національної поліції.....218

**Поляков Є.В., Гонтарук Е.Л.**

Кібертероризм як загроза національній безпеці України.....221

**Шевчук О.Ю.**

Кіберпростір та оперативно-розшукова діяльність .....222

Наукове видання

# **КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ**

**Матеріали  
Всеукраїнської науково-практичної конференції**

**21 жовтня 2016 року**

Підписано до друку 03.11.2016. Формат 60х90/8. Папір офсетний.

Гарн. «Times New Roman» Друк цифровий. Ум. друк .арк. 26,1.

Наклад 500 прим.

Видавництво ОДУВС

м. Одеса, вул. Успенська, 1

Свідоцтво суб'єкта видавничої справи ДК № 3507 від 25.06.2009 р.

тел. 0487024884; 0949547884 email – [ndrvv1@gmail.com](mailto:ndrvv1@gmail.com)



