**Видання: Філософія та політологія в контексті сучасної культури. Дніпро.**

**УДК 327. 7**

**Виклики на шляху до ефективної протидії кіберзлочинності**

**в Європейському Союзі**

**Дерещук Тетяна Миколаївна**

Кандидат юридичних наук, доцент кафедри міжнародних відносин, Прикарпатський національний університет імені Василя Стефаника, вул. Шевченка, 57, м. Івано-Франківськ, 76018, Україна.

**E-mail:** [**tetiana.dereshchuk@pnu.edu.ua**](mailto:tetiana.dereshchuk@pnu.edu.ua)

**Tetiana Dereshchuk**

Candidate of Juridical Sciences (Ph.D). Associate Professor of the International Relations Department, Vasyl Stefanyk Precarpathian National University, Shevchenka Str., 57, Ivano-Frankivs'k, 76018, Ukraine.

ORCID: <https://orcid.org/0000-0002-5348-9394>

**Струтинська Тетяна Зіновіївна**

Кандидат політичних наук, доцент кафедри міжнародних відносин, Прикарпатський національний університет імені Василя Стефаника, вул. Шевченка, 57, м. Івано-Франківськ, 76018, Україна.

**E-mail:** [**tetiana.z.strutynska@pnu.edu.ua**](mailto:tetiana.z.strutynska@pnu.edu.ua)

**Tetiana Strutynska**

PhD in Political Science. Associate Professor of the International Relations Department, Vasyl Stefanyk Precarpathian National University, Shevchenka Str., 57, Ivano-Frankivs'k, 76000, Ukraine.

ORCID: <https://orcid.org/0000-0003-3328-628Х>

**Романченко Вікторія Василівна**

Студентка спеціальності "Міжнародні відносини, суспільні комунікації та регіональні студії", Прикарпатський національний університет імені Василя Стефаника, вул. Шевченка, 57, м. Івано-Франківськ, 76018, Україна.

**E-mail:** [**viktoriia.romanchenko.17@pnu.edu.ua**](mailto:viktoriia.romanchenko.17@pnu.edu.ua)

**Viktoriia Romanchenko**

Student of International Relations, Public Communications and Regional Studies, Vasyl Stefanyk Precarpathian National University, Shevchenka Str., 57, Ivano-Frankivs'k, 76018, Ukraine.

ORCID: <https://orcid.org/0000-0002-5358-2572>

**Анотація**

У публікації охарактеризовано ключові виклики в боротьбі з кіберзлочинністю в ЄС на сучасному етапі. На основі звітів установ правопорядку та спеціалізованих агентств Європейського Союзу здійснено огляд та систематизацію сфер, з викликами в яких найчастіше стикаються організація під час боротьби з кіберзлочинністю, а також вказано на заходи, що вже були прийняті для їх вирішення. Наголошується на змінах в тенденціях кіберзагроз ЄС, які спостерігаються в порівнянні зі звітами минулих років, та підкреслюється вплив геополітики на дану сферу, зокрема, теперішній конфлікт між Росією та Україною.

**Ключові слова:** кіберзлочинність, кібербезпека, Європейський Союз (ЄС), Європол, Євроюст, ENISA, виклик, міжнародні електронні комунікації, міжнародна інформація.

CHALLENGES ON THE WAY TO EFFECTIVE COUNTERACTION TO CYBERCRIME IN THE EUROPEAN UNION

**Abstract**

The publication describes the key challenges in the fight against cybercrime in the EU at the present stage. They were carried out based on reports by law enforcement agencies and special agencies of the European Union (the European Police Agency - Europol, the European Agency in cooperation with the judicial and police authorities of EU member states - Eurojust, the European Agency for Network and Information Security - ENISA, etc.). They analyze and systematize those areas with challenges that law enforcement agencies most often face when fighting cybercrime. In addition, these reports indicate what measures have already been taken to solve them.

Cybercrime knows no borders. The reports emphasize noticeable changes in the development and spread of cyber threats in the EU. Compared to the reports of previous years, today almost any type of crime can be carried out with the help of the Internet. In addition, the impact of geopolitics on this area is emphasized. In particular, the current conflict between Russia and Ukraine has opened and strengthened new areas of cybercrime (operations with cryptocurrency allow Russian citizens to circumvent sanctions imposed by the world community, hacktivism is when political ideas are promoted using the Internet, cyberattacks by pro-Russian hackers, etc.).

As for measures to combat cybercrime, the European Union adopted a number of legal documents that were supposed to contribute to this. In particular, in order to prevent the illegal circulation of cryptocurrency, a bill on the regulation of cryptocurrencies MiCA (Markets in Crypto Assets) was developed, which received the support of many EU countries; Europol and Eurojust jointly launched the SIRIUS project to simplify the procedure for cross-border access to electronic evidence; in May 2018, a Joint Memorandum of Understanding was signed between Europol, ENISA (European Network and Information Security Agency), EDA (European Defense Agency) and CERT-EU (Computer Emergency Response Team Computer Emergency Response Team); in March 2019, the Protocol on the response of EU law enforcement agencies to emergency situations (including large-scale cross-border cyber attacks) and many others was adopted. Some of them are still in the planning and development stage.**Keywords:** cybercrime, cybersecurity, European Union (EU), Europol, Eurojust, ENISA, challenge, international electronic communications, international information.

**Постановка проблеми.** Ефективна реалізація політики кібербезпеки та боротьба з кіберзлочинністю в ЄС ускладнена низкою унікальних факторів. По-перше, за своєю природою кіберзлочинність не має кордонів та розвивається набагато швидше, ніж на те можуть реагувати національні та наднаціональні владні структури. По-друге, ця ситуація ускладняється горизонтальною природою кіберзлочинності – практично будь-який тип злочину зараз може буде здійснено за допомогою мережі Інтернет. Більш того, докази таких незаконних діянь зібрати набагато важче через нестабільність електронних даних та обсяг необхідних знань для такої роботи. По-третє, для вчасного та безпечного збереження електронних доказів і гарантування їх допустимості під час судового процесу необхідне тісне та ефективне міжнародне судове співробітництво. Такому співробітництву на заваді часто стають суттєві відмінності у правових системах окремих держав-членів ЄС та конфлікти юрисдикцій. Ситуація ускладнюється і динамічністю сфери: кіберпростір постійно розвивається та є досить залежний від світових тенденцій (наприклад, підвищення активності кіберзлочинців в період пандемії COVID-19) та, у випадку з ЄС, локальних геополітичних чинників. Саме тому робота над виявленням та вирішенням труднощів та викликів в боротьбі з кіберзлочинністю ЄС є постійною та невід’ємною складовою діяльності як самої організації та її спеціалізованих установ, так і наукової спільноти.

**Аналіз останніх досліджень та публікацій.** Дослідженням правових засад політики кібербезпеки ЄС, а також потенційних труднощів в цій сфері займались А. Грубінко, О. Звоздецька, А. Марущак, В. Пазюк. Л. Могілевський розглядав моніторингову діяльність правоохоронних органів ЄС та функціонування окремих проектів, складовою яких є протидія кіберзлочинності. М. Саєнко, Є. Савела та Ю. Тополянський вивчали досвід міжнародної спільноти в боротьбі з кібершахрайством та кіберзлочинністю.

**Мета та завдання.** Метою даної статті є аналіз поточних викликів в Європейському Союзі на шляху до ефективної реалізації політики кібербезпеки. Для досягнення даної мети було поставлено наступні завдання: проаналізувати звіти Європолу та Євроюсту та ENISA за останні роки; охарактеризувати основні труднощі, з якими стикається ЄС під час протидії злочинності; розглянути вплив геополітичного чинника конфлікту в Україні на тенденції в кіберзагрозах для ЄС.

**Виклад основного матеріалу.** В червні 2019 року Європейське агентство, зі співпраці з судовими та поліцейськими органами країн-членів ЄС (Євроюст) та Європейський центр з протидії кіберзлочинності (EC3) Європейського поліцейського агентства (Європолу) опублікували Спільний звіт «Загальні проблеми у боротьбі з кіберзлочинністю» [Europol 2019]. В даному документі було окреслено головні виклики в сфері кіберзлочинності, що базувались на оперативному та практичному досвіді, на спільних обговореннях, висновках, звітах та оцінках міжнародних експертів, а також на підсумкових звітах кількох тематичних і стратегічних зустрічей з національними експертами та відповідними зацікавленими сторонами. Виявлені та визначені виклики було розділено на п’ять сфер:

1) втрата даних;

2) втрата локації;

3) виклики, пов’язані з національними правовими рамками держав-членів ЄС;

4) труднощі в міжнародному співробітництві;

5) виклики публічно-приватного партнерства.

В свою чергу, сфера втрати даних може бути розділена на кілька категорій, таких як збереження даних, шифрування даних, поширення використання криптовалюти.

Цікаво, що до розвитку першої категорії викликів вклад було зроблено самим ЄС, оскільки рішенням від 8 квітня 2014 року, Судом Європейського Союзу було скасовано Директиву про збереження даних (Директива 2006/24/ЄС Європейського Парламенту та Ради від 15 березня 2006 р. про збереження даних, створених або оброблених у зв’язку з наданням загальнодоступних електронних комунікаційних послуг або громадських комунікаційних мереж, та про внесення змін до Директиви 2002/58/ЄС). Це скасування унеможливило отримання даних від приватних осіб правоохоронними органами та прокуратурою. Так, в деяких державах-членах ЄС досі діє законодавство, яке дозволяє та навіть гарантує збереження даних провайдерами Інтернет-послуг для правоохоронних цілей, тоді як в інших державах ЄС це було скасовано у зв’язку з рішенням Суду. В останніх, деякі дані зберігаються виключно для бухгалтерських чи комерційних цілей, але дані, що могли б бути корисними для кримінальних розслідувань видаляються. Така розбіжність ускладнює ефективність роботи відповідальних правоохоронних органів. Більше того, ця ситуація змушує слідчі органи розставляти пріоритети своєї оперативної діяльності згідно з різними існуючими системами зберігання даних замість того, щоб зосередитись на важливіших цілях [Rojszczak 2021].

Після даного рішення Суду ЄС саме відсутність уніфікованої політики зберігання даних електронних комунікацій держав-членів стала основним викликом для розслідування транснаціональних кіберзлочинів, зокрема кібератак, сексуальної експлуатації дітей в Інтенеті, транскордонного платіжного шахрайства, злочинів в «темній мережі» (Dark Web) і т. д. Комплексний аналіз, проведений Євроюстом та Європолом засвідчив цінність даних електронних комунікацій та підтвердив, що більшість правоохоронних та судових органів держав-членів ЄС підтримали б створення законодавчої бази на рівні ЄС. У грудні 2015 року на засіданні Ради з питань юстиції та внутрішніх справ (JHA) було підтримано потребу спільноєвропейського підходу до зменшення фрагментації правової бази в питаннях збереження даних та закликано до законодавчої ініціативи щодо її повноцінного функціонування [Europol 2019].

Серед кроків, які вже були прийняті ЄС в цій сфері є зокрема розвиток концепції обмеженого збереження даних та цільового доступу до даних за результатами двох експертних семінарів, що були проведені Європолом в березні і травні 2018 року. Також Європолом та Євроюстом здійснюється моніторинг впливу анулювання Директиви про збереження даних рішенням Суду ЄС у справах Tele2 Sverige та Watson на проведення кримінальних та судових розслідувань. Проте питання потреби в новій законодавчій базі, що регулювала б питаннях зберігання даних з метою їх використання в правоохоронних цілях на рівні ЄС залишається відкритим.

Ще одним фактором, що ускладнює боротьбу з кіберзлочинністю є широке застосування шифрування інформаційних даних злочинцями [Могілевський 2021]. Безумовно, шифрування є невід’ємним елементом цифрової демократії і саме воно допомагає забезпечити безпеку цифрової економіки та основні прав людини. Та з іншої сторони, ці технології доступні і злочинцям для приховування своїх даних чи доказів злочинної комунікацій.

Законне перехоплення електронних комунікацій стає не ефективним або ж навіть технічно недоступним через збільшення кількості постачальників електронних послуг, що впроваджують особисте шифрування або анонімізацію електронних комунікацій у своїх послугах за замовчуванням.

Ця проблема була підтверджена і в оцінках IOCTA (Internet Organised Crime Threat Assessment), що публікується Європейським центром протидії кіберзлочинності [Europol (ІOCTA) 2022]. У звіті ІОСТА, особливо підкреслюється використання віртуальних приватних мереж (VPN), анонімізуючих мереж, таких як Tor, та використання шифрування. Наприклад, сексуальні злочинці щодо дітей використовують наскрізно зашифровані додатки для завантаження та обміну незаконними матеріалами, що створює значну проблему в розслідуванні кіберзлочинів пов’язаних з сексуальною експлуатацією дітей в Інтернеті.

На даний час для вирішення цього виклику впроваджуються заходи, запропоновані в 11-му та 13-му звітах Європейської Комісії про хід реалізації безпекової політики Союзу. Це включає в себе спостереження за шифруванням для аналізу технічних і правових змін (проводиться EC3 при Європолі, Євроюсті та Європейській судовій мережі по боротьбі з кіберзлочинністю (EJCN)) та підтримку Європолу в розширенні його можливостей з дешифрування. Тим не менш, для протидії злочинному зловживанню шифруванням необхідно забезпечити правоохоронні органи ширшим асортиментом інструментів та методів.

Серед основних викликів ЄС в протидії кіберзлочинності також стало і поширення криптовалюти. Багато інвесторів звернули увагу на криптовалюту після її різкого зростання в ціні наприкінці 2017 року. Наприклад, для біткоїна кількість транзакцій збільшилась до понад 300 000 євро на день. Не дивно, що таким видом розрахунків зацікавились і злочинці для проведення незаконних транзакцій. Зловживання біткоїном досі є одним з основних факторів, що допомагають кіберзлочинності в Інтернеті (до прикладу, для покупки чи оренди інструментів для кіберзлочинів), проте є і інші валюти, що орієнтовані на анонімність (Monero), і які від 2017 року все частіше використовуються в цифровому андеграунді. Зараз для вирішення цієї проблеми ЄС зокрема встановлює партнерські стосунки з біржами криптовалюти та платіжними системами та проводить щорічну конференцію з віртуальних валют [Europol 2019].

Одним з кроків на шляху вирішення цього виклику також став законопроект про регулювання криптовалют MiCA (Markets in Crypto Assets). Законопроект отримав підтримку багатьох країн ЄС. Зокрема, Президент Франції Еммануель Макрон висловив підтримку такому кроку, оскільки сам він «не вірить у саморегульований фінансовий сектор». На думку політика, «Саме державні органи мають визначити правильні умови, які дозволять сектору впевнено розвиватися, заохочуючи інновації» [Мінфін (регулювання криптовалют) 2022]. 5 жовтня 2022 року члени Ради ЄС підписали текст законопроекту, який зобов’язує всіх постачальників послуг криптоактивів дотримуватись чітких норм та вимог, що будуть спрямовані на захист споживачів [MiCA 2022].

Проте, низка питань досі залишається невирішеними, оскільки все частіше проведення операцій з криптовалютою веде до розширення бази потенційних жертв.

Ще більш актуальним для ЄС це питання постало після початку повномасштабного воєнного наступу Росії на Україну та запровадження санкцій щодо країни-агресора, оскільки росіяни мають змогу обходити санкції саме за допомогою криптовалюти. В березні 2022 року Європейський центрбанк висловив стурбованість такою ситуацією [Financial Times 2022]. Також варто згадати, що криптовалюта вже легалізована в Україні від 16 березня 2022 року після підписання закону «Про віртуальні активи», який вступить в силу після змін в Податковому кодексі [Мінфін (закон про криптовалюту) 2022].

Втрата локації є ще одним важливим викликом для ЄС в боротьбі з кіберзлочинністю, оскільки через часте використання шифрування та здійснення криптовалютних транзакцій правоохоронним органам важче визначити фізичне місцезнаходження кіберзлочинця, злочинної організації чи доказів. Крім того, в таких ситуаціях важко встановити країну, що має юрисдикцію і правову базу для регулювання збору доказів. Більш того, зберігання даних в хмарних сховищах означає, що фізично вони можуть знаходитись в різних юрисдикціях.

17 квітня 2018 року Європейською Комісією було висунуто Пропозицію про електронні докази, яка досі перебуває на стадії обговорення [Europol 2019]. Відкритим залишається питання міжнародної правової бази для прямого транскордонного доступу до інформації.

Серйозною завадою на шляху до ефективної протидії кіберзлочинності є різниця між національними правовими системами держав-членів ЄС та міжнародними інструментами, оскільки перенесення останніх в національне законодавство є неповним.

Серед основних відмінностей – є відмінність у визначенні криміналізації поведінки та положень про розслідування кіберзлочинів та збору електронних доказів. Наприклад, у різних держав ЄС різні покарання та заходи в боротьбі з шахрайством, що пов’язане з безготівковими платіжними засобами. Через швидкий розвиток географії та розмаїття кіберзагроз, адаптація нормативно-правової бази є надзвичайно складним завданням. Ефективним інструментом для компенсації відсутності відповідного законодавства могла б бути судова практика (прецедентне право), проте поки що не існує достатньо прецедентів для ліквідації чи хоча б контролю кіберзлочинності [Europol 2019].

Схожа ситуація склалась і по відношенню до спеціального законодавства, яке б конкретніше регулювало дії правоохоронних органів в кіберсередовищі. Спільні оперативні дії, як от усунення масштабних бот-мереж чи підпільних злочинних форумів, могли б стати більш ефективними завдяки гармонізації відповідного законодавства на рівні ЄС.

Цей виклик стає все більш нагальним у зв’язку з посиленням заходів з безпеки злочинцями у «темній мережі» (дворівнева аутентифікація, зашифровані повідомлення тощо) після успішних операцій правоохоронних органів з закриття величезних незаконних онлайн-ринків Hansa Market та AlphaBay, а також RAMP влітку 2017 року [Саєнко 2021].

На даний час ЄС вже прийняв низку заходів для подолання даного виклику. Наприклад, розробляється Дорожня карта щодо скоординованого підходу правоохоронних органів ЄС у боротьбі зі злочинністю в «темній мережі» (Dark Web); більш того, при Європолі була створена нова група з питань «темної мережі». Також поступово відбуваються зміни у національному законодавстві, наприклад, у США прийнято Закон «Про хмарні технології» [Europol 2019]. Проте відкритим залишається питання розробки загальноєвропейської правової бази для проведення кіберрозслідувань, зокрема в Deep Web («глибокій мережі») і Dark Web.

Серед труднощів в міжнародному співробітництві ЄС в боротьбі з кіберзлочинністю існують виклики, що пов’язані з взаємною правовою допомогою. Причиною таких викликів є відсутність єдиної правової бази для швидкої передачі та отримання (а також збереження) доказів. На практиці це проявляється в ситуаціях, коли навіть при наявності збережених доказів проходить дуже багато часу до того моменту, коли вони будуть надані запитуючій країні для кримінального розслідування. Навіть наявність Європейського ордеру для проведення конкретного розслідування не забезпечує потрібну для збору доказів швидкість. Більш того, Директива про Європейський ордер на проведення розслідування (Директива 2014/41/ЄС Європейського Парламенту та Ради від 3 квітня 2014 року Про європейський ордер на розслідування в кримінальних справах) не передбачає конкретних механізмів, що сприяли б пришвидшеному збору електронних доказів. Безумовно, необхідно розробити більш налагоджену систему для розслідування, запобігання та захисту від кіберзлочинів, а також яка б гарантувала надання взаємної правової допомоги запитуючої країни. Велике значення в цьому контексті може мати встановлення розмежування між запитами на отримання інформації, котрі повинні бути оформлені у відповідності з процедурою надання взаємної допомоги, та запитами, які такої процедури зазвичай не потребують (наприклад, прямий запит даних в постачальників електронних послуг в США). Коли така кооперація здійснюється в межах спільної слідчої групи, то відповідні органи можуть проводити транснаціональні слідчі дії та обмін доказами без потреби перенаправлення додаткових офіційних запитів.

Згідно зі звітом Європолу та Євроюсту, теперішні відмінності в правових системах та неефективна міжнародна співпраця можуть стати причиною появи «гарячих точок» кіберзлочинності та віртуальних «безпечних гаваней», в яких кримінальне розслідування чи збирання доказів буде практично неможливим [Europol 2019].

Для подолання цих викликів проводяться переговори щодо законодавчої пропозиції Європейської Комісії від 17 квітня 2018 року про електронні докази де пропонується запровадження нових інструментів для прямого транскордонного співробітництва з постачальниками послуг (Пропозиція до Регламенту Європейського Парламенту та Ради ЄС Про європейський ордер на пред’явлення та збереження електронних доказів у кримінальних справах COM/2018/225 фінал - 2018/0108 (COD)). Також розробляється захищений онлайн-портал для обміну слідчими даними та електронними доказами в межах ЄС. Європол спільно з Євроюстом запустили проект SIRIUS який має допомагати в інтернет-розслідуваннях та спрощувати доступ до електронних доказів.

Складним викликом для ЄС є і реагування на великомасштабні кібератаки. WannaCry і NotPetya – дві транскордонні кібератаки безпрецедентного масштабу – довели, що реагування на великі кібератаки, яке ґрунтується на минулих інцидентах, є недостатньо ефективним в протистоянні швидкозмінним методам кіберзлочинців [Bendiek 2021]. Цікаво, що від цих двох атак одночасно постраждали безліч галузей в різноманітних регіонах; вражала і швидкість проведення атак. Саме ці дві атаки дали поштовх до удосконалення законодавства в сфері міжнародного співробітництва для боротьби з кіберзлочинністю. Фундаментальне значення має раннє залучення правоохоронних та судових органів до розслідування масштабних кіберінцидентів. Їх активна участь у тренуваннях та навчаннях з імітацією кіберзагроз також має велике значення, оскільки сприяє зміцненню довіри та співробітництва з мережевою та інформаційною спільнотою з питань інформаційної безпеки.

Для вирішення цього виклику, у вересні 2017 року було опубліковано План скоординованого реагування на великомасштабні транскордонні інциденти та кризи у сфері кібербезпеки (проте він ще досі не введений в дію), а в травні 2018 року було підписано Спільний Меморандум про взаєморозуміння між Європолом, ENISA (European Network and Information Security Agency – Європейська агенція мережевої та інформаційної безпеки), EDA (European Defence Agency – Європейське оборонне агенство) та CERT-EU (Computer Emergency Response Team – Команда реагування на комп’ютерні надзвичайні ситуації). В березні 2019 року було ухвалено Протокол реагування правоохоронних органів ЄС на надзвичайні ситуації (в тому числі широкомасштабні транскордонні кібератаки). Центральна роль в такій діяльності згідно з протоколом відводиться Європейському центру Європолу по боротьбі з кіберзлочинністю [Марущак 2018].

Ще однією групою викликів, яка була виокремлена у Спільному звіті Європолу та Євроюсту є виклики публічно-приватного партнерства. Таке партнерство має відігравати ключову роль у зниженні кіберзлочинності. Левова доля доказів кіберзлочинів зберігається у приватному секторі, а ліквідація кримінальної інфраструктури приватними особами, усунення незаконного контенту та сповіщення правоохоронних органів про витоки даних є одним з найбільш ефективних заходів для протидії кіберзлочинності. Також публічно-приватне партнерство відіграє ключову роль у боротьбі з кіберзлочинністю та підвищенні кібербезпеки шляхом запобігання таких видів злочинів та обізнаності про них. Тим не менш, досі немає єдності у думках щодо необхідної нормативно-правової бази для довірчої співпраці з приватним сектором, яка б одночасно регулювала питання прозорості, пов’язані з такою кооперацією.

Часто ЄС також звинувачується в надмірній бюрократизації та відсутності балансу в практичному розвитку систем кіберзахисту та виділенні коштів на програми організаційно-управлінської складової забезпечення кібербезпеки [Грубінко 2021].

ENISA, як агентство ЄС, на яке покладена функція виявлення та запобігання кібератакам [Саєнко 2021], 3 листопада 2022 року опублікувала десяте видання щорічного звіту про стан загроз кібербезпеки (ENISA Threat Landscape – ETL) [ENISA 2022]. В цьому документі описуються ключові загрози та їх тенденції, також вказуються необхідні заходи для протидії кіберзлочинам. В створенні звіту цього року також приймала участь спеціальна робоча група ENISA з питань ландшафту загроз кібербезпеці.

В порівнянні з минулорічним звітом спостерігаються певні зміни в основних загрозах. Наприклад, в цьогорічному звіті відсутні криптоджекінг та загрози, пов’язані з електронною поштою; натомість, до списку додались загрози, пов’язані з соціальною інженерією.

В звіті відзначається і вплив геополітики на кіберзагрози, зокрема конфлікт між Росією та Україною. В цьому контексті спостерігається нова хвиля хактивізму (англ. hacktivism – словозлиття від хакер і активізм) – просування політичних ідей за допомогою мережі Інтернет. У звіті, випадок з «Інформаційною армією України», створеною 26 лютого 2022 року міністром цифрової трансформації України Михайлом Федоровим, називається унікальним, зважаючи на труднощі в її класифікації: адже таку армію можна вважати і групою добровольців-хактивістів, так і групою, що підтримується державою або гібридною групою. Заява міністра була звернена до добровольців, які координували свої дії на кіберфронті через Telegram-канал. Вони здебільшого проводили атаки типу DDoS (denial-of-service attack – атаки на відмову в обслуговуванні) [Foreign Policy 2022].

Варто зазначити, що на момент вторгнення російських військ в Україні не існувало військового органу, який би міг керувати такими діями. У зв’язку з цим Україна була вимушена створити гібридну структуру, яку важко класифікувати через різноманітність її складу – українські військовослужбовці, українські та закордонні цивільні громадяни, а також, навіть, приватні компанії. Наприклад, компанія Microsoft підтримала українських посадовців з питань кібербезпеки у боротьбі зі шкідливим програмним забезпеченням FoxBlade, а також допомогла з розвідувальними та інформаційними звітами про російські кібероперації [DW 2022]. Досі ведуться дискусії щодо обов’язків та ролі приватних компаній в майбутніх кіберопераціях.

Більш того, конфлікт в Україні поляризував світовий кіберпростір: з’явились проукраїнські та прокремлівські хакери. ЄС, як і більшість його країн-членів, в цьому конфлікті стали на сторону України, таким чином піддавши себе ризику хакерських атак зі сторони країни-агресора. Проросійські хакерські колективи (наприклад, Killnet) здійснили кібератаки як на українські, так і на європейські організації та офіційні веб-сайти, що було підтверджено 10 травня 2022 року керівником Центру урядового зв’язку Великої Британії Джеремі Флемінгом [The Guardian. Sabbagh 2022].

**Висновки.** Отже, боротьба з кіберзлочинністю в ЄС є надзвичайно динамічною та нестабільною сферою, виклики в якій досить важко регулювати та передбачити. Згідно з офіційними звітами спеціалізованих органів та агенцій ЄС за 2019–2022 роки, під час протидії кіберзлочинності організація найчастіше стикається з викликами, пов’язаними з втратою даних чи локації, національно-правовими рамками, а також труднощами в міжнародному співробітництві та державно-приватному партнерстві. Незважаючи на те, що ці виклики та загрози досить швидко виявляються та ретельно моніторяться, процес прийняття заходів щодо їх усунення зазвичай досить повільний. Надмірна схильність ЄС до бюрократизації також відзначається дослідниками, як один з викликів в ефективній боротьбі з кіберзлочинністю. Згідно з звітом ENISA, протягом останнього року все більше кіберзагроз для ЄС було пов’язано з геополітичним чинником, а саме військовим конфліктом в Україні.

**ЛІТЕРАТУРА:**

Борисюк О. (2022). Кібер-ризики та їх страхування в сучасних умовах. *Трансформація національної, закордонної моделей економічного розвитку та законодавства в умовах воєнного часу*: матеріали ІІІ міжн. наук.-практ. конф., 27–29 червня 2022 р. Луцьк : ВНУІЛУ,. 159–161.

Грубінко А. (2021). Особливості формування політики кібербезпеки Європейського Союзу: правові аспекти. *Актуальні проблеми правознавства.* Вип. 1. С. 5–10.

Марущак А. І. (2018). Міжнародне співробітництво у боротьбі з транснаціональною кіберзлочинністю. *Інформація і право*. Вип. 3. С. 104–110

Мінфін (закон про криптовалюту) (2022*).* В Україні остаточно легалізували криптовалюту: Зеленський підписав закон. [Електронний ресурс]. Режим доступу: <https://minfin.com.ua/ua/2022/03/16/82176211/> (дата звернення: 08.11.2022).

Мінфін (регулювання криптовалют) (2022). Макрон підтримав регулювання криптовалют у ЄС. [Електронний ресурс]. Режим доступу: <https://minfin.com.ua/ua/2022/04/22/84201072/> (дата звернення: 08.11.2022).

Могілевський Л. В. (2021) Кіберзлочинність у проєкті Європолу SOCTA. *Протидія кіберзлочинності та торгівлі людьми* : зб. матеріалів міжнарод. наук.-практ. конф., 18 травня 2021 р. Харків : ХНУВС, С. 16–18.

Саєнко М. І., Савела Є. А., Тополянський Ю. (2021) Міжнародний досвід протидії кіберзлочинності та кібершахрайству. *Науковий вісник Ужгородського Національного Університету, Серія Право.* 2021. Вип. 64. С. 386–391.

ВВС (2022). AlphaBay and Hansa dark web markets shut down. [Електронний ресурс]. Режим доступу: <https://www.bbc.com/news/technology-40670010> (дата звернення: 08.11.2022).

Bendiek A., Schulze M. (2021). Attribution: A major challenge for EU cyber sanctions. An analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the attack on the OPCW. *Stiftung Wissenschaft und Politik.* № 11.

*DW*. (2022) Ukraine: Microsoft reports malware after cyberattack. [Електронний ресурс]. Режим доступу: <https://www.dw.com/en/ukraine-microsoft-reports-destructive-malware-after-cyberattack/a-60440990> (Last accessed: 08.11.2022).

ENISA (2022). Threat Landscape. [Електронний ресурс]. Режим доступу: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022> (Last accessed: 08.11.2022).

Europol. (2019) Common challenges in combating cybercrime: As identified by Eurojust and Europol. [Електронний ресурс]. Режим доступу: <https://www.europol.europa.eu/cms/sites/default/files/documents/common_challenges_in_combating_cybercrime_2018.pdf> (Last accessed: 08.11.2022).

*Europol* (ІOCTA). (2022). Internet Organised Crime Threat Assessment [Електронний ресурс]. Режим доступу: <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment> (Last accessed: 08.11.2022).

*Financial Times*. (2022). Ukraine war latest from March 22: US and European allies to escalate Russia sanctions, Ukraine urges international banks to leave Russia. [Електронний ресурс]. Режим доступу: <https://www.ft.com/content/795b432f-b189-4c91-b202-bbcb2c8b655a> (Last accessed: 08.11.2022).

Foreign Policy. (2022). Don’t underestimate Ukraine’s volunteer hackers. [Електронний ресурс]. Режим доступу: https://foreignpolicy.com/2022/04/11/russia-cyberwarfare-us-ukraine-volunteer-hackers-it-army/ (Last accessed: 08.11.2022).

MiCA (2022). Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 [Електронний ресурс]. Режим доступу: <https://data.consilium.europa.eu/doc/document/ST-13198-2022-INIT/en/pdf> (Last accessed: 08.11.2022).

Rojszczak M. (2021). The uncertain future of data retention laws in the EU: Is a legislative reset possible? *Computer Law & Security Review*. Vol. 41.

*The Guardian.* Sabbagh D. (2022). Russian hackers targeting opponents of Ukraine invasion, warns GCHQ chief.  [Електронний ресурс]. Режим доступу: <https://www.theguardian.com/technology/2022/may/10/russian-hackers-targeting-opponents-of-ukraine-invasion-warns-gchq-chief> (Last accessed: 08.11.2022).

**References**

BBC (2022).AlphaBay and Hansa dark web markets shut down. Retrieved from <https://www.bbc.com/news/technology-40670010>

Bendiek A., Schulze M. (2021). Attribution: A major challenge for EU cyber sanctions. An analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the attack on the OPCW. Stiftung Wissenschaft und Politik. № 11.

Borysiuk O. (2022). Kiber-ryzyky ta yikh strakhuvannia v suchasnykh umovakh [Cyber risks and their insurance in modern conditions]. *Transformatsiia natsionalnoi, zakordonnoi modelei ekonomichnoho rozvytku ta zakonodavstva v umovakh voiennoho chasu: materialy III mizhn. nauk.-prakt. konf.* (pp. 159–161). Lutsk: VNUILU. [in Ukrainian].

DW (2022).Ukraine: Microsoft reports malware after cyberattack.Retrieved from <https://www.dw.com/en/ukraine-microsoft-reports-destructive-malware-after-cyberattack/a-60440990>

ENISA (2022). Threat Landscape. Retrieved from <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022>

Europol (2019). Common challenges in combating cybercrime: As identified by Eurojust and Europol. 2019.  Retrieved from <https://www.europol.europa.eu/cms/sites/default/files/documents/common_challenges_in_combating_cybercrime_2018.pdf>

Europol (IOCTA) (2022). Internet Organised Crime Threat Assessment (IOCTA). Retrieved from <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment>

Foreign Policy (2022). Don’t underestimate Ukraine’s volunteer hackers. Retrieved from https://foreignpolicy.com/2022/04/11/russia-cyberwarfare-us-ukraine-volunteer-hackers-it-army/

Financial Times (2022). Ukraine war latest from March 22: US and European allies to escalate Russia sanctions, Ukraine urges international banks to leave Russia. Retrieved from <https://www.ft.com/content/795b432f-b189-4c91-b202-bbcb2c8b655a>

Hrubinko A. (2021). Osoblyvosti formuvannia polityky kiberbezpeky yevropeiskoho soiuzu: pravovi aspekty [Peculiarities of cybersecurity policy formation in the European Union: legal aspects]. *Aktualni problemy pravoznavstva.* Vyp. 1. P. 5–10. [in Ukrainian].

Marushchak A. I. (2018). Mizhnarodne spivrobitnytstvo u borotbi z transnatsionalnoiu kiberzlochynnistiu [International cooperation in combating transnational cybercrime.]. *Informatsiia i pravo*. Vyp. 3. P. 104–110. [in Ukrainian].

MiCA (2022). Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937. Retrieved from <https://data.consilium.europa.eu/doc/document/ST-13198-2022-INIT/en/pdf>

Minfin (cryptocurrency law) (2022). V Ukraini ostatochno lehalizuvaly kryptovaliutu: Zelenskyi pidpysav zakon [Ukraine finally legalized cryptocurrency: Zelensky signed the law]. Retrieved from <https://minfin.com.ua/ua/2022/03/16/82176211/> [in Ukrainian].

Minfin (regulation of cryptocurrencies) (2022). Makron pidtrymav rehuliuvannia kryptovaliut u YeS [Macron supported the regulation of cryptocurrencies in the EU]. Retrieved from <https://minfin.com.ua/ua/2022/04/22/84201072/> [in Ukrainian].

Mohilevskyi L. V. (2021). Kiberzlochynnist u proiekti Yevropolu SOCTA [Cybercrime in the Europol SOCTA project]. *Protydiia kiberzlochynnosti ta torhivli liudmy* : zb. materialiv mizhnarod. nauk.-prakt. konf. (pp. 16–18). Kharkiv : KhNUVS. [in Ukrainian].

Saienko M. I., Savela Ye. A., Topolianskyi Yu. (2021). Mizhnarodnyi dosvid protydii kiberzlochynnosti ta kibershakhraistvu [International experience in combating cybercrime and cyber fraud]. *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu, Seriia Pravo*. Vyp. 64. P. 386–391. [in Ukrainian].

Rojszczak M. (2021). The uncertain future of data retention laws in the EU: Is a legislative reset possible? *Computer Law & Security Review*. Vol. 41.

The Guardian Sabbagh D. (2022). Russian hackers targeting opponents of Ukraine invasion, warns GCHQ  chief.  Retrieved from<https://www.theguardian.com/technology/2022/may/10/russian-hackers-targeting-opponents-of-ukraine-invasion-warns-gchq-chief>