ДВНЗ «Прикарпатський національний університет імені Василя Стефаника»

Кафедра безпеки життєдіяльності

Збірник статей
на тему «Інформаційна безпека в реаліях сьогодення»

Дисципліна «Безпека життєдіяльності і цивільний захист»

Івано-Франківськ

2018

План

1. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам / У. Ільницька // Humanitarian vision. - 2016. - Vol. 2, Num. 1. - С. 27-32. - Режим доступу: http://nbuv.gov.ua/UJRN/hv_2016_2_1_7
2. Боднар І. Р. Інформаційна безпека як основа національної безпеки / І. Р. Боднар // Mechanism of Economic Regulation. - 2014. - № 1. - С. 68-75. - Режим доступу: http://nbuv.gov.ua/UJRN/Mre_2014_1_8
3. Єсімов С. С. Використання інформаційних технологій як предмет адміністративно-правового регулювання / С. С. Єсімов // Вісник Національного університету "Львівська політехніка". Юридичні науки. - 2015. - № 827. - С. 24-29. - Режим доступу: http://nbuv.gov.ua/UJRN/vnulpurn_2015_827_6
4. Мехед Д. Інформаційна безпека в соціальних мережах. Методи поширення інформації в соціальних мережах / Дмитро Мехед // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науково-технічний збірник. – 2015. – Вип. 2(30). – С. 14-18.
5. Варивода К. С. Інформаційна безпека підлітків в Інтернет мережі / К. С. Варивода // Молодий вчений. - 2016. - № 3. - С. 365-368. - Режим доступу: http://nbuv.gov.ua/UJRN/molv_2016_3_87
6. Мікаел Кроґерус, Ганнес Ґрассуґґер «Я ТІЛЬКИ ПОКАЗАВ, ЩО ІСНУЄ БОМБА» //Інтернет видання «Збруч» . - Режим доступу: https://zbruc.eu/node/59714

Vol. 2, No. 1, 2016

УДК: 329.09.5

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ: СУЧАСНІ ВИКЛИКИ, ЗАГРОЗИ ТА МЕХАНІЗМИ ПРОТИДІЇ НЕГАТИВНИМ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИМ ВПЛИВАМ

Ільницька Уляна
Національний університет "Львівська політехніка"

(стаття надійшла до редколегії – 1.03.2016 р., прийнята до друку – 27.04.2016 р.)

Досліджено проблему інформаційної безпеки України та захисту національного інформаційного простору від негативних пропагандистсько-маніпулятивних інформаційно-психологічних впливів. Проаналізовано теоретичні підходи до визначення сутності поняття інформаційна безпека; всебічно досліджено види реальних і потенційних інформаційних загроз для медіапростору України, охарактеризовано специфіку експансіоністської політики Російської федерації проти України; надано практичні рекомендації щодо вдосконалення державної інформаційної політики та створення ефективної системи інформаційної безпеки України.

***Ключові слова**: інформаційна безпека України, національний інформаційний простір; інформаційні загрози; інформаційно-психологічні впливи; інформаційна експансія, інформаційні війни та операції; механізми протидії інформаційним загрозам; державна інформаційна політика.*

INFORMATION SECURITY OF UKRAINE: MODERN CHALLENGES, THREATS AND MECHANISMS OF COUNTERACTING NEGATIVE INFORMATION-PSYCHOLOGICAL INFLUENCES

Uljana Ilnytska

The article is devoted to the topical issue of Ukrainian information security and protection of the national information space from negative propagandistic and manipulative information-psychological impacts. It is emphasized that the problem is actualized under conditions of the Ukraine-Russia conflict when ensuring information security turns into a factor of preserving national identity of Ukraine and its functioning as a sovereign independent state.

The article is an attempt to analyze theoretical approaches to defining the nature of such notions as information security and a threat to information security. Particular attention is paid to investigation of information expansion by the Russian Federation aimed at securing its domination within the Ukrainian media space. Technologies of Russian information-psychological operations based on biased and tendentious coverage of facts and phenomena, distortion, misrepresentation, and miscommunication of information are analyzed.

The article comprehensively studies types and kinds of real and potential information threats to media space of Ukraine and Ukrainian sovereignty; analyzes mechanisms of exerting negative propagandistic information-psychological influences. Particular attention is paid to methods of national information space protection, counteraction to wide-scale information-psychological influences, wars and operations. The research introduces developed recommendations concerning formation of strategic directions of the state policy in the sphere of ensuring Ukrainian information security, improving normative and legal basis for preserving information sovereignty of Ukraine, protecting its national space.

***Key words**: information security of Ukraine, national information space; information threats; information-psychological influences; information expansion, information wars and operations; mechanisms of information threats counteraction; state information policy.*

В умовах сучасних глобальних та регіональних інформаційних протистоянь, деструктивних комунікативних впливів, зіткнення різновекторних національних інформаційних інтересів, поширення інформаційної експансії та агресії, захист національного інформаційного простору та гарантування інформаційної безпеки стають пріоритетними стратегічними завданнями сучасних держав у системі глобальних інформаційних відносин. Збереження інформаційного суверенітету, формування ефективної системи безпеки в інформаційній сфері є *актуальною проблемою* і для України, яка часто є

об'єктом зовнішньої інформаційної експансії, маніпулятивних пропагандистських технологій та руйнівного інформаційного вторгнення. В умовах російсько-українського конфлікту захист національного інформаційного простору від негативних інформаційно-психологічних впливів, операцій та війн, гарантування інформаційної безпеки та інформаційного суверенітету набувають особливого значення і стають чинниками збереження національної ідентичності України та функціонування її як суверенної та незалежної держави.

Інформаційну безпеку, проблеми захисту національного інформаційного простору досліджували багато науковців. Зокрема, проблему відображено у працях А. Марущака, В. Петрика, В. Ліпкана, Б. Кормича, В. Почепцова та інших фахівців. Проблемні питання забезпечення кібернетичної безпеки досліджували Р. Лук'янчук, В. Бурячок, А. Бабенко, В. Гавловский, Д. Дубов, В. Номоконов, М. Погорецький, В. Шеломенцев та інші науковці. Однак у працях вищезазначених фахівців інформаційна безпека досліджувалась, радше, як складова національної безпеки, її невід'ємний компонент. Поза увагою науковців залишились проблеми чіткого окреслення інформаційних загроз, вивчення їхніх джерел, всебічне дослідження технологій ведення інформаційно-психологічних війн і операцій, а також визначення та обґрунтування методів протидії інформаційно-психологічним негативним впливам.

Зважаючи на вищевикладені малодосліджені аспекти проблеми інформаційної безпеки, *метою* статті є всебічне дослідження проблеми гарантування інформаційної безпеки України, захисту національного інформаційного простору з огляду на реальні й потенційні загрози та деструктивні пропагандистсько-маніпулятивні інформаційні впливи. *Завданнями* статті є: характеристика та аналіз реальних та потенційних загроз інформаційній безпеці України; окреслення сутності понять інформаційна безпека держави, інформаційні загрози; визначення ступеня інформаційних загроз національному простору України; аналіз особливостей та специфіки експансіоністської політики Російської федерації проти України; надання практичних рекомендацій щодо вдосконалення державної інформаційної політики та створення ефективної системи інформаційної безпеки України.

Інформаційна безпека є інтегрованою складовою національної безпеки і її розглядають як пріоритетну функцію держави. Інформаційна безпеки, з одного боку, передбачає забезпечення якісного всебічного інформування громадян та вільного доступу до різних джерел інформації, а з іншого – це контроль за непоширенням дезінформації, сприяння цілісності суспільства, збереження інформаційного суверенітету, протидія негативним інформаційно-психологічним пропагандистським впливам та захист національного інформаційного простору від маніпуляцій, інформаційних війн та операцій. Рішення комплексної проблеми інформаційної безпеки дасть змогу як захистити інтереси суспільства і держави, так і гарантувати права громадян на отримання всебічної, об'єктивної та якісної інформації.

Існує два аспекти трактування інформаційної безпеки у контексті національної безпеки. З одного боку, інформаційну безпеку розглянуто як самостійний елемент національної безпеки будь-якої країни, а з іншого – інтегрована складова будь-якої іншої безпеки: військової, економічної, політичної тощо. Найповнішим є таке визначення: інформаційна безпека – це стан захищеності життєво важливих інтересів особистості, суспільства і держави, за якого зводиться до мінімуму завдання збитків через неповноту, невчасність і недостовірність інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації [5]. Це визначення є оптимальним та відображає усі аспекти взаємодії суб'єктів інформаційних відносин.

Увага до проблем гарантування інформаційної безпеки України зумовлена антиукраїнськими впливами, які пропагують ідеї сепаратизму, насильства, національної ворожнечі і є спробами руйнування національної ідентичності України, знищення міжнаціональної злагоди, посягання на конституційний лад України, територіальну цілісність держави. Проблема гарантування інформаційної безпеки України актуалізується в умовах війни на Сході, коли з боку Російської Федерації відбувається інформаційна експансія, упереджене та тенденційне висвітлення фактів та явищ, а технології російських інформаційно-психологічних операцій спрямовані на забезпечення домінування в українському (а також у глобальному) інформаційному просторі та на утримання медійної переваги. Через російські пропагандистські інформаційно-психологічні кампанії, акції, медіазаходи відбувається вплив не лише на суспільну свідомість громадян України, а й на світову громадськість.

Представник об'єднання "Інформаційний спротив" В. Гусаров, досліджуючи проблему інформаційної безпеки України, наголошує, що Росія здійснює інформаційно-психологічні атаки, щоб активізувати ескалацію конфлікту на сході України, чинити тиск на українське керівництво з метою

змусити його погодитись на московський сценарій урегулювання конфлікту. В. Гусаров виокремлює напрями інформаційно-психологічних атак проти України: 1) нав'язування думок про неспроможність української влади керувати державою та приймати раціональні рішення; 2) формування негативних суджень про воєнно-політичне керівництво України та про те, що хаотичні бойові дії призводять до невиправданих жертв серед сил АТО; 3) поширення поглядів про те, що українська армія на Сході України деморалізована та неспроможна вести бойові дії, а також про недовіру особового складу до керівництва; 4) нав'язування думки про те, що Україна не обійдеться без російського газу та що сторонам необхідно повернутися до перегляду газових контрактів. Експерт зазначає, що цільовою аудиторією Кремля зараз є населення РФ, російськомовна діаспора за кордоном, населення України, зокрема в окупованих районах Донбасу, громадяни західних країн, а також країн БРІКС та Митного союзу, близькі Росії за політичними поглядами [3].

Україна стала об'єктом інформаційно-психологічних впливів, операцій, війн та її інформаційна безпека опинилась під загрозою. Можна констатувати, що: 1) український інформаційний простір є незахищеним від зовнішніх негативних пропагандистсько-маніпулятивних впливів і стає об'єктом інформаційної експансії; 2) у світовому медіапросторі відсутній український національний інформаційний продукт, що поширював би об'єктивну, неупереджену та актуальну інформацію про події в Україні. Як наслідок – світова громадськість відчуває брак інформації або отримує її з інших джерел, які часом дезінформують, надають викривлену, спотворену, неповну інформацію. Водночас проти України активно застосовується потужний медіаресурс, здійснюється експансія іноземних суб'єктів на ринку інформаційних послуг, активізуються негативні інформаційні впливи, які спрямовані на викривлення реальності, заниження міжнародного іміджу держави; 3) діяльність вітчизняних ЗМІ щодо систематичного, об'єктивного висвітлення фактів, подій та явищ є недостатньою та позбавлена стратегічного планування; інформаційно-комунікативна політика України у сфері національної безпеки потребує невідкладного перегляду та удосконалення.

Рівень інформаційної безпеки держави, значною мірою, зумовлений рівнем її інформаційної інфраструктури. На жаль, як зазначає В. Петрик, низький загальний рівень інформаційної інфраструктури України сприяє експансії іноземними компаніями ринку інформаційних послуг, що створює сприятливі умови для перерозподілу ефірного часу на користь іноземних програм, окремі з яких засмічують український інформаційний простір своїм баченням подій, пропагують спосіб життя та традиції, тим самим деструктивно впливаючи на суспільство і державу, руйнуючи морально-етичні основи генофонду української нації. Недостатній професійний, інтелектуальний і творчий рівень вітчизняного виробника інформаційного продукту та послуг, його неконкурентоспроможність не лише на світовому ринку, а й в Україні, призводить до того, що українська аудиторія, природно, віддає перевагу іноземним інформаційним програмам. Недостатній контроль з боку держави за дотриманням законів України політичними силами, ЗМІ та окремими особами, які займаються підприємницькою діяльністю в інформаційній сфері, призводить до того, що нині трапляються непоодинокі випадки надання ефірного часу теле- та радіопрограмам, спрямованим на руйнування моральних цінностей, свідомості української нації [13].

Отже, національний інформаційний простір України, на жаль, зазнає суттєвих загроз, викликів, які становлять небезпеку функціонування держави, її політичного та економічного розвитку, інтеграції у європейські та євроатлантичні структури.

Загрози національній безпеці України в інформаційній сфері це – сукупність умов та чинників, які становлять небезпеку життєво важливим інтересам держави, суспільства і особи через можливість негативного інформаційного впливу на свідомість та поведінку громадян, а також на інформаційні ресурси та інформаційно-технічну інфраструктуру [13].

Як зазначено у Законі України "Про основи національної безпеки" однією з основних загроз інформаційній безпеці є "намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації" [16]. У Доктрині інформаційної безпеки України, визначено такі загрози інформаційній безпеці країни: поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України; зовнішні деструктивні інформаційні впливи на суспільну свідомість через ЗМІ , а також мережу Інтернет; деструктивні інформаційні впливи, які спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності та недоторканності України; прояви сепаратизму в ЗМІ, а також у мережі Інтернет за етнічною, мовною, релігійною та іншими ознаками [4].

Як зазначає Р. Р. Марутян, найсуттєвішою загрозою національній безпеці України в інформаційній

сфері є здійснення іноземними державами негативного інформаційно-психологічного впливу на суспільну свідомість громадян України та світову громадськість через проведення інформаційних акцій та кампаній, спеціальних інформаційних операцій. Це відбувається через систематичне поширення тенденційної, неповної або упередженої інформації про Україну та політичні процеси, що відбуваються на її теренах. Усе це впливає на зовнішню та внутрішню політику нашої держави, знижує її міжнародний імідж, має політичне та економічне підґрунтя. Метою таких інформаційних операцій є забезпечення власних національних інтересів інших держав [10].

До загроз національній безпеці України в інформаційній сфері також варто зарахувати: прояви обмеження свободи слова та доступу громадян до інформації; викривлення, спотворення, блокування, замовчування упереджене та тенденційне висвітлення інформації; несанкціоноване її поширення; відкриту дезінформацію; інформаційну експансію з боку інших держав та руйнівне інформаційне вторгнення у національний інформаційний простір, коли країни з потужнішим інформаційним потенціалом отримали можливість розширити свій вплив через ЗМІ на населення і громадськість менш потужної держави; виникнення і функціонування у національному інформаційному просторі держави непідконтрольних й інформаційних потоків; поширення засобами масової інформації культу насильства, жорстокості; повільність входження України у світовий інформаційний простір; невиваженість державної інформаційної політики та відсутність необхідної інфраструктури в інформаційній сфері; розміщення дезінформації в Інтернеті.

Варто наголосити, що проти України з боку Російської федерації ведеться інформаційна війна, яка спрямована на нав'язування певних ідеологічних стереотипів, тієї чи іншої суспільної думки за допомогою засобів масової інформації, зокрема через електронні видання [12]. Війни такого типу є досить поширеними у глобальному інформаційному просторі та їх всебічно досліджують науковці та фахівці. Зокрема, Інститут національно-стратегічних досліджень США та деякі західні експерти і вчені виокремлюють кілька складових елементів інформаційної війни. Один із них – ведення психологічної війни. Головне завдання психологічної війни полягає в маніпулюванні масами. Метою такої маніпуляції є: внесення в суспільну та індивідуальну свідомість ворожих ідей та поглядів; дезорієнтація та дезінформація мас; послаблення певних переконань, залякування народу образом ворога; залякування супротивника власною могутністю [2].

У сучасному глобалізованому інформаційному суспільстві, де кіберпростір перетворюється на поле боротьби, вагомими загрозами інформаційній безпеці держави (і України, зокрема) є комп'ютерна злочинність, кібертероризм, кібервійни, які передбачають протистояння національних інтересів у просторі Інтернету, застосування комп'ютерних та інтернет-технологій для нанесення шкоди супротивнику. Найчастіше технології кібервійни, кібертероризму спрямовані на сферу державної безпеки й оборони і становлять реальну загрозу суверенітету держави.

Отже, проти України широко використовують сучасні технології негативних інформаційно-психологічних впливів, які стають загрозою українському національному інформаційному простору та суверенітету держави. Гарантування інформаційної безпеки України в умовах дестабілізвальнчих негативних інформаційно-психологічних впливів та експансіоністської агресивної інформаційної політики Російської федерації, потребує консолідації зусиль на усіх рівнях державної влади та громадянського суспільства.

Як протидія масштабним негативним інформаційно-психологічним впливам, операціям та війнам, пріоритетними напрямами державної інформаційної політики та важливими кроками з боку владних органів України мають бути: 1) інтеграція України до світового та регіонального європейського інформаційного просторів; 2) інтеграція у міжнародні інформаційні та інформаційно-телекомунікаційні системи та організації; 3) створення власної національної моделі інформаційного простору та забезпечення розвитку інформаційного суспільства; 4) модернізації усієї системи інформаційної безпеки держави та формування й реалізація ефективної інформаційної політики; 5) удосконалення законодавства з питань інформаційної безпеки, узгодження національного законодавства з міжнародними стандартами та дієве правове регулювання інформаційних процесів; 6) розвиток національної інформаційної інфраструктури; 7) підвищення конкурентоспроможності вітчизняної інформаційної продукції та інформаційних послуг; 8) впровадження сучасних інформаційно-комунікативних технологій у процеси державного управління; 9) ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації та коригуванні державної політики в інформаційній сфері.

З метою недопущення інформаційної експансії, діяльність держави в інформаційному просторі має здійснюватись за такими напрямами: 1) реалізація упереджувальної стратегії та тактики (превентивні

заходи); 2) здійснення реагувальної стратегії (оперативне реагування на інформаційні атаки супротивника та активний наступ); 3) захист національного інформаційного простору. Головна ціль – забезпечення домінування та медійної переваги в інформаційному просторі. Крім того, пріоритетними завданнями інформаційних структур владних органів мають бути: контроль за інформаційними потоками; надання об'єктивної, вичерпної інформації, представлення фахових коментарів та пояснень щодо подій; систематичне висвітлення офіційної позиції посадових осіб та політичних лідерів.

Варто зазначити, що з метою захисту національного інформаційного простору, створення ефективної системи забезпечення інформаційної безпеки, з боку української влади здійснюються певні заходи. Зокрема, 14 січня 2015 року Кабінет Міністрів України ухвалив Постанову, згідно з якою створено *Міністерство інформаційної політики України*, пріоритетними завданнями якого є протидія інформаційній агресії з боку Російської федерації; розроблення ефективної стратегії інформаційної політики держави та Концепції інформаційної безпеки України; узгодженість та координація функціонування і діяльності органів державної влади і інформаційній сфері.

З метою протидії негативним впливам інформаційної пропаганди та інформаційних війн, задля нейтралізації та упередження реальних та потенційних загроз в інформаційному просторі України, Рада національної безпеки і оборони України ухвалила рішення *"Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України"*. У документі зазначено, що РНБО, враховуючи необхідність вдосконалення нормативно-правового забезпечення та запобігання й нейтралізації потенційних і реальних загроз національній безпеці в інформаційній сфері, вирішила: розробити і внести на розгляд Верховної Ради України законопроекти про внесення змін до деяких законів України щодо протидії інформаційній агресії іноземних держав, передбачивши, зокрема, визначення механізму протидії негативному інформаційно-психологічному впливу, зокрема забороною ретрансляції телевізійних каналів; посилити контроль за додержанням законодавства з питань інформаційно-психологічної та кібернетичної безпеки; ужити заходів щодо забезпечення поширення у світі об'єктивних відомостей про суспільно-політичну ситуацію в Україні, зокрема, через створення відповідного медіахолдингу для підготовки якісного конкурентоздатного інформаційного продукту; розробити порядок аналізу інформаційних матеріалів іноземних ЗМІ, що мають представництва в Україні, з метою впровадження дієвого механізму акредитації журналістів; ужити заходів до активізації міжнародного співробітництва з питань протидії негативним інформаційно-психологічним впливам та кібернетичній злочинності [15].

Крім вищезазначеного документа, основні напрями державної політики з питань національної безпеки в інформаційній сфері визначені у Законах України "Про основи національної безпеки України", "Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки", у "Доктрині національної безпеки" та в інших нормативно-правових документах.

Отже, в умовах сучасних інформаційних протистоянь, експансіоністської політики Російської федерації, національний інформаційний простір України є недостатньо захищеним від зовнішніх негативних пропагандистських інформаційно-психологічних впливів, загроз. Тому захист інформаційного суверенітету, створення потужної та ефективної системи інформаційної безпеки України, розроблення дієвих стратегій і тактик протидії медіазагрозам повинні стати пріоритетними завданнями органів державної влади та недержавних інститутів.

Актуальність досліджуваної у статті проблематики – незаперечна і потребує поглибленого вивчення. *Перспективами подальших наукових досліджень* є: аналіз зарубіжного досвіду протидії негативним пропагандистсько-маніпулятивним інформаційним впливам, а також глибше дослідження технологій здійснення інформаційних операцій та війн.

1. Бондаренко В. О. Інформаційна безпека сучасної держави: концептуальні роздуми [Електронний ресурс] / В. О. Бондаренко, О. В. Литвиненко. – Режим доступу: http://www.crime-research.iatp.org.ua/library/strateg.htm 2. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення [Електронний ресурс] / Ю. О. Горбань. – Режим доступу: http://www.visnyk.academy. gov.ua/wp-content/uploads/2015/04/20.pdf 3. Гусаров В. Кремль розпочав нову інформаційну операцію проти України [Електронний ресурс] / В.Гусаров. – Режим доступу: http://www.osvita. mediasapiens.ua/material/34281 4. Доктрина інформаційної безпеки України [Електронний ресурс]. – Режим доступу: http://www.zakon3.rada.gov.ua/laws/show/514/2009 5. Захист інформаційної безпеки як функція держави [Електронний ресурс]. – Режим доступу: http://www.mego.info/матеріал/23-захист-інформаційної-безпеки-як-функція-держави 6. Інформаційна безпека держави у контексті протидії інформаційним війнам: Навчальний посібник / за заг. ред. В. Б. Толубка. – К. : НАОУ, 2004. – 315 с. 7. Концепція національної безпеки України [Електронний ресурс]. – Режим доступу: http://www.w1 . c1.rada.gov.ua/pls/zweb2/webproc4_1 8. Кормич Б. А.

Організаційно-правові засади політики інформаційної безпеки України [Текст] : монографія / Б. А. Кормич. – Одеса : Юридична література, 2007.– 471 с. 9. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції [Текст] : навч. посіб. / В. А. Ліпкан, Ю. Є. Макименко, В. М. Желіховський. – К. : КНТ, 2006. 10. Марутян Р. Р. Рекомендації щодо вдосконалення політики забезпечення інформаційної безпеки України [Електронний ресурс] / Р. Р. Марутян. – Режим доступу: http://www.dsaua.org/index.php?option=com_content&view=article&id=198%3A2014-08-13-12-55-48&catid=66%3A2010-12-13-08-48-53&Itemid=90&lang=uk; 11. Медвідь Ф. Інформаційна безпека України: виклики та загрози [Електронний ресурс] / Ф. Медвідь. – Режим доступу: http://www.nato.ru.if.ua/journal/2009-2-28.pdf. 12. Методи інформаційного захисту простору. Інформаційна безпека України [Електронний ресурс]. – Режим доступу: http://www.ua.textreferat.com/referat-7471.html 13. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи [Електронний ресурс] / В. Петрик. – Режим доступу: http://www.justinian.com.ua/article.php?id=3222 14. Почепцов Г. Сучасні інформаційні війни / Г. Почепцов. – К. : Вид.дім "Києво-Могилянська академія", 2015. – 497 с. 15. "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України" Рішення Ради національної безпеки і оборони України від 28 квітня 2014 р. [Електронний ресурс]. – Режим доступу: http://www.zakon5.rada.gov.ua /laws/show/n0004525-14. 16. Про основи національної безпеки України : Закон України // Відомості Верховної Ради України. – 2003. – № 39. – Ст. 351. Із змінами, внесеними згідно із Законом № 3200-IV (3200-15) від 15.12.2005. ВВР. – 2006. – № 14. – Ст. 116.

1. Bondarenko V. O. Informatsiina bezpeka suchasnoi derzhavy: kontseptualni rozdumy [Elektronnyi resurs] / V. O. Bondarenko, O. V. Lytvynenko. – Rezhym dostupu: http://www.crime-research.iatp.org.ua/library/strateg.htm 2. Horban Iu.O. Informatsiina viina proty Ukrainy ta zasoby yii vedennia [Elektronnyi resurs] / Iu. O. Horban. – Rezhym dostupu: http://www.visnyk.academy.gov.ua/wp-content/uploads/2015/04/20.pdf 3. Husarov V. Kreml rozpochav novu informatsiinu operatsiiu proty Ukrainy [Elektronnyi resurs] / V. Husarov. – Rezhym dostupu: http://www.osvita. mediasapiens.ua/material/34281 4. Doktryna informatsiinoi bezpeky Ukrainy [Elektronnyi resurs]. – Rezhym dostupu: http://www.zakon3.rada.gov.ua/laws/show/514/2009 5. Zakhyst informatsiinoi bezpeky yak funktsiia derzhavy [Elektronnyi resurs]. – Rezhym dostupu: http://www.mego.info/material/23-zakhyst-informatsiinoi-bezpeky-iak-funktsiia-derzhavy 6. Informatsiina bezpeka derzhavy u konteksti protydii informatsiinym viinam: Navchalnyi posibnyk / Za zah. red. V. B. Tolubka. – K. : NAOU, 2004. – 315 s. 7. Kontseptsiia natsionalnoi bezpeky Ukrainy [Elektronnyi resurs]. – Rezhym dostupu: http://www.w1.c1.rada.gov.ua/pls/zweb2/webproc4_1 8. Kormych B. A. Orhanizatsiino-pravovi zasady polityky informatsiinoi bezpeky Ukrainy [Tekst]: monohrafiia / B. A. Kormych.– Odesa : Yurydychna literatura, 2007. – 471 s. 9. Lipkan V. A. Informatsiina bezpeka Ukrainy v umovakh yevrointehratsii [Tekst] : Navch. posibn. / V. A. Lipkan, Iu. Ie. Makymenko, V. M. Zhelikhovskyi. – K. : KNT, 2006. 10. Marutian R. R. Rekomendatsii shchodo vdoskonalennia polityky zabezpechennia informatsiinoi bezpeky Ukrainy [Elektronnyi resurs] / R. R. Marutian. – Rezhym dostupu: http://www.dsaua.org/ index.php?option=com_content&view= article&id=198%3A2014-08-13-12-55-48&catid=66%3A2010-12-13-08-48-53&Itemid=90&lang=uk. 11. Medvid F. Informatsiina bezpeka Ukrainy: vyklyky ta zahrozy [Elektronnyi resurs] / F. Medvid. – Rezhym dostupu: http://www.nato.ru.if.ua/journal/2009-2-28.pdf. 12. Metody informatsiinoho zakhystu prostoru. Informatsiina bezpeka Ukrainy [Elektronnyi resurs]. – Rezhym dostupu: http://www.ua.textreferat.com/referat-7471.html 13. Petryk V. Sutnist informatsiinoi bezpeky derzhavy, suspilstva ta osoby [Elektronnyi resurs] / V. Petryk. – Rezhym dostupu: http://www.justinian.com.ua/article.php?id=3222 14. Pocheptsov H. Suchasni informatsiini viiny / H. Pocheptsov. – K. : Vyd.dim "Kyievo-Mohylianska akademiia", 2015. – 497 s. 15. "Pro zakhody shchodo vdoskonalennia formuvannia ta realizatsii derzhavnoi polityky u sferi informatsiinoi bezpeky Ukrainy" Rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 28 kvitnia 2014 r. [Elektronnyi resurs]. – Rezhym dostupu: http://www.zakon5.rada.gov.ua /laws/show/n0004525-14.; 16. Pro osnovy natsionalnoi bezpeky Ukrainy : Zakon Ukrainy // Vidomosti Verkhovnoi Rady Ukrainy. – 2003. – No. 39. – St. – 351. Iz zminamy, vnesenymy zghidno iz Zakonom No. 3200-IV (3200-15) vid 15.12.2005. VVR. – 2006. – No. 14. – St. 116.

Опубліковано: // Механізм регулювання економіки. - Суми. – 2014

Інформаційна безпека як основа національної безпеки

І. Р. Боднар[1]

Державна інформаційна політика є важливою складовою зовнішньої і внутрішньої політики країни та охоплює всі сфери життєдіяльності суспільства. Бурхливий розвиток інформаційної сфери супроводжується появою принципово нових загроз інтересам особистості, суспільства, держави та її національній безпеці. У статті розглянуто складові державної інформаційної політики щодо забезпечення інформаційної безпеки країни і визначені основні напрямки діяльності органів державної влади у цій сфері. Проаналізовані внутрішні та зовнішні інформаційні загрози національній безпеці України та шляхи гарантування інформаційної безпеки країни. Інформаційна безпека розглядається як складова національної безпеки країни, а також як глобальна проблема захисту інформації, інформаційного простору, інформаційного суверенітету країни та інформаційного забезпечення прийняття урядових рішень. Запропоновані підходи щодо забезпечення процесу безперервності функціонування системи інформаційної безпеки держави з метою моніторингу нових загроз, визначення ризиків та рівнів їх інтенсивності.

Ключові слова: держава, політика, безпека, загрози, ресурси

Абревіатури:

БІ	– безпека інформації
НБ	– національна безпека
ІР	– інформаційний ресурс

УДК 65.012.8:007+32(477) *JEL коди:* D8, L98

Вступ. Захищаючи свої інформаційні інтереси, кожна держава має дбати про свою інформаційну безпеку. Цього ж вимагає і зміцнення української державності. Збалансована державна інформаційна політика України формується як складова частина її соціально-економічної політики, виходячи з пріоритетності національних інтересів та загроз національній безпеці країни. Із правової точки зору вона ґрунтується на засадах правової демократичної держави і впроваджується шляхом розробки та реалізації відповідних національних доктрин, стратегій, концепцій та програм згідно із чинним законодавством. В Україні назріла об'єктивна потреба у державно-правовому регулюванні науково-технологічної та інформаційної діяльності, що відповідала б реаліям сучасного світу та

[1] *Боднар Ірина Романівна,* кандидат економічних наук, доцент, доцент кафедри міжнародних економічних відносин Львівської комерційної академії

рівню розвитку інформаційних технологій, нормам міжнародного права, але водночас ефективно захищала б власні українські національні інтереси. Відносини, пов'язані із забезпеченням інформаційної безпеки, як найважливіші сьогодні для суспільства та держави вимагають найшвидшого законодавчого регулювання.

*

Постановка проблеми. Проведення вдалої інформаційної політики може суттєво вплинути на розв'язання внутрішньополітичних, зовнішньополітичних та військових конфліктів. Інформаційна безпека є однією із суттєвих складових частин національної безпеки країни, її забезпечення завдяки послідовній реалізації грамотно сформульованої національної інформаційної стратегії в значній мірі сприяло б забезпеченню досягнення успіху при вирішенні завдань у політичній, соціальній, економічній та інших сферах державної діяльності.

Вивченням ролі держави у формуванні інформаційного суспільства займаються такі вчені як Арістова І. [1], Почепцов Г. [2] та ін. Ряд публіцистів Супрун В. [3], Ярочкін В. [4] розробили основні принципи забезпечення інформаційної безпеки. В той же час, окремого дослідження вимагають структурно-функціональні аспекти процессу гарантування інформаційної безпеки.

Метою дослідження є виявлення та аналіз основних напрямів державної інформаційної політики з метою захисту національного інформаційного простору та гарантування інформаційної безпеки.

Результати дослідження. У ст.17. Конституції України зазначено: "Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу" [5]. Інформаційну безпеку слід розуміти як сукупність засобів забезпечення інформаційного суверенітету України [6], захист інформаційної сфери від зовнішніх і внутрішніх інформаційних загроз. Ця безпека має включати ефективну протидію сукупності інформаційних загроз.

Необхідність гарантування інформаційної безпеки зумовлюється, по-перше, потребою забезпечення національної безпеки України в цілому, по-друге, існуванням таких загроз інформаційній сфері країни, які можуть завдавати значної шкоди загальним національним інтересам, по-третє, врахуванням того, що за допомогою інформації можна впливати на зміну свідомості і поведінку людей. Завдання інформаційної безпеки - створення системи протидії інформаційним загрозам [7] та захист власного інформаційного простору, інформаційної інфраструктури, інформаційних ресурсів держави. При виникненні криз, загостренні конфліктів інформаційна боротьба може перерости в інформаційну війну, яка здійснюється за допомогою інформаційної зброї. Показниками, виступають цілеспрямованість, масштабність та комплексність дій тощо.

Деякі засоби, які зараз прийнято відносити до інформаційної зброї, такі, наприклад, як спеціальні психологічні операції, існують та активно застосовуються досить давно, інші, зокрема, специфічні комп'ютерні засоби боротьби, з'явилися лише кілька років тому. Але всі вони мають дещо спільне - вони засновані на ідеї опосередкованого впливу на матеріальний світ.

Головна інформаційна загроза національній безпеці – це загроза впливу іншої сторони на інформаційну інфраструктуру країни, інформаційні ресурси, на суспільство, свідомість, підсвідомість особистості, з метою нав'язати державі бажану (для іншої сторони) систему цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної й державної діяльності, керувати їхньою поведінкою і розвитком у бажаному для іншої сторони напрямку. Власне, це є загрозою суверенітету України в життєво важливих сферах суспільної й державної діяльності, що реалізовується на інформаційному рівні. Стратегічне інформаційне протистояння є самостійним і принципово новим видом протистояння, здатним вирішувати конфлікт без застосування збройних сил у традиційному розумінні. Для вивчення закономірностей інформаційного протистояння та аналізу його кількісних характеристик необхідно формалізувати як поняття рівня інформаційної озброєності держави, так і механізм еволюції ресурсного потенціалу конкретної держави та вплив зовнішнього оточення. В даному випадку за основу аналізу вибраний інформаційний стан України.

Як базову розглянемо модель вирішення інформаційного конфлікту двох країн, яка складена на основі моделі Річардсона - Каспарова [8]. В основу моделі покладені наступні гіпотези:

- у процесі інформаційних атак кожна з двох країн прагне забезпечити зростання ефективності своєї інформаційної зброї пропорційно рівню інформаційності суперника;
- економічний потенціал кожної з країн надає/обмежує вплив на темп зростання інформаційних потужностей країни;
- держави ініціюють збільшення рівня інформаційних потужностей, керуючись власними прагненнями.

Введемо позначення N_1 (t), N_2 (t) рівнів інформаційних потужностей кожної з сторін конфлікту, де t - час. Тоді перераховані вище умови дії моделі можуть бути формалізовані у вигляді системи двох звичайних диференціальних рівнянь:

$$\begin{aligned} \dot{N}_1 &= M_1(L_1 - N_1)[1 - \exp(-p_1(k_1N_2 - a_1N_1 + g_1))] \\ \dot{N}_2 &= M_2(L_2 - N_2)[1 - \exp(-p_2(k_2N_1 - a_2N_2 + g_2))], \end{aligned} \quad (1)$$

де M_1, M_2 , L_1, L_2, p_1, p_2, a_1, a_2, k_1, k_2 є позитивними коефіцієнтами, що не залежать від часу.

Параметри моделі (1) за аналогією Т. Сааті [4] визначені наступним чином:

k_1, k_2 - коефіцієнти реакції на інформаційні атаки;

a_1, a_2- показники витрат на генерацію інформаційної зброї;

$g_1 g_2$- коефіцієнти претензії (агресивності), якщо вони позитивні, або коефіцієнти доброї волі, якщо вони негативні;

M_1, M_2- вартість наявного інформаційного забезпечення;

L_1, L_2- граничні значення рівнів інформаційних потужностей;

p_1, p_2- коефіцієнти ступеня важливості інформаційних витрат.

Модель (1) допускає існування чотирьох особливих розв'язків, що визначають координати положень рівноваги:

$$\begin{aligned} &\text{а) } N_1^p = N_1^*, N_2^p = N_2^* && \text{б) } N_1^p = N_1^*, N_2^p = L_2 \\ &\text{в) } N_1^p = L_1, N_2^p = N_2^* && \text{г) } N_1^p = N_2^*, N_2^p = L_2 \end{aligned} \quad (2)$$

де N_1^*, N_2^*- є рішення системи лінійних алгебраїчних рівнянь.

Нехай функції $u_1 = r_1^0(x_1 - x_2)$ і $u_2 = r_2^0(x_2 - x_1)$ характеризують політику кожної країни в сфері інформаційного протистояння, де змінні $x_1 = N_1 - N_1^*$, $x_2 = N_2 - N_2^*$ мають значення відхилень від рівноважних рівнів інформаційної потужності. Тут r_1^0, r_2^0 - стаціонарні параметри управління. З врахуванням вигляду функції u_1, u_2 система (1) набуває вигляду:

$$\begin{aligned} \dot{x}_1 &= M_1(\delta_1 - x_1)[1 - \exp(p_1(a_1x_1 - k_1x_2))] + r_1^0(x_1 - x_2) \\ \dot{x}_2 &= M_2(\delta_2 - x_2)[1 - \exp(p_2(a_2x_2 - k_2x_1))] + r_2^0(x_2 - x_1) \end{aligned} \qquad (3)$$

Можна зробити такі висновки: кожна держава, що є частиною світового інформаційного простору, має виробити комплекс заходів для власного сталого інформаційного розвитку в умовах жорсткої конкуренції з урахуванням чинників інформаційної безпеки. Для цього необхідно:

- розуміння інформаційних атак та протистояння ним.
- створення программного забезпечення протистояння інформаційним атакам;
- аналіз показників інформаційних загроз з метою вдосконалення механізмів прийняття рішень в системах державного управління;
- забезпечення максимального захисту від зовнішніх впливів;
- аналіз стану і технічний аудит всіх засобів комунікації;
- консолідація діяльності органів державної влади та ЗМІ у сфері політичного інформування суспільства для нейтралізації негативного психологічного впливу в умовах криз та конфліктів.

В Україні всі види інформаційних технологій, їхнього виробництва та засоби забезпечення цих технологій становлять спеціальну сферу діяльності, розвиток якої визначається державною інформаційною політикою та Національною програмою інформатизації. Визначення завдань Національної програми інформатизації, пріоритетних напрямів розвитку інформатизації, обсягів, джерел і порядку їх бюджетного фінансування покладається на Кабінет Міністрів України і щорічно затверджується Верховною Радою України.

Національну безпеку України в інформаційній сфері слід розглядати як інтегральну цілісність чотирьох складових – персональної, публічної (суспільної), комерційної (корпоративної) й державної безпеки. Тому в процесі визначення характеру ризиків слід брати до уваги наступні елементи:

- концептуальне засади політичної безпеки [9], її принципів, стандартів та правил, погоджених із чинним законодавством й принципами забезпечення безперервності системи інформаційної безпеки особистості, суспільства, комерційних (корпоративних) структур та держави;
- визначення об'єктів та цілей;
- визначення прийнятних з погляду забезпечення інтересів усіх суб'єктів структур встановлення контролю над об'єктами безпеки, а також оцінки ризиків та управління ризиками;
- визначення статусно-функціональних ролей, очікувань та міри відповідальності задіяних суб'єктів включно зі звітністю про події, які несуть потенційні загрози.

Україна також проводить активне співробітництво у галузі безпеки інформації в рамках програми НАТО "Безпека через науку". Ця програма використовує такі механізми підтримки у галузі інформаційної безпеки:

- гранти на налагодження та укріплення існуючих зв'язків;
- створення дослідницьких центрів;
- підтримка проектів досліджень.

Процес забезпечення безперервності гарантування інформаційної безпеки можна поділити на шість основних стадій (рис.1).

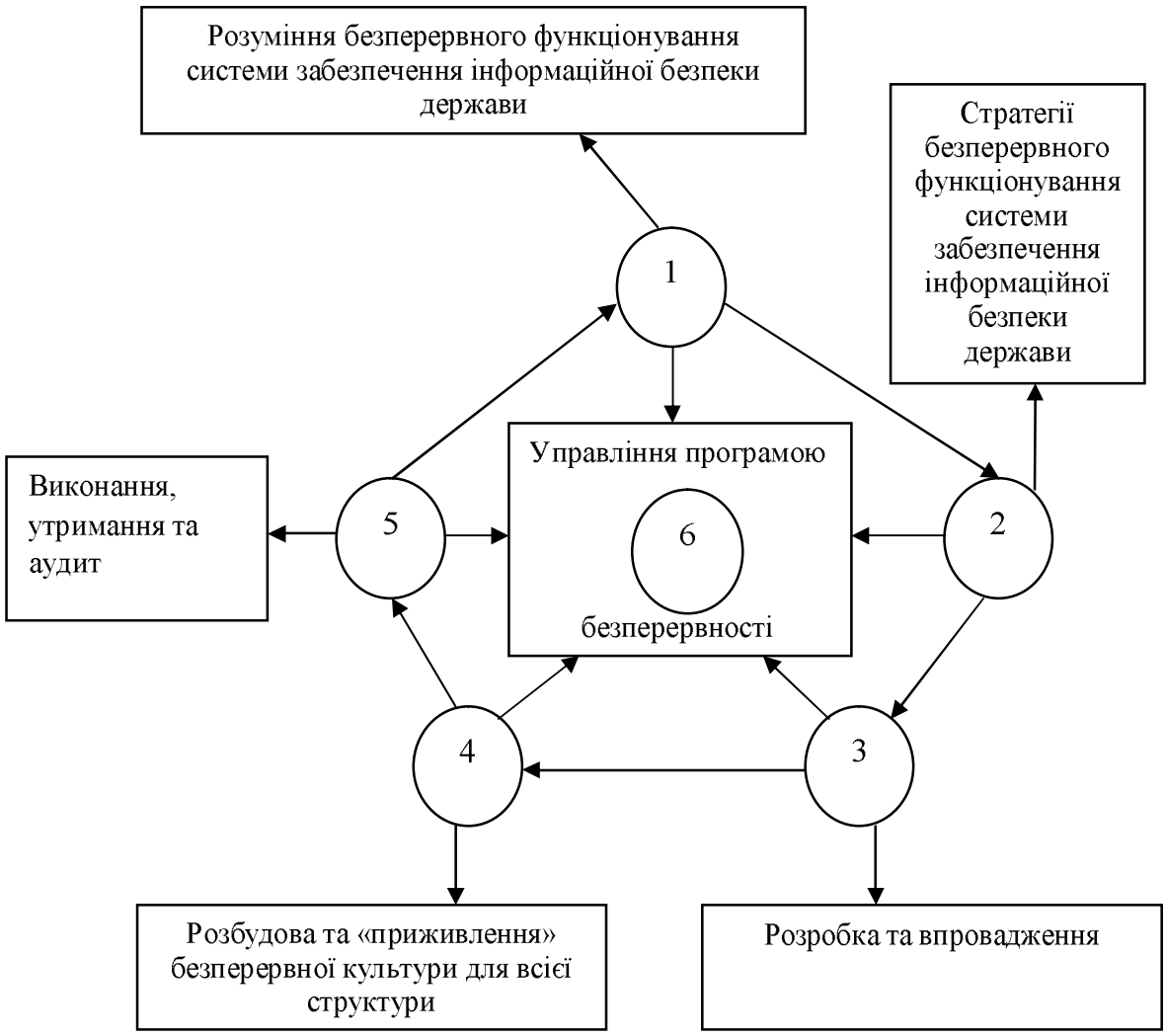

Рис. 1. Процес забезпечення безперервності функціонування системи інформаційної безпеки держави [авторська розробка]

Аналізуючи рис. 1 бачимо, що всі етапи взаємопов'язані в рамках державної системи забезпечення інформаційної безпеки. Державна політика забезпечення інформаційної безпеки країни визначає основні напрямки діяльності органів державної влади у цій сфері. Ці напрями обумовлені змістом національних інтересів держави, суспільства та особистості. По суті це є вірним, оскільки завданням заходів з інформаційної безпеки є мінімізація шкоди через неповноту, несвоєчасність або недостовірність інформації чи негативного інформаційного впливу через наслідки функціонування інформаційних технологій, а також несанкціоноване поширення інформації. Саме тому інформаційна безпека передбачає наявність певних державних інститутів і умов існування її суб'єктів, що встановлені міжнародним і вітчизняним законодавством.

Розглянемо основні структурні блоки рис.1.

1. Розуміння безперервності функціонування системи забезпечення інформаційної безпеки держави. Ця фаза пов'язана з ідентифікацією критично важливих точок (об'єктів) захисту. Йдеться також про виокремлення основних внутрішніх та зовнішніх загроз, що можуть стати критичними для системи.

2. Стратегії забезпечення безперервності функціонування системи. В цьому випадку завдання зосереджуються на визначенні та доборі альтернативних рішень щодо відновлення системи з метою мінімізації загроз. Пошук рішень балансує між собівартістю систем захисту та їхньою ефективністю.

3. Розробка та впровадження. На цій фазі зусилля зосереджуються на структуруванні та документуванні Програми безперервності державного управління.

4. Розвиток культури інформаційної безпеки держави передбачає забезпечення процесу розробки державної інтегральної системи захисту інформації.

5. Виконання, підтримка та аудит процесу регулювання безперервного функціонування системи інформаційної безпеки держави за умов різноманітних криз та конфліктів.

6. Управління програмою інформаційної безпеки держави шляхом розподілу функцій, що передбачає відповідальність, страхування (гарантії) та керування у контексті реалізації загального плану безперервності функціонування системи забезпечення інформаційної безпеки держави.

Якщо наноситься шкода в результаті недосконалості інформаційних відносин, використанні неякісної інформації тощо, то це свідчить про зниження інформаційної безпеки [10]. Це дає змогу розглядати як невирішені проблеми гарантування інформаційної безпеки в Україні:

- недосконалість інформаційної політики та політики інформаційної безпеки держави;
- недосконалість нормативно-правової бази в сфері інформаційних відносин та інформаційної безпеки;
- недостатню розвиненість інформаційної інфраструктури держави;
- введення іноземними державами обмежень по відношенню до України щодо розповсюдження інформації та отримання нових інформаційних технологій;
- протиправна діяльність посадових осіб, різних формувань та груп у сфері інформаційних інтересів громадян та держави;
- недосконалість державної системи забезпечення інформаційної безпеки;

- можливість виникнення непередбачених ситуацій у системах та процесах, що базуються на використані інформаційних технологій.

Висновки і перспективи подальших наукових розробок. Державна інформаційна політика повинна відбивати нагальні питання, що склалися у міжнародній сфері та сфері інформаційної безпеки тощо. Необхідним є забезпечення законодавчого захисту прав та інтересів всіх суб'єктів інформаційних відносин. Найскладнішими тут є такі завдання, що передбачають гармонійне забезпечення інформаційної безпеки держави, особи і суспільства з одночасним виокремленням нагальних пріоритетів, до яких слід віднести створення/відновлення основних точок захисту системи національної безпеки в інформаційній сфері, практичну реалізацію наведеної вище схеми створення ефективної системи інформаційної безпеки держави, перегляд списку нових інформаційних загроз, усунення наявних із визначенням ступеня можливих наслідків та рівнів їх інтенсивності.

Основні акценти державної інформаційної політики повинні базуватись на забезпеченні права на достовірну, повну та своєчасну інформацію, свободу слова та інформаційну діяльність, недопущення втручання в зміст та внутрішню організацію інформаційних процесів, крім випадків, визначених законодавством відповідно до Конституції України; збереженні та вдосконаленні вітчизняного національного інформаційного продукту та технологій, забезпеченні інформаційної та національно-культурної ідентифікації України у світовому інформаційному просторі; гарантуванні державної підтримки та розвитку ресурсів науково-технічної продукції та інформаційних технологій.

Література

1. *Арістова І. В.* Діяльність органів внутрішніх справ щодо реалізації державної інформаційної політики : монографія [Текст] / І. В. Арістова. - Х. : Нац. ун-т внутр. справ, 2006. – 354 с.

2. *Почепцов Г.* Інформаційна політика : навч. посібник [Текст] / Г. Г. Почепцов – К.: Знання, 2006. – 663 с.

3. *Супрун В. М.* Інформаційний суверенітет як один з елементів інформаційної безпеки держави: теоретико-правовий аспект [Електронний ресурс]. – Режим доступу : http : // www. nbuv.gov.ua/portal/natural/vkhnu / Pravo / 2009.

4. *Ярочкін В.* Система безпеки фірми [Електронний ресурс]. – Режим доступу : http : // www. nbuv. gov. ua.

5. *Закон України.* Про інформацію / [Електронний ресурс] - Режим доступу: http : // zakon. rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12.

6. *Боднар І. Р.* Сучасні реалії інформаційного суспільства: проблеми становлення та перспективи розвитку: монографія [Текст] / І. Р. Боднар. – Львів: Видавництво Львівської комерційної академії, 2013. – 320 с.

7. *Бондаренко В., Литвиненко О.* Інформаційна безпека сучасної держави: концептуальні роздуми [Електронний ресурс] / В. Бондаренко, О. Литвиненко - Режим доступу: http://www.crime-research. iatp. org. ua/ library/strateg. htm.

8. *Саати Т. Л.* Математические модели конфликтных ситуаций. - М. : "Сов. Радио", 1977. - 304 с.

9. *Державна* інформаційна політика [Електронний ресурс]. – Режим доступу : http : // merega. org. ua / law / projects / derzh polityka.

10. *Боднар І. Р.* Роль держави у формуванні інформаційної політики [Текст] / І. Р. Боднар. – Вісник ЛКА. – Львів: Видавництво ЛКА. – Випуск 34. – Серія економічна. – 2011. – С. 291-296.

Информационная безопасность как основа национальной безопасности

*Боднар Ирина Романовна**

**кандидат экономических наук, доцент, доцент кафедры международных экономических отношений Львовской коммерческой академии,*
ул. Туган-Барановского, 10, г. Львов, 79005, Украина,
тел.: 038-032-2448626, iryna.bod@gmail.com

Государственная информационная политика является важной составляющей внешней и внутренней политики страны и охватывает все сферы жизнедеятельности общества. Бурное развитие информационной сферы сопровождается появлением принципиально новых угроз интересам личности, общества, государства и его национальной безопасности. В статье рассмотрены составляющие государственной информационной политики по обеспечению информационной безопасности и определены основные направления деятельности органов государственной власти в этой сфере. Проанализированы внутренние и внешние информационные угрозы национальной безопасности Украины и пути обеспечения информационной безопасности страны. Информационная безопасность рассматривается как составляющая национальной безопасности страны, а также как глобальная проблема защиты информации, информационного пространства, информационного суверенитета страны и информационного обеспечения принятия правительственных решений. Предложены подходы по обеспечению процесса непрерывности функционирования системы информационной безопасности государства с целью мониторинга новых угроз, определения рисков и уровней их интенсивности.

Ключевые слова: государство, политика, безопасность, угрозы, ресурсы.

Information Security as the foundation of national security

Iryna R. Bodnar*

** PhD, Associate Professor, Department of International Economic Relations, Lviv Academy of Commerce, Tugan-Baranovsky Street, 10, Lviv, 79005, Ukraine, phone: 038-032-2448626, e-mail: iryna.bod@gmail.com*

Manuscript received 11 November 2013

National information policy is an important component of foreign and domestic policy of the country and covers all areas of society. The rapid development of the information field is accompanied by a fundamentally new security interests of the individual , society, the state and its national security. The components of the state information policy on information security and the basic activities of public authorities in this field are reviewed in the article. The internal and external information challenges facing Ukraine and ways of ensuring information security are analyzed. Information security is seen as a component of national security , as well as a global problem of information security, information space, information sovereignty and information support decision-making. The proposed approach to ensure continuity of operation of the process of information security to monitor new threats, the risks and levels of intensity.

Keywords: government , politics, security, threats , resources

JEL Codes: D8, L98 Figures: *1*; Formulas: 3; References: *6*

Language of the article: Ukrainian

References

1. Aristova I. V. (2006) "Activity of the Interior to implement the state information policy," Kharkiv, 354. (*In Ukrainian*)
2. Pocheptsov H. (2006) "Information Policy," Kyiv, 663. (*In Ukrainian*)
3. Suprun V. M. (2009) "Information sovereignty as part of information security: theoretical and legal aspects", http: / / www. nbuv.gov.ua / portal / natural / vkhnu / Pravo / 2009. (*In Ukrainian*)
4.Yarochkin V. "The security system company", http: // www. nbuv. gov. ua. (*In Ukrainian*)
5.The Law of Ukraine. (1992) "On information," http://zakon.rada.gov.ua/cgi-bin/laws/ main.cgi? nreg=2657-12. (*In Ukrainian*)
6. Bodnar I. R. (2013) "Modern Realities of the information society: Problems of Establishment and prospects for development," Lviv, Commercial Academy Publishing House, 320. (*In Ukrainian*)
7. Bondarenko V. and Litvinenko O. "Information security of the modern state: conceptual reflections," http://www.crime-research.ru/library/strateg.html. (*In Ukrainian*)
8. Saaty T. L. (1977) "Mathematical models of conflict situations," Moscow, 304. (*In Russian*)
9. National Information Policy, http: // merega. org. ua / law / projects / derzh polityka. (*In Ukrainian*)
10. Bodnar I. R. (2011) "The state's role in shaping the Information Policy," *Journal of LKA,* Lviv, Publishing LKA, Release of 34, A series of economic, 291-296. (*In Ukrainian*)

УДК [342.951:351.85]:316.776

С. С. Єсімов
Навчально-науковий інститут права та психології
Національного університету "Львівська політехніка",
канд. юрид. наук, доц., доцент кафедри адміністративного та інформаційного права

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ЯК ПРЕДМЕТ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ

Розглянуто використання інформаційних технологій як предмет адміністративно-правового регулювання. Аналізуються особливості інформаційного простору та нормативно-правового регулювання використання інформаційних технологій у діяльності державних органів і органів місцевого самоврядування, завдання адміністративно-правового регулювання щодо інформації, інформаційно-інфраструктурних відносин.

Ключові слова: адміністративно-правове регулювання, інформаційний простір, інформаційна інфраструктура, інформаційна система.

С. С. Єсимов

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ КАК ПРЕДМЕТ АДМИНИСТРАТИВНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ

Рассмотрено использование информационных технологий как предмет административно-правового регулирования. Анализируются особенности информационного пространства и нормативно-правового регулирования использования информационных технологий в деятельности государственных органов и органов местного самоуправления, задачи административно-правового регулирования по информации, информационно-инфраструктурных отношений.

Ключевые слова: административно-правовое регулирование, информационное пространство, информационная инфраструктура, информационная система.

S. S. Yesimov

USING INFORMATION TECHNOLOGY AS SUBJECT ADMINISTRATIVE AND LEGAL REGULATION

In the article the use of information technology as a subject of administrative and legal regulation. Specific features information space and legal regulation of the use of information technology in government bodies and local authorities, the problem of administrative and legal regulation of media, information and infrastructure relations.

Key words: administrative legal regulation, information space, information infrastructure and information system.

Постановка проблеми. В останнє десятиліття одним з пріоритетних напрямів державної політики країн-членів Європейського Союзу стало виробництво і використання інформаційних технологій практично у всіх сферах суспільного життя. Використання інформаційних технологій у сфері державного управління істотно змінює зміст різних видів діяльності, виводить на новий, вищий

рівень інформаційне забезпечення суспільних процесів на всіх щаблях владної ієрархії. У зв'язку з цим до пріоритетних завдань держави належить формування та розвиток інформаційної інфраструктури на державному та регіональному рівнях. Інформаційні технології сприяють формуванню нових ефективних засобів управління і взаємодії органів влади, місцевого самоврядування, господарських структур і громадян. Це нова можливість підвищення якості управління за рахунок надання послуг державних органів електронними засобами. Доцільність дослідження інформаційних технологій і вивчення потенціалу їх практичного застосування як інструменту органів державної влади визначається необхідністю вдосконалення впливу на суспільні процеси.

Мета статті – дослідження використання інформаційних технологій у контексті предмета адміністративно-правового регулювання.

Виклад основного матеріалу. На сучасному етапі розвитку суспільства потоки інформації зростають з кожним днем, причому як загалом у країні, так і всередині окремих галузей управління. Такі процеси ведуть до глобалізації світового простору, трансформуючи його. У зв'язку з цим особливої актуальності набувають дії суб'єктів права не тільки в звичайному фізичному просторі, а й в інформаційному. Інформаційний простір формується не тільки завдяки розвитку інформаційних технологій, але й на основі відповідних нормативних актів. Наприклад, Закон України від 17.04.2014 р. № 1227-VII 13 "Про Суспільне телебачення і радіомовлення України" визначає порядок задоволення інформаційних потреб суспільства, залучення громадян до обговорення та вирішення найважливіших соціально-політичних питань, забезпечення національного діалогу, сприяння формуванню громадянського суспільства. Стратегія розвитку інформаційного суспільства в Україні передбачає напрями розвитку національної інформаційної інфраструктури та її інтеграцію до світової інфраструктури [1]. Значні досягнення в науково-технічному прогресі, зокрема в інформатиці та зв'язку, забезпечили можливість практичної реалізації ідей формування інформаційного суспільства загалом.

Створення інформаційного суспільства тісно взаємопов'язане з упровадженням інформаційних технологій в усі сфери суспільного та державного життя. У країнах Європейського Союзу державні органи влади активно впроваджують інформаційні технології. У реалізацію цих цілей вкладаються великі фінансові ресурси. Директива 2014/61/ЄС Європейського Парламенту та Ради Європейського Союзу від 15.05.2014 р. передбачає заходи, спрямовані на зменшення витрат на розгортання високошвидкісних мереж електронного зв'язку що дасть змогу забезпечити до 2020 року доступ для всіх європейців до високошвидкісного Інтернету, понад 30 Мбіт/с, зменшивши витрати на впровадження новітніх технологій за рахунок інтеграції та уніфікації національних програм [2]. В органах державного управління утворюються спеціальні структури в сфері розробки, впровадження та супроводу державних інформаційних систем і мереж.

В. Б. Авер'янов у 1999 р. вказував, що адміністративно-правове регулювання в практичній діяльності охоплює три поняття: державне управління, державно-адміністративне регулювання та державні послуги [3].

Саме такий підхід дозволяє обґрунтувати не просто зв'язок понять "адміністративно-правове регулювання" і "використання інформаційних технологій", а й перспективи розвитку адміністративно-правового регулювання з урахуванням сучасних тенденцій, розглядаючи ці поняття у контексті предмета інформаційного права. З огляду на дослідження В. Б. Авер'янова, Р. В. Ігоніна, у контексті визначення предмета адміністративного права як соціальних відносин у сферах державного управління, державного регулюванню та державних послуг, доцільно позначити інформаційні технології як фактор, що потребує державної регламентації, причому регламентації адміністративного типу [4, с. 139; 5, с. 129–130].

Як зазначає А. І. Марущак: "У такому контексті актуальними видаються наступні напрями досліджень інформаційного права: закріплення національних інтересів України в інформаційній сфері у нормативно-правових актах; правові засади забезпечення інформаційної безпеки держави, суспільства та особи; правові механізми забезпечення інформаційної безпеки; теоретико-правові засади протидії загрозам інформаційній безпеці України; теоретичні і правові основи захисту інформаційного простору України; теоретичні і правові основи захисту інформаційних ресурсів України; компетенція державних органів України, зокрема правоохоронних, щодо забезпечення

інформаційної безпеки України; взаємодія державних органів України в процесі забезпечення інформаційної безпеки держави; теоретико-правові основи оцінювання протиправних дій учасників інформаційно-психологічного протиборства; теоретико-правові основи використання комунікаційних каналів з метою здійснення інформаційного впливу; міжнародний досвід діяльності державних органів із забезпечення інформаційної безпеки тощо" [6, с. 23].

Треба враховувати, що використання інформаційних технологій в діяльності державних і місцевих органів є предметом адміністративно-правового регулювання як різновид поведінки фізичних і юридичних осіб.

Водночас інформаційні технології взаємодіють, перетворюють і організують рух інформаційних ресурсів. О. О. Денісова зазначає, що поняття "інформаційна система" (як система, що об'єднує по каналах передачі даних створені інформаційні ресурси, збережені й оброблювані на комп'ютерах з дотриманням вимог інформаційної безпеки [7, с. 18]) – це організаційно-технічна система, яка забезпечує вироблення рішень на основі автоматизації інформаційних процесів у різних сферах людської діяльності, точніше відображає сутність інформаційних процесів у діяльності органів влади [8].

Інформаційні технології є складовою частиною інформаційного простору, а використання інформаційних технологій слугує засобом забезпечення взаємодії органів влади, організацій та громадян. Звідси випливає, що інформаційний простір може бути об'єктом управлінського впливу з боку органів державного управління.

Основні структурні елементи інформаційного простору – це інформаційний ресурс, інформаційні технології та інформаційні системи, спрямовані на забезпечення інформаційних потреб суспільства і держави. Об'єктом державного управління можуть бути інформаційні технології, інформаційні мережі та системи, інформаційний ресурс, оскільки інформаційний простір, що є складним динамічним утворенням, може мати об'єкти й зв'язки, які складно, а часом і неможливо виявити і врахувати під час планування та реалізації керуючих впливів.

На думку А. В. Манойло, основні структурні елементи інформаційного простору – це суб'єкти, які реалізують масове інформування та генерують великі й значущі інформаційні потоки [9, с. 73–74]. Досліджуючи інформаційно-психологічний простір (що є різновидом загальнішого поняття "інформаційний простір"), вказаний автор відзначає, що серед об'єктів інформаційно-психологічного простору доцільно виділити: суспільну свідомість; приватну свідомість індивіда; інформаційну інфраструктуру; інформаційні та психологічні ресурси [9, с. 86–88].

А Концепція Національної програми інформатизації, як зазначає В. В. Гришин, виділяє в інформаційному просторі такі елементи, як: бази і банки даних, технології їх ведення та використання, інформаційно-телекомунікаційні системи та мережі, які функціонують на єдиній основі та забезпечують задоволення інформаційних потреб [10, с. 62]. Лексикологічно термін "інформаційний простір" охоплює поняття простору й інформації.

У філософській науці категорія "простір" розроблена доволі повно. Простір характеризується протяжністю, структурністю, співіснуванням і взаємодією елементів у всіх матеріальних системах. Загальними властивостями простору є протяжність, єдність перервності та неперервності, він необмежений, неосяжний і до кінця незбагненний, його будову формує практично незчисленна множина створених природою і людиною об'єктів і відношень між ними, що передбачає необмеженість спектра різноманітних аспектів їх багатоцільового розгляду і / або використання [11].

У розглянутому аспекті простір передбачає інформаційне наповнення. Інформація нетлінна, характеризується зростанням в часі і поширенням у просторі, нерідко її трактують як організованість із заздалегідь заготовленим місцем і способом застосування у системах діяльності.

О. В. Буньківська під інформаційним простором розуміє територію поширення інформації за допомогою конкретних компонентів системи інформації і зв'язку, і функціонування інформаційної діяльності має гарантоване правове забезпечення. До таких компонентів варто зарахувати: матеріальні (технологічні) можливості поширення інформації по горизонталі й вертикалі, її передачі в будь-яких напрямах та наявність регіональних і міждержавних угод, основаних на розумінні того, що жоден із процесів інформації не може розглядатися як феномен винятково національного характеру. Спеціальними вимірами інформаційного простору можуть стати: загальна кількість засобів масової комунікації, загальний обсяг її продукції, яка розповсюджується і

приймається на певній території; опосередкована фіксація тих або інших результатів контакту із продукцією засобів масової комунікації реципієнтів [12, с. 9].

Фіксація знаків на матеріальних носіях зумовила виникнення документа. Отже, виникла можливість успішніше формувати простір. Поява і використання документів надає інформаційному простору матеріальність. Складність формування інформаційного простору пов'язана з дискретністю обох компонентів інформаційного процесу.

Документ являє собою самостійний елемент інформації, але ця самостійність відносна, оскільки у документа завжди є попередній документ і він слугує підставою для створення наступного. Наступним значним етапом розвитку інформаційного простору можна вважати появу технологій типу Інтернет, які забезпечують миттєвість передачі інформації, що, своєю чергою, дозволяє говорити про формування практично безмежного інформаційного простору.

Водночас єдність інформаційного простору повинна забезпечуватися передусім адміністративно-правовим регулюванням. На факт необхідності участі урядів різних держав у формуванні єдиного інформаційного простору вказують І. В. Арістова, А. І. Марущак [6, с. 24].

Зазначимо, що економісти давно досліджують цю категорію. Глобалізація як економічне, інформаційне, технологічне об’єднання світу розширює просторові та часові межі діяльності суб’єктів бізнесу не лише як реального сектору національної економіки за рахунок створення нових інформаційних продуктів, а й формуванням нового віртуального сектору глобальної економіки, в якому компанії і споживачі послуг інтерактивно взаємодіють через систему Інтернету, що слугує віртуальним посередником глобального масштабу. Інформатизація бізнесу в останнє десятиліття набула глобальних ознак [13, с. 13]. Інформаційний простір діє на основі правил, які поєднують державне регулювання та саморегулювання, що забезпечує інформаційну взаємодію держави та суспільства, задовольняючи їхні інформаційні потреби, зберігаючи баланс інтересів у контексті міжнародного інформаційного простору та забезпечення інформаційної незалежності.

З огляду на дослідження Н. А. Новікової сутність інформаційного простору охоплює форму існування та взаємодію інформаційних систем [14, с. 368].

На думку О. П. Дубаса, інформаційний простір, постійно розширюючись і відіграючи дедалі важливішу роль у житті людей, формує новий життєвий простір у вигляді цілісного поля, усередині якого індивіди взаємодіють між собою. Специфіка його полягає в розірваності двох рівнів буття: реального й віртуального, що зумовлює нові норми й ситуації існування. інформаційний простір безмежний і вбирає в себе різні об'єкти [15, с. 224].

З погляду Д. В. Андреєва, можна виділити інформаційний простір фізичної особи, суспільства загалом, юридичної особи тощо [16, с. 9–10].

В інформаційному просторі, як зазначає В. І. Левенко, існує інформаційне керування, яке характеризує процес вироблення та реалізації управлінських рішень у ситуації, коли керуючий вплив неявний, непрямий, а об’єктові керування надана обумовлена суб’єктом управління інформація про ситуацію (інформаційна картина), орієнтуючись на яку, цей об’єкт немовби самостійно вибирає лінію власної поведінки. Механізми інформаційного керування пов’язані з прагненням так сформувати повідомлення про навколишню реальність, щоб людина сприймала їх як цілком зрозумілі та діяла відповідно, незважаючи навіть на їхню неадекватність. Таємна сторона високої ефективності інформаційного керування полягає у дотику до позасвідомого людини, витонченому маніпулюванні сприйняттям дійсності [17, с. 25].

Залежно від цього змінюються підходи до адміністративно-правового регулювання, використання інформаційних технологій у різних видах інформаційного простору. Такі підходи до визначення інформаційного простору дають підстави зробити висновок про те, що це явище було б точніше визначити як інформаційне середовище, оскільки поняття “інформаційний простір” в юридичному сенсі – доволі умовна категорія, яка не може існувати з погляду єдиних правил регулювання поведінки в інформаційній сфері. Основними елементами, що утворюють структуру інформаційного середовища, виступають суб'єкти та об'єкти інформаційного впливу. А оскільки інформаційне середовище є базою управлінського впливу в інформаційній сфері, то можна виділити об'єкти і суб'єкти державного управління в інформаційній сфері.

Як зазначає Н. А. Новікова: “Вважається необхідним для українського законодавця окреслити основні риси, межі, складові інформаційного простору держави з метою здійснення регулювання відносин в інформаційній сфері. Це дозволить визначити межі впливу держави на циркулюючу в ній інформацію та більш повно відобразити таку категорію, безпосередньо пов'язану з інформаційним простором, як інформаційний суверенітет” [14, с. 368].

Державні та місцеві органи, засоби масової інформації, громадські та політичні об'єднання можна зарахувати до суб'єктів адміністративно-правового регулювання в умовах використання інформаційних технологій.

Згідно з проектом Концепції інформаційної безпеки України як одного з документів, що регламентують інформаційну сферу, об'єкти інформаційної безпеки включають: сукупність інформаційних технологій, ресурсів, продукції і послуг, інформаційної інфраструктури, суб’єктів інформаційної діяльності та системи регулювання суспільних інформаційних відносин [18].

Доцільно погодитися з Ю. П. Бурило в тому, що до об'єктів державного управління інформаційної сфери входять інформаційні відносини, об’єктом яких є інформація, інформаційно-інфраструктурні відносини, об’єктом яких є засоби зв’язку, інформатизації та інформаційної безпеки (елементи інформаційних систем, мереж тощо) [19, с. 5].

Основна мета державного управління у сфері інформаційно-інфраструктурних відносин полягає у створенні умов, за яких інформаційна інфраструктура стійко розвивається і функціонує, доступна для всіх і забезпечує всі можливості для професійної та комунікативної діяльності.

Серед основних завдань адміністративно-правового регулювання щодо інформації, інформаційно-інфраструктурних відносин, об’єктом яких виступають засоби зв’язку, інформатизації та інформаційна безпека, можна виділити контроль за інформаційними потоками, забезпечення інформаційної безпеки (в інформаційному та технічному аспектах).

Інформаційна сфера країни одночасно є сферою реалізації державної інформаційної політики і об'єктом керуючого впливу. Складна структура цього явища передбачає можливість здійснення керуючого впливу на окремі об'єкти, які теж виступають структурними елементами інформаційної сфери. Водночас використання інформаційних технологій являє собою сполучну ланку, яка об'єднує всю сукупність об'єктів державного управління в інформаційній сфері, оскільки використання інформаційних технологій у діяльності державних і місцевих органів забезпечує не тільки інформаційну взаємодію органів влади, а й підвищує рівень якості здійснення державних послуг у сфері соціальних відносин.

Предметом адміністративно-правових відносин можуть бути матеріально-технічні дії, наприклад, дії з використання інформаційних технологій в діяльності державних органів, тобто такі дії, відповідно до цієї тези, також є предметом адміністративно-правових відносин. Як зазначає Ю. П. Бурило: “Правовою основою державного управління в інформаційній сфері є підгалузь адміністративного права, яка являє собою систему однорідних предметно-споріднених правових інститутів, що включають в себе ієрархічно побудовану сукупність первинних і вторинних спеціальних правових норм, які регулюють здійснення галузевого та міжгалузевого управління в різних галузях і сферах, що входять до інформаційної сфери як складного об’єкта державного управління, шляхом визначення завдань і основних напрямів діяльності держави, системи та адміністративно-правового статусу органів (суб’єктів) державного управління та керованих ними суб’єктів інформаційних та інформаційно-інфраструктурних відносин, а також регулювання взаємодії між ними” [19, с. 11]. Отже, адміністративно-правове регулювання використання інформаційних технологій забезпечує: надання державних послуг інформаційної та соціальної спрямованості; дає змогу підвищити ефективність внутрішньої організації управління, за рахунок зміни системи контролю та налагодження зворотного зв’язку. Тому використання інформаційних технологій в державному управлінні є предметом адміністративно-правових відносин, а самі інформаційні технології як елемент інформаційної сфери, поряд з інформаційним ресурсом, являють собою один з об'єктів державного управління.

Висновки. У системі державних органів і в управлінських процесах інформаційні технології виступають сполучними ланками, що забезпечує взаємодію і інтеграцію всіх рівнів і елементів системи та виконання нею (і її інститутами) всіх основних функцій. Механізми використання інформаційних технологій мають адміністративно-організаційні, адміністративно-правові й інформаційно-комунікаційні складові. Особливість адміністративно-правової складової механізму

використання інформаційних технологій у сфері державного управління полягає в тому, що він поки що на етапі свого формування. Впровадження сучасних інформаційних технологій забезпечує цілісність інформаційної сфери, що розвивається згідно з певними закономірностями. Якщо ігнорувати закономірності розвитку інформаційної сфери, то знижується дієвість рішень, зменшується ефективність впровадження інформаційних систем в роботу органів влади, виникає необхідність реформування системи управління. Інформаційне забезпечення якісно і ефективно реалізується тільки в умовах наявності достатнього адміністративно-правового регулювання використання інформаційних технологій. Розроблення та впровадження адміністративно-правового регулювання використання інформаційних технологій сприяють переходу до нової суспільної формації – інформаційного суспільства. Отже, адміністративно-правове регулювання використання інформаційних технологій забезпечує ефективне державне управління на всіх рівнях.

1. Розпорядження Кабінету Міністрів України від 15.05.2013 р. № 386-р "Про схвалення Стратегії розвитку інформаційного суспільства в Україні" [Електронний ресурс]. – Режим доступу: http://zakon3. rada. gov. ua/laws/show/386-2013-%D1%80 2. Директива 2014/61/ЄС Європейського Парламенту та Ради від 15 травня 2014 року про заходи, спрямовані на зменшення витрат на розгортання високошвидкісних мереж електронного зв'язку / Офіційний вісник Європейського Союзу L.155/1 23.5.2014. UA. [Електронний ресурс]. – Режим доступу: http://www. nkrzi. gov. ua/ index. php?r=site/ index&pg=104&language=uk 3. Авер'янов В. Б. Державне управління: теорія і практика / В. Б. Авер'янов, В. В. Цвєтков, В. М. Шаповал, С. П. Кисіль, Л. Т. Кривенко. – К.: Юрінком Інтер, 1998. – 431 с. [Електронний ресурс]. – Режим доступу: http://ukrkniga. org. ua/ukrkniga-text/692/38/ 4. Авер'янов В. Державне управління у змісті предмета адміністративного права / В. Авер'янов // Вісник Академії правових наук України. – 2004. – № 2 (37). – С. 139–149 5. Ігонін Р. В. Предмет адміністративного права у в умовах трансформації вітчизняної системи права / Р. В. Ігонін / Наук. вісник Херсон. держ ун-ту. Серія "Юридичні науки". – 2015. – Вип. 2. – Т. 2. – С. 126–130. 6. Марущак А. І. Пріоритети розвитку інформаційного права України / А. І. Марущак // Інформація і право: наук.-практ. журнал. – 201. – № 1(1). – С. 20–24. 7. Інформаційні технології в юридичній діяльності: навч. посіб. / О. В. Співаковський, М. І. Шерман, В. М. Стратонов, В. В. Лапінський. – Херсон: ХДУ, 2012. – 220 с. 8. Денісова О. О. Інформаційні системи і технології в юридичній діяльності: навч. посіб. / О. О. Денісова. – К.: КНЕУ, 2003. – 315 с. [Електронний ресурс]. – Режим доступу: http://ukrkniga. org. ua/ukrkniga-text/817/4/ 9. Манойло А. В. Государственная информационная политика в особых условиях / А. В. Манойло. – М.: МИФИ, 2003. – 388 с. 10. Гришин В. В. Особливості формування єдиного інформаційного простору України на державному рівні / В. В. Гришин // Наук. вісник Харк. держ. акад. культури. – 2011. – Вип. 33. – С. 62–69. 11. Буньківська О. В. Інформаційний простір: соціокультурна сутність, стан та проблеми функціонування в Україні: автореф. дис. … канд. Культурології: спец. 26.00.01 "Теорія й історія культури" / О. В. Буньківська. – К., 2009. – 22 с. 12. Простір: словник української мови: в 11 томах. – Том 8, 1977. – С. 298. [Електронний ресурс]. – Режим доступу: http://sum. in. ua/s/prostir 13. Фалько Є. А. Розвиток інформатизації міжнародного туристичного бізнесу в умовах глобалізації: автореф. дис. … канд. екон. наук: спец. 08.00.02 "Світове господарство і міжнародні економічні відносини" / Є В. Фалько. – Львів, 2015. – 21 с. С 13. 14. Новікова Н. А. Інформаційний простір як основа інформаційної функції сучасної держави / Н. А. Новікова // Актуальні проблеми держави і права зб. наук. пр. / Нац. ун-т "Одеська юридична академія". – Одеса: Юрид. л-ра, 2011. – Вип. 61. – С. 365–373. 15. Дубас О. П. Інформаційно-комунікаційний простір: поняття, сутність, структура / О. П. Дубас. [Електронний ресурс]. – Режим доступу: http://dspace. nbuv. gov. ua/xmlui/bitstream/handle/123456789/26693/22-Dubas. pdf? sequence=1 16. Андреєв Д. В. Соціально-правові комунікації в забезпеченні взаємодії влади та громадянського суспільства: автореф. дис. ... д-ра юрид. наук : спец. 12.00.12 / Д. В. Андреєв. – К., 2014. – 36 с. 17. Ливенко В. І. Інформаційне керування: концептуальне ядро інформаційного протиборства / В. І. Ливенко // Нова парадигма : журнал наук. пр. Нац. пед. ун-т ім. М. П. Драгоманова, 2012. – Вип. 114. – С. 23–33. 18. Концепції інформаційної безпеки України. Проект. [Електронний ресурс]. – Режим доступу: http://mip. gov. ua/done_img/d/30-project_08_06_15. pdf 19. Бурило Ю. П. Організаційно-правові питання державного управління в інформаційній сфері : автореф. дис... канд. юрид. наук: 12.00.07 "Адміністративне право і процес; фінансове право; інформаційне право" / Ю. П. Бурило. – К., 2008. – 18 с.

Список використаної літератури. **1.** *Ленков С. В. Методы и средства защиты информации. В 2-х томах /Ленков С. В., Перегудов Д. А., Хорошко В. А.– К.: Арий,2008.* **2.** *Емельянов С. Л. Проблемы защиты информации от утечки и пути ее решения / Емельянов С. Л.– Одесса: Фенікс, 2011. – с. 624* **3.** *Артемов В. Ю. Нормативно-правовий довідник з охорони інформації в Україні. У 4-х томах / Артемов В. Ю., Лєнков О. С., Пашков А. С., Стаднік О. М., Хорошко В. О. – К.: Вид. ДУІКТ, 2010.* **4.** *Бабак В. П. Теоретические основы защиты информации / Бабак В. П., Ключников А. А. – НАН Украины, Ин-т проблем безопасности АЭС.– Чернобыль (Киев.обл.): Ин-т проблем безопасности АЭС, 2012.– с.776* **5.** *Хорошко В. О. Методичне забезпечення підготовки та перепідготовки спеціалістів з інформаційної безпеки / Хорошко В. О., Орєхова І. І. // Сучасна спеціальна техніка, №3, 2011. – С. 22-27.*

Дмитро Мехед
Чернігівський національний технологічний університет

УДК 004.773

ІНФОРМАЦІЙНА БЕЗПЕКА В СОЦІАЛЬНИХ МЕРЕЖАХ. МЕТОДИ ПОШИРЕННЯ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ

Анотація: **Розглядаються соціальні мережі, основні методи поширення інформації в соціальних мережах, зроблено аналіз переваг і недоліків різних методів захисту інформації. Проаналізовано метод визначення стратегії розповсюдження інформації в соціальній мережі, виділено основні параметри, які є базовими для забезпечення захисту інформації, можливість втрати інформації, а також методи її захисту.**

Summary: **In the article the social networks, the main methods of dissemination of information in social networks, the analysis of the advantages and disadvantages of various methods of data protection. The analysis method for determining the strategy of information dissemination in social networks highlights the main parameters that are fundamental to protect information, the possibility of loss of information, as well as methods of protection.**

Ключові слова: **Інформація, інформаційна безпека, соціальні мережі.**

Характерною особливістю сучасності є та обставина, що до активної участі в інформаційних процесах у дуже стислі строки долучилися широкі маси користувачів, що в переважній більшості не мають відповідного рівня підготовки до участі в суспільно корисній інформаційній діяльності. Для значної частини учасників інформаційних обмінів самовираження в Інтернеті поки що є значущим як процес. І тому сьогодні інформаційний простір перевантажений випадковою, низькоякісною інформацією, що ускладнює використання суспільно значущих ресурсів. Однак останнім часом з розвитком інформаційних технологій, удосконаленням загальносуспільної системи соціальних інформаційних комунікацій в Україні ми спостерігаємо характерний також і для інших країн світу процес самоорганізації вітчизняного інформаційного простору, формування системи соціальних інформаційних мереж [1].

Є два різні способи, за допомогою яких людина отримує інформацію в мережі: – через зв'язки в соціальних мережах і під впливом зовнішніх немережевих джерел, таких як традиційні ЗМІ [2]. Хоча більшість нинішніх моделей сприйняття інформації в мережах виходять з того, що інформація лише передається від одного вузла до іншого по краях (периферії) базової мережі, доступність даних в масових соціальних мережах в Інтернеті дозволяє нам докладніше дослідити цей процес. Таким чином соціальні мережі відіграють фундаментальну роль у поширенні інформації.

Соціальна мережа (від англ. Social networking service) – платформа, онлайн сервіс або веб-сайт, призначені для побудови, відображення та організації соціальних взаємовідносин, візуалізацією яких є соціальні графи [3]. Наразі кількість соціальних мереж в Інтернеті і число їх користувачів швидко зростає (соціальні мережі стартували в 1995 р, в 2000-і набули глобального розмаху).

Соціальні мережі – явище нове, але йому передував ряд філософських концепцій. Наприклад, китайська концепція Guanxi про використання особистого впливу на основі особливого виду особистих відносин, таких як повага, дружнє ставлення та готовність надати один одному взаємну допомогу або послугу [3]. Цю концепцію пов'язують з поняттями «суспільство», в якому індивіди більш орієнтовані на дотримання інтересів оточуючих, ніж своїх власних.

Особиста інформація ще ніколи не була такою доступною, як нині. Ситуація загострюється ще й через те, що більшість користувачів не знає елементарних правил безпеки онлайнового спілкування і використання

соціальних мереж. Більшість людей намагаються перетворити на реальність слова: «все, що ви скажете в соціальних мережах, може бути використано проти вас». В сучасному суспільстві є звичка використовувати соціальні мережі й інтернет, але практично не вироблена культура онлайн-спілкування і використання соціальних сервісів [4].

Аналіз останніх досліджень і публікацій. Дослідженню питань інформаційної безпеки присвячені роботи В. М. Богуна, С. В. Віхорева, І. Д. Горбенко, Ю. І. Грицюк, М. А. Жалдака, С. В. Казмирчук, Г. Ф. Конаховича, О. Г. Корченка, М. Г. Луцького, А. І. Марущака, В. П. Мельнікова, В. В. Мохора, О. М. Новікова, О. В. Олійника, С. А. Ракова, О. В. Сосніна, С. В. Толюпи, В. О. Хорошко, О. К. Юдіна та ін.

Виділення не вирішених раніше частин загальної проблеми. Незважаючи на значний обсяг накопичених у даній сфері знань, недостатньо дослідженою залишилась проблема захисту інформації соціальних мереж.

Метою дослідження було охарактеризувати та систематизувати методи поширення інформації в соціальних мережах, висвітлити основні причини можливості втрати інформації та методи її захисту.

Виклад основного матеріалу. Поняття «соціальні мережі» вперше ввів соціолог Джеймс Барнс: «Соціальна мережа (Social Network) – це соціальна структура, що складається з групи вузлів, якими є соціальні об'єкти (люди або організації), і зв'язків між ними» [5].

У найпростішій формі соціальна мережа - це карта всіх релевантних зв'язків між вузлами. Формально соціальна мережа являє собою граф S (G, E), в якому G = {1, 2, ..., n} - множина вершин (агентів) і E - безліч ребер, що відображають взаємодію агентів. Агент - це вузол соціальної мережі (вершина графа). Агентами можуть стати різні субагенти, наприклад сім'ї, групи, організації. Зв'язки між агентами - це відносини, наприклад, знайомство, дружба, співпраця, комунікації. Агенти залежно від інформації, якою вони володіють, можуть впливати на прийняття рішення, на інших агентів, інформаційне управління та інформаційне протиборство.

Якщо розглядати соціальну мережу більш глибоко, можна виявити, що зв'язки діляться за типами: односторонні і двосторонні; мережі друзів, знайомих, колег, однокласників, однокурсників, однодумців і т. д. Соціальна мережа – це ще й засіб спілкування. Будь-якій людині емоційно важлива думка інших людей, в тому числі, коли все добре – їх визнання, а коли наступила смуга невдач – співчуття і співучасть. Ритм життя стає таким, що часу на традиційне спілкування з друзями зараз залишається все менше і менше. І соціальні мережі з цієї точки зору – незамінна річ, оскільки дають можливість спілкуватися, не витрачаючи часу на дорогу, не погоджуючи зручні проміжки часу.

Одним з результатів взаємодії людей за допомогою таких мереж є отримання величезної кількості інформації різних форматів: тексти, картинки, аудіо, відео та ін. Сьогодні соціальні мережі надають користувачам широкий функціонал для обміну інформацією, їх відвідує більш ніж дві третини онлайн-аудиторії у всьому світі, і це четверта за популярністю онлайн-категорія після пошукових і інформаційних порталів та програмного забезпечення.

Розглянемо методи поширення інформації в соціальних мережах.

Контекстна реклама. Даний метод поширення інформації в соціальній мережі дозволяє демонструвати рекламні оголошення на особистій сторінці користувача і в додатках соціальної мережі згідно з обраними параметрами. Основною перевагою даного методу є можливість вибору цільової аудиторії по ряду параметрів: демографія, географія, інтереси, освіта, робота та інші параметри. Даний вид поширення інформації є платним, але має високу ефективність. Інформація, поширювана через контекстну рекламу, має обмеження, встановлені адміністрацією соціальної мережі. Вся поширювана інформація проходить модерацію перед розповсюдженням. Протизаконна інформація не може бути поширена через контекстну рекламу.

Масова розсилка особистих повідомлень (спам). Даний вид поширення інформації в соціальній мережі передбачає розсилку особистих повідомлень користувачам. Розсилка спаму є безкоштовним засобом доставки контенту користувачам, але адміністрація соціальної мережі бореться з цим явищем. Для обмеження розсилки спаму адміністратори блокують акаунти, обмежують кількість відправлених повідомлень, вимагають прив'язки аккаунта до телефону, обмежують обсяг вибірки за запитом, встановлюють спам-фільтри, дають можливість вносити користувачів в чорні списки і позначати повідомлення як спам для виключення подальшого їх отримання. Даний метод поширення інформації є частково неконтрольованим; користувач може поширювати будь-яку інформацію, у тому числі протизаконну.

Несанкціонована розсилка повідомлень по «стінам» великих спільнот. Даний метод поширення інформації в соціальних мережах є більш ефективним, ніж розсилка особистих повідомлень. Даний метод дозволяє охопити більшу аудиторію, також не схильний модерації з боку адміністрації соціальної мережі. Захистом спільноти від нелегітимної інформації в даному випадку займаються адміністратори спільноти.

Розміщення інформації у власному співтоваристві або тематичному обліковому записі. Даний метод поширення інформації в соціальній мережі є найпопулярнішим серед безкоштовних методів. Для охоплення необхідної аудиторії співтовариство спочатку має набрати необхідну масу учасників. З ростом популярності спільноти підвищується його пошуковий індекс в соціальній мережі, що в свою чергу дозволяє залучати більшу кількість користувачів. Важливою перевагою даного методу є високий ступінь довіри користувачів до інформації, що публікується.

Конкурси в соціальній мережі. Даний метод є наймолодшим і передбачає проведення промо-конкурсів для залучення користувачів. Для участі в даному конкурсі користувач повинен поділитися інформацією зі своїми друзями, у відсилаємому повідомленні якраз міститься поширювана інформація і запрошення взяти участь у конкурсі. Перевагою даного методу поширення інформації є висока швидкість розповсюдження і довіра до інформації з боку користувачів.

Розглянуті вище методи поширення інформації є ефективними інструментами для охоплення онлайн-аудиторії. Кожен метод має свої переваги і недоліки. Важливою з точки зору ініціатора поширення інформації є задача вибору методів поширення з мінімальними затратами ресурсів. Для вирішення даної задачі розробимо метод визначення стратегії розповсюдження інформації в соціальній мережі.

На підставі наведених значень характеристик методів можна розробити метод визначення стратегії розповсюдження інформації в соціальній мережі. Метод включає наступні елементи:

1) визначення характеристик рекламного проекту;

2) визначення переліку застосовних методів поширення інформації;

3) визначення можливостей одночасного застосування доступних методів, або окремих найбільш ефективних в даних умовах методів;

4) оцінка охоплення аудиторії поширення інформації.

Будучи однією зі складових інформаційної безпеки суспільства культурна безпека впливає на інші складові національної стабільності та благополуччя. У соціальних мережах міститься велика кількість особистої інформації про учасників, наприклад, інтереси, друзі, демографія та ін. Це може призвести до несанкціонованого поширення особистої інформації в мережах. У рішенні такого типу завдань корисно застосовувати моделі на основі механізмів конфіденційності.

Учасники соціальної мережі, щоб вона існувала, повинні ділитися один з одним певною частиною своєї особистої інформації. В останні 3 – 4 роки тема інформаційної безпеки та приватності в соціальних мережах привертає багато уваги. Це цілком зрозуміло: мережі все більше відкриваються зовнішньому світу, були випадки витоку особистих даних, аккаунти користувачів легко зламуються, а в адміністрації мереж є доступ до будь-якої інформації. Але все це тільки зовнішня частина, яка лежить на поверхні і про яку пише преса, проте далеко не повна картина потенційних загроз для особистих даних. Із психологічної точки зору Інтернет сприймається людиною на рівні натовпу. А в натовпі, як відомо, обличчя і індивідуальність зникає, а з нею і відповідальність [6].

Самим нешкідливим, на перший погляд, варіантом використання особистих даних без дозволу користувача можна вважати внутрішні механізми соціальних мереж для показу реклами, підбору потенційних знайомих або відбору потенційно цікавого контенту. Ці механізми стали стандартом майже у всіх соціальних мережах, і ніхто не приховує даний факт: всі вони збирають і аналізують особисті дані, яких у будь-якій мережі дуже багато, а потім використовують їх у комерційних цілях. Більше того, соціальні мережі передають особисті дані у зовнішній світ, і вже офіційно встигли визнати цей факт.

Більше проблем користувачам створює витік особистих даних з вини мережі, що неодноразово траплялося в різних проектах. Однією з найбільших за розмірами можна вважати витік особистих даних 77 млн. користувачів ігрової мережі PlayStation Network у квітні 2011 року, і ще до кінця не ясні наслідки цього інциденту. Як правило, у подібних випадках має місце витік платіжних даних користувачів.

Ще більш серйозні проблеми може викликати злом окремих аккаунтів і отримання доступу до всієї особистої інформації окремого користувача, якщо мета зловмисників – певна людина. Зробити сьогодні це не складно навіть для буденного користувача, який просто знає людину і може використовувати соціальну інженерію, а крім того є спеціальні послуги по злому, вартість цього всього 20 $. Мотивація зловмисників може бути різноманітною, від злому аккаунтів посадових осіб певної компанії з метою промислового шпигунства до особистих цілей. Так, наприклад, шлюбні юристи США вже зараз фіксують кожен п'ятий випадок розлучення через соціальні мережі: подружжя отримують доступ до профілю партнера, знаходять там переписку з коханцем / коханкою, і в результаті це призводить до розлучення [7].

Окремо варто згадати про віруси і фішинг, які можуть непомітно для користувача красти логіни і паролі і після використовувати їх для незаконних дій (наприклад, автоматична розсилка спаму від імені користувача).

Однак найбільша загроза полягає в тому, що доступ до всієї особистої інформації є у досить великої групи людей, і вони можуть в будь-який момент її переглядати, навіть, якщо людина видалила щось з

мережі. По-перше, це співробітники самої соціальної мережі: у них є доступ до баз даних, в яких міститься вся інформація, а також спеціальні інструменти входу в аккаунти користувачів, як, наприклад, спеціальний майстер-пароль в Facebook, який дозволяє увійти в будь-який аккаунт. По-друге, доступ до інформації також мають правоохоронні органи, такі як ЦРУ в США або ФСБ в Росії.

Останнім часом користувачі все менше довіряють соціальним мережам і все частіше починають фільтрувати інформацію, яку готові довірити мережі, давати неправдиву інформацію або взагалі видаляються з мережі, однак навіть видалення не дає впевненості: часто інформація зберігається на серверах компанії і може використовуватися в подальшому. Зокрема так робить Facebook, ВКонтакте і інші мережі.

Виділимо основні параметри, які є базовими для забезпечення захисту інформації:

- конфіденційність - гарантія того, що конкретна інформація доступна тільки тому колу осіб, для кого вона призначена; порушення цієї категорії називається розкраданням або розкриттям інформації;
- цілісність - гарантія того, що інформація зараз існує в її початковому вигляді, тобто при її зберіганні або передачі не було проведено несанкціонованих змін; порушення цієї категорії називається фальсифікацією повідомлення;
- автентичність - гарантія того, що джерелом інформації є саме та особа, яку заявлено як її автора; порушення цієї категорії також називається фальсифікацією, але вже автора повідомлення;
- апелюємість - гарантія того, що при необхідності можна буде довести, що автором повідомлення є саме заявлена людина, і не може бути ніхто інший; відмінність цієї категорії від попередньої в тому, що при підміні автора, інша людина намагається привласнити собі авторство повідомлення, а при порушенні апеллюємості – сам автор намагається «відхреститися» від своїх слів.

Загрози інформаційної безпеки – це зворотний бік використання інформаційних технологій. Загроза – це потенційна можливість певним чином порушити інформаційну безпеку.

При системному розгляді різних видів порушень захисту конфіденційної інформації в соціальній мережі відповідно до якісно-кількісних характеристик циркулюючої всередині мережі інформації необхідними для оцінки її вразливостей за ступенем важливості для механізмів захисту можна виділити наступні типи основних загроз інформації в соціальній мережі:

- загроза конфіденційності (витік конфіденційної інформації та заподіяння прямого або непрямого збитку користувачеві соціальної мережі);
- загроза цілісності (модифікація інформації усередині мережі інформації і втрата її адекватності);
- загроза доступності (порушення доступу до мережевої інформації і блокування доступу до ресурсу);
- загроза повноті (знищення інформації усередині мережі та заподіяння прямого або непрямого збитку як користувачеві соціальної мережі, так і її власнику);
- загроза актуальності (затримка отримання легальним користувачем мережі інформації);
- загроза важливості (несанкціоноване читання конфіденційної мережевої інформації, що призводить до втрати її ціннісних характеристик);
- загроза адресності (переадресація мережевої інформації, що може призводити до зниження її конфіденційності та доступності);
- загроза надмірності інформації (багаторазове дублювання мережевої інформації).

На жаль, на законодавчому рівні проблема щодо захисту інформації користувача недостатньо опрацьована. Забезпечення безпеки персональних даних в більшості випадків регламентується виключно правилами захисту інформації про користувачів і правилами користування сайтом.

Висновки. Розвиток електронних технологій дозволяє мільйонам людей вільно користуватись мережею, що дає змогу використовувати їх творчий потенціал для вирішення інтелектуальних, наукових, суспільно значимих питань. В силу причин, описаних у даній статті, можна зробити висновок, що тема захисту інформації користувачів в соціальних мережах залишатиметься актуальною як мінімум в найближчі роки. Проблеми захисту інформації в даній сфері досі остаточно не вирішені і можуть вирішитися тільки в результаті комплексного підходу, що включає в себе спільну роботу творців і розробників мережі, користувачів і держави. Особливого значення набуває питання захисту інформації на фоні формування горизонтальних, корпоративних зв'язків з використанням електронних технологій, зокрема у сфері освіти, а також серед наукової спільноти.

Список використаної літератури. ***1.*** *Соціальні мережі як чинник розвитку громадянського суспільства : [монографія] / [О. С. Онищенко, В. М. Горовий, В. І. Попик та ін.] ; НАН України, Нац. б-ка України ім. В. І. Вернадського. – К., 2013. – 220 с.* **2.** *Типове положення про службу захисту інформації в автоматизованій системі. – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=39738&cat_id=38.* ***3.*** *Соціальна мережа (Інтернет) . – Режим доступу: https://uk.wikipedia.org/wiki/Соціальна_мережа_(інтернет)* ***4.*** *Баловсяк Н. Соціальні мережі вбивають приватність / Тиждень.ua., 2013/ - Режим доступу: http://tyzhden.ua/Society/70950.* ***5.*** *Barnes J. A. Class and Committees in a Norwegian*

Island Parish // Human Relations. 1954. №7. Pp. 39-58. **6.** *Соціальні мережі – реальні загрози віртуального світу. – Режим доступу:* http://ogo.ua/articles/view/2011-02-23/26490.html. **7.** *Как социальные сети разрушают брак. – Режим доступу:* http://letidor.ru/article/kak_sotsialnye_seti_razrushayu_138521/

Владимир Бурячок, Андрей Орехов, Владимир Хорошко
Национальный Авиационный Университет

УДК 004.621.5

ОПТИМИЗАЦИЯ АРХИТЕКТУРЫ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА СУВД

Аннотация: ***Приведена методика формирования профиля защищенности, которая позволяет осуществить выбор оптимального варианта построения системы комплексной защиты информации для информационного пространства системы управления воздушным движением (СУВД).***

Annotation: ***The article describes the method of forming the profile of security, which allows for selection of the optimal variant of building a system of complex information protection to the information space air traffic control system.***

Ключевые слова: ***система защиты информации, информационное пространство, система управления воздушным движением, профиль защищенности, архитектура.***

I Введение

Важным является вопрос оптимизации и унификации подходов к реализации мероприятий по обеспечению информационной безопасности как наиболее сложному и трудоемкому компоненту, обеспечивающему безопасность информации в системе управления воздушным движением. Особую роль играет при этом правильный выбор архитектуры системы защиты.

Целью защиты информации в СУВД является деятельность, направленная на предотвращение утечки ее по различным каналам и их блокирования.

Основной стратегией защиты информации является выбор основных и наиболее важных базовых системно-концептуальных положений и ориентиров при планировании, разработке и реализации этой стратегии. Основы стратегии защиты информации включают в себя необходимость использования двух терминологических понятий [1, 2]:

- стратегия технической защиты информации;
- стратегия безопасности защищаемой информации.

На практике в большинстве случаев системы защиты состоят из нескольких звеньев и рубежей. При попытке преодолеть защиту злоумышленник пытается использовать наиболее слабое направление или рубеж в этой системе. По этой причине итоговая прочность системы комплексной защиты информации (СКЗИ) будет определяться прочностью наиболее слабого направления или рубежа в этой системе.

II Основная часть

Так как итоговая прочность СКЗИ определяется прочностью наиболее слабого звена, рубежа или направления в этой системе, то, следовательно, если прочность слабого звена, рубежа или направления не удовлетворяет заданным и требуемым уровням, то это звено, рубеж или направление укрепляется или заменяется на более прочный.

Исходя из этого вероятность эффективной защиты информации при многорубежной системе определяется зависимостью:

$$P_{ИТ} = P_{СКЗИ_1} \cdot P_{СКЗИ_2} \cdot \ldots \cdot P_{СКЗИ_N},$$

где $P_{СКЗИ_N}$ - вероятность эффективной защиты *n*-го рубежа СКЗИ, *n* – порядковый номер рубежа.

Под задачей синтеза комплексной системы защиты информации понимается этап формирования профиля защищенности информационного пространства (ИП) как основополагающий при создании СКЗИ. В общем виде задача синтеза сводится к формированию оптимального варианта реализации профиля защищенности, обеспечивающего максимум предотвращенного ущерба от воздействия угроз при допустимых затратах на создание СКЗИ информационного пространства СУВД. В соответствии со стандартом [3], известным также как "Общие критерии, разработка профиля защищенности" предполагается выполнение следующих мероприятий:

УДК 373.1:004.056

ІНФОРМАЦІЙНА БЕЗПЕКА ПІДЛІТКІВ В ІНТЕРНЕТ МЕРЕЖІ

Варивода К.С.
Переяслав-Хмельницький державний педагогічний університет
імені Григорія Сковороди

Інтернет несе в собі великий інформаційний та освітній потенціал, але водночас містить і ризики, особливо для підлітків. Саме тому у статті розглядається проблема інформаційного захисту підлітків у віртуальному просторі. У статті підкреслюється, що для ефективного забезпечення інформаційної безпеки підлітків необхідно дотримуватися єдності вимог та співпраці вчителів і батьків у цьому питанні. Визначено заходи щодо забезпечення інформаційної безпеки підлітків: правові, технічні та програмні, виховні та організаційні, моральні та етичні, захист психіки і здоров'я людини. Зазначається, що навчання і виховання підлітків з питань інформаційної безпеки повинно сприяти розвитку інформаційно-комунікаційних компетентностей, серед яких: грамотний і успішний пошук інформації; критична оцінка інформації; творення, перетворення і презентація інформаційного змісту; правові засади творення й поширення інформаційного змісту; емпатія й образотворення; безпека і приватність; участь у мережних спільнотах.
Ключові слова: підлітки, інтернет, інформаційна безпека, он-лайн безпека підлітків.

Постановка проблеми. Сучасні підлітки живуть в інформаційну суспільстві, де будь-який медійний продукт – це, в певному сенсі, реклама способу життя та тих чи інших цінностей, які впливають на результати їх вибору. Підліткова психіка нерідко виявляється непідготовленою до інформаційного вибуху і без адекватного захисту постає достатньо вразливою. Таким чином, гостро постає питання стосовно інформаційної безпеки підлітків. Уміння добирати, аналізувати, оцінювати й використовувати інформацію є сьогодні актуальним для підлітків. Адже їм бракує життєвого досвіду, моральної позиції та принциповості. Підлітки схильні до некритичного наслідування, ототожнюють себе із побаченим, копіюють учинки й дії своїх кумирів. Саме тому, в сучасних умовах потрібні механізми фільтрації, а також інструменти захисту від небажаних

інформаційних потоків. Водночас у підлітків слід формувати компетентності роботи з інформацією в Інтернет мережі.

Аналіз останніх досліджень і публікацій. Проблеми інформаційної безпеки підростаючого покоління є одними з найважливіших у процесі виховання та навчання. Становлення наукового напрямку інформаційна безпека пов'язане з іменами таких видатних учених, як В.А. Гераськенко, П.Д. Зегжда, А.О. Малюк, В.В. Мельшков, В.В. Хорошко, В.І. Ярочкін. та ін. Питання інформаційної безпеки в педагогічній науці є новою та мало дослідженою галуззю міждисциплінарного знання. Методику навчання інформаційної безпеки в школі та підготовки непрофільних спеціалістів, зокрема вчителів інформатики, розробляють: М.О. Абіссова, О.А. Алтуф'єва, Л.В. Астахова, В.О. Гріцик, І.М. Кірко, П.С. Ломаско, В.П. Поляков, Е.В. Татова, Г.Н. Чусавітіна. Проблему забезпечення інформаційної безпеки школяра в умовах ЗНЗ досліджують М.І. Бочаров, Т.О. Малих, Н.І. Саттарова, О.Ю. Федосов та ін.

Виділення не вирішених раніше частин загальної проблеми. Питанням інформаційної та комп'ютерної безпеки у сімейному та позакласному вихованні в нашій країні приділяється ще недостатньо уваги. Не достатньо враховуються особливості психолого-вікової періодизації у формуванні інформаційно безпечної особистості. Адже методи забезпечення інформаційної безпеки підлітків та виховний вплив має бути адекватний віковим особливостям та рівню розвитку дитини, для того щоб отримати оптимальний результат виховних заходів і забезпечити безпечну соціалізацію особи в інформаційному середовищі.

Мета статті. Головна мета цієї роботи полягає в комплексному розгляді питань навчання та виховання, пов'язаних із застосування інформаційно-комп'ютерних технологій підлітками, з урахуванням проблем інформаційної безпеки неповнолітніх користувачів.

Виклад основного матеріалу. Для підлітків Інтернет стає частиною життя. Вони знайомляться з новими людьми і проводять чимало часу в он-лайн, шукають необхідну інформацію, яка має відношення до їхніх шкільних завдань або відповідає їхнім інтересам. Завдяки більш високому рівню грамотності це відкриває багато можливостей використання Інтернету. Водночас, чимало дітей і підлітків, використовуючи Інтернет, навіть не замислюються про те, яка небезпека чекає на них [3, с. 60].

Водночас варто зазначити, що естетичні смаки та моральні якості підлітків 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. Також, існує причинно-наслідковий зв'язок між «розважальним медіанасильством» і проявами агресії серед підлітків. Негативна інформація впливає на ціннісні орієнтації особистості і підлітки, у яких ще недостатньо сформована психіка, вважають, що насильство – прийнятний шлях вирішення соціальних конфліктів. Все це підтверджує і той факт, що досить часто неповнолітні правопорушники серед причин, які штовхнули їх на скоєння злочину, називають перегляд відповідних відеоматеріалів.

Окрім цього, використовуючи Інтернет підлітки (добровільно чи неупереджено) дізнаються про секс і сексуальність шляхом доступу до порнографічних матеріалів. Також існують випадки потрапляння в сексуальне рабство через спілкування з особами, які пропонують знайомства, просять надіслати фотокартки, а потім використовуючи монтаж, розміщують їх на порно-сайтах [4, с. 7].

Занепокоєння викликає і той факт, що останнім часом серед підлітків 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. bulling, від bully – хуліган, забіяка, грубіян, ґвалтівник). Це поняття означає залякування, фізичний або психологічний терор стосовно особистості з боку групи підлітків, 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» [3, с. 61].

Однією з основних проблем для вчителів і батьків є не контрольованість Інтернету як джерела інформації, відомостей і даних. Оскільки глобальна комп'ютерна мережа містить багато матеріалів, які не тільки не є корисними для дітей і підлітків, але й можуть завдати шкоду їх психічному, моральному чи навіть фізичному здоров'ю.

Для того щоб захистити підлітків від психологічного, морального та фізичного насильства в Інтернеті, а також загроз і викликів, які несе сьогодні інформаційний простір, необхідна взаємодія сім'ї та загальноосвітніх навчальних закладів, зокрема щодо питання формування у підлітків компетенцій безпечної роботи з інформацією в Інтернеті [2, с. 45].

Одним зі шляхів забезпечення інформаційної безпеки підлітків є організація безпечного особистісного інформаційного простору як у школі, так і в сім'ї. Організувати безпечний інформаційний простір можливо шляхом реалізації засобів та заходів щодо інформаційної безпеки підлітків, серед яких: правові, технічні та програмні, виховні й організаційні, моральні й етичні [6, с. 75].

Правові засоби – це спеціальні закони й інші нормативні акти, правила, процедури та заходи щодо забезпечення особистісного інформаційного середовища підлітків на законодавчій і правовій основі для реалізації єдиної державної політики у сфері захисту дітей від інформаційних матеріалів, що завдають шкоди їх здоров'ю та психіці.

Технічні і програмні заходи передбачають використання різного роду апаратного і програмного забезпечення для перешкоджання нанесення матеріальної та моральної шкоди підлітку (програми Батьківського контролю, мережних фільтрів, технічних засобів захисту даних).

Виховні заходи – формування у підростаючого покоління культури безпеки, відповідальності за здійснені дії в інформаційному просторі, виховання й укріплення духовно-моральних цінностей, патріотизму, готовність батьків і педагогів до прийняття позиції дитини та поваги до її самостійності.

Організаційні заходи – це регламентація інформаційної діяльності підлітків, контроль за

використанням мережевих сервісів і спільнот, що виключає або послаблює нанесення шкоди особистому інформаційному середовищу дитини.

Моральні та етичні заходи включають в себе дотримання підлітками під час здійснення інформаційної діяльності норм і правил поведінки в суспільстві, а також мережевої культури й етики, що утворюються з розповсюдженням інформаційних технологій у сучасному інформаційному суспільстві [1, с. 16].

Варто зазначити, що батьківський і виховательський контроль за тим, що саме підлітки роблять в Інтернеті є часто малоефективний з огляду на недостатню компетентність педагогів і батьків щодо застосування програм-фільтрів, що блокують звертання до відомих адрес із сумнівним змістом. Відомий спеціаліст з питань безпеки дітей в Інтернеті Паррі Афтаб справедливо підкреслює, що найкращий фільтр, який може дійсно забезпечити безпеку дитини в мережі й розв'язати багато інших проблем, – у голові в самої дитини, а дорослим потрібно тільки «налаштувати» цей фільтр. Отже основна роль у забезпеченні власної безпеки належить особистості, тому провідну роль у недопущенні доступу підлітків до матеріалів, несумісних із завданнями навчання, особливо за переважної відсутності контент-фільтруючих програм у школі і вдома, є навчання і виховання з метою формування інформаційно безпечної особистості [2, с. 48].

Суттєву роль у забезпеченні інформаційної безпеки неповнолітніх має відігравати система освіти. Вона зобов'язана забезпечувати умови безпечної соціалізації особистості у комп'ютерно орієнтованому навчальному середовищі та формувати культуру й компетентність в галузі інформаційної безпеки.

Першочергово вчителям основ здоров'я та інформатики, класним керівникам та заступникам директора з виховної роботи слід ініціювати проведення загальних батьківських зборів щодо питань безпеки при використанні підлітками Інтернету та їхнього спілкування в різноманітних соціальних мережах. Батьків учнів на батьківських зборах потрібно переконувати у важливості довірливого спілкування зі своїми дітьми на предмет виявлення соціальних зв'язків через Інтернет та ЗМІ, слід надавати їм поради щодо безпеки стосунків із невідомими людьми, як у побуті, так і віртуальному світі [6, с. 76].

Окрім цього, на уроках основ здоров'я вивчають тему «Соціальні чинники здоров'я» (7 клас), яка розглядає питання захисту від жорстокості, дискримінації і насилля. Як доповнення на уроках інформатики в ході вивчення теми «Всесвітня мережа Інтернет» варто зупинитися на тому, що учень у такому віці не здатен адекватно оцінювати достовірність інформації, наданої Інтернет-мережею. Тому вчителям інформатики під час вивчення цієї теми й учителю основ здоров'я в ході викладання уроків теми «Профілактика соціально небезпечних захворювань» (розділу «Соціальні чинники здоров'я»), а класним керівникам – у позакласній виховній роботі, слід застерігати учнів від небезпеки, яку несе пропаганда хибних цінностей, комерційна реклама та романтизація насилля. Так, скажімо, телебачення демонструє привабливі рольові моделі, але деякі з них спотворюють уявлення про добро і зло та романтизують насилля. Підлітки часто сприймають це з піднесенням, ніби стають на місце героя. У цій ситуації потрібно запропонувати учням уявити себе не на місці героя, а на місці жертви. Як би вони себе почували в ролі переможеного і скривдженого?

У восьмому класі на уроках основ здоров'я вивчають тему «Інформаційна безпека», у якій розглядаються поняття «інформації», варто обговорити питання впливу інформаційної зброї на здоров'я учнів, методи та засоби запобігання впливу негативної інформації тощо. На уроках інформатики проводячи дискусію, під час якої обговорюються ці питання, слід підвести учнів до висновку, що від впливу негативної інформації можна уберегтися, якщо усвідомлювати можливі наслідки. Важливо підкреслити учням, що з будь-яких питань стосовно інформаційної безпеки вони завжди можуть звернутися за порадою до вчителів і батьків [7, с. 10].

Основним завданням спільної взаємодії батьків і вчителів в процесі навчання і виховання підлітків з питань інформаційної безпеки повинно бути формування у них інформаційно-комунікаційних компетентностей щодо користування Інтернетом. Зокрема серед таких компетентностей слід виділити:

1. Грамотний і успішний пошук інформації: розпізнавання інформаційних потреб; формулювання питань, що відображають інформаційні потреби; знання про існування багатьох інформаційних джерел; пошук, вибір і оцінка інформаційного джерела; зберігання інформації.

2. Критична оцінка інформації: розуміння змісту інформаційного повідомлення; вибір і оцінювання інформації; прийняття рішення про те, що є фактом, а що точкою зору; вирізнення рекламних текстів.

3. Творення, перетворення і презентація інформаційного змісту: творення нового інформаційного змісту; перетворення знайденого в Інтернеті або раніше самостійно створеного інформаційного змісту; презентація нового або перетвореного інформаційного змісту.

4. Правові засади творення й поширення інформаційного змісту: усвідомлення правового й етичного вимірів творення інформації; знання, який інформаційний зміст можна перетворювати відповідно до правових засад; знання своїх прав як творця інформації, розміщеної в Інтернеті; усвідомлення різниці між Інтернет-комунікацією й спілкуванням поза Інтернетом.

5. Емпатія й образотворення: знання про те, що Інтернет є простором спільної комунікації з іншими людьми; виявлення емпатії в мережі; створення обдуманого й адекватного власного образу.

6. Безпека і приватність: знання про загрози, пов'язані з перебуванням в Інтернеті; уміння запобігти небезпекам в Інтернеті; здійснення контролю над інформацією, яка передається іншим; усвідомлення різниці між Інтернет-комунікацією й спілкуванням поза Інтернетом; застосування гігієнічних засад, пов'язаних з використанням комп'ютера.

7. Участь у соціальних електронних мережах: розпізнання елементів Інтернет-культури; активна участь у мережних соціальних спільнотах; ініціативність в розвитку мережних соціальних спільнот, створених для спільних дій [5, с. 37].

Висновки і пропозиції. Таким чином, інформаційна безпека безпосередньо залежить від рівня і якості освіченості молодого покоління, ступеня зрілості особистості й готовності її до самореалізації в суспільстві. Саме тому виникає гостра необхідність розширення змісту загальної середньої освіти, використання нових компонентів, пов'язаних із навчанням підлітків інформаційної безпеки. Основною запорукою усунення основних проблем інформаційної небезпеки віртуального світу є об'єднання зусиль вчителів, батьків і громадськості задля більш ефективного навчання підлітків правилам безпечного поводження у світовій мережі.

Список літератури:

1. Богатырева Ю. И. Модель обеспечения информационной безопасности школьников при создании инфобезопасной среды образовательного учреждения / Ю. И. Богатырева // Известия Тульского государственного университета. Гуманитарные науки. – 2013. – Выпуск № 3-2. – С. 14-25.
2. Ковальчук В. Н. Забезпечення інформаційної безпеки старшокласників у комп'ютерно-орієнтованому навчальному середовищі: дис. ... канд. пед. наук: 13.00.10 / Ковальчук Вікторія Наумівна. – Житомир, 2011. – 291 с.
3. Ковальчук В. Н. Проблеми інформаційної безпеки дітей різних вікових категорій / В. Н. Ковальчук // Комп'ютер у школі та сім'ї. – 2010. – № 8. – С. 58-62.
4. Куницький В. В. Захист неповнолітніх в інформаційному просторі як об'єкт гуманітарної експертизи: український та зарубіжний досвід. [Електронний ресурс] / В. В. Куницький // Державне управління: теорія та практика. – К.: 2011. Режим доступу: http://www.academy.gov.ua/ej/ej14/txts/Kunitskiy.pdf
5. Лещенко М. П. Підходи до стандартизації сформованості інформаційно-комунікаційної компетентності учнів: польський досвід / М. П. Лещенко, Л. І. Тимчук // Інформаційні технології і засоби навчання. – 2014. – Т. 42, № 4. – С. 33-46.
6. Підгорна Т. Деякі аспекти організації інформаційної безпеки учнів / Т. Підгорна, І. Берест // Педагогіка і психологія професійної освіти. – 2014. – № 6. – С. 70-78.
7. Шахненко В. І. Пропаганда інформаційної безпеки на уроках основ здоров'я й інформатики / В. І. Шахненко, А. В. Тріщук // Основи здоров'я. – 2015. –№ 3 (51). – С. 9-11.

Варывода Е.С.
Переяслав-Хмельницкий государственный университет
имени Григория Сковороды

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПОДРОСТКОВ В ИНТЕРНЕТ СЕТИ

Аннотация
Интернет несет в себе большой информационный и образовательный потенциал, но одновременно содержит и опасности, особенно для подростков. Именно поэтому, в статье рассматривается проблема информационной защиты подростков в виртуальном пространстве. В статье подчеркивается, что для эффективного обеспечения информационной безопасности подростков необходимо соблюдать единство требований и сотрудничества учителей и родителей в этом вопросе. Определены аспекты по обеспечению информационной безопасности подростков: правовые, технические и программные, воспитательные и организационные, моральные и этические, защита психики и здоровья человека. Отмечается, что обучение и воспитание подростков по вопросам информационной безопасности должно способствовать развитию информационно-коммуникационных компетенций, среди которых: грамотный и успешный поиск информации; критическая оценка информации; создание, преобразование и презентация информационного содержания; правовые основы создания и распространения информационного содержания; эмпатия и создание образов, безопасность и приватность, участие в сетевых сообществах.
Ключевые слова: подростки, интернет, информационная безопасность, он-лайн безопасность подростков.

Varyvoda E.S.
Pereyaslav-Khmelnitskiy Gregory Skovoroda State Pedagogical University

INFORMATIONAL SECURITY OF TEENS IN THE INTERNET

Summary
Internet contains great the potential of information and education but simultaneous contain some risks especial for teens. Therefore, the article examines the problem of informational security teens in virtual space. The article emphasizes that the effective maintenance of teens informational safety requires of teachers and parents in this regard to comply with the requirements of unity and cooperation. It analyses the measures to ensure the information security of teenagers: legal, technical and programmatic, organizational and educational, moral and ethical, mental and health protection. It is noted that the education and upbringing of teens on issues of informational safety should promote the development of information-communications competences, including: literate and successful information search, critical evaluation of information, creation, transformation and presentation of information content, legal principles of creation and distribution of informational content, empathy and image making, security and privacy; participation in the online communities.
Keywords: teens, Internet, informational security, online safety of teenagers.

«Я ТІЛЬКИ ПОКАЗАВ, ЩО ІСНУЄ БОМБА»

Мікаел Кроґерус і Ганнес Ґрассуґґер

Психолог Міхал Косінський розробив метод, щоб детально аналізувати людей на підставі їхньої поведінки в Facebook. І так допоміг Дональду Трампу перемогти.

Дев'ятого листопада, десь о пів на дев'яту, Міхал Косінський прокинувся в готелі *Sunnehus* в Цюріху. Тридцятичотирьохрічний науковець приїхав з доповіддю в Центр ризиків *ETH* (Швейцарська вища технічна школа) — пояснювати про небезпеки Біґ-дата і так званий цифровий переворот. Косінський робить такі доповіді постійно, по всьому світі. Він є провідним експертом у психометрії — підрозділі психології про аналіз даних. Увімкнувши того ранку телевізор, він зрозумів: бомба розірвалася. Дональда Трампа обрано президентом США, всупереч усім прогнозам провідних соціологів.

Косінський довго оглядає новини про тріумф Трампа, про результати голосування в різних штатах. Він підозрює, що це якось пов'язано з його науковими розробками. Потім Косінський зітхає і вимикає телевізор.

Того ж таки дня досі ледве відома лондонська фірма розсилає прес-реліз з цитатою Алєксандра Джеймса Ешбернера Нікса: «Ми вражені тим, що наш революційний підхід до заснованих на даних комунікацій зробив такий істотний внесок у перемогу Дональда Трампа». Ніксу 41 рік, він британець і очолює компанію *Cambridge Analytica*. Він завше носить костюм індивідуального пошиву, дизайнерські окуляри, його світле хвилясте волосся зачесане назад.

Задумливий Косінський, бездоганно вдягнений Нікс і широко усміхнений Трамп — перший зробив цифрову революцію можливою, другий її здійснив, останній її використав.

Наскільки небезпечні Біґ-дата?

Сьогодні кожен, хто не жив на Місяці останні п'ять років, знайомий з терміном «Біґ-дата». Біґ-дата також означає, що все, роблене нами в мережі чи поза нею, залишає цифровий слід. Кожне купування платіжною карткою, кожен запит в Ґуґлі, кожне переміщення зі смартфоном в кишені, кожен лайк в соцмережі — все це зберігається. Зокрема, кожен лайк. Довший час не було ясності, як ці дані можуть знадобитися — хіба що, коли в стрічці Фейсбуку з'являється реклама засобів від гіпертонії, бо недавно ми шукали в Ґуґлі, «як знизити тиск». Не було ясності й щодо того, чим же є Біґ-дата для людства — великою небезпекою чи великим виграшем? Але після 9 листопада ми знаємо відповідь. Адже і за електоральною онлайн-кампанією Трампа, і за кампанією на підтримку Брекзиту стоїть одна й та сама фірма, що досліджує Біґ-дата, — *Cambridge Analytica* — і її директор Алєксандр Нікс. Хто хоче зрозуміти результат цих голосувань (і що може статись у Європі найближчими місяцями), мусить почати з дивного інциденту в Кембриджському університеті 2014 року. А саме у відділенні психометрії Косінського.

Психометрія, іноді звана психографією, — це наукова спроба виміряти людську особистість. В сучасній психології стандартом став так званий «метод океану» [OCEAN: openness, conscientiousness, extraversion, agreeableness, neuroticism]. У 1980-і роки два психологи довели, що кожна риса характеру може бути виміряна за допомогою п'яти вимірювань. Це так звана *Велика п'ятірка*: відкритість (наскільки ви готовий до нового), сумлінність (наскільки ви перфекціоніст), екстраверсія (наскільки ви товариський), доброзичливість (наскільки ви доброзичливий і наскільки кооперуєтесь) і нейротизм (наскільки ви уразливий). На підставі цих вимірювань порівняно точно можна сказати, з ким маєш справу, які в цієї особи бажання і страхи, нарешті, як вона зазвичай поводитиметься. А проблема полягала в надто великій кількості часу на збір даних, бо для визначення характеристик треба було заповнити складну і дуже особистісну анкету. Але потім з'явився Інтернет. Потім Фейсбук. Потім Косінський.

Для варшавського студента Міхала Косінського нове життя почалося, коли він вступив до престижного Кембриджського університету в Англії, до Центру психометрії, лабораторії Кевендіш, найпершої лабораторії з психометрії в світі. Зі своїми однокурсниками він придумав і запустив маленький додаток для тоді ще прозорого Фейсбуку: на *MyPersonality*, так називався додаток, можна було заповнити низку психологічних питань з анкети *OCEAN* («Чи легко вас вивести з себе в стані стресу? Чи є у вас схильність критикувати оточення?»). Як оцінку ви отримували свій «профіль особистості», власні значення *OCEAN*, а дослідники діставали цінну особистісну інформацію. Замість очікуваних кількох десятків однокурсників свої потаємні переконання швидко розголосили сотні, тисячі, а потім і мільйони. Несподівано два докторанти заволоділи найбільшою з будь-коли зібраних психологічною базою даних.

Метод, розроблений Косінським з колеґами за наступні кілька років, власне, досить простий. Спочатку тестований отримує анкету. Це онлайн-вікторина. За відповідями на неї психологи обчислюють *OCEAN*-значення респондентів. Далі, команда Косінського порівнює її з онлайн-діяльністю тестованих: що вони лайкають і репостять у Фейсбуці, а також із вказаними статтю, віком і місцем проживання. Так дослідники отримують взаємозалежності. З простої онлайн-діяльності випливають дивовижно надійні висновки. Наприклад, якщо чоловік підписаний на сторінку косметичного бренду *MAC*, то він з високою ймовірністю є ґеєм. Один з кращих показників гетеросексуальності — якщо людина поставила лайк для *Wu-Tang Clan*, хіп-хоп групи з Нью-Йорка. Шанувальник Леді Ґаґа з високою ймовірністю є екстравертом, а людина, що лайкає філософію, — інтровертом.

Косінський і його колеґи постійно вдосконалювали свою модель. У 2012 році Косінський довів, що пересічно 68 фейсбук-лайків досить, щоб визначити колір шкіри випробуваного (95% ймовірності), чи він є ґеєм (88% імовірності) і прихильність до Демократичної чи Республіканської партії США (85% імовірності). А далі: можна обчислити інтелектуальний розвиток, релігійні уподобання, пристрасть до алкоголю, тютюну чи наркотиків. Дані навіть дозволяли дізнатися, чи до повноліття (21 рік) тестованого його батьки розлучилися чи ні. Модель виявилася настільки добра, що уможливлювала передбачати відповіді тестованого на певні запитання. Сп'янілий від успіху, Косінський працював далі: незабаром за 10 лайками модель змогла краще оцінювати особистість, ніж колеґи по роботі. За 70 лайками — краще, ніж товариш. Після 150 лайків — краще, ніж батьки. Після 300 лайків — краще, ніж партнер. За ще більшою кількістю — можна було б людину оцінити краще, ніж вона сама. В день, коли Косінський опублікував статтю про свою модель, він дістав два дзвінки: з погрозою судового позову і з пропозицією роботи. Обидва дзвінки були з *Facebook*.

Видно тільки френдам

Тепер на *Facebook* можна позначати свої пости як відкриті і приватні. В приватному режимі переглядати їх може лише певне коло френдів. Але для збирачів даних це не проблема. Якщо Косінський завжди питав про згоду користувачів *Facebook*, сучасні тести вимагають доступу до персональних даних як обов'язкової умови для їх проходження. (Хто не надто переживає про власні дані і хоче себе оцінити за допомогою лайків на *Facebook*, може пройти опитування на сторінці Косінського applymagicsauce.com і потім порівняти його результати з однією з «класичних» анкет *OCEAN*: discovermyprofile.com/personality.html).

Але йдеться не лише про лайки у Фейсбуці: Косінський і команда можуть оцінювати людей за *OCEAN*-критеріями, виходячи з їхніх аватарів. Або навіть за числом контактів в соціальних мережах (добрий показник для екстраверсії). Але ми розголошуємо свої особисті дані і в офлайні. Сенсор руху, наприклад, показує, як сильно ми розмахуємо телефоном або як далеко подорожуємо (корелює з емоційною нестабільністю). Як зауважує Косінський, смартфон — це величезний психологічний опитувальник, який ми невпинно — свідомо чи несвідомо — заповнюємо. Однак важливо розуміти, що це працює і у зворотний бік: можна не тільки створювати з даних психологічний портрет, можна також шукати, навпаки, певні профілі: наприклад, всіх стурбованих голів сімейств, всіх озлоблених інтровертів. Або всіх невизначених демократів. Те, що винайшов Косінський, — це, власне, пошуковик людей.

Косінський дедалі виразніше розумів потенціал — але також і небезпеку — своєї роботи.

Мережа йому завжди видавалася даром небес. Вона спонукає віддати, поділитися, розшарити. Дані копіюються, їх мусять мати всі інші. Це дух цілого покоління, початок нової епохи без фізичних кордонів. Але що станеться, думав Косінський, коли хтось вирішить скористатися цим пошуковиком людей, щоб ними маніпулювати? І він починає у всіх своїх наукових публікаціях розміщати попередження. Про те, що його методи «можуть нести загрозу благополуччю, свободі чи навіть життю людей». Але ніхто, здається, не розумів, що він має на увазі.

Під той час, на початку 2014 року, до Косінського звернувся молодий професор-ассистент на ім'я Алєксандр Коґан. В нього було замовлення від фірми, яка цікавилась методом Косінського. Психометрично треба було виміряти профілі десяти мільйонів американських фейсбук-користувачів. Про мету співрозмовник не міг нічого сказати з міркувань конфіденційності. Косінський спершу був погодився, адже йшлося про великі суми для його інституту, але потім загальмував. Зрештою, він витиснув з Коґана назву фірми: *SCL*, *Strategic Communications Laboratories*. Косінський поґуглив про фірму. «Ми є ґлобальною компанією з менеджменту електоральних кампаній», — читає він на сайті фірми. *SCL* пропонує маркетинґ на основі психологічної моделі. Головне фокусування: вплив на виборця. Розгублений Косінський клікає по сайту. Що це за фірма? Що ці люди планують в США?

Косінський тоді ще не знав: за *SCL* стоїть складна структура фірм, кінці якої ховаються в податкових раях — як пізніше на це було вказано в *Panama Papers* і викриттях *Wikileaks*. Деякі з них були задіяні у переворотах в країнах, що розвиваються, інші — помагали НАТО розробляти методи психологічної маніпуляції населенням Афганістану. Одночасно *SCL* — материнська компанія і для *Cambridge Analytica*, сумнівного закладу, що організував онлайн-кампанії на підтримку Брекзиту і Трампа.

Косінський нічого про це не знає, але підозрює щось недобре. «Це почало зле пахнути», — згадує він. Розслідивши, він дізнався, що Алєксандр Коґан таємно зареєстрував компанію, яка має бізнес із *SCL*. З документа, який є в розпорядженні *Das Magazin*, виглядає, що *SCL* отримала дані про метод Косінського саме з рук Коґана. Раптово Косінського осінило, що Коґан міг скопіювати або відтворити *OCEAN*-модель, щоб продати фірмі для впливу на виборців. Він негайно розриває зв'язок з Коґаном й інформує інститутське начальство. В університеті розгорається складний конфлікт. Інститут тривожиться за свою репутацію. Коґан переїхав у Сінгапур, одружився і почав іменувати себе доктором Спектром. Міхал Косінський переходить до Стенфордського університету в США.

Більше року все йде спокійно, але в листопаді 2015-го оголошується, що дві радикальні кампанії — Брекзит і «leave.eu», — підтримувані Найджелом Фараджем, свою онлайн-кампанію доручають Біґ-дата-фірмі — *Cambridge Analytica*. Сутнісна компетенція фірми: політичний маркетинґ нового типу, так званий мікротаргетинґ — заснований на психологічній *OCEAN*-моделі.

Косінському в зв'язку з цим починають надходити мейли — при ключових словах «Кембридж», «OCEAN» і «аналітика», багато хто думає насамперед про нього. Але він вперше чує про цю фірму. З жахом він переглядає її сайт. Його страшний сон збувся: його методологія використовується у великій політичній грі.

Після Брекзиту, в липні, на його адресу посипалися прокляття: дивись, що ти наробив! Щоразу Косінський мусить пояснювати, що він не має нічого спільного з цією фірмою.

Спочатку Брекзит, потім Трамп

Десять місяців по тому. 19 вересня 2016 року, вибори у США в розпалі. Гітарні рифи наповнюють ґранатову залу нью-йоркського готелю *Grand Hyatt, Creedence Clearwater Revival*: «Bad Moon Rising». *Concordia Summit*, це щось як світовий економічний форум у мініатюрі. Найвпливовіші особи запрошені з цілого світу, серед гостей є федеральний президент Шнайдер-Амманн. «Прошу вітати Алєксандра Нікса, директора *Cambridge Analytica*», — оголошує м'який жіночий голос за кадром. Стрункий чоловік у темному костюмі виходить на середину сцени. В залі — заворожена тиша. Багато хто вже знає, що перед ними новий експерт Трампа з цифрових технологій. «Скоро ви будете називати мене Містер Брекзит», — таємничо написав Трамп у Твіттері кількома тижнями раніше. Політичні оглядачі вже тоді звернули увагу на подібність аґенди Трампа до правого Брекзит-табору. Але мало хто помітив зв'язок Трампа з невідомою в ширших колах маркетинґовою фірмою *Cambridge Analytica*.

Досі цифрова кампанія Трампа складалася згрубша з однієї людини: Бреда Парскейла, маркетинґового бізнесмена і засновника одного проваленого стартапу, що створив для Трампа за $1500 рудиментарний веб-сайт. Сімдесятирічний Трамп — не цифровий типаж: на його робочому столі комп'ютер навіть не стоїть. Такого явища, як електронний лист від Трампа, не існує, — якось здала його персональна асистентка. Саме вона й привчила його до смартфона — і з нього він безконтрольно цвіріньокає в Твіттері.

Гілларі Клінтон, навпаки, спиралася на спадщину Барака Обами як першого «президента соцмереж». У неї були адресні списки Демократичної партії, мільйони передплатників, підтримка *Google* і *Dreamworks*. Коли в червні 2016 року Трамп найняв *Cambridge Analytica*, багато хто у Вашинґтоні покрутив носом. Чужоземці в костюмах індпошиву, які не розуміють ні країни, ні людей? Серйозно?

«Це честь для мене, шановні пані та панове, розповідати вам про силу Біґ-дата і психометрії у виборчій кампанії», — за спиною в Алєксандра Нікса логотип *Cambridge Analytica*: мозок, складений з мереж яко географічна мапа. «Ще пару місяців тому Тед Круз був одним з найменш популярних кандидатів, — промовляє блондин з британськими переливами, що впливають на американців, як на швейцарців *Hochdeutsch* (літературна німецька мова). — Тільки 40 % електорату знали його ім'я». Всі присутні пам'ятали історію стрімкого злету сенатора-консерватора Круза. Це був один з найдивніших моментів кампанії. Останній з поважних внутрішньопартійних опонентів Трампа вискочив нізвідки. «Як це робиться?» — провадить далі Нікс. Наприкінці 2014 року *Cambridge Analytica* увійшла в передвиборчу кампанію в США саме як консультант Теда Круза, фінансованого мільярдером Робертом Мерсером. Доти,

каже Нікс, передвиборчі кампанії провадилися за демографічними критеріями: «Безглузда ідея, якщо серйозно про це подумати: всі жінки дістають однаковий меседж, тому що вони однієї статі, всі афроамериканці — дістають інший, виходячи з їх раси». Так по-дилетантськи (це Нікс може навіть не згадувати) провадила кампанію команда Клінтон: розділити суспільство на формально гомогенні групи, підказані соціологічними інститутами, тими, що до самого кінця бачили в ній переможця.

Натомість Нікс клацає на інший слайд: п'ять різних граней, кожна відповідає певному профілю особистості. Це *OCEAN*-модель. «Ми в *Cambridge Analytica* розробили модель, яка дозволить обчислити особистість кожного дорослого в США», — заявляє Нікс. В цей момент у залі абсолютна тиша. Маркетинґовий успіх *Cambridge Analytica* заснований на трьох складових. Це психологічний поведінковий аналіз за *OCEAN*-моделлю, використання Біґ-дата і таргетована реклама (*Ad-Targeting*). *Ad-Targeting* — це персоналізована реклама, тобто така, що якнайточніше підрихтовується під характер окремого споживача.

Нікс відверто пояснює, як його компанія це робить (лекція доступна на *YouTube*). Його фірма закуповує персональні дані з усіх можливих джерел: кадастрові списки, бонусні програми, списки виборців, членство в клубах, передплата періодики, медичні дані. Нікс показує логотипи ґлобальних дистриб'юторів даних, таких як *Acxiom* і *Experian*, — у США можна купити майже будь-які персональні дані. Якщо ви хочете дізнатися, припустимо, де живуть жінки-єврейки, можна спокійно купити базу даних. Разом з номерами телефонів. Потім *Cambridge Analytica* схрещує ці дані зі списками зареєстрованих виборців Республіканської партії і даними лайків-репостів у *Facebook* — так вираховують *OCEAN*-профіль особи: з цифрових слідів раптом виникають реальні люди зі страхами, потребами та інтересами — і з адресами проживання.

Процедура ідентична моделям, які розробив Міхал Косінський. *Cambridge Analytica* також використовує *IQ*-тести та інші невеликі додатки, щоб діставати доступ до достовірних лайків користувачів Фейсбуку. І компанія Нікса робить те, про що попереджав Косінський: «У нас є психограми всіх повнолітніх американців, це 220 мільйонів, — Нікс відкриває скріншот. — Наш контрольний центр виглядає так. Дозвольте ж показати, що ми з ними робимо». З'являється цифрова кабіна. Висвічується карта Айови, де Тед Круз зібрав несподівано велику кількість голосів на праймеріз. На карті видно сотні тисяч маленьких крапок: червоні і сині, за партійними кольорами. Нікс називає критерії: «республіканці» — і сині точки зникають; «поки що невизначені» — точок стає менше; «чоловіки» — ще менше. І так далі. Аж поки з'являється ім'я однієї людини: з віком, адресою, інтересами, політичними уподобаннями. Але як *Cambridge Analytica* редагує політичний меседж для окремої особи?

В іншій презентації Нікс на прикладі закону про вільне володіння зброєю показав, як можна звертатися до психографічно окресленого виборця: «Для боязких людей з високим рівнем невротизації ми подаємо зброю як засіб безпеки. — На лівій картинці зображена рука злодія, що розбиває вікно. Права картинка показує чоловіка з сином на фоні заходу сонця, обоє в полі з рушницями, очевидно, качине полювання. — Це для консервативних типажів з високою екстраверсією».

Як відіпхнути виборця Клінтон від урни

Виразна суперечливість Трампа, його безпринципність і пов'язана з цим величезна маса різних повідомлень несподівано зіграли йому на руку: кожному окремому виборцю — свій меседж. «Трамп діє як ідеальний опортуністичний алгоритм, який керується тільки реакцією публіки», — зазначала ще в серпні математик Кеті О'Найл. В день третіх дебатів між Трампом і Клінтон команда Трампа надіслала в соцмережі — переважно *Facebook* — понад 175 тисяч різних варіацій меседжів. Переважно меседжі відрізнялися лише в мікроскопічних деталях, щоб найоптимальніше психологічно задовольнити реципієнтів: різні заголовки, кольори, підзаголовки, з фото чи з відео. Дрібнозернистість дає змогу йти до дрібних груп, пояснює Нікс в розмові з *Das Magazin*: «Ми можемо цілеспрямовано дотягнутися до сіл чи кварталів. Навіть до окремих людей». В районі Літтл Гаїті в Майамі було запущено інформацію про неспроможність Фонду Клінтон після землетрусу в Гаїті — щоб запобігти їхньому голосуванню за Клінтон. Це одна з цілей: відіпхнути потенційний електорат Клінтон — невизначених лівих, афроамериканців і молодих дівчат — від урни, «придусити», за висловом одного зі співробітників Трампа, їхній вибір. У так званих «темних постах» (*dark posts* — куплені в *Facebook* платні оголошення в рядку новин, які можуть потрапляти лише групам осіб з певним профілем відповідності) показували, наприклад, афроамериканцям відео, де Клінтон порівнювала чорношкірих чоловіків з хижаками.

«Мої діти, — закінчує Нікс свій виступ на *Concordia Summit*, — не зможуть пояснити, що означає рекламний плакат з однаковим повідомленням для всіх і кожного. Дякую всім за увагу і можу вам сказати, що зараз ми працюємо для одного з двох кандидатів, що залишилися ». Потім він покидає сцену.

Наскільки цілеспрямовано американців вже в цей момент обробляє цифрове військо Трампа, сказати важко, бо воно вкрай рідко атакує на центральних телеканалах, а здебільшого — персоналізовано в соціальних мережах та на цифровому телебаченні. І поки команда Клінтон заколисувала себе демографічними зважуваннями, в Сан-Антоніо, де базувалась цифрова кампанія Трампа, виникає, зі слів кореспондента *Bloomberg* Саші Іссенберґа, «друга штаб-квартира». Тузінь співробітників *Cambridge Analytica* отримав від Трампа у липні $100 тис., в серпні — ще $250 тис., у вересні — ще $5 млн. За підрахунками Нікса, загалом вони отримали $15 млн.

Але і заходи цієї фірми теж були радикальними: з липня 2016 року волонтери кампанії Трампа вже мали додаток, який підказує політичні уподобання та особистісні типи мешканців того чи іншого будинку. Коли люди Трампа дзвонять в двері, то тільки в ті, які сприйнятливі до їхніх меседжів. Аґітатори, виходячи з цих даних, модифікували свою розмову з мешканцями. Зворотну реакцію волонтери записували в той-таки додаток — і дані надсилалося просто в аналітичний центр *Cambridge Analytica*.

Фірма розбиває американське населення на 32 особистісні типажі, сконцентрувавшись лише на 17 штатах. І так само, як Косінський з'ясував, що чоловіки-прихильники косметики *MAC* радше є ґеями, в *Cambridge Analytica* довели, що прихильники автівок «made in USA» однозначно є потенційними прихильниками Трампа. Такі відкриття допомогли й самому Трампу зрозуміти, які меседжі і де є найкращими. Рішення зосередитися в останні тижні на Мічиґані та Вісконсині було ухвалено на підставі попереднього аналізу даних. Кандидат став інструментом впровадження моделі.

Що робить *Cambridge Analytica* в Європі?

Але наскільки великим був вплив психометрії на результат виборів? *Cambridge Analytica* не хоче надавати докази успішності своєї кампанії. Цілком можливо, що на це питання взагалі неможливо відповісти. Хоча є певний факт: завдяки підтримці *Cambridge Analytica* Тед Круз виринув нізвідки і перетворився на серйозного конкурента Трампа на праймеріз. Тут зростання голосів сільських мешканців. Тут скорочення електоральної активності афроамериканців. Навіть той факт, що Трамп витратив на проект так мало грошей, може говорити про ефективність персоналізованого просування. Як і те, що три чверті рекламного бюджету він розмістив у цифровій сфері. *Facebook* перетворився на досконалу зброю і найкращого помічника на виборах, як написав у Твіттері один із сподвижників Трампа. До речі, в Німеччині антиелітарна «Альтернатива для Німеччини» має в Фейсбуці більше френдів, ніж провідні партії ХДС і СДПН разом узяті.

Так що не можна казати, що статистики програли вибори, бо вони систематично помилялися у своїх опитуваннях. Правдою є протилежне: статистики виграли вибори. Але лиш ті, що використовували новітні методи. Іронія історії: Трамп постійно критикував науку, але виглядає, що саме завдяки їй і виграв.

Другий переможець — компанія *Cambridge Analytica*. Її член правління, видавець ультраправої онлайн-газети *Breitbart News* Стів Беннон, нещодавно був призначений старшим стратегом в команді Трампа. Маріон-Марешаль Ле Пен, активістка французького «Національного фронту» і племінниця лідера партії, вже написала в Твіттері про співпрацю з фірмою, на внутрішньому корпоративному відео якої викладено запис наради «Італія». Зі слів Нікса, зараз ним зацікавлені клієнти з усього світу. Вже були запити на співпрацю зі Швейцарії та Німеччини.

Все це спостерігає і Косінський зі свого кабінету в Стенфорді. Після виборів у США в університеті все стоїть догори ногами. На розвиток подій Косінський відповідає найгострішою доступною дослідникові зброєю: науковим аналізом. Разом зі своєю колеґою Сандрою Матц він перепровадив серію тестів, результати яких незабаром будуть опубліковані. Деякі з висновків, якими науковець поділився з *Das Magazin*, шокують. Наприклад, психологічне тарґетування, подібне до того, що використовували у *Cambridge Analytica*, підвищує кількість кліків на рекламі в Фейсбуці на 60 %. А так званий коефіцієнт конверсії — ймовірність того, що внаслідок персоналізованої реклами люди зреагують відповідними діями: куплять чи проголосують, — зростає на неймовірні 1 400 відсотків*.

Тепер світ перевернувся: Британія покидає ЄС, в Америці правитиме Трамп. Все це почалося з людини, яка хотіла, власне, попередити нас про небезпеку. Тепер знову приходять мейли зі звинуваченнями. «Ні, — каже Косінський. — Тут немає моєї провини. Це не я зробив бомбу, я лише показав, що вона існує».

———

* Згадане дослідження стосується серії порівнянь: споживчий продукт рекламується в Інтернеті. Порівнювалась реакція на персоналізовану рекламу і на загальну.

Mikael Krogerus, Hannes GrasseggerIch habe nur gezeigt, dass es die Bombe gibt Das Magazin, 3.12.2016
Зреферував О.Р.