МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ЮРИДИЧНИЙ УНІВЕРСИТЕТ
імені ЯРОСЛАВА МУДРОГО

НАЦІОНАЛЬНА АКАДЕМІЯ ПРАВОВИХ НАУК УКРАЇНИ

КРИМІНАЛЬНІ ЗАГРОЗИ В СЕКТОРІ БЕЗПЕКИ: ПРАКТИКИ ЕФЕКТИВНОГО РЕАГУВАННЯ

Матеріали панельної дискусії
ІІІ Харківського міжнародного юридичного форуму
м. Харків, 26 вересня 2019 р.

Харків
«Право»
2019

УДК 343.9-049.5
К82

К82 **Кримінальні** загрози в секторі безпеки: практики ефективного реагування : матеріали панельної дискусії III Харків. міжнар. юридичного форуму «Право», м. Харків, 26 верес. 2019 р. / редкол.: В. Я. Тацій, Ю. Г. Барабаш, Б. М. Головкін, О. В. Таволжанський. – Харків : Право, 2019. – 176 с.

ISBN 978-966-937-785-2

ISBN 978-966-937-785-2

ЗМІСТ

Авдєєва Г. К., кандидат юридичних наук, старший науковий співробітник, провідний науковий співробітник НДІ вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України, м. Харків,Україна

ПРОБЛЕМИ ЗАСТОСУВАННЯ ІННОВАЦІЙНИХ ПРОДУКТІВ У РОЗСЛІДУВАННІ ЗЛОЧИНІВ, ЩО ВЧИНЯЮТЬСЯ З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Щороку в усьому світі вчиняються десятки тисяч злочинів з використанням інформаційно-комунікаційних технологій та програмно-апаратних засобів (кібернетичних злочинів). Генеральний секретар ООН Антониу Гуттереш зазначає, що щорічні збитки від кіберзлочинності у світі складають 1,5 трлн доларів. На думку експертів з кібербезпеки в майбутньому кількість даних злочинів та збитків від кібератак лише зростатиме тому, що правопорушники спочатку використовують певні новітні інформаційні технології для вчинення злочину, а лише після цього розпочинається розроблення відповідних механізмів щодо їх запобігання і розкриття [1]. Тобто, кіберзлочинці завжди випереджають осіб, які їм протидіють.

Останніми роками великі державні і приватні установи України неодноразово потерпали від кібератак. Прикладом слугує розповсюдження вірусу Petya влітку 2017 року, через який було тимчасово заблоковано роботу аеропорту «Бориспіль», «Ощадбанку», «Укртелекому», «Укрпошти», «Укрзалізниці» та низки інших державних і приватних установ. Частково була пошкоджена інформація в інформаційних системах Кабінету Міністрів, окремих міністерств і навіть кіберполіції.

Правова основа кібернетичної безпеки в Україні складається з відповідних норм Конституції України, Кримінального кодексу України, законів України «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки» та ін., Доктрини інформаційної безпеки України, Конвенції Ради Європи про кіберзлочинність та інших міжнародних нормативно-правових актів, ратифікованих Верховною Радою України.

Реалізацію державної політики України у сфері боротьби з кіберзлочинністю здійснює низка державних органів, а саме: Державна служба

спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України. В кожному із зазначених державних органів створено відповідні підрозділи, співробітники яких постійно підвищують свою кваліфікацію. Зокрема, у 2016–2017 р.р. співробітники Департаменту кіберполіції пройшли курси з підвищення кваліфікації на базі Харківського національного університету внутрішніх справ та прийняли участь у тренінгах за участі експертів Великої Британії.

Протягом 2018 року працівники Департаменту кіберполіції були залучені до розслідування більше 11 тисяч кримінальних проваджень та викрили більше 800 осіб, якими вчинено злочини з використанням інформаційних технологій. Більшість правопорушень здійснена за допомогою вірусних програм, придбаних через анонімну «мережу» DarkNet. В межах міжнародної співпраці співробітники кіберполіції у 2018 році викрили 8 транснаціональних хакерських угруповань та взяли участь у понад 30 міжнародних операціях [2].

Кіберзлочини умовно поділяються на такі види: 1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем; 2) правопорушення, пов'язані з комп'ютерною технікою; 3) правопорушення, пов'язані з виготовленням, розповсюдженням та зберіганням дитячої порнографії; 4) порушення авторських та суміжних прав [3].

В криміналістиці можна визначити як мінімум три напрями виявлення розробки інновацій – техніко-криміналістичний, тактико-криміналістичний та напрямок забезпечення методики розслідування окремих видів злочинів. Найбільш активно в інноваційному плані розвивається техніко-криміналістичний напрямок [4, с. 49].

У боротьбі з кіберзлочинністю використовуються інноваційні продукти у вигляді стандартного і спеціального програмного забезпечення, сучасних програмно-апаратних приладів і систем, а також методів і методик їх застосування. Такі інноваційні продукти створюються і постійно оновлюються в усьому світі. Представники Координації проектів ОБСЄ в Україні та інші міжнародні донори передають Україні не лише свій досвіт у боротьбі з кіберзлочинністю, а й інноваційні продукти у вигляді спеціального програмного забезпечення та спеціалізованої техніки [5].

На базі Департаменту кіберполіції Національної поліції України впроваджені новітні технології та сервіси, які дозволяють миттєво реагувати на звернення громадян про кіберзлочин чи кібератаку. Зокрема, працює

цілодобовий «call-центр» для прийому заяв та звернень від громадян про злочини та правопорушення, що вчиняються за допомогою інформаційних технологій. [6].

На сьогодні українська кіберполіція співпрацює з багатьма міжнародними органами та організаціями як державного, так і приватного сектору, здійснюючи швидкий та безпечний обмін інформацією захищеними каналами за допомогою спеціальної системи «Еуе 24/7» та використовуючи 17 баз даних, які включають 81 мільйон різноманітних поліцейських документів. Щоденно кіберполіцією проводиться близько 13 мільйонів пошуків. [7]. Однак, виходячи з показників роботи кіберполіції [8], відсоток розкриття злочинів, що вчиняються з використанням інформаційних технологій, є не достатньо високим.

Основними чинниками, які впливають на якість та ефективність боротьби з кіберзлочинністю, є рівень підготовки фахівців та результативність роботи інноваційних засобів, які вони використовують у своїй роботі.

В. Ю. Шепітько та В. А. Журавель зазначають, що на шляху впровадження інновацій у практику боротьби зі злочинністю існує низка перешкод і бар'єрів, а саме: недостатність знань співробітників слідчих органів в даній галузі і відсутність можливості їх отримати, професійна деформація або неправильне відношення до всього нового, передового та ін. [9, с. 18]. Гальмують впровадження інновацій у слідчу діяльність і втрата професійного ядра співробітників слідчого апарату і оперативних підрозділів органів внутрішніх справ, недостатність наявних тактичних засобів здійснення слідчої діяльності, наявність складнощів у залученні кваліфікованих ІТ-спеціалістів до участі у слідчих діях; проблеми взаємодії слідчого з обізнаними особами; недостатність інформації про розслідувану подію; недостатність надійних джерел отримання інформації; наявність протидії розслідуванню з боку зацікавлених осіб та ін. [10, с. 22]. Більше того, в усіх країнах світу існують проблеми визнання «цифрових» доказів судом через їх неналежну фіксацію.

На думку В. Г. Андрєєвої серед причин низького рівня використання інноваційних продуктів в Україні є недостатнє бюджетне фінансування. Вона стверджує, що практично єдиним джерелом фінансування інноваційної діяльності в Україні у 97,2% випадках є власні кошти розробників інноваційних продуктів [11, с. 15].

У зв'язку з бурхливим розвитком комп'ютерної техніки і телекомунікаційних мереж методики судово-експертного дослідження даних об'єктів

вимагають постійного оновлення та доопрацювання у зв'язку з тим, що через кожні 2–3 роки змінюються формати даних, операційні та файлові системи, протоколи і середовище перенесення даних, технічні засоби, що забезпечують процес передавання інформації. Однак, здійснити розробку нових та удосконалення існуючих експертних методик неможливо без використання високооплачуваної праці вчених в галузі телекомунікаційних мереж і кваліфікованих ІТ-фахівців [12, с. 9].

Подолання існуючих проблем застосування інноваційних продуктів у розслідуванні злочинів, що вчиняються з використанням інформаційних технологій, є можливим за умови системної державної підтримки, яка передбачатиме тісну співпрацю розробників і користувачів інноваційних продуктів та державне фінансування процесів розроблення і впровадження інновацій в практику боротьби з кіберзлочинністю.

Список використаних джерел:

1. Нікулеско Д. Кібербезпека: вразливі моменти. Юридична газета. 14 травня 2019. URL: http://yur-gazeta.com/publications/practice/inshe/kiberbezpeka-vrazlivi-momenti.html (дата звернення: 02.09.2019).
2. Підсумки 2018 року в цифрах. Офіційний сайт кіберполіції України. URL: https://cyberpolice.gov.ua/results/2018/ (дата звернення: 01.09.2019).
3. Конвенція про кіберзлочинність. Конвенцію ратифіковано 07.09.2005. ВВР, 2006, № 5–6, ст.71 URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 03.09.2019).
4. Берназ П. В. Інновації – основа криміналістичного забезпечення діяльності з розслідування злочинів. Південноукраїнський правничий часопис. № 4, 2015. С. 49.
5. Кіберполіція отримала 194 одиниці спеціального обладнання для протидії кіберзагрозам. Прес-центр кіберполіції. URL: https://mvs.gov.ua/ua/news/9208_Kiberpoliciya_otrimala_194_odinic_ specialnogo_obladnannya_dlya_protidii_kiberzagrozam_FOTO_VIDEO.htm (дата звернення: 05.09.2019).
6. Кіберполіція впровадила нові шляхи оперативного реагування на кіберзлочини. Урядовий портал. https://www.kmu.gov.ua/ua/news/250050267(дата звернення: 02.09.2019).
7. Підрозділи кіберполіції України та Сінгапуру співпрацюватимуть у протидії кібертероризму. URL: https://www.cyberpolice.gov.ua/news/pidrozdily-kiberpolicziyi-ukrayiny-ta-singapuru-spivpraczyuvatymut-u-protydiyi-kiberteroryzmu-6275/ (дата звернення: 02.09.2019).
8. Підсумки 2018 року в цифрах. Офіційний сайт кіберполіції України. URL: https://cyberpolice.gov.ua/results/2018/ (дата звернення: 01.09.2019).

9. Шепітько В. Ю., Журавель В. А., Авдєєва Г. К. Інновації в криміналістиці. Інноваційні засади техніко-криміналістичного забезпечення діяльності органів кримі-нальної юстиції : монографія / за заг. ред. В. Ю. Шепітька, В. А. Журавля. Харків : Вид. агенція «Апостіль», 2017. С. 18.
10. Шепітько В. Ю., Авдєєва Г. К. Інновації у правозастосовній діяльності. Інноваційні засади техніко-криміналістичного забезпечення діяльності органів кримі-нальної юстиції : монографія / за заг. ред. В. Ю. Шепітька, В. А. Журавля. Харків : Вид. агенція «Апостіль», 2017. С. 22.
11. Андрєєва В. Г. Оцінка стану інноваційної активності України в міжнародному контексті. Проблеми та перспективи розвитку інноваційної діяльності в Україні: матер. X міжнар. бізнес-форуму, 21 березня 2017р. Київ: Київ.нац.торг. – екон. ун-т, 2017. С. 15.
12. Авдеева Г. К. Бобрицкий С. М. Организационно-методические и нормативно-правовые проблемы обеспечения производства новых видов судебных экспертиз. Методологические, правовые и организационные проблемы новых родов (видов) судебных експертиз : матер. междунар. научн.-практ. конф. М. : Проспект, 2014. С. 9.

Батиргареєва В. С., доктор юридичних наук, старший науковий співробітник, в.о. директора Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України

УРБАНІСТИЧНА КРИМІНОЛОГІЯ ЯК АКТУАЛЬНИЙ НАПРЯМ ЗНАННЯ У ЗАПОБІГАННІ ЗЛОЧИННОСТІ

1. Як повідомляється Департаментом з економічних і соціальних питань ООН, сьогодні у містах проживає 54% населення планети, питома вага якого до 2050 р. збільшиться до 66% [1, с. 1]. Розвиток та трансформації ідей про запобігання тим чи іншим видам злочинності в урбанізованому середовищі раніше найчастіше знаходили своє відбиття у таких напрямах кримінологічного знання, як топографічна урбаністика (Г. Й. Шнайдер, П. Уілсон,); урбаністична віктимологія (С. Сміт, К. В. Вишневецький); «топографія злочинності» (О. Ігнатов); захищений урбанізований простір (К. Рей Джеффері, О. Ньюман, П. Уілсон); регіональні особливості злочинності (А. М. Бабенко, І. Г. Богатирьов, Р. С. Веприць-

кий), екологічна урбаністика (Е. Берджес, Р. Маккензі, Р. Парк, К. Шоу), екологічне проектування (дизайн) (L. Fennelly, T. Crowe) та ін. Нерідко зміст перелічених напрямів співпадає або розвиває та доповняє один одного. До того ж заходи, що п пропонуються, у своєму підґрунті мають один й той самий актуальний матеріал. Це дає підстави стверджувати, що положення цих напрямів у кримінологічній площині фактично переплітаються в єдине знання щодо убезпечення людини від злочинних проявів.

2. Урбаністична кримінологія, як й будь-яке знання, що розвивається, спрямована на вивчення властивості й закономірності розвитку кримінологічного об'єкта пізнання – злочинності у конкретних умовах місця та часу, визначених просторовими й часовими межами. Тому цей самостійний напрям кримінологічної науки щодо пізнання злочинності доповнює та розширює можливості кримінологічного аналізу різноманітних чинників походження правопорушень, виявляючись іманентним атрибутом сучасних теоретичних і прикладних кримінологічних розвідок, особливо коли йдеться про походження злочинності у населених пунктах. Зауважимо, що перш ніж почати затверджуватися як самостійний науковий напрям на пострадянському просторі, урбаністична кримінологія за минулих часів розглядалася як явище і процес, що характеризує прогрес суспільства і є антиподом причин злочинності (А. В. Павлінов) [2, с. 1069].

3. Доцільно виокремити ці чинники, що зумовлюють необхідність розробки й реалізації у практичній площині ефективних заходів запобігання злочинності (насамперед в умовах великих населених пунктів) з урахуванням ідей, що складають серцевину урбаністичної кримінології. Отже, зазначені чинники полягають у такому. По-перше, значна кількість населення країни сконцентрована у великих промислових центрах східних областей і Центрального Придніпров'я, навколо приморських міст Північного Причорномор'я, Південного узбережжя Криму, у столиці та навколо неї. При цьому рівень урбанізованості досить високий (70,1%) [3]. Виходячи із цього, на території міст концентрується й більша кількість потенційних об'єктів запобіжного впливу. Таким чином, саме міське населення є первинним об'єктом вживання найпотужніших заходів відповідної спрямованості. По-друге, у спеціальній літературі відмічається той факт, що в останні два десятиліття відбувається достатньо потужний вплив урбанізації на процеси віктимізації так само й мешканців сільських районів [4, с. 68]. По-третє, негативні процеси зростання морально-психологічної кризи українського суспільства, яка є свідченням аномії останнього, у теперішній час особливо стає помітним саме у середовищі великих

агломерацій [5, с. 157]. По-четверте, у соціальному міському просторі кінця XX – початку XXI століть відбувається формування нового типу ідентичності – так званого феномену *Homo Urbanus*, що згодом виявлятиметься комплексним об'єктом запобіжного впливу у великих містах [6]. По-п'яте, затребуваність відповідного знання на практиці стимулює й розвиток наукової думки, оформлення якої відбувається у межах цілісного кримінологічного напряму.

4. На теперішній час значна роль у системі відповідних запобіжних заходів має належати особливостям територій, взятих у ракурсі їх урбаністичних характеристик, оскільки будь-які заходи, якщо вони розробляються з урахуванням цих особливостей, виявляються найбільш ефективними. На противагу такому підходу, знеособлені заходи запобігання, іншими словами, взяті без урахуванням територіальних властивостей місцевості, не здатні призвести до відчутного покращення криміногенної ситуації у тій чи іншій місцевості. Зараз таке розуміння змісту запобіжної діяльності відбивається насамперед на рівні регіональних програмних документів протидії тим чи інших злочинам, що розраховані на реалізацію у міських агломераціях, ядром яких є урбаністичний центр, тобто велике або особливо велике місто. Наведемо кілька прикладів зазначеного підходу. Так, у Стратегічних напрямах забезпечення публічної безпеки і порядку на території Харківської області на 2018–2019 роки, затверджених Рішенням Харківської обласної ради від 7 грудня 2017 р. №557-VII, наголошується, зокрема, на забезпечення безпеки дорожнього руху, підвищення швидкості реагування на вчинені правопорушення, забезпечення публічного порядку та протидія злочинності в громадських місцях, включаючи зниженні рівня учинених у громадських місцях убивств та тяжких тілесних ушкоджень, зменшення кількості майнових злочинів тощо [7]. Про вжиття заходів із запобігання правопорушенням у великих містах, наприклад, йдеться у Програми «Безпечне місто Харків» на 2016–2020 рр. [8], Міській цільовій комплексній програмі профілактики та протидії злочинності в місті Києві «Безпечна столиця» на 2016–2018 роки, затвердженої Рішенням Київської міської ради від 14 квітня 2016 р. №334/334 [9], Міській комплексній програмі зміцнення законності, безпеки та порядку на території міста Одеси «Безпечне місто Одеса» на 2017–2019 роки, затвердженої Рішення Одеської міської ради від 15 березня 2017 р. №1778-VII та ін. [10].

5. Таким чином, проблематика убезпечення людини, її прав і свобод від злочинності у великих населених пунктах є сьогодні вельми актуаль-

ною темою з огляду на те, що кримінальна реальність не є застиглим феноменом і що потужним осередком злочинних проявів виступають саме міські агломерації. Тому ця проблематика успішно може вирішуватися з урахування напрацювань урбаністичної кримінології як потужного напряму розвитку кримінологічної думки, заснованого на знаннях економіки, архітектури, географії, будівництва, історіографії, культурології та ін. До речі, зазначені питанні сьогодні успішно розробляються в Науково-дослідного інституті вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України у межах виконання фундаментальне дослідження під назвою «Стратегія зменшення можливостей вчинення злочинів: теорія та практика».

Список використаних джерел:

1. World Urbanization Prospects The 2014 Revision / Department of Economic and Social Affairs. ST/ESA/SER.A/352. New York: United Nations, 2014. 27 p.
2. Криминология: учебник / под общ. ред. О. С. Капинус; под науч. ред. В. В. Меркурьева. 2 изд., пер. и доп. Москва: Юрайт, 2019. 1132 с.
3. Населення України. URL: https://uk.wikipedia.org/wiki/Населення_України.
4. Вишневецкий, К. В. Урбанизация и ее влияние на процессы виктимизации населения. Юридический мир. 2006. №3. С. 65–70.
5. Бойко В. В. Кримінологічна характеристика та запобігання тяжкій насильницькій злочинності проти життя та здоров'я особи в особливо великих містах України: дис. … канд.. юрид. наук: 12.00.08 / Нац. юрид. ун-т імені Ярослава Мудрого; НДІ ВПЗ імені академіка В. В. Сташиса НАПрН України. Харків, 2019. 280 с.
6. Рижкова Д. С. Homo Urbanus як нова ідентичність: автореф. … канд. філософ. наук: 09.00.04 / Харк. нац. ун-т ім. В. Н. Каразіна. Харків, 2018. 15 с.
7. Стратегічні напрями забезпечення публічної безпеки і порядку на території Харківської області на 2018–2019 роки: затв. Рішенням Харківської обласної ради від 7 грудня 2017 р. №557-VII. URL: http://www.gov.lica.com.ua/b_ text.php?type=3&id=18422&base=77 (дата звернення: 14.08.2019).
8. Програма «Безпечне місто Харків» на 2016–2020 рр.: затв. Рішенням Харківської міської ради від 14.09.2016 р. №364/16. URL: http://kharkiv.rocks/reestr/652546 (дата звернення: 14.08.2019).
9. Міська цільова комплексна програма профілактики та протидії злочинності в місті Києві «Безпечна столиця» на 2016–2018 роки: затв. Рішенням Київської міської ради від 14 квітня 2016 р. №334/334. URL:

http://kmr.ligazakon.ua/SITE2/l_docki2.nsf/alldocWWW/DA8AD8E2C84E253EC2257FB 2006870C9? OpenDocument (дата звернення: 14.08.2019).
10. Міська комплексна програма зміцнення законності, безпеки та порядку на території міста Одеси «Безпечне місто Одеса» на 2017–2019 роки: затв. Рішенням Одеської міської ради від 15 березня 2017 р. № 1778-VII. URL: http://document.ua/pro-zatverdzhennja-miskoyi-kompleksnoyi-programi-zmicnennja-doc309397.html (дата звернення: 31.08.2019).

Бурда О. М., аспірант кафедри кримінології та кримінально-виконавчого права Національного юридичного університету імені Ярослава Мудрого, м. Харків, Україна

ЗАПОБІГАННЯ КРАДІЖКАМ З МАГАЗИНІВ ЗА ДОПОМОГОЮ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ ВІДЕОАНАЛІТИКИ

Штучний інтелект інтенсивно запроваджується в багатьох сферах людської життєдіяльності. Завдяки новітнім технологіям намагаються автоматизувати більшість виробничих процесів, а в окремих випадках роботи виконують надскладні операції замість лікарів, складають позовні заяви замість юристів. Впроваджують штучний інтелект й для боротьби з організованою злочинністю у фінансовій системі [1] та сфері економіки. Користь від штучного інтелекту помітили й міжнародні ритейлери, які все частіше запроваджують окремі досягнення науки у власних магазинах.

В першу чергу, запровадження технологій із штучним інтелектом спрямоване на мінімізацію ризиків вчинення крадіжок всередині магазину. Так, за повідомленням «JapanToday» запровадження в тестовому режимі технології штучного інтелекту в магазинах електроніки «Bic Camera», фармацевтичній мережі «Kirindo» та магазинах спортивних товарів «Xebio» дозволило зменшити збитки від крадіжок на 40% [3]. По-друге, використання технології штучного інтелекту дозволяє підвищувати ефективність роздрібної торгівлі, оптимізуючи роботу магазинів та торгових мереж.

Однією із перших можливостей штучного інтелекту стало запровадження камер відеоспостереження із функцією розпізнавання обличчя.

Такі камери монтуються, як правило, при вході до магазину або біля входу та виходу з торгового залу. Програмне забезпечення smart-камер дозволяє сканувати та розпізнавати обличчя людини, яка підходить до контрольних камер. При цьому не потрібно, щоб людина зупинялась чи дивилась прямо в камеру. У випадку виявлення співпадіння із базами даних злочинців відправляється попередження службі безпеки магазину. Крім того, для невеликих ритейлерів сьогодні розроблені зручні мобільні додатки для різноманітних операційних систем, які працюють за аналогічним алгоритмом, проте не вимагають великих фінансових затрат.

Крок уперед в розвитку smart-камер зробили в Японії. Так, компанія «NTT East» та стартап «Earth Eyes» розробили систему відеоспостереження, яка аналізує поведінку людей та виявляє потенційних магазинних крадіїв. В програмне забезпечення системи закладена інформація з різних посібників з організації безпеки в торгівельних приміщеннях. Зокрема, в них містяться рекомендації, як розпізнати злодія з його дій. Крім того, при розробці були використані відеозаписи дрібних крадіжок [4]. Така технологія запрограмована на розпізнавання міміки людей та передбачення наступних дій людини. Головним завданням штучного інтелекту «AI Guardsman» є виявлення підозрілої активності; наприклад, намагання уникнути покупцем камер відеоспостереження та пошук сліпих зон, перенесення товарів в кишенях, а не в корзині тощо. В такому разі система відправляє попередження на смартфон продавця із зазначенням фотографії та розташування людини.

Аналогом японського штучного інтелекту є система відеоспостереження розроблена каліфорнійською компанією Standard Cognition для магазинів самообслуговування. Як і в Японії відеокамери стежать за рухом і діями покупців. Вони фіксують такі показники як довжина кроків, швидкість руху, напрям погляду, визначення товару, який привертає увагу відвідувача магазину. На підставі всіх зібраних даних програма визначає так званий рівень «благонадійності» покупця [5].

Проте в такого штучного інтелекту є свої недоліки. Так, система є доволі дорогою, а отже є недоступною для широкого загалу. Окрім того, системі ще важко відрізняти потенційних крадіїв від покупців, які передумали купувати товар та кладуть його назад на полицю, або ж працівників магазину, які займаються розміщенням товару в торговому залі [6]. Складнощі виникають й при розпізнаванні облич різних рас.

Практика показує, що найчастіше предметом злочину стають продукти харчування. Найбільша проблема постає із свіжими продуктами, які

неможливо обладнати протикрадіжними мітками, оскільки це призведе до значного удорожчання таких продуктів, а по-друге, може вплинути на їх якість та свіжість. Відсутність можливості забезпечити безпеку таких товарів означає, що в зоні підвищеного ризику опиняються такі товари як свіже та заморожене м'ясо, домашня птиця, морепродукти, сири, фрукти та овочі.

Розробники програмного забезпечення для камер відеоспостереження пропонують в таких випадках застосовувати камери із функцією тепловізору. Тепловізійні камери дозволяють виявляти об'єкти нижче температури людського тіла і автоматично запускати сигнал тривоги. Вони забезпечують надійне виявлення і розпізнавання завдяки поєднанню високої контрастності зображення з виявленням руху для ідентифікації прихованих об'єктів. Алгоритм працює так, що не викликає сигнал тривоги, якщо товар не буде захований, а знаходитиметься в руках клієнта або на касі. Застосування таких камер за оцінками розробників дозволяє зменшити втрати від крадіжок на 50% [9].

Слід зазначити, що smart-камери вже тривалий час використовуються в Україні для убезпечення об'єктів критичної інфраструктури та громадської безпеки [7]. Наступним кроком повинно стати запровадження таких камер й українськими ритейлерами.

Застосування smart-камер втім не зменшує кількість крадіжок, які вчиняють співробітники магазинів. Вирішення цієї проблеми запропонували шведські розробники шляхом створення оф-лайн магазину. Ідея полягає в тому, щоб магазини самообслуговування працювали повністю без персоналу. Так, шведська компанія «Wheelys» розробила додаток, який потрібно встановити на смартфон і прив'язати до банківської карти. Двері в оф-лайн магазин відкриваються лише тоді, коли до них наближається зареєстрований клієнт. Покупки скануються покупцем через смартфон, кошти з кредитної картки знімаються в кінці кожного місяця [8]. Більш удосконалену версію додатку запропонувала компанія «Amazon». Так, додаток «grab and go» (бери і йди – англ.) автоматично формує віртуальну корзину, скануючи, коли продукти знімаються з полиць і повертаються на місце. На виході сума списується з рахунку клієнта[1]. В таких магазинах немає ні касирів, ні служби безпеки.

В цілому запобігання злочинності на сьогодні носить міжнародний характер [2, с. 10], а відтак вимагає активного міжнародного співробітництва та перейняття кращих міжнародних практик та новітніх розробок.

[1] https://www.ustor.com.ua/ua/news/magaziny-bez-prodavcov/

З наведеного слідує, що майбутнє пропонує зовсім інші підходи до розуміння сутності ритейлінгового ринку, його функцій та завдань. Роздрібну торгівлю очікує неминуча роботизація та автоматизація. Перші ознаки таких процесів помітні на безпековому ринку, який пропонує великий асортимент smart-технологій. Звісно, вибір того чи іншого варіанту запобіганням крадіжкам на сьогодні залежить виключно від ритейлера та його фінансових можливостей. Вбачається, що вирішення проблеми крадіжок в сфері ритейлу на сьогодні можливе завдяки широкому впровадженню магазинів типу оф-лайн та он-лайн торгівлі.

Список використаних джерел:

1. Bohdan Holovkin, Kostyantyn Marysyuk. Foreign experience in countering (preventing) organized crime in the financial system: special law enforcement bodies and strategic priorities. *Baltic Journal of Economic Studies* Vol. 5, No. 3, 2019. p. 25–34
2. Serhii S. Cherniavskyi, Bohdan M. Holovkin, Yuliia M. Chornous, Vasyl Y. Bodnar, Ilona V. Zhuk. International Cooperation in the Field of Fighting Crime: Directions, Levels and Forms of Realization. Journal of Legal, Ethical and Regulatory Issues Volume 22, Issue 3, 2019. URL: https://www.abacademies.org/articles/International-cooperation-in-the-field-of-fighting-crime-directions-levels-and-forms-of-realization-1544-0044-22-3-348.pdf
3. Vigilant 'AI Guardman' system aims to cut shoplifting losses. Japantoday. 2018. URL:https://japantoday.com/category/features/kuchikomi/vigilant-%27ai-guardman%27-system-aims-to-cut-shoplifting-losses
4. В боротьбі з магазинними крадіжками в Японії почали використовувати штучний інтелект. *Ukr.Media*. 2019. URL: https://ukr.media/science/392639/
5. Владельцы «магазина без продавцов» обучили ИИ вычислять воров. 2018. URL: https://novate.ru/news/5906/
6. В Японии создали систему видеонаблюдения, определяющую воров в супермаркетах. https://vesti-ukr.com/mir/293928-v-japonii-sozdali-sistemu-videonabljudenija-opredeljajushchuju-vorov-v-supermarketakh
7. Головкін Б. М. Електронна система запобігання злочинності. *З нагоди 100-річчя від дня народження професора М. В. Салтевського: зб. матеріалів круглого столу, м. Харків, 30 жовт. 2017 р.* Харків, 2017. С. 48–52. URL: http://dspace.nlu.edu.ua/bitstream/123456789/13692/1/Golovkin_48–52.pdf
8. Магазини без продавців. URL:https://www.ustor.com.ua/ua/news/magaziny-bez-prodavcov/

9. Чому системи безпеки в супермаркетах вимагають рішень на основі технологій теплобачення. URL: https://worldvision.com.ua/ua/articles/pochemu-sistemi-bezopasnosti-v-supermarketah-trebuyut-resheniy-na-osnove-tehnologiy-teplovideniya

Бусол О. Ю., доктор юридичних наук,старший науковий співробітник, головний науковий співробітник відділу з вивчення проблем захисту національних інтересів в економічній сфері та протидії корупції Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Раді національної безпеки і оборони України, м. Київ, Україна

КІБЕРНЕТИЧНІ ВІЙНИ ТА КІБЕРТЕРОРИЗМ ЯК ЗАГРОЗИ МІЖНАРОДНІЙ БЕЗПЕЦІ: ДИФЕРЕНЦІАЦІЯ ЗЛОЧИНІВ ВІД ТРАДИЦІЙНОЇ ВІЙНИ

Нині інформація використовується не тільки у мирних цілях, але з деструктивною метою, або захисту від дій держави-агресора. Таким чином, війни ведуться як на землі, морі та повітрі, так і в кіберпросторі (інформаційні війни). При визначенні терміну «кібервійна» доцільно ураховувати поняття війни у класичному розумінні. Традиційна війна (конвенційна війна) передбачає кардинальну зміну характеру відносин між учасниками, як правило, і розрив дипломатичних відносин. Для традиційної війни притаманні також такі риси, як комплексність, досить чіткі часові (початок і завершення) і просторові (поле бою) обмеження, заздалегідь сплановані учасниками стратегії і тактики ведення боротьби, наявність принаймні двох учасників з конкретними політичними цілями, а також значні людські жертви та руйнування інфраструктури задіяних сторін [1]. Критерієм, що відрізняє конвенційні війни, є поділ населення і об'єктів і інфраструктури на військові та цивільні. Отже, кібервійна як своєрідна форма війни має зберігати базові характеристики традиційної війни.

Подібно до класичної війни кібервійна передбачає масштабне вторгнення на «територію» супротивника, якою в даному випадку є електронні

системи і мережі об'єкта впливу; наявність певного стратегічного плану; використання насильницьких засобів у вигляді шкідливого програмного забезпечення; завдання значної шкоди цим системам (тобто певні руйнування і жертви) тощо. Кібервійна так само є продовженням політики іншими засобами й використовується для здійснення впливу на волю і можливості прийняття рішень політичного та військового керівництва супротивника [2, с. 81]. Саме тому веденню кібернетичних війн надається важливе значення у здійсненні міждержавної політики,адже кіберпростір перетворюється на арену боротьби між акторами міжнародних відносин.

Термін «кібервійна» ввійшов в обіг військових, фахівців з інформаційної безпеки та політиків, хоча понятя не закріплено в офіційних документах на національному та міжнародному рівнях. Вітчизняними вченими кіберпростір визначається як об'єкти інформаційної інфраструктури, що керуються інформаційними (автоматизованими) системами управління, а також інформація, що в них циркулює [3]. Таким чином, кібернетична війна – це інформаційне протистояння в кіберпросторі, в тому числі комп'ютерне протистояння в інтернеті, один з різновидів інформаційної війни. Кібервійна спрямована насамперед на дестабілізацію комп'ютерних систем і доступу до інтернету державних установ, фінансових і ділових центрів і створення безладу і хаосу в житті держав. Міждержавні відносини та політичне протистояння у вигляді вандалізму, пропаганди, шпигунства та безпосередніх атаках на комп'ютерні системи та сервера здійнюються з використанням інтернету і пов'язаних з ним технологічних та інформаційних засобів однією державою з метою заподіяння шкоди військовій, технологічній, економічній, політичній, інформаційній безпеці та суверенітету іншої держави.

Кібервійни можуть бути спрямовані не тільки на збір конфіденційної інформації розвідувальними органами, а також на здійснення військових дій, здатних викликати економічний збиток, пошкодити важливу інфраструктуру, а також вплинути на результат звичайних збройних конфліктів. Інструкція у «Талліннському посібнику» НАТО містить 95 правил, на котрі можуть орієнтуватись держави НАТО на випадок кібервійни. Сукупність «кібератак», які перевищують своїм загальним негативним впливом певний поріг, можуть розглядатися як початок «кібервійни». Класичним прикладом «кібератаки є виведення з ладу системи управління протиповітряної оборони Іраку під час операції «Буря в пустелі». Тоді спецслужбам США вдалося заразити вірусами комп'ютерну систему з пам'яті принтерів, придбаних для цієї системи у однієї комерційної фірми. Екс-

перти з НАТО розглядають мілітаризацію інтернету в якості одного з найголовніших і найбільш небезпечних трендів розвитку «кіберпростору». На їх думку, цілком допустимо, щоб країни НАТО здійснювали «кібернаступ» по недружніх їм державам [4]. Стратегія операцій в кіберпросторі міністерства оборони США містить перелік «стратегічних переваг в кіберпросторі», до яких відносяться оперативний зв'язок і можливості обміну інформацією та знаннями в сфері інформаційних технологій, у тому числі здійснення експертиз у сфері кібербезпеки. Військова стратегія США явно вказує, що кібератака на США є Casus belli в тій же мірі, як і акт звичайної війни [5].

Слід зазначити, що проблема кібервійн загострилася в останнє десятиріччя. Цілеспрямовані кібератаки планують навіть самі уряди окремих держав. Так, 12 січня 2010 р. Google розмістив на своєму офіційному блозі повідомлення, що він виявив «ретельно розроблені та спрямовані атаки», які походять з Китаю, мета яких полягала в крадіжці інтелектуальної власності. Найбільша загроза з Китаю йде для мережі військового командування ВМС США. Стратегія США передбачає, що на атаки хакерів держава вважатиме за можливе відповідати воєнними акціями, якщо кібератака спричинить істотні руйнування чи фінансові втрати, тим паче – загибель людей.

Існують проблеми або певна специфіка ведення кібернетичної війни. Наприклад, в кібервійні зазвичай неможливо ідентифікувати нападника, навіть коли причетність до кібератаки державних структур держави є безумовною. Географічним джерелом кібератаки , зазвичай, є не та держава, якій така атака об'єктивно вигідна. Характерною рисою кібервійни є прихованість впливу та відсутність видимих руйнувань (без людських жертв) [6]. Як наслідок, надзвичайно складно виявити початок кібератаки, застосувати превентивні заходи для попередження таких атак, а також адекватно оцінити рівень загрози та масштаб завданих збитків. Кібервійна відрізняється надзвичайною швидкістю проведення атак, коли проміжок часу між початком «агресії» та її наслідками скорочується до мінімуму. До того ж, шкідливі програми мають здатність швидко «розмножуватись» копіями і практично безперешкодно поширюватись [7]. На відміну від звичайної зброї, кіберзброя необов'язково знищує об'єкт впливу, а скоріше впроваджує певний набір даних і команд, що змінюють існуючі алгоритми функціонування системи й активізують потрібні реакції (від виконання бажаних дій чи невиконання певних функцій аж до самознищення).

До особливості кібервійни можна віднести її незавершеність і невизначену тривалість, оскільки жодна сторона конфлікту не може стверджувати, що супротивник більше не здійснює кібер-атак. Наступною особливістю кібервійни є те, що вона може проводитись як у мирний час, так і в період ведення військових дій. Однак, попри потенційний масштаб кібервійна має досить обмежені можливості у досягненні політичних, економічних та військових цілей. За допомогою кібервійни неможливо роззброїти супротивника, окупувати його територію або змінити політичний режим в державі. Кібервійна слугує більше засобом здійснення психологічного тиску на ворога, а також може на певний час завадити йому використовувати свої інформаційні системи та мережі належним чином [8], що на мою думку, є більш суттєвим наслідком.

Мережеві інформаційні потоки напряму вплинули на характер, форми та способи ведення бойових дій. Все більше держав починають приділяти захисту від кібервійн першочергову увагу та виділяють кошти для організації систем захисту та підтримки інституцій, завданням яких є забезпечення кібербезпеки держави. Можна прогнозувати, що зважаючи на надзвичайно високий ступень суспільної небезпеки, кібервійни відіграватимуть дедалі значущу роль у міждержавній політиці, військовій стратегії не лише високорозвинутих держав, а й тих, які знаходяться ще на шляху до економічного зростання. В найближчій перспективі може змінитися підхід до розуміння поняття кібервійни, а саме – вона може бути прирівняна та вважатися повноцінною та невід'ємною часткою війни у формі бойових дій між збройними силами в усіх державах, а можливо, стане єдиним способом ведення міждержавних та світових війн, та застосовуватися для демонстрації сили – в мілітаризованих міждержавних конфліктах. Це, відповідно, вплине і на методи протидії кібервійнам та кібертероризму як злочинам проти національної безпеки, миру, безпеки людства та міжнародного правопорядку.

Список використаних джерел:

1. Социология: Энциклопедия / Сост. А. А. Грицанов і др. Минск. Интерпрессервис. Книжный Дом, 2003. с. 179.
2. Запорожець, О. Ю. Кібервійна: концептуальний вимір. Актуальні проблеми міжнарод них відносин. 2014. Вип. 121 (частина І). С. 80–86.
3. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування. Аналітична записка. URL: http://www.niss.gov.ua/articles/454/.

4. Эдуардо Феббро. Кибервойна между Россией и Западом («Pagina 12», Аргентина). URL: http://inosmi.ru/world/20140930/223333408.html.
5. Друг В., Матковський В. Кібервійни, Інтернет-розвідка. URL: http://www.polpravozhit.in.ua/2015/05/blog-post_4.html
6. Schreier F. On Cyber warfare. URL: http://www.dcaf.ch/content/download/67316/1025687/file/OnCyberwarfare-Schreier.pdf.
7. Clarke R. A., Knake R. K. Cyberwar (2010). The Next Threat to National Security and What to Do About It. Ecco, HarperCollins. 290 p.
8. Libicki M. Cyberdeterrence and Cyberwar. URL: http://www.rand.org/ content/dam/rand/pubs/…/2009/RAND_MG877.pdf.

Ігор Воронов, доктор юридичних наук, старший науковий співробітник, провідний науковий співробітник Одеського державного університету внутрішніх справ, адвокат адвокатського об'єднання «Саєнко Харенко»

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В МЕРЕЖІ ІНТЕРНЕТ

Статтею 32 Конституції України гарантовано право людини на невтручання в її особисте життя. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Необхідно розрізняти між собою поняття «*інформації про особу» та «персональні дані»*. До інформації про особу відносяться будь-які відомості, що її стосується. Це й біографічні дані, характеристика, наприклад, її вподобання, суспільні та політичні погляди тощо. Тобто це досить дуже широкий обсяг різноманітної інформації. Закономірно постає питання – чи є будь-яка інформація про фізичну особу її персональними даними? Наприклад, Закон України «Про інформацію» ототожнює ці два поняття, стаття 11 зазначає, що інформація про особу: *(персональні дані)* – це *відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована*. Майже аналогічне визначення персональних даних закріплено у статті 1 Закону «Про захист персональних даних».

Отже, під обсяг персональних даних, а й слід під захист підпадає значний обсяг інформації. Таким чином, відомості, які ідентифікують конкретну фізичну особу і знаходяться в цифровій формі, також належать до персональних даних. Проте слід окремо відзначити, що публічно оголошені відомості про фізичну особу або відомості, які не можна зберегти на матеріальних носіях, згідно із Законом «Про інформацію» персональними даними не вважаються.

Нагадаємо, що 25 травня 2018 року набули чинності нові вимоги Європейського парламенту щодо захисту персональних даних. Правила закріплені в General Data Protection Regulation (далі – GDPR), Відповідно до GPPR персональні дані – це будь-яка інформація, яка дозволить визначити фізичну особу. Тобто це можуть бути й IP-адреси, місце заходження (локація).

Останні роки переконливо свідчать, що кількість кібератак в інформаційному середовищі швидко зростає, отже ризики доступу до даних також знаходяться постійно під загрозою.

Таким чином, захист права на недоторканість приватного життя людини в контексті розвитку інформаційних технологій, є необхідним елементом функціонування демократичного суспільства та фундаментальним правом людини.

Різні аспекти проблематики захисту персональних даних в мережі Інтернет ґрунтовно розглядалися такими вченими, як К. Бєляков В. Глушков, М. Моїсеєв, А. Ракітов, А. Соколов, К. Колін, В. Брижко, І. Жиляєв, Р. Калюжний, Д. Ланде, В. Фурашев, В. Цимбалюк, М. Швець, І. Забара, А. Пазюк, О. Баранов, В. Брижко, А. Пазюк, А. Чернобай, А. Тунік, А. Марущак та інші.

Загальновідомо, що процес ідентифікації користувачів характеризується декількома способами. Кожен з них має свої переваги і недоліки, завдяки чому деякі технології підходять для використання в одних системах, інші – в інших.

Види ідентифікації:

1. Парольна ідентифікація (найбільш поширений і водночас простий спосіб, проте спрощене використання одного паролю для всіх записів (акаунтів) може одночасно призвести до масштабних негативних наслідків);
2. Апаратна ідентифікація (досить висока надійність);
3. Біометрична ідентифікація (найпоширеніше використання на основі відбитків пальців і райдужної оболонки ока);

4. Багатофакторна ідентифікація (для визначення особистості застосовується відразу кілька параметрів).

Найпопулярніша технологія – це використання двофакторної аутентифікації. Профіль користувача Google постійно пропонує налаштувати подвійне підтвердження входу. Найчастіше – це СМС-повідомлення або дзвінок.

Питання обробки і захисту персональних даних є одним з найактуальніших для бізнесу.

Так, організація роботи з персональними даними включає реалізацію наступних завдань:

1. Організація самого збору персональних даних (на жаль дуже часто такий процес оминає найголовнішу стадію – отриманням згоди суб'єктів персональних даних у спосіб передбачений законодавством).
2. Організація процесу обробки персональних даних і їх зберігання.
3. Впровадження технічних, організаційних та правових заходів, спрямованих на захист персональних даних.

Одне із головних прав суб'єкта персональних даних – це знати про місцезнаходження бази персональних даних, яка містить його персональні дані, її призначення та найменування, місцезнаходження або місце проживання (перебування) володільця чи розпорядника персональних даних.

Через низький рівень правової свідомості громадяни не приділяють достатньої уваги проблемним аспектам, пов'язаним із захистом персональних даних. Пересічна людина як учасник сучасних інформаційних відносин у мережі Інтернет, натискуючи «згоду» на обробку персональних даних подекуди потрапляє вже в іншу «інформаційну гру», залежність від маркетингових процесів, інформаційної діяльності супермаркета, банка тощо. Не важко здогадатися, що численні телефонні дзвінки на мобільний телефон, десятки СМС-повідомлень, постійні листи на поштову скриньку мережі Інтернет – це все негативні наслідки витоку й подальшого розповсюдження персональних даних. Особливо це стосується зростаючої активності користувачів у соціальних мережах.

Також одним із найактуальніших та найпоширеніших питань є т захист персональних даних пацієнтів, які звертаються до лікарів для отримання медичних послуг, а також захист персональних даних при участі у публічних закупівлях (всі документи після розкриття пропозицій становляться доступними для перегляду).

Список використаних джерел:

1. Русак Д. М., Березовська І. Р. Вдосконалення правового регулювання захисту персональних даних в мережі Інтернет в контексті інтеграції України в світовий інформаційний простір // Actual problems of international relations. Release 124 (part II). 2015.
2. Марущак А. І., Мельник К. С. Особливості обробки та захисту персональних даних у мережі Інтернет: європейський досвід та законодавство України // Інформаційна безпека людини, суспільства, держави № 3 (13), 2013.
3. Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. – К., 2015. – 220 с.

Денисова Т. А., доктор юридичних наук, професор, заслужений юрист України, м. Чернігів, Україна
Шеремет О. С., доктор юридичних наук, доцент, депутат Чернігівської міської ради, професор кафедри правових дисциплін Національного університету «Чернігівський колегіум» імені Т. Г. Шевченка, м. Чернігів, Україна

ЗАПОБІЖНІ ЗАХОДИ В МЕЖАХ ІНФРАСТРУКТУРНОГО, ТЕХНОЛОГІЧНОГО ТА СОЦІАЛЬНОГО РОЗВИТКУ СУЧАСНИХ МІСТ: ЗАВДАННЯ ТА РІШЕННЯ

Здобуття незалежності Україною та зміни вектору розвитку держави викликали необхідність глибокого реформування суспільних відносин і кардинальних змін усіх галузей права. Сьогодні держава перебуває у процесі постійного вдосконалення кримінально-правової політики та законодавства, приведення їх у відповідність до конкретних соціально-правових потреб суспільства. На цьому етапі досить важливим є визначення того, які основні профілактичні заходи можливо застосовувати органам місцевого самоврядування, встановити їх форму та зміст, окреслити завдання та знайти відповідні рішення. Адже у XXI столітті створення надійної системи запобігання злочинам має бути одним із пріоритетних напрямків державної політики по забезпеченню безпеки суспільства. Разом з тим,

запобіжна діяльність практично неможлива без достатнього правового регулювання, а також участі органів місцевого самоврядування, оскільки злочинність традиційно пов'язана з місцевими особливостями.

Відповідно до Закону України «Про місцеве самоврядування в Україні» (ст. 2. «Поняття місцевого самоврядування») передбачено, що місцеве самоврядування в Україні спроможне самостійно або під відповідальність органів та посадових осіб місцевого самоврядування вирішувати питання місцевого значення в межах Конституції і Законів України. Місцеве самоврядування здійснюється територіальними громадами сіл, селищ, міст як безпосередньо, так і через сільські, селищні, міські ради та їх виконавчі органи, а також через районні та обласні ради, які представляють спільні інтереси територіальних громад сіл, селищ, міст. Проте, незважаючи на особливу роль органів місцевого самоврядування у системі суб'єктів запобігання злочинам, на жаль, активізації діяльності у цій частині поки не відбувається. Ми не будемо зупинятись на причинах такого загального висновку, оскільки їх перераховувати й пояснювати – справа довготривала. Акцентуємо увагу на тому, що діяльність територіальної громади із запобігання злочинам, суспільне усвідомлення й посилення її роботи, розширення змісту такої діяльності повинно бути реалізоване органами місцевого самоврядування якомога швидше. На прикладі м. Чернігова з існуючими проблемами та неузгодженостями, ми проілюструємо які завдання можливо вирішувати органам місцевого самоврядування задля досягнення аксіоми: «Безпечні міста – безпечна країна».

Необхідно підкреслити, що основні проблемні питання, що провокують зростання правопорушень й злочинів у м. Чернігові, як мабуть і в інших українських містах, полягають у наступному: трудова міграція з міста, тіньова зайнятість, молодіжне безробіття; застаріла система професійної освіти, що не є привабливою для молоді; незбалансованість наповненості ДНЗ та ЗНЗ міста в розрізі їх проектної потужності; відсутність системи комплексної реабілітації, особливо колишніх військовослужбовців, воїнів АТО/ООС, дітей з особливими потребами тощо; невідповідність між можливостями сучасних цифрових технологій та технічним станом й інформаційно-аналітичним забезпеченням освіти Чернігова; складна медико-демографічна ситуація; відмова автоперевізників від обслуговування міських маршрутів через зношеність доріг та високу аварійність тощо.

За таких складних умов органами місцевого самоврядування було прийнято низку стратегічних завдань, зокрема:

1) «Чернігів – конкурентоспроможне та інноваційне місто»;

2) «Розвиток житлово-комунального господарства та інфраструктури м. Чернігова «Комфортне місто»;

3) «Розвиток людського потенціалу «Людина – понад усе»;

4) «Міська мобільність і безпека дорожнього руху» (у тому числі, заходи зі створення максимально адаптованої інфраструктури для велосипедистів, пішоходів та людей з особливими потребами);

5) «Можливості інтелектуальної відеоаналітики в здійсненні контролю за безпекою міського трафіку, виявленні правопорушень і надзвичайних подій, розшуку людей і майна»;

6) «Цифрова трансформація міського середовища»;

7) «Соціальний контроль як один із ефективних профілактичних заходів з боку суспільства».

Кожне з поставлених завдань знайшло підтримку більшості членів територіальної громади і поступово втілюються у життя.

Так, загальновідомо, що життя людини та її безпека, правопорядок та громадський спокій – це пріоритетні завдання сучасної України. Загострення криміногенної ситуації на Сході країни вимагають створення надсучасної системи попередження надзвичайних ситуацій, протидії тероризму, «інтелектуальних» заходів безпеки громадян та критичної інфраструктури міст та селищ. У м. Чернігові використання цифрових технологій запроваджує новий рівень координації діяльності оперативних, чергових, диспетчерських та муніципальних служб, відповідальних за громадську безпеку та повсякденну життєдіяльність місцевих громад, а також забезпечує механізми швидкого реагування відповідних служб з метою усунення наслідків правопорушень та надзвичайних ситуацій.

Окремої уваги потребував напрям безпеки, пов'язаний з дорожньою інфраструктурою, контролем та спостереженням за дорожнім рухом. Доведено, що кількість дорожньо-транспортних пригод можна потенційно зменшити втричі за умови використання технологій та значного світового досвіду щодо зменшення аварійності на дорогах. Було проведено моніторинг безпечності доріг, небезпечних перехресть та транспортних магістралей, паркувальних майданчиків, автоматичної фіксації порушень правил дорожнього руху, керування інфраструктурою світлофорів тощо. Завдяки отриманню та аналізу інформації, рішенням стало термінове переобладнання дорожнього покриття, убезпечення дорожнього руху і т. ін. Варто підкреслити, що зараз м. Чернігів перетворилося на сучасний будівничий комплекс. Одночасно із дорогами відбудовуються тротуарні покриття,

встановлюється освітлення, запроваджується відеоспостереження тощо. Як результат, майже втричі зменшилось вчинення порушень правил дорожнього руху, перевищення швидкості та недотримання технічних параметрів транспортних засобів. Нестандартні ситуації завдяки сигналам громадян вдалося вирішувати оперативно й найменшими втратами. Підкреслимо, що обсяги капітальних інвестицій зросли на 47,2% і склали 549,6 млн грн, що становить 15,6% капітальних інвестицій Чернігівської області; загальний обсяг прямих іноземних інвестицій (на 01.07.2018) склав 30551,0 тис. дол. США, що на 274,8 тис. дол. США більше, ніж на початок року. Лише протягом 6 місяців 2019 р. збудовано або реконструйовано та введено в експлуатацію сім об'єктів виробничої сфери. Капітально відремонтовано дорожнє покриття вулиць площею 47,9 тис. м^2, із заміною 5,4 тис. метрів погонних бортового каменю; виконано капітальний ремонт покриття доріг приватного сектору площею 5,7 тис. м^2; проведено грейдування з підсипкою асфальтобетонної крихти на 19-и вулицях (площею 28,9 тис. м^2) приватного сектору, де зовсім не було асфальтного покриття; проведено поточний ремонт на 45-и вулицях приватного сектору (площею 11,5 тис. м^2) із встановленням освітлення та відеоспостереження; відновлено 27,9 тис. м^2 покриття тротуарів; влаштовано велодоріжок довжиною 19,8 км; нанесено 37,3 км дорожньої розмітки та 3,9 тис. м^2 на регульованих та нерегульованих пішохідних переходах, стоп-лініях; нанесена пластикова дорожня розмітка ліній довжиною 5,2 км тощо.

У рамках Програми «Безпечне місто Чернігів» на 2018–2020 роки додатково встановлено 81 камеру відеоспостереження; проведений капітальний ремонт 14 ліфтів у житловому фонді міста; відновлено 18 ігрових та спортивних майданчиків. Цей перелік може бути продовжено. Зрозуміло, що для великих міст, скажімо, столиці – м. Києва, або м. Харкова – ці показники не є значними. Але для міст з населенням не більш як триста осіб, це не просто цифри – це дійсно прагнення створити безпечне місто й поступове досягнення такого результату. Завдяки такій постановці питання можливо окреслити не тільки шляхи співпраці органів місцевого самоврядування з правоохоронними органами, а й визначити позитивні напрямки профілактики правопорушень громадянами міста.

Варто зазначити, що завдання влади щодо формування соціального капіталу, підняття рівня моральності й духовності являється необхідною умовою здійснення повноцінних контактів між органами місцевого самоврядування та окремими верствами населення. З цього напрямку діяльність розпочинається з перших кроків, зокрема, на базі закладів дошкільної

освіти №4 та №22 організовано центри розвитку дитини; впроваджуються елементи дуальної форми навчання у закладах професійно-технічної освіти і т.ін. Крім того, затверджено Програму розвитку фізичної культури та спорту м. Чернігова на 2019–2023 роки. Нажаль, важко зберегти молоде покоління в межах країни, що сьогодні поки не стала привабливою для молоді: їдуть на навчання, шукати кращої долі… Не можна сказати, що потік еміграції можна швидко припинити, проте, необхідно створити такі умови, щоби молодь свідомо залишалася на Батьківщині.

Сьогодні політика запобігання злочинам повинна відповідати гуманістичним традиціям, що є результатом історичного розвитку сучасного суспільства багатьох країн світу. Саме громадянське суспільство, особливо органи місцевого самоврядування на місцях, повинні відігравати суттєву роль у протидії протиправної поведінки громадян та вчинення ними злочинів. Впевнені, що лише радикальні зміни в діяльності органів місцевого самоврядування, діяльності для людей і спільно із людьми, допоможе українському суспільству об'єднатися в боротьбі із злочинністю за безпечне місто і безпечну країну.

Жаровська Галина, доктор юридичних наук, доцент, завідувач кафедри кримінального права Чернівецького національного університету імені Юрія Федьковича

ПРОТИДІЯ ТРАНСНАЦІОНАЛЬНІЙ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ: СКЛАДОВА БЕЗПЕКОВОЇ ПОЛІТИКИ УКРАЇНИ

Актуальність теми. На початку XXI століття у світі відбуваються кардинальні трансформації, що супроводжуються зміною безпекових викликів і загроз. В умовах глобалізації та інтернаціоналізації все активніше заявляє про себе транснаціональна організована злочинність, для якої немає кордонів, а характер і способи кримінальної діяльності мають підвищену соціальну небезпеку. Закономірності її появи і розвитку обумовлені як процесами, що відбуваються у світі, так і прагненням злочинності до постійного розширення сфери свого впливу, наявністю істотних регіональних і національних відмінностей у методах кримінально-право-

вого впливу на конфліктні суспільні відносини. При цьому сучасна транснаціональна злочинність стає вже не тільки кримінально-правовим економічним явищем, але і отримує нові властивості, входячи у сферу міжнародних політичних відносин. Вона не просто шкодить суспільним відносинам, вона руйнує їх, створюючи по суті альтернативну модель існування певних соціальних угруповань, яка базується на вчиненні ними злочинів. За рахунок виходу за межі національних кордонів злочинна діяльність таких угруповань стає більш різноманітною, вони отримують можливості залучати додаткові фінансові ресурси, людські резерви, краще маскувати свої дії та уникати переслідування з боку національних правоохоронних органів країни їх походження, налагодити взаємодію із злочинними угрупованнями інших країн, запозичувати в них нові способи вчинення злочинів. Все це свідчить про те, що транснаціональна організована злочинність є новим, самостійним видом злочинної організованої діяльності, яка становить гостру проблему для всіх країн світу. Особливого значення ця проблема набуває для нашої країни, оскільки Україна ще перебуває у стані кризи і є вразливою в економічному, політико-правовому та соціальному відношенні для негативного впливу з боку організованих злочинних угруповань як українських, так і зарубіжних.

У цьому зв'язку актуальним є необхідність удосконалення безпекової політики держави, спрямованої на протидію транснаціональній організованій злочинності, яка повинна вивести цю боротьбу на новий рівень ефективності.

Виклад основного матеріалу. Розробка ефективної політики держави, спрямованої на боротьбу з транснаціональною злочинністю, передбачає створення ідеальної моделі, яка, включивши в себе позитивний міжнародний досвід у сфері протидії транснаціональним злочинним організаціям, буде в змозі врахувати національні особливості криміногенної обстановки в Україні і забезпечити власну суверенність держави.

Першим елементом, який входить до діяльності держави з формування політики, спрямованої на боротьбу з транснаціональною злочинністю, є її розробка з урахуванням положень, що окреслюють проблематику транснаціональної злочинності на міжнародному рівні.

Згідно ст. 3 Конвенції ООН проти транснаціональної організованої злочинності організована злочинна діяльність стає транснаціональною, якщо: вона пов'язана з незаконними операціями з переміщення матеріальних і нематеріальних засобів через державні кордони, які приносять значну економічну вигоду; при її здійсненні використовується сприятлива

ринкова кон'юнктура інших держав, значні відмінності у системах кримінального правосуддя різних країн, а також проникнення в їх легальну економіку з допомогою корупції і насилля.

Таке розуміння транснаціональної організованої злочинності дозволило Управлінню ООН з наркотиків та злочинності (United Nations Office on Drugs and Crime) розробити такі документи: Типові законодавчі положення про боротьбу з організованою злочинністю; Типовий закон про боротьбу з незаконним виготовленням і обігом вогнепальної зброї, її складових частин і компонентів, а також боєприпасів до неї; Типовий закон про боротьбу з торгівлею людьми; Типовий закон про боротьбу з незаконним ввезенням мігрантів; Типові положення про відмивання грошей, фінансуванні тероризму, превентивні заходи і доходи від злочинної діяльності (для країн загального права); Типовий закон про взаємну правову допомогу у кримінальних справах; Типове законодавство про відмивання грошей і фінансування тероризму [1].

Ці документи, є базисом створення оптимальної політики, спрямованої на боротьбу з транснаціональною злочинністю, сприяють забезпеченню єдності підходів у протидії актуальним викликам і загрозам кримінального і криміногенного характеру з боку транснаціональної організованої злочинності. Вони стають свого роду стандартом нормативно-правового забезпечення боротьби із транснаціональною злочинністю на національному рівні.

Другим елементом формування такої політики є закони, стратегії, концепції і доктрини, щодо забезпечення різних аспектів національної безпеки і розвитку кримінально-правової політики. На часі є розробка Стратегія національної безпеки яка створюється не вперше, але вперше вона буде створена на основі нового закону «Про національну безпеку України», який заклав основи для структурних реформ у цій надважливій сфері. Ця стратегію має реально оцінити виклики і загрози безпеці та пріоритети політики у цій сфері. Поширення організованої злочинної діяльності, корупції в органах державної влади; зрощення бізнесу і політики; поширення міжнародного тероризму; загроза використання з терористичною метою ядерних та інших об'єктів на території України; торгівля людьми і нелегальна міграція; можливість незаконного ввезення/вивозу в країну лікарських препаратів, творів мистецтва, зброї, боєприпасів, вибухових речовин і засобів масового ураження, радіоактивних і наркотичних засобів; недостатнє облаштування державного кордону України – нині фактично є ідеальним підґрунтям для розвитку транснаціональної злочинності на території України.

Уся нормативно-правова база, яка тим або іншим чином належить до сфери боротьби із транснаціональною злочинністю, має бути належним чином проаналізована, при цьому відповідні законодавчі положення доцільно оцінювати з точки зору їх науковості, реалістичності, обґрунтованості. Цей нормативно-правовий масив має зазнати змін у відповідності до напрацювань ООН з урахуванням національної специфіки, особливостей тих проблем, що утворюють транснаціональні злочинні організації на теренах нашої держави.

На нашу думку, доцільним є прийняття Закону України «Про протидію транснаціональній організованій злочинності», в якому відповідно до Конституції України, законів України та загальновизнаних норм міжнародного права буде визначено основи правового регулювання відносин, що виникають у зв'язку з діяльністю державної системи протидії транснаціональній організованій злочинності.

Зважаючи на загострення криміногенної обстановки, постає необхідність вжиття великомасштабних комплексних заходів, що мали б забезпечити її стабілізацію на найближчі роки. За цих умов має бути надано пріоритет питанням удосконалення системи профілактики правопорушень, посиленню протидії організованій злочинності, забезпеченню охорони публічного порядку та безпеки, розширенню міжнародного співробітництва у боротьбі із злочинністю, а також науковому та інформаційно-технічному забезпеченню правоохоронної діяльності. У цьому зв'язку вбачаємо за доцільне розробити і прийняти державну програму невідкладних заходів протидії транснаціональній організованій злочинності.

Третім елементом політики, спрямованої на боротьбу з транснаціональною злочинністю, є забезпечення її суверенності. Для України це набуває принципового значення, оскільки, як зазначають західні вчені, міжнародне правосуддя нерідко демонструє політичну вмотивованість, а вимоги і рекомендації світової спільноти, виражені у багатосторонніх угодах, не повинні обмежувати інтереси окремої держави і тим більше створювати загрози для національної безпеки. У зв'язку з цим, з одного боку, повинні розвиватися міждержавні правові відносини, що забезпечують колективні зусилля організаційно-управлінського змісту у протидії транснаціональній злочинності [2]. З другого боку слід бачити «межі поступливості», коли держава має активно відстоювати власну позицію у міжнародних судах, у міжнародних організаціях, домагаючись видачі злочинців, які переховуються за кордоном та є недоступними українському кримінальному судочинству.

Четвертим елементом розробки політики, спрямованої на боротьбу з транснаціональною злочинністю, є позитивний кримінально-політичний досвід окремих держав. На нашу думку позитивним орієнтиром є інтегрована модель національної політики, що включає в себе низку базових ідей (концептів):

1. Національна політика, що спрямована на протидію транснаціональній злочинності, має бути побудована на ідеології соціальної справедливості.

2. Така політика повинна мати міцну конституційно-правову основу.

3. Формування такої національної політики вимагає забезпечення високого престижу кримінології. Реалізація цієї ідеї має не тільки наукове, але і практичне значення, зокрема політика, спрямована на протидію транснаціональній злочинності передбачає здійснення кримінолого-правового моніторингу. Як видно з назви, його зміст утворюють дві сторони:

а) кримінологічний. На наше переконання кримінологічний моніторинг має у першу чергу відповідати вимогам системності і комплексності спостереження, аналізу, оцінки злочинності та інших, пов'язаних з нею явищ. Найбільш актуальними напрямами кримінологічного моніторингу в Україні, на наш погляд, є: детермінанти транснаціональної організованої злочинності; криміналізація економічних відносин; нерозкрита злочинність; тенденції розвитку економічної організованої злочинності; фінансування екстремізму і тероризму; криміногенні наслідки соціальної напруженості;

б) правовий моніторинг. На нашу думку, основними напрямами правового моніторингу є: узгодженість адміністративно-правової та кримінальної політики у сфері протидії посадовій та економічній злочинності; корупційна злочинність і караність; процеси криміналізації і декриміналізації діянь; співвідношення тяжкості вчинених злочинів і суворості покарань. У результаті повинна бути побудована єдина система кримінолого-правового моніторингу, у якій центральні органи управління моніторингом будуть доповнені мережевою структурою науково-дослідних і освітніх установ.

4. Наступне, надзвичайно важливе завдання, – модернізація організаційної структури протидії транснаціональній злочинності відповідно до тих викликів і загроз, які реально впливають на стан національної безпеки.

Очевидно, що запорукою створення надійної системи охорони права сьогодні може бути тільки зміцнення самої української держави та її ор-

ганів, відповідальних за забезпечення в країні законності і правопорядку. У зв'язку з цим, перед українською державою постали масштабні завдання, пов'язані з виробленням стратегії розвитку всієї правоохоронної системи та її важливої складової – правоохоронних органів, пошуку принципово нових, нестандартних форм їх організації, взаємодії, координації діяльності, удосконалення системи управління правоохоронними органами. На нашу думку, на часі перехід правоохоронних органів на якісно новий рівень планування та управління, зокрема, упровадження в діяльність правоохоронної системи елементів стратегічного менеджменту [3].

Актуальним завданням стратегічного управління правоохоронною системою України слід вважати створення дієвої стратегії протидії транснаціональній організованій злочинності, яка відповідає криміногенній ситуації в Україні, враховує політичні та військові реалії, що характеризують розвиток транснаціональної організованої злочинності. Розроблення такої стратегії може відбуватися за наступним алгоритмом: політичне, пропагандистське та дипломатичне супроводження протидії транснаціональній організованій злочинності; виявлення та перекриття каналів проникнення транснаціональної організованої злочинності у країну, її впровадження в структури влади, у суспільство та економіку; забезпечення законності та безпеки економічної діяльності; розроблення територіальних стратегій протидії з урахуванням специфіки кожного регіону України; розроблення та прийняття спеціальних програм, що забезпечують безпеку і захист учасників досудового розслідування і судового розгляду у кримінальних провадженнях щодо організованої (транснаціональної) злочинності.

Наведені вище елементи політики, спрямованої на протидію транснаціональній злочинності, на наше переконання є ключовими, оскільки вони утворюють той базис, на якому має грунтуватися протидія даному виду злочинності, визначають першочергові напрями діяльності держави у реальній боротьбі з таким явищем, яким є сучасна транснаціональна злочинність.

Список використаних джерел:

1. Деятельность Управления ООН по наркотикам и преступности, направленная на содействие осуществлению положений о международном сотрудничестве, содержащихся в Конвенции ООН против транснациональной организованной преступности: доклад Секретариата Конференции участников Конвенции ООН против транснациональной организованной

преступности 2014 г. Режим доступа: http://www.unodc. CTOC/COP/WG.3/2014/2.org
2. Beare M., Woodiwiss M. U. S. Organized Crime Control Policies Exported Abroad. *The Oxford Handbook of Organized Crime.* Oxford-New York, 2014. P. 554–557.
3. Жаровська Г. П. Реформування правоохоронної системи як відповідь на децентралізацію державної влади в Україні. *Вісник Чернівецького факультету Національного університету «Одеська юридична академія»:* зб. наук. пр. Чернівці: Чернівец. ф-т Нац. ун-ту «ОЮА», 2014. Вип. 3. С. 200–212.

Іжевський Р. П., аспірант кафедри кримінології та кримінально-виконавчого права Національного юридичного університету імені Ярослава Мудрого, м. Харків, Україна

ЕЛЕКТРОННІ СИСТЕМИ ЗАПОБІГАННЯ ЗЛОЧИННОСТІ В СФЕРІ БУДІВНИЦТВА АВТОМОБІЛЬНИХ ДОРІГ

Сфера дорожнього господарства традиційно вважається однією з найкорумпованіших. Про негативний стан справ в цій галузі зазначають як в середині країни, так і в міжнародному співтоваристві. За оцінками міжнародних експертів якість українських доріг гірша, ніж в Молдові та Мозамбіку і прирівнюється до якості доріг у Парагваї. Із 137 країн, що розташовані в рейтингу індексу глобальної конкурентоздатності Україна посідає 130 місце [3].

За останні два роки на галузь з державного бюджету було виділено близько 100 млрд грн. В той же час збільшення розміру бюджетних асигнувань не призвело до збільшення кількості та якості відремонтованих й побудованих автомобільних доріг. Відповідно до звітів про фінансову діяльність Укравтодору, кількість відремонтованих доріг за основною бюджетною програмою в 2018 році в порівнянні із 2017 роком виросла лише на 56 (!) км, при тому що фінансування збільшилось майже вдвічі. З огляду на зазначене, виникає припущення, що або в галузі здійснюється неефективне управління бюджетними коштами, або (що більш вірогідно) такі кошти розкрадаються недобросовісними чиновниками та підрядниками. На користь останньої тези красномовно свідчить кримінальна

статистика, за даними якої за останні чотири роки злочинність в сфері будівництва автомобільних доріг зросла більше ніж в 3,5 рази.

Для того, щоб мінімізувати численні схеми незаконного використання бюджетних коштів було розроблено ряд електронних систем, які прямо чи опосередковано спрямовані на запобігання злочинам у сфері будівництва автомобільних доріг.

До спеціальних електронних систем варто віднести платформи «Антикорупційний монітор», «Моніторинг витрат на будівництво і ремонт доріг» та мобільні додатки «Дороги України» й «Navizor».

Громадська організація «Антикорупційний монітор» займається виявленням формалізованих ознак корупційних ризиків. Це платформа, яка дозволяє здійснити громадський аудит укладених угод із переможцями публічних закупівель методом кредитного скорингу. Моніторинг закупівель здійснюється шляхом автоматизованого серфінгу за введеним пошуковим запитом. Після сортування всіх можливих результатів формується звіт про проведену антикорупційну експертизу та оцінку якості переможця закупівлі. У звіті на підставі встановлених зв'язків та виявлених закономірностей вказується індекс «ФОКС» (формалізовані ознаки корупційної складової). На підставі такої оцінки можна провести «червоні лінії», які не дозволять укласти угоду із недобросовісним чи ненадійним підрядником.

На сьогодні досить важко прослідкувати увесь рух бюджетних коштів, що спрямовані на дорожньо-будівельні роботи. Залучення низки субпідрядних організацій та контрагентів обтяжує цей процес. Як показує практика, віднайти кінцевого вигодонабувача досить складно, а в окремих випадках майже неможливо.

Вирішити цю проблему спробували представники Офісу ефективного регулювання (BRDO), які запустили платформу «Моніторинг витрат на будівництво і ремонт доріг». Вона дозволяє в режимі реального часу здійснювати фінансовий моніторинг дорожньо-будівельних робіт. Дані для моніторингу отримуються із відкритих джерел інформації та відображаються у формі графіків та діаграм. Моніторинг можна здійснювати відносно обсягу бюджетних асигнувань за областями; результатів тендерів на проведення дорожньо-будівельних робіт; розміру бюджетних коштів, які фактично витрачено. На сьогодні портал пропонує інформацію тільки станом на 2018 рік.

Успішно використовується й закордонний досвід мобільного контролю дорожньої інфраструктури. Українські стартапери розробили ряд мобільних додатків, які дозволяють контролювати якість виконання дорожньо-буді-

вельних робіт. Завдяки додатку «Дороги України» та «Navizor» водії за допомогою смартфонів визначають стан автомобільних доріг. Мобільний додаток реагує на вибоїни, ями, тріщини, деформації дорожнього полотна, фіксує місце розташування та рівень вібрацій власника смартфона та передає дані на сервер, де з них формується карта якості доріг. Такий корисний функціонал можна успішно використовувати для поточного моніторингу дотримання стандартів виконання дорожньо-будівельних робіт. В майбутньому це може слугувати підставою для перевірки законності використання бюджетних коштів на певному об'єкті дорожньої інфраструктури.

Електронні системи, які опосередковано спрямовані на запобігання порушенням під час виконання дорожньо-будівельних робіт, включають насамперед «Єдину систему електронних публічних закупівель ProZorro». До неї належать офіційний портал оприлюднення інформації про публічні закупівлі, база даних та модуль електронного аукціону. Дані системи є відкритими та доступними будь-якій особі, можуть безперешкодно копіюватись та використовуватись усіма зацікавленими сторонами. Здійснення закупівель за допомогою «ProZorro» відбувається через авторизовані електронні майданчики.

Після початку роботи системи «ProZorro» в Україні також було створено ряд інструментів спрямованих на моніторинг публічних закупівель. Зокрема перевірити підрядника або конкретну закупівлю можна завдяки функціонування моніторингового порталу DoZorro. Дана платформа передбачає існування декількох аналітичних інструментів у вигляді публічного та професійного модуля аналітики, які дозволяють швидко аналізувати ситуацію та знаходити ефективне рішення. Крім того, авторизовані електронні майданчики на сьогодні обладнанні смарт-технологіями, які дозволяють сформувати уявлення про потенційного виконавця робіт та послуг. Зокрема на майданчику «BiProZorro» формується загальна інформація щодо участі постачальника в торгах та їх результатах. Аналізується відсоток відхилених пропозицій та виграних тендерів, укладені договори та конкуренти такого учасника. Така картка учасника надає замовнику загальну інформацію про формальні ризики, які можуть виникнути із потенційним контрагентом.

Більше інформації про одержувачів бюджетних коштів можна отримати через такі ресурси як Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань, «YouControl», «Опендатабот». Через функціональні модулі зазначених ресурсів можна успішно здійснювати процедуру «due diligence», аналізувати ринок, про-

водити розслідування, отримувати відомості про порушення бюджетно-фінансової дисципліни. Завдяки функціональному аналізу та моніторингу можна встановити кінцевих бенефіціарних власників підприємств, пов'язаних осіб та попередити антиконкурентні узгоджені дії.

Ефективним аналітичним інструментом на сьогодні слугує база даних та система аналітики «Clarity Project». Це волонтерський проект, який в режимі реального часу аналізує публічні закупівлі, виявляє зв'язки між контрагентами та визначає ступінь ризику кожної окремо взятої закупівлі. Використання такого інструмента дозволяє попередити незаконне використання бюджетних коштів у момент проведення торгів.

Опосередковано моніторинг можна здійснювати також завдяки функціонуванню в тестовому режимі порталу «open budget» (державний веб-портал бюджету для громадян) та порталу «spending» (єдиний веб-портал використання публічних коштів).

Розглянуті вище інструменти попри їхню широку функціональність не встановлюють всі наявні корупційні ризики в момент укладення угод. Виявлення таких ризиків та їх оцінка зводиться в кінцевому результаті до механічного пошуку таких даних зацікавленими особами. Як правило, це здійснюється виключно під час реалізації контрольних заходів компетентними органами або громадськими організаціями. Практика показує, що основна корупційна складова закладається ще до моменту проведення публічних закупівель, що нівелює всі переваги вищеописаних аналітичних інструментів.

Виникає необхідність поєднання найбільш оптимальних модулів аналітики в єдину електронну аналітичну систему, яка б давала можливість виявляти ознаки незаконного використання коштів на кожному етапі руху бюджетних асигнувань. Необхідна також активна імплементація кращого міжнародного досвіду боротьби з фінансовою злочинністю [1, с. 34]. Використання даних автоматизованої системи дозволить підвищити якість інформаційно-аналітичного забезпечення, швидкість прийняття управлінських рішень та покращити рівень організації ефективної взаємодії між всіма зацікавленим сторонами [4, с. 52].

З огляду на особливості злочинності у сфері будівництва автомобільних доріг важливим є перейманння міжнародного досвіду з цього питання. Однією із форм міжнародного співробітництва має стати обмін інформацією та досвідом роботи компетентних органів держав в цьому напрямку, організація навчально-методичних, наукових заходів [2, с. 3]. Імплементація кращих міжнародних практик гармонізує систему запобігання злочинності та зробить її більш ефективною.

Список використаних джерел:

1. Bohdan Holovkin, Kostyantyn Marysyuk. Foreign experience in countering (preventing) organized crime in the financial system: special law enforcement bodies and strategic priorities. *Baltic Journal of Economic Studies* Vol. 5, No. 3, 2019. p. 25–34.
2. Serhii S. Cherniavskyi, Bohdan M. Holovkin, Yuliia M. Chornous, Vasyl Y. Bodnar, Ilona V. Zhuk. International Cooperation in the Field of Fighting Crime: Directions, Levels and Forms of Realization. Journal of Legal, Ethical and Regulatory Issues Volume 22, Issue 3, 2019. URL: https://www.abacademies.org/articles/International-cooperation-in-the-field-of-fighting-crime-directions-levels-and-forms-of-realization-1544-0044-22-3-348.pdf
3. The Global Competitiveness Report 2017–2018. URL: https://www.weforum.org/reports/the-global-risks-report-2018.
4. Головкін Б. М. Електронна система запобігання злочинності. *З нагоди 100-річчя від дня народження професора М. В. Салтевського: зб. матеріалів круглого столу, м. Харків, 30 жовт. 2017 р.* Харків, 2017. С. 48–52. URL: http://dspace.nlu.edu.ua/bitstream/123456789/13692/1/Golovkin_48–52.pdf

Карманний Є. В., кандидат технічних наук, доцент кафедри трудового права
Ковжога С. О., кандидат хімічних наук, доцент кафедри трудового права
Луценко Є. М., студент 6 курсу фінансово-правового факультету Національного юридичного університету імені Ярослава Мудрого м. Харків, Україна

ОРГАНІЗАЦІЙНО-ПРАВОВІ АСПЕКТИ ПРОТИДІЇ ЗЛОМУ ПЛАТІЖНИХ СИСТЕМ У СУЧАСНИХ УМОВАХ ДІДЖИТАЛІЗАЦІЇ

Останні зміни в електронній промисловості, об'єднання інфокомунікаційних і комп'ютерних мереж в єдиний простір істотно розширили спектр послуг автоматизованих банківських систем, і при цьому стали однією з найбільш небезпечних загроз для економіки України є порушення її фі-

нансово-банківської системи. Сфера банківських послуг володіє великою кількістю інформації стосовно своїх користувачів, якими виступають як пересічні українці, так і органи влади. За результатами опитування організованого Світовим банком у 2017 році приблизно 67% дорослого населення світу і 63% українців мають зареєстровані банківські рахунки.

Аспекти протидії злому платіжних систем у сучасних умовах діджиталізації невід'ємні від поняття кібербезпеки. Кібербезпека охоплює захист персональної інформації, а саме – виявлення, уникнення або реакція на атаки. Стандарт ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity – дає чітке розуміння зв'язку терміну cybersecurity (кібербезпека) з мережевою безпекою, прикладною безпекою, інтернетом-безпекою і безпекою критичних інформаційних інфраструктур [1].

Відповідно до зростаючої ролі кіберпростору багато держав створюють власні національні законодавчі норми та стратегії кібербезпеки. Так, нині 27 країн-членів НАТО, Європейський Союз, 12 країн Європи, що не є членами НАТО, а також 38 країн із інших частин світу мають власні національні стратегії кібербезпеки [2]. Серед них і Україна, де у 2016 р. Указом Президента України №96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про стратегію кібербезпеки України» було затверджено національну стратегію кібербезпеки. Раніше, у 2009 р., штаб-квартира НАТО ухвалила стратегічний документ «Рамки співробітництва у питаннях кібернетичного захисту між НАТО та державами-партнерами». Цим актом було закладено підґрунтя для налагодження співробітництва у сфері кібербезпеки між країнами-учасниками, зокрема й Україною [3].

У травні 2018 року, в Україні набув чинності Закон «Про основні засади забезпечення кібербезпеки України», який спрямований на формування загальної державної політики кібербезпеки. Ним передбачено створення Національної системи кібербезпеки, та появу переліку об'єктів критичної інформаційної інфраструктури. До об'єктів критичної інфраструктури можуть бути віднесені підприємства, в тому числі, й банківського і фінансового сектора. Якщо підприємство потрапляє в подібний перелік, відповідно до закону, його керівники автоматично стають відповідальними за забезпечення кіберзахисту комунікаційних систем і захист технологічної інформації. Також, одним з істотних моментів цього законі є фактичне прирівнювання злочинів в кіберпросторі до звичайних, за які передбачена кримінальна відповідальність.

У правове поле також вводиться державно-приватна взаємодія як один з принципів забезпечення кібербезпеки. Взаємодія передбачає обмін інформацією про інциденти кібербезпеки, реалізацію спільних науково-дослідних проектів, навчання кадрів у цій сфері та інше [4].

Після атаки вірусу «Petya.A» не залишилося сумнівів, що займатися інформаційною безпекою треба, й особливо в банківській системі. Ефективним результатом після цих подій стала Постанова № 95 Національного банку України (НБУ). Згідно з якою, банки повинні поетапно до вересня 2019 року ввести комплекс заходів з інформаційної безпеки [5]. За великим рахунком НБУ не вимагає від банків нічого зайвого, а самі вимоги досить сучасні. Біда в тому, що фінустанови не дуже сучасні. У багатьох випадках їм доведеться поміняти всю IT-інфраструктуру і програмне забезпечення. У найскладнішому становищі опиняться великі банки з розгалуженою мережею і застарілими технологіями. Особливо в старих відділеннях, де не було інвестицій в IT.

НБУ не став зупинятися на найпростіших питаннях інформаційної безпеки, на зразок вимог до довжини пароля. Вимоги настільки серйозні, що їх виконання порівняно з процедурою отримання сертифіката PCI DSS (Payment Card Industry Data Security Standard) – стандарт безпеки даних індустрії платіжних карт. Іншими словами, це документація зі списком критеріїв, яким повинен відповідати сервіс, якщо він якось управляє такими речами, як номер карти, термін її дії та CVV-код. Платіжних карт можна нарахувати досить багато, а оскільки мова йде про стандарт індустрії, то було б незайвим всім компаніям домовитися між собою про те, що вони будуть вважати безпечним. Для цього існує Рада PCI SSC (Payment Card Industry Security Standards Council) – Рада зі стандартів безпеки індустрії платіжних карт, утворена п'ятьма найбільшими платіжними системами. Саме вона створює правила «безпечної гри», і саме її правилам повинні слідувати компанії, які бажають отримати «Сертифікат PCI–DSS». Проходити таку сертифікацію необхідно щороку [6].

Стосовно витрат, для реалізації всіх вимог вказаного стандарту, мова може йти про мільйони гривень і навіть – доларів для окремих фінустанов. Наприклад, стандарт PCI DSS вимагає, щоб мережі прокладалися кабелем не нижче «категорії 5е». Виходить, що, якщо в якомусь відділенні банку мережу прокладена іншим кабелем, потрібно повністю перекласти мережу. А крім того, кожна банківська установа повинна підготувати і зберігати докладні схеми всіх комунікацій і вести кабельний журнал, тощо. Часом ситуація настільки запущена, що відділення дешевше буде закрити, ніж намагатися привести його у відповідність з новим регламентом.

Також банківським установам доведеться виконати вимоги щодо до захисту від шкідливого коду і забезпечення аутентифікації при доступі користувачів до уразливих даних. Для їх реалізації більшості банків потрібно буде дооснастити свої ІТ системи додатковим дорогим обладнанням. У багатьох випадках банкам доведеться сильно витратитися на заміну застарілого програмного забезпечення і навчання персоналу роботі з новим.

Виходячи з результатів дослідження можна зробити висновок, що Україна обрала важкий та затратний шлях, котрий може значно скоротити список банківських установ держави, але в той же час забезпечить захищеність економічної складової країни. На нашу думку, удосконалити організаційно-правові аспекти протидії злому платіжних систем було б доцільно шляхом комплексного, чітко спланованого, поетапного проекту вдосконалення систем її захисту. Такий комплекс має включати наступні основні підходи щодо виявлення загроз для функціонування інформаційних систем банку [7]:

– технологічний – першочерговий аудит, впровадження оновлених методів захисту та подальша оптимізація всієї ІТ-інфраструктури банку з метою не лише позбутися недоліків, але й попередити їх у майбутньому;

– робота з персоналом та адміністрацією банку – на цьому етапі необхідно не лише перевірити належне регламентне забезпечення роботи інформаційних систем, але й провести подальші роз'яснювальні роботи з персоналом, що має забезпечити розуміння всіх можливих ризиків наступних кібератак та санкцій НБУ за невідповідність положенням Постанови №95 чи інших.

Швидке й рішуче запровадження такого комплексного підходу дозволить побудувати довгострокові відносини між банками та вузькоспеціалізованими ІТ-компаніями, які надають послуги у сфері кібербезпеки. А це, у свою чергу приведе до зрозуміння фінустановами того, що санкції НБУ – це найменша загроза їхній роботі, у порівнянні з вірусною атакою, яка наступного разу може вразити персональні дані клієнтів й привести до злому платіжних систем.

Список використаних джерел:

1. Євсєєв С. П. Король О. Г., Коц Г. П. Аналіз законодавчої бази в системі управління банківською безпекою. / Східно-європейський журнал передових технологій. – Харків. – 2015. – Вип. 5/3 (77). – С. 48–59.
2. Melikishvili Alexander. Recent events suggest cyber warfare can become new threat / WMD Insights, December 2008/January 2009 Issue. – 2009. /

[Electronic resource]. – Access mode: http://www.wmdinsights.com/I29/I29_G3_RecentEvents.htm.
3. Камчатний М. В. Історія міжнародно-правового регулювання питань, пов'язаних із застосуванням комп'ютерних технологій. / Збірник наукових праць «Проблеми законності». – Харків. – 2016. – Вип. 134. – С. 199–207.
4. Юрлагіна В. В., Карманний Є. В. Сучасні аспекти державно-приватного партнерства у сфері кібербезпеки та їх позитивні тенденції для України // Матеріали X-ї наукової інтернет-конференції студентів і аспірантів Національного юридичного університету імені Ярослава Мудрого «Реалізація права на працю і безпека людини в сучасних умовах життєдіяльності», 25–26 квітня 2019 р. – Х.: Нац. юрид. ун-т, 2019. – С. 576–583.
5. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України: Постанова Національного банку України від 28.09.2017 р. №95 / [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/v0095500–17
6. An Introduction to PCI DSS (Payment Card Industry Data Security Standard) by Asim Mehmood (guest) on 23 March 2018. / Cryptomathic – global provider of secure server solutions to businesses. – 2018. / [Electronic resource]. – Access mode:https://www.cryptomathic.com/news-events/blog/an-introduction-to-pci-dss
7. Луценко Є. М., Карманний Є. В. Удосконалення аспектів кібербезпеки у банківській сфері // Матеріали X-ї наукової інтернет-конференції студентів і аспірантів Національного юридичного університету імені Ярослава Мудрого «Реалізація права на працю і безпека людини в сучасних умовах життєдіяльності», 25–26 квітня 2019 р. – Х.: Нац. юрид. ун-т, 2019. – С. 336–344.

Карчевський М. В., доктор юридичних наук, професор, Луганський державний університет внутрішніх справ імені Е. О. Дідоренка, м. Сєвєродонецьк, Луганська область, Україна

«КЛАСИЧНІ» ТА НОВІТНІ ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ ІНФОРМАТИЗАЦІЇ

Найбільш помітні соціальні зміни пов'язані з інформатизацією. Розвиток та розширення сфери застосування інформаційних технологій

обумовили в тому числі істотні трансформації правового регулювання. Нібито очевидні положення, але відповідь на питання *«Що саме змінилося?»* не є простою. Спробуємо сформулювати відповідь на поставлене питання.

1. Необхідність правового стимулювання позитивних та мінімізації негативних наслідків інформатизації обумовила появу відносно самостійної групи суспільних відносин. Для позначення цієї групи будемо використовувати термін *«інформаційна безпека»* та визначимо його наступним чином: система суспільних відносин щодо реалізації інформаційної потреби особи, суспільства, держави. Складається дана система з трьох взаємопов'язаних та взаємообумовлених елементів: відносини в сфері використання інформаційних технологій, відносини в сфері забезпечення доступу до інформації, відносини в сфері формування інформаційного ресурсу.

2. Найбільш очевидно проблеми правового регулювання певних суспільних відносин проявляються у сфері кримінального права. На сьогодні можна казати про існування *«класичних» проблем* кримінально-правового регулювання кожної з означених груп. Стосовно так званих «комп'ютерних злочинів» головне питання полягає у *відсутності чітких критеріїв* суспільної небезпечності на рівні законодавчих визначень. Через це в сфері дії кримінальної юстиції опиняються не тільки діяння, що дійсно є суспільно небезпечними, але й ті, які такими не є. Ефективність протидії кіберзлочинності зменшується. Проблеми кримінально-правового регулювання відносин в сфері забезпечення доступу до інформації стосуються головним чином *розбалансованості законодавства*, існуванні численних конкуруючих норм, надмірного рівня кількості кримінально-правових заборон у даній сфері. Необхідною є оптимізація означеної системи норм, заміни наявної розосередженої системи спеціальних кримінально-правових заборон такими, які б забезпечували регулювання більш широких сегментів інформаційної безпеки. Основне питання кримінально-правового регулювання в сфері формування інформаційного ресурсу полягає у чіткому та послідовному *визначенні межі можливостей ефективного впливу* на суспільні відносини засобами права в тому числі кримінального. У суспільно-політичному дискурсі, в науці небезпеки інформаційних впливів та зловживань обговорюються достатньо широко. Багатомірність та масштабність шкоди від неконтрольованого інформаційного простору не викликає сумнівів. Разом з цим розв'язання означених проблем шляхом доповнення КК новими нормами навряд чи є доцільним.

3. Сферою широкого застосування комп'ютерної техніки є банківська діяльність та платіжні системи тому велика частка злочинів проти власності так чи інакше пов'язана зі злочинами в сфері використання комп'ютерної техніки. Разом з оновленням способів вчинення та приховування слідів злочинів проти власності істотні зміни спостерігаються й у питанні предмету злочину проти власності. Доволі дискусійним як для науковців так і для практиків стало питання юридичного змісту таких категорій як *«безготівкові гроші», «електронні гроші», «криптовалюта»*. Криптовалюта представляє собою наступний крок у розвитку технологій розрахунків з використанням сучасних інформаційних технологій. Сьогодні маємо ситуацію, коли фактично існуючі та динамічні суспільні відносини опиняються поза межами правового регулювання за умови очевидної необхідності такого. Наприклад, особа вимагає певну суму у Bitcoin або отримує хабар у такій формі. Яким чином встановити ознаки предмета злочину? Чи можна розглядати відомості інтернет-джерел щодо курсу Bitcoin як достатній доказ для встановлення економічної ознаки відповідних предметів злочинів? На сьогодні чіткої відповіді на поставлені питання не має. Очевидно криптовалюти будуть дедалі частіше використовуватися для вчинення злочинів або ставати їх предметом. В таких умовах найбільш доцільно сформулювати прості та прозорі правила для сфери кримінально-правового регулювання, зокрема передбачити механізм оцінки. Представлення у процесуальній формі даних про криптовалюти створить нові умови для якісного оновлення діяльності правоохоронців. Виникнуть принципово нові види тактичних операцій, що збільшить можливості протидії злочинності.

4. *Новітні проблеми.* Сучасний рівень розвитку *робототехніки* актуалізує проблематику відповідного юридичного забезпечення. Разом із цим, поява штучного інтелекту – не єдина гіпотеза розвитку технологій. І науці також широко представлена гіпотеза технологій *трансгуманізму*, розвитку здібностей людини за рахунок технологічних змін у її організмі. Передумовою ефективної наукової дискусії з правового регулювання як соціалізації роботів так і технологій трансгуманізму є визначення структури досліджуваного проблемного поля, *формулювання ключових питань, які підлягають першочерговому аналізу*. Спробуємо запропонувати один з можливих підходів до розв'язання означеного завдання.

5. *Перше питання* правового регулювання розвитку штучного інтелекту стосується доцільності заборони (обмеження) наукових розробок у даній сфері. Відносна дешевизна розробки систем штучного інтелекту

(обумовлена успіхами технології) з невідворотністю забезпечить розвиток не тільки систем автономного озброєння. Вельми вірогідною є поява роботів (в тому числі складних апаратно-програмних комплексів для Інтернет) спеціально призначених для вчинення злочинів. При цьому інтелектуальні та фізичні здатності роботів на певному етапі перевищать людські. Однак, як справедливо зазначає знаний український вчений В. І. Борисов, технології, які б небезпечні вони не були, обов'язково будуть винайдені та розповсюджені незалежно від нашого бажання та відношення до них. На нашу думку такий підхід є прагматичним та реалістичним. Заборона досліджень в сфері штучного інтелекту принципово не може стати дієвою. Таким чином, відповідь на перше питання правового регулювання соціалізації штучного інтелекту наступна: попри ризик небезпек, абсолютна заборона розробки систем штучного інтелекту є неможливою, правове регулювання в даній сфері має забезпечувати стимулювання соціально ефективного використання технологій та мінімізацію ризиків зловживання технологією.

Наступне питання правового регулювання в сфері соціалізації штучного інтелекту – яким чином здійснювати правове регулювання використання штучного інтелекту. У науковій літературі представлено два підходи. У класичній системі юридичних координат вже сьогодні маємо певні рішення: визначаються права та обов'язки розробників, власників та осіб, що експлуатують роботів. Інший підхід полягає у розгляді роботів як суб'єктів права. Сьогодні таке рішення може виглядати як фантастика з ознаками безпідставного юридичного романтизму. Найбільш вагомий аргумент у тому, що створений штучно робот слідує закладеній програмі та, відповідно, не має свободи вибору, свободи волі. Оскільки остання є атрибутом суб'єкта права, питання нібито закрите. Проте, не викликає сумнівів, що на певному етапі розвитку технологій та ускладнення відносин в сфері робототехніки, процес прийняття рішення роботом, нехай і на підставі програми, стане настільки складним, що його можна буде розглядати як акт поведінки людини.

Отже, представлені підходи не є взаємовиключними, їх можна розглядати як різні етапи правового регулювання робототехніки. Зрозуміло, що розгляд досліджуваних питань за класичною схемою «розробник-власник-користувач» є актуальним та затребуваним для сучасного рівня технологій. Запропоновані в межах цього розуміння, рішення можуть забезпечити достатньо ефективне юридичне забезпечення сучасних військових, промислових, соціальних роботів тощо. Очевидно і те, що ускладн-

нення технологій вимагатиме переходу до нової, більш складної схеми правового регулювання. Скоріше за все правове регулювання соціалізації штучного інтелекту пройде шлях від розгляду робота як об'єкта відносин до наділення його правами та обов'язками.

З отриманням роботами статусу суб'єкта права виникнуть нові сфери юстиції. Крім традиційної юстиції можна буде казати про появу двох нових видів, умовно назвемо їх «змішана юстиція» та «юстиція штучного інтелекту». До змішаної юстиції будуть відноситися форми вирішення правових спорів між фізичними, юридичними особами, суспільством та роботами. До юстиції штучного інтелекту будуть відноситися форми вирішення правових спорів між роботами. Крім цього функціонування даної системи юстиції буде забезпечувати протидію роботам, що представляють загрозу для соціального розвитку та стабільності. Цілком зрозуміло, що копіювати людську систему юстиції для штучного інтелекту немає сенсу. Принципово різні фізичні характеристики та потреби вимагають апріорі відмовитися від такого підходу. Разом з цим створення даної системи є необхідною умовою для того, щоб забезпечити людству можливість контролювати розвиток суспільних процесів. Скоріше за все юстиція штучного інтелекту буде створена на основі роботів.

6. Технічний прогрес може піти шляхом фізичної інтеграції людини та технологій. Як у такому випадку зміниться правовий статус людини, що підсилює свої можливості численними технологічними імплантатами? Комплекс означених питань розглядають дослідники проблематики *трансгуманізму*. До соціальних трансформації, що можуть бути викликані використанням технологій трансгуманізму, як правило, відносять: абсолютно контрольована еволюція людини в інтересах глобальних корпорацій; нові види реалізації морфологічної свободи та права на репродукцію; принципово нові види посягань – біогенетичні та когнитивні; нові способи вчинення злочинів проти життя та здоров'я. Регулювати чи забороняти? Відповідь на це питання є аналогічною тій, що отримана в контексті гіпотези автономного штучного інтелекту: заборона є неможливою, правове регулювання у сфері використання технологій трансгуманізму має забезпечувати максимально ефективне використання їх переваг та мінімізацію негативних наслідків.

У який спосіб здійснювати регулювання? На нашу думку, відповідь на це запитання полягає в екстраполяції принципу *диверсифікації* проектних рішень для підвищення надійності резервних систем на проблематику правового регулювання технологій трансгуманізму. Якщо право буде

формувати умови/вимоги для створення якомога більшої кількості різноманітних рішень у сфері технологій трансгуманізму, «глобальна відмова» стане просто неможливою, ефективне попередження розвитку негативних наслідків буде забезпечено.

Окремим аспектом правового регулювання має стати забезпечення правових гарантій реалізації морфологічної та репродуктивної свободи. Зрозуміло, що для ефективного розв'язання цієї проблеми треба накопичувати досвід можливих видів зловживань такими свободами. Однак це вже доволі типове завдання правового регулювання – пошук балансу між реалізацією права певною особою та потребою забезпечити загальну безпеку, стабільність та розвиток. Новелами кримінально-правового регулювання стануть заборони біогенетичних та когнітивних утручань, суспільно-небезпечних порушень морфологічної або репродуктивної свободи, а також порушень вимог диверсифікації технологічних рішень.

Очевидно, що завдання контролю за розвитком та використанням певних технологій вимагатиме ефективної системи моніторингу. Навіть більше, аналіз отриманої інформації стане набагато складнішим та вимагатиме принципово нових професійних компетенцій. Традиційний розподіл завдань між юристами та спеціалістами стане вкрай неефективним. Буде спостерігатися *конвергенція юридичних та технічних наук*, виникатимуть нові види юридичних професій.

7. Як глобальну проблему слід розглядати формування правових гарантій *ефективного розвитку навколишнього інформаційного середовища*. Це комплекс питань, що стосуються правового регулювання використання інформаційних технологій, забезпечення доступу до інформації, а також формування інформаційного ресурсу. При цьому регулювання формування інформаційного ресурсу має включати не тільки зрозумілі сьогодні питання створення баз даних, діяльності ЗМІ, попередження маніпуляцій суспільною свідомістю тощо. Самостійним аспектом проблеми має стати побудова оптимального правового режиму збереження накопичуваних людством даних та забезпечення доступу до цього ресурсу. Живі істоти, які сотні мільйонів років тому спостерігали формування вугільних пластів (або самі ставали їх часткою) навряд чи могли передбачити появу вугільної промисловості, металургії, теплоелектростанцій тощо. Сьогодні відбувається схожий процес. Людство накопичує величезні об'єми даних. Як вони будуть використовуватися через значний проміжок часу невідомо, однак очевидно що їх використання відбуватися буде. Якщо так, необхідно досліджувати можливості (доцільність) правового регулювання збері-

гання та використання даних, що накопичує людство. Потребуватиме розв'язання питання власності таких активів, переходу їх у статус виключної власності народу держави (планети) або даних, що можуть вільно використовуватися будь ким. Можливо є сенс режим великих масивів відпрацьованих даних організовувати на основі правових механізмів, що використовуються сьогодні для регуляції використання надр або археологічної діяльності.

В решті решт, регулювання інформаційного навколишнього середовища можна розглядати як встановлення координатної системи для майбутньої правової оцінки як штучного інтелекту так і технологічно вдосконалених людей, оскільки саме в цій сфері відбуватиметься переважна частина їх соціально значимої активності.

Колб О. Г., доктор юридичних наук, професор, професор кафедри кримінального права та процесу НУ «Львівська політехніка»
Дучимінська Л. М., начальник управління контрольно-перевірочної роботи головного управління Пенсійного фонду України у Волинській області

ПРО ДЕЯКІ ПРОЯВИ КІБЕРЗЛОЧИННОСТІ У МІСЦЯХ ПОЗБАВЛЕННЯ ВОЛІ

Як показали результати вивчення наукової літератури, поняття «кіберзлочинність» нерідко вживається з такими його аналогами, як «комп'ютерна злочинність», злочинність у сфері високих (інформаційних технологій», високотехнологічна злочинність» тощо [1, с. 294]. У совою чергу, на нормативно-правовому рівні, зокрема у чинному Кримінальному кодексі України, законодавець закріпив спеціальний розділ в Особливій частині – XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів) систем та комп'ютерних мереж і мереж електрозв'язку» [2].

Виходячи з того, що на сьогодні на доктринальному рівні досі тривають жваві дискусії з цих питань, можна у цьому контексті говорити про такий підвид кіберзлочинності в Україні, як «пенітенціарна кіберзлочинність».

Такий висновок ґрунтується на наступних міркуваннях:

1. Щорічно у засуджених, позбавлених волі, та ув'язнених під варту вилучається значна кількість мобільних телефонів, які ці особи використовують у злочинних цілях. Так, тільки у 2016 році в установах виконання покарань (УВП) було вилучено 3 тис. 817 мобільних телефонів, що на 247 штук більше, ніж у 2015 році [3, с. 19], а в слідчих ізоляторах (СІЗО) – 1 тис. 894 таких заборонених предметів (у 2015 р. – 2 тис. 109) [3, с. 20]. При цьому варто зазначити, що відповідно до вимог ч. 4 ст. 107 Кримінально-виконавчого кодексу (КВК) України та додатку 3 до Правил внутрішнього розпорядку установ виконання покарань (ПВР УВП), придбання та використання засудженими до позбавлення волі у ході відбування даного покарання мобільних телефонів заборонено [4].

Виявлені у цих осіб зазначені та інші заборонені предмети вилучаються, про що складається протокол. За клопотанням УВП слідчий суддя розглядає питання про їх конфіскацію та передачу на зберігання адміністрації відповідної установи згідно до положень розділу VIII Кримінального процесуального кодексу України (ч. 7 ст. 102 КВК),

Проведений аналіз свідчить про те, що у місцях позбавлення волі є умови, які сприяють вчиненню кіберзлочинів з боку засуджених, позбавлених волі, та ув'язнених під варту.

2. У структурі пенітенціарної злочинності майже 4% складають такі кримінальні правопорушення, як крадіжки (ст. 185 КК) та шахрайство (ст. 190 КК), які мають пряме відношення до незаконного використання засудженими до позбавлення волі мобільних телефонів. Так, у 2016 році із 298 зареєстрованих в УВП злочинів, вчинених цими особами, 5 припадало на шахрайство, а 2 – на крадіжку [3, с. 1].

Крім цього, все частіше засуджені використовують мобільні телефони при вчиненні завідомо неправдивого повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності (ст. 259 КК); злочинів у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів (р. XIII Особливої частини КК) (зокрема, щорічно у цих осіб вилучають більше 6 кг наркотичних засобів (у СІЗО – майже 2,5 кг [3, с. 18–20]0 , а також організації дій, що дезорганізують роботу УВП (ст. 292 КК).

Як з цього приводу слушно зауважив А. А. Музика, через надходження до засуджених заборонених предметів справляється негативний вплив на процес виконання та відбування покарання, що викликає його дезорганізацію [5, с. 5].

3. Незаконне використання мобільних телефонів у місцях позбавлення волі дає реальну можливість злочинним авторитетам як на свободі, так і в УВП та СІЗО підтримувати постійний взаємозв'язок поміж собою та впливати на стан правопорядку у сфері виконання покарань. Про це, зокрема, на офіційному рівні заявляє й Адміністрація Державної кримінально-виконавчої служби Міністерства юстиції України. так, у 2016 році засуджені негативної спрямованості (а, таких на профілактичних обліках УВП перебувало 3 тис. 304 засуджені [3, с. 16] фактично паралізували діяльність 15 УВП (Райківської № 73, Софіївської № 55, Кам'янської № 101 та інших виправних колоній) та одного СІЗО (м. Київ) [3, с. 12].

При цьому, у подальші роки (2017-2019) зазначені тенденції у місцях позбавлення волі не змінились, про що свідчать надзвичайні події у виправних колоніях Одеської, Черкаської, Миколаївської та інших областей, що були пов'язані з груповою непокорою засуджених та діями, що дезорганізують роботу УВП, які були організовані злочинними авторитетами з числа осіб, що перебували на свободі та відбували покарання у відповідних виправних колоніях.

Отже, в наявності складна прикладна проблема, що стосується змісту пенітенціарної кіберзлочинності в Україні, яка має стати предметом активних наукових розробок, а також більш ефективної взаємодії поміж собою оперативних підрозділів УВП і СІЗО та інших правоохоронних органів, які протидіють кіберзлочинності в нашій державі.

Список використаних джерел:

1. Кримінологія : підручник / В. В. Голіна, Б. М. Головін, М. Ю. Валуйська та ін.; за заг. ред. В. В. Голіни, Б. М. Головіна. Харків: Право, 2014. 440 с.
2. Кримінальний кодекс України : прийнятий законом України від 5 квітня 2001 року № 2341-III. Відомості Верховної Ради України. 2001. № 25–26. Ст. 131.
3. Про стан правопорядку, ізоляції та нагляду, діяльність підрозділів охорони, пожежної безпеки та воєнізованих формувань Державної кримінально-виконавчої служби України у 2016 році. Інформ. бюлет. Київ : Департамент ДКВС Міністерства юстиції України, 2017. 34 с.
4. Правила внутрішнього розпорядку установ виконання покарань : затв. наказом Міністерства юстиції України від 28 серпня 2018 року № 2823/5 Офіційний вісник України, 2018, № 70.
5. Музики А. А. Методичні рекомендації щодо запобігання проникненню заборонених предметів до установ виконання покарань і слідчих ізоляторів. Київ : ПАЛИВОДА А. В., 2016. 94 с.

Колодяжний М. Г., кандидат юридичних наук, старший науковий співробітник, завідувач відділу кримінологічних досліджень Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України, м. Харків, Україна

PREDICTIVE POLICING – ІННОВАЦІЯ У СФЕРІ ПРОГНОЗУВАННЯ І ПРОФІЛАКТИКИ ЗЛОЧИННОСТІ

Наразі процеси глобалізації, інтернаціоналізації, інформатизації, бурхливого розвитку технологій прямим чином позначаються на злочинності, її характері, структурі, способах і знаряддях учинення злочинів. Злочинний світ дуже швидко реагує на перелічені процеси. Це виражається у зміні трендів і тенденцій сучасної світової і регіональної злочинності. Зокрема, суцільний доступ громадян до Інтернету (з 7,7 млрд населення планети 4,5 млрд є користувачами глобальної мережі [1]), відбився на поширенні кіберзлочинності, різних формах шахрайства. Сучасні технології вміло використовують не лише економічні злочинці, терористи, наркоторговці, а й злодії, викрадачі автомобілів та інші категорії правопорушників.

З метою адекватного реагування світової спільноти, включаючи й Україну, на сучасні виклики кримінального світу, органи кримінальної юстиції зобов'язані упроваджувати у своїй діяльності продукти Smart технологій. Їх фахівці часто називають «розумними» технологіями, адже вони базуються на широкому використанні комп'ютерних систем, штучного інтелекту, обробці великого масиву даних, одержаних також за допомогою спеціального обладнання (супутників, камер відеоспостереження) тощо.

До Smart технології можна з упевненістю віднести Predictive Policing – PredPol (прогнозна поліцейська діяльність). Її можна назвати одним з останніх know how у сфері запобігання злочинності у розвинених країнах світу. У 2002 р. у прокат вийшов голлівудський кінофільм «Особлива думка». Сюжет кінострічки переносить глядача у далекий 2054 р., коли підрозділи поліції за допомогою людей-провідців запобігатимуть убивствам ще до моменту їх вчинення. PredPol наразі фактично є своєрідним аналогом фантастичних технологій майбутнього, описаних у фільмі, оскільки дозволяє прогнозувати і профілактувати різні злочини. Однак інструментом передбачення виступають не провідці, а сучасні технології:

штучний інтелект (спеціальне програмне забезпечення, розроблені алгоритми), комп'ютери та ін.

До характерних ознак PredPol можна віднести:

– мета – прогнозування і профілактика злочинності;

– об'єкт вивчення – час, місце вчинення злочинів, особа підозрюваного та його оточення, інші соціальні та економічні дані;

– суб'єкт здійснення – органи і підрозділи поліції, приватні компанії;

– засіб реалізації – комп'ютерне програмне забезпечення у виді штучного інтелекту;

– тісна взаємодія зі спеціалістами у сфері інформаційних технологій, програмістами, математиками;

– пов'язаність із картографуванням злочинності;

– ефективність у запобіганні злочинам, особливо у містах.

У широкому розумінні PredPol є засобом запобігання й прогнозування злочинності за допомогою аналізу та узагальнення даних, визначення складних статистичних закономірностей. У вузькому значенні з урахуванням виділених вище характерних ознак PredPol уявляє собою діяльність органів поліції та комерційних структур щодо обробки за допомогою сучасних технологій кримінологічно значущої інформації про місце, час вчинення злочину, особу злочинця тощо, спрямованої на виділення потенційних місць кримінальних посягань, прогнозування майбутньої незаконної діяльності з боку певних осіб, виділення груп осіб або окремих громадян з підвищеним степенем віктимності, а також посилення результативності профілактики злочинності на місцевому рівні.

Країною-піонером у розробці та практичному впровадженні прогнозної поліцейської діяльності вважаються США. Ще у 2009 р. департамент поліції Чикаго одержав від Національного інституту юстиції цієї країни грант розміром 2 млн дол. США на розробку системи, що дозволятиме запобігати злочинам ще до їх вчинення. Для цього було використано досвід фахівців Іллінойського технологічного інституту із застосування технології штучного інтелекту. Відповідна інформаційна система наповнюється даними про місця, де фіксується найбільша кількість учинених злочинів, та про осіб, які вже притягались до кримінальної відповідальності [2]. На підставі цієї важливої інформації створюються спеціальні карти злочинності, на яких виділені «гарячі» точки у виді ділянок міського простору, де має місце високий ступінь вірогідності вчинення того чи іншого кримінального правопорушення. Причому ці дані оновлюються з періодичністю у кілька годин.

Поліцією багатьох міст США враховується подібна оперативна інформація для формування щодня нових маршрутів патрулювання або посилення охорони громадського порядку у тих місцях, де патрулювання вже здійснюється. Цим і досягається висока ефективність застосування прогнозної поліцейської діяльності [3, с. 152, 153]. Упровадження PredPol в окремих країнах вплинуло й на зміну критеріїв оцінки діяльності поліції. На теперішній час пріоритетом є не кількість арештів, а показник реального скорочення рівня різних злочинів.

Згодом у США була створена приватна компанія з однойменною назвою «PredPol», яка тісно співпрацює з поліцією Лос-Анджелеса. Основу визначення потенційних місць учинення різних злочинів складає алгоритм, що застосовується для передбачення землетрусів. Згідно із результатами експерименту, здійсненого вченими Каліфорнійського університету, результативність PredPol є мінімум у два рази більшою за традиційні підходи, що застосовуються поліцейськими у їх буденній професійній діяльності. Зокрема, розкриття злочинів після застосування вказаної технології підвищується від 10% до 50% [4]. Щодо окремих злочинів, то застосування прогнозної поліцейської діяльності дозволяє скорочувати рівень грабежів до 50%, а крадіжок, поєднаних із проникненням у житло, – до 70% [5].

Подібні Smart технології у сфері прогнозування злочинності існують також у деяких європейських країнах, таких як Велика Британія, ФРН та ін. Останнім часом поліція Японії зацікавилась технологією штучного інтелекту щодо обробки великого масиву даних, які можна використати для прогнозування злочинності. Цю технологію планується впровадити в Японії на експериментальній основі до 2020 р. [6].

Безперечно, що у технології PredPol є певні недоліки. Вони полягають у можливості порушення прав тих осіб, які визначені штучним інтелектом в якості потенційного правопорушника. Очевидно, що цим порушується конституційний принцип презумпції невинуватості. У США є прецеденти, коли до громадян навідуються поліцейські, які висловлюють своє припущення про можливість учинення першими злочину на підставі наявності певних даних (проживання у неблагополучному житловому кварталі, спілкування з друзями із кримінальним минулим, відсутність постійного місця роботи, наявність непогашеного кредиту тощо). Деякі з таких громадян вимушені захищати свої права, звертаючись до послуг юристів.

Суцільна і непереборна інформатизація й діджиталізація усіх сфер сучасного суспільства, включаючи правоохоронну, викликають необхідність у предметному дослідженні Smart технологій в Україні. Це особли-

во стосується Predictive Policing, яка дозволяє вміло використовувати дані для прогнозування злочинності та її профілактики.

Поштовхом до поступового впровадження прогнозної поліцейської діяльності у нашій державі має стати організація роботи Управління кримінального аналізу Національної поліції України. На цей підрозділ має покладатись функція узагальнення й обробки кількісних та якісних показників злочинності не лише у масштабах країни, а за окремими містами, районами й житловими кварталами. Лише зосередження уваги поліції на запобіганні злочинності на місцевому рівні здатне забезпечити належний рівень громадської безпеки і публічного порядку, захистити права громадян й зменшити їх страх перед злочинністю.

Список використаних джерел:

1. Internet World Stats. URL: https://www.internetworldstats.com/stats.htm (дата звернення: 1.09.2019).
2. Mann A. How Science Is Helping Stop Crime Before It Occurs. URL: www.nbcnews.com/mach/science/how-science-helping-stop-crime-it-occurs-ncna805176 (дата звернення: 1.09.2019).
3. Колодяжний М. Г. Стратегія зменшення можливостей учинення злочинів: зарубіжні реалії, перспективи запровадження в Україні: монографія. Харків: Право, 2018. 228 с.
4. Smith M. Can we predict when and where a crime will take place? URL: https://www.bbc.com/news/business-46017239 (дата звернення: 2.09.2019).
5. Predpol. URL: https://www.predpol.com (дата звернення: 2.09.2019).
6. Jouvenal J. Police are using software to predict crime. Is it a 'holy grail' or biased against minorities? *The Washington Post*. 2016. November 17. URL: https://www.washingtonpost.com/local/public-safety/police-are-using-software-to-predict-crime-is-it-a-holy-grail-or-biased-against-minorities/2016/11/17/525a6649-0472-440a-aae1-b283aa8e5de8_story.html?noredirect=on&utm_term=.652f0e5bd00d (дата звернення: 2.09.2019).

Лариса Компанцева, Національна академія СБ України, м. Київ

ЛІНГВІСТИЧНА ЕКСПЕРТИЗА СОЦІАЛЬНИХ МЕРЕЖ ЯК ІНСТРУМЕНТ ІДЕНТИФІКАЦІЇ ГІБРИДНИХ ЗАГРОЗ

Сучасна лінгвістика все більше набуває статусу *метапарадигмальної* науки, мета якої – створення всеохоплюючої, уніфікуючої доктрини, що

здатна замінити конфронтацію наукових напрямів їхнім синтезом. Такий синтез зумовлює вирішення суто практичних завдань, зокрема у сфері лінгвістичної експертизи соціальних мереж.

Дискурс соціальних мереж стає все більш технологізованим за умови гібридної війни та встановлення соціального контролю. *Технологічний дискурс* – механізм, який дозволяє отримувати економічні, соціально-політичні, воєнні та інші переваги безпосередньо від власне дискурсу без додаткових фінансових ресурсів, перемагати суб'єктів, які не використовують такий дискурс.

Технологізація дискурсу здійснюється за допомогою різноманітного інструментарію: прийомів НЛП, лінгвокогнітивних механізмів інспірації, позиціювання, залучення до комункації, фреймування ситуацій, створення «кола своїх», амальгамування, дрейфування понять тощо. Впливовість цих технологій посилюється комунікативними можливостями кіберпростору, який, за моделлю Д. Кларка [2], має чотири рівні організації.

1. *Фізичний:* апаратні пристрої, які включають маршрутизатори, перемикачі, носії, супутники, датчики та інші технічні з'єднувачі, як дротові, так і бездротові. Фізична інфраструктура географічно розташована у «реальному просторі», і, таким чином, є предметом різних національних юрисдикцій.

2. Логічний: код, який містить як програмне забезпечення.

3. Контентний: вся інформація (знання, що стосуються об'єктів, наприклад, факти, події, процеси або ідеї), що зберігається та обробляється в кіберпросторі.

4. Соціальний: фактичний інтернет людей і потенційних відносин. Соціальний шар включає уряди, приватний сектор, громадянське суспільство і суб'єкти технічного співтовариства. Якщо в «реальному» житті люди можуть бути ідентифіковані за їх унікальним кодами ДНК, атрибуція в мережі набагато складніше. Люди в кіберпросторі мають більше можливостей для створення множинної ідентичності. Це має не тільки важливе значення з точки зору захисту безпеки або авторських прав, але й ставить питання про те, як кіберсвіт позиціонується реальному світі.

Лінгвістична експертиза враховує третій та четвертий рівні організації кіберпростору. *Лінгвістична експертиза соціальних мереж* розуміється у широкому значенні як мовознавчий аналіз дискурсів соціальних мереж із застосування тріангуляційного підходу, результати якого можуть бути оформлені у вигляді консультативного висновку або прогнозу щодо впливу віртуальної комунікації на соціально-політичні дії в реальному світі. Результати лінгвістичної експертизи соціальних мереж, в першу чергу,

відносяться до лінгвокультурної сфери, але за необхідністю можуть бути використані як в юридичній, так і в комерційній сферах.

Лінгвістична експертиза соціальних мереж – новітній напрям лінгвістичної експертизи, оскільки сьогодні визнано лише такі функціональні типи лінгвістичної експертизи:

1) *юридичну*, зокрема а) правову (експертиза законодавчих документів) та б) судову (експертиза текстів, що фігурують як доказова база під час судових процесів);

2) *лінгвокультурну*, що включає: а) власне лінгвокультурну експертизу (аналіз текстів як феноменів культури: визначення авторства, часу написання тощо), б) лінгвосоціальну (аналіз характеру впливу текстів на суспільні цінності);

3) *лінгвокомерційну* (аналіз ефективності рекламних текстів, товарних інструкцій тощо).

Законодавче закріплення мети, завдань та призначення отримала лише судова лінгвістична експертиз (Інструкція про призначення та проведення судових експертиз та експертних досліджень, редакція № 1350/5 від 27.07.2015 р.).

Гібридні війни, посилення міжкультурних комунікацій, формування єдиного геополітичного простору, формування системи стратегічних комунікацій, зокрема деструктивних, збільшили кількість ситуацій, у яких лінгвіст може виступати експертом. Існує низка питань, для вирішення яких можна застосовувати лінгвістичну експертизу. Більшість із них пов'язана з використанням мовознавчих методів для підготовки доказової бази, на яку спираються під час розгляду справ у суді:

1. Чи міститься у дискурсі певної соціальної мережі наклеп – навмисне поширення явно недостовірних відомостей, що ганьблять честь і гідність іншої особи? Чи поширюється цей наклеп по інших соціальних мережах?

2. Чи розпалюється у соціальній мережі національна, релігійна ворожнеча? Чи можна визначити персонажів, що розпалюють ворожнечу? Який їхній психолінгвістичний та соціолінгвістичний портрет?

3. Як впливає дискурс соціальних мереж на політичні та соціальні перетворення?

4. Чи існують протестні настрої в соціальних мережах? Які персонажі їх продукують?

5. Чи мобілізуються спільноти соціальних мереж для дій в реальності? Який рівень інтернет-активності?

6. Під час виборчих кампаній чи ведеться в соціальних мережах агітація? Чи обіцяються певне грошове винагородження або інші матеріальні блага за результатами голосування?

7. Чи міститься в соціальних мережах інформація, мета якої – розпалювання національної ворожнечі, приниження національної гідності, а також інші ознаки екстремістської діяльності?

8. Чи міститься в дискурсах завуальована інформація щодо пропозиції хабара, незаконного обігу наркотиків, зброї тощо, чи передається інформація конспіративно? Чи є спроби завуалювати дійсний зміст висловлювання?

9. Чи використовуються сугестивні засоби для маніпулювання думкою відвідувачів? Як здійснюється медіавірусний вплив?

10. Чи об'єднуються мережі за певною спрямованістю в єдиний ланцюг?

11. Які засоби залучення нових відвідувачів до мережі використовуються?

12. Чи є серед відвідувачів мережі тролі? Який напрям і мета тролінгу?

Не зважаючи на нещодавнє виникнення, категоріальний апарат лінгвістичної експертизи соціальних мереж є сформованим, а принципи проведення визначеними, зокрема:

1. Принцип лінгвістичної визначеності. Аналізуючи дискурс/текст, який має юридичні наслідки, експерт виходить з принципової можливості встановити лінгвістичними методами несуперечливі змістові й граматичні зв'язки в межах такого дискурсу/тексту та з'ясувати значення окремих слів і висловів із застосуванням формалізованих процедур лінгвістичного аналізу. Цей принцип корелює з принципом юридичної визначеності (англ. *legal certainty*), який вимагає передбачуваності законодавства та однаковості трактування й застосування юридичної норми.

2. Принцип встановлення комунікативної норми. Комунікативна норма встановлюється на підставі наявних дискурсивних практик певного жанру, вона є константою, що задає інваріантне значення, у зіставленні з яким виявляються комунікативно вагомі смислові нашарування тексту.

3. Принцип аргументацій. Лінгвістична аргументація має бути переконливою і підтверджуватися кількома методиками лінгвістичного аналізу, що забезпечує вірогідність висновків.

4. Принцип цілісності. Дискурс соціальних мереж переважно є креолізованим. Його експертизу слід здійснювати як цілісної єдності із врахуванням розширеного контенту.

5. Принцип реконструкції. Комунікація в соціальних мережах передбачає циркулювання вторинних текстів – текстів, створених на основні інших (первинних), а саме: перекладів висловлювань певних осіб, отриманих із різних інтернет-джерел; фотографій, що позиціонуються як

аутентичні, але є запозиченими з інших медіаджерел; перепостів; гіперпосилань тощо. Експерт перш за все має вирішити два питання: а) чи є вторинний текст трансформованим задля здійснення певного впливу на відвідувачів соціальної мережі; б) що є першоджерелом вторинного тексту; в якому контексті він був застосований.

6. Принцип експертної презумпції. Цей принцип є актуальним для експертизи щодо комунікацій екстремістської спрямованості. Оскільки саме ця група є найбільш представленою дискурсами/текстами різних жанрів, сферами функціонування, використанням різних типів знакових систем тощо. Для здійснення вірогідної експертизи необхідно залучення фахівців інших галузей, наприклад, релігієзнавців або фахівців по знаках та символах. Це сприятиме уникненню двозначності трактування.

Отже, наступним кроком становлення лінгвістичної експертизи соціальних мереж вбачається нормативне врегулювання її статусу та створення пулу професійних експертів.

Список використаних джерел:

1. Компанцева Л. Ф. Лінгвістична експертиза соціальних мереж : [підручник] / Л. Ф. Компанцева. – К. : АграрМедіаГруп, 2018. – 318 с.
2. Clark D. Characterizing Cyberspace: Past, Present and Future / D. Clark [Електронний ресурс]. – Режим доступу : ecir.mit.edu/.../112-characterizing-cyberspace-past-present-a.

Копотун І. М., проректор з міжнародних зв'язків Академії ГУСПОЛ (Чеська Республіка), доктор юридичних наук, професор, заслужений юрист України

Довбань І. М., кандидат юридичних наук

ВИДИ КІБЕРЗЛОЧИНІВ ВІДПОВІДНО ДО МІЖНАРОДНИХ НОРМАТИВНИХ АКТІВ

Об'єктом кіберзлочинів відповідно до Конвенції є широкий спектр охоронюваних нормами права суспільних відносин, що виникають при провадженні інформаційних процесів із приводу виробництва, збору, об-

робки, накопичення, зберігання, пошуку, передачі, поширення та споживання комп'ютерної інформації, а також в інших сферах, де використовуються комп'ютери, комп'ютерні системи та мережі. Серед них, ураховуючи підвищену суспільну значущість, виділяються правовідносини, що виникають у сфері забезпечення конфіденційності, цілісності та доступності комп'ютерних даних і систем, законного використання комп'ютерів і комп'ютерної інформації (даних), авторського та суміжних прав.

Об'єктивна сторона кіберзлочинів характеризується виділенням чотирьох груп суспільно небезпечних діянь.

Конвенція поділяє злочини в кіберпросторі на чотири групи.

У першу групу злочинів, спрямованих *проти конфіденційності, цілісності та доступності комп'ютерних даних і систем*, входять:

− протизаконний доступ − отримання доступу до комп'ютерної системи загалом або її частини без права на це, який може розглядатися як злочин, якщо вчинено в обхід заходів безпеки і з наміром заволодіти комп'ютерними даними або іншим безчесним наміром, або щодо комп'ютерної системи, поєднаної з іншою комп'ютерною системою (ст. 2);

− протизаконне перехоплення даних, здійснене з використанням технічних засобів перехоплення без права на це непублічних передач комп'ютерних даних у комп'ютерну систему, з неї або всередині такої системи, у тому числі електромагнітні випромінювання комп'ютерної системи, що несе такі комп'ютерні дані, якщо він зроблений в обхід заходів безпеки і з наміром заволодіти комп'ютерними даними або іншим безчесним наміром, або щодо комп'ютерної системи, поєднаної з іншою комп'ютерною системою (ст. 3);

− порушення цілісності даних − ушкодження, стирання, псування, зміну або блокування комп'ютерних даних без права на це, у тому числі виключно у випадках, які спричинили серйозні наслідки (ст. 4);

− втручання у функціонування системи – створення без права на це серйозних перешкод функціонуванню комп'ютерної системи через уведення, передачу, пошкодження, знищення, псування, зміну або приховування комп'ютерних даних (ст. 5);

− протиправне використання пристроїв − (а) виробництво, продаж, придбання для використання, імпорт, оптова продаж або інші форми надання в користування: (1) пристроїв, у т. ч. комп'ютерних програм, розроблених або адаптованих, насамперед для цілей вчинення злочинів, (2) комп'ютерних паролів, кодів доступу або інших подібних даних, за допомогою яких може бути отримано доступ до комп'ютерної системи

загалом або її частини, з наміром використовувати їх для вчинення злочинів, та (3) володіння одним із предметів, що згадуються вище, з наміром використовувати його для вчинення злочинів (ст. 6).

Об'єктом злочину виступають не тільки комп'ютерні програми, розроблені або адаптовані для вчинення злочинів, передбачених у статтях 2–5 Конвенції, а й комп'ютерні паролі, коди доступу та їх аналоги, за допомогою яких може бути отримано доступ до комп'ютерної системи загалом або її частини (з урахуванням злочинного наміру). Норми ст. 6 Конвенції застосовуються лише в тому разі, якщо використання (поширення) спеціальних технічних пристроїв спрямоване на вчинення протиправних діянь.

У другу групу входять *злочини, пов'язані з використанням комп'ютерних засобів*: фальсифікація та шахрайство з використанням комп'ютерних технологій (статті 7, 8 Конвенції):

– підроблення з використанням комп'ютерів – уведення, зміну, знищення або блокування комп'ютерних даних, що призводять до порушення автентичності даних із наміром, щоб вони розглядалися або використовувалися в юридичних цілях, як ніби вони залишаються справжніми, незалежно від того, чи є ці дані безпосередньо читабельні і зрозумілі (ст. 7);

– шахрайство з використанням комп'ютерів – позбавлення іншої особи його власності через уведення, зміну, стирання або приховування комп'ютерних даних або втручання у функціонування комп'ютера або системи задля неправомірного отримання економічної вигоди для себе чи для іншої особи (ст. 8).

Третю групу складають *злочини, пов'язані з контентом (змістом) даних*.

Правопорушення, пов'язані з дитячою порнографією (порнографічними матеріалами, візуально відображають участь неповнолітнього чи удаваної повнолітньої особи в сексуально відвертих діях, а також реалістичні зображення, що представляють неповнолітніх у сексуально відвертих діях), а саме: виробництво задля поширення через комп'ютерні системи; пропозиція або надання через комп'ютерні системи; поширення або передача через комп'ютерні системи; придбання через комп'ютерну систему для себе чи іншої особи; володіння дитячою порнографією, що міститься в комп'ютерній системі або в середовищі для збереження комп'ютерних даних.

У четверту групу ввійшли *порушення авторського права і суміжних прав*:

– порушення авторського права, передбаченого нормами внутрішньодержавного законодавства з урахуванням вимог Паризького акта від 24 липня 1971 р. до Бернської конвенції про захист творів літератури та мистецтва, Угоди про пов'язані з торгівлею аспекти прав на інтелектуальну власність і Договору про авторське право Всесвітньої організації інтелектуальної власності (ВОІВ), за винятком будь-яких моральних прав, що надаються цими Конвенціями, коли такі дії навмисно відбуваються в комерційному масштабі й за допомогою комп'ютерної системи;

– порушення прав, пов'язаних з авторським правом (суміжними правами), передбачених нормами внутрішньодержавного законодавства, з урахуванням вимог Міжнародної конвенції про захист прав виконавців, виробників звукозаписів та радіомовних організацій (Римська конвенція), Угоди про пов'язані з торгівлею аспекти прав інтелектуальної власності та Договору ВОІВ про виконавців і звукозаписи, за винятком будь-яких моральних прав, які надаються цими Конвенціями, коли такі дії вчинені умисно в комерційному масштабі та за допомогою комп'ютерної системи.

Шкідливими наслідками перерахованих діянь Конвенцією визнається порушення прав законних користувачів комп'ютерної інформації, комп'ютерів, їх систем чи мереж. Установлення як обов'язкової ознаки більш тяжких наслідків (матеріального збитку, протиправного використання отриманої комп'ютерної інформації тощо) Конвенцією залишено на розсуд держав. Загалом норми Конвенції не передбачають обов'язковості настання шкідливих наслідків.

Суб'єктом кіберзлочинів може бути фізична особа, яка вчинила означені вище дії.

Виходячи з усталеної в різних країнах практики, ст. 12 Конвенції вимагає встановлення відповідальності юридичних осіб за правопорушення, передбачені нею. Умовами настання відповідальності юридичної особи є: (1) вчинення дії (2) задля отримання вигоди на користь юридичної особи (3) його посадовою особою, яка займає керівну посаду, (4) з використанням його повноважень за поданням юридичної особи, прийняття рішень або здійснення контролю за його діяльністю. Крім того, конвенція наказує встановлювати відповідальність юридичних осіб також у разі вчинення протиправних дій іншим працівником, який перебуває під керівництвом посадової особи, яка займає керівний пост, задля отримання вигоди на користь юридичної особи.

Суб'єктивна сторона. У всіх злочинах, згаданих у Конвенції, відповідальність настає тільки в разі вчинення їх умисно. У деяких статтях, із

посиланням на «традиційні» злочини, вчинені з використанням комп'ютера або комп'ютерної інформації, передбачено, що умисна форма вини має характеризувати не тільки саме діяння, а й протиправне їх використання, хоча це і є кваліфікуючою ознакою таких злочинів (наприклад, ст. 8 – шахрайство з використанням комп'ютера).

Поряд із закінченими злочинами Конвенцією передбачається необхідність установлення відповідальності за замах, співучасть чи підбурювання до його вчинення (ст. 11).

Згідно з ч. 1 ст. 13 Конвенції встановлення конкретних санкцій за вчинення зазначених діянь віднесено до відання держав. На їх розсуд може встановлюватися кримінальна відповідальність для фізичних осіб, а також кримінальна, цивільно-правова або адміністративна відповідальність юридичних осіб. Передбачені внутрішньодержавним законодавством санкції повинні бути ефективні, пропорційні та переконливі.

Згідно з Додатковим протоколом до Конвенції про кіберзлочинність, який стосується криміналізації *дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи* до кіберзлочинів слід додати п'яту групу діянь:

− поширення або в інший спосіб надання громадськості доступу через комп'ютерні системи до расистського та ксенофобного матеріалу;

− погроза, зроблена через комп'ютерну систему, вчинення тяжкого злочину, визначеного в національному законодавстві, проти (I) осіб через їх належність до групи, яка відрізняється за ознаками раси, кольору шкіри, національним або етнічним походженням, а також віросповіданням, якщо вони використовуються як привід для будь-якої з цих дій; або (II) групи осіб, котра відрізняється за будь-якою з цих характеристик;

− публічна образа через комп'ютерну систему (I) осіб з причини їх належності до групи, яка відрізняється за ознаками раси, кольору шкіри, національним або етнічним походженням, а також віросповіданням, якщо вони використовуються як привід для будь-якої з цих дій; або (II) групи осіб, яка відрізняється за будь-якою з цих характеристик;

− поширення або в інший спосіб надання громадськості доступу через комп'ютерні системи до матеріалу, який заперечує, значно мінімізує, схвалює або виправдовує дії, які є геноцидом або злочинами проти людства, як це визначено в міжнародному праві та як це визнано заключними та обов'язковими рішеннями Міжнародного військового трибуналу, заснованого згідно з Лондонською угодою від 8 серпня

1945 року, або будь-якого іншого міжнародного суду, заснованого відповідними міжнародними документами, юрисдикція якого визнана Стороною угоди (вчинені з наміром підбурити до ненависті, дискримінації чи насильства проти будь-якої особи чи групи осіб на підставі ознак раси, кольору шкіри, національного чи етнічного походження, а також віросповідання, якщо вони використовуються як привід для будь-якої з цих дій).

Список використаних джерел:

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31.05.2005 р. №2594-IV. Відомості Верховної Ради. 2005. №26. Ст. 347.
2. Закон України «Про інформацію» від 02.10.1992 р. №2657-XII. Відомості Верховної Ради України. 1992. №48. Ст. 650.
3. Копотун І. М., Боровик А. В. Кримінально-правова характеристика кіберзлочинів в Україні: академ. курс. Київ: ФОП Кандиба, 2018. 164 с.
4. Копотун І. М. Актуальність викликів та потенціальних загроз, спричинених міжнародним тероризмом//Актуальні проблеми кримінального права, процесу, криміналістики та оперативно-розшукової діяльності: матеріали 2-ї Всеукр. наук.-практ. конф. (Хмельницьк, 2 берез. 2018 р.)/ Нац. акад. держ. прикорд. служби України ім. Богдана Хмельницького. Харків: Нац. акад. держ. прик. служби, 2018. С. 57−61.

Кудінов С. С., доктор юридичних наук, доцент, генерал-майор

ЩОДО УДОСКОНАЛЕННЯ ПРАВОВОЇ ПОЛІТИКИ ФОРМУВАННЯ АНТИТЕРОРИСТИЧНОЇ КОМПЕТЕНТНОСТІ В УКРАЇНІ

Проблема тероризму вже багато років не втрачає своєї актуальності як для правової теорії, так і для практики державного управління. Але таких загрозливих масштабів вона набула лише в наш час. Нині, тероризм належить до числа найбільш небезпечних і важкопрогнозованих явищ сучасності, що посідає одне із чільних місць серед тих проблем, які турбують людство. У результаті теоретико-емпіричного аналізу сучасних наукових розвідок встановлено, що в умовах сьогодення протидія теро-

ризму на державному рівні зосереджена, в основному, на застосуванні правових норм і силовому вирішенні даної проблеми, що не завжди призводить до бажаних результатів. Недосконалість профілактики тероризму, антитерористичного захисту, ефективного використання можливостей суспільства із самозбереження та самозахисту вказує на певну кризу стратегій боротьби із тероризмом.

На сучасному етапі розвитку нашої держави із надзвичайною гостротою постало питання визначення шляхів оптимізації правової політики в аспекті формування антитерористичної компетентності не тільки уповноважених суб'єктів, які безпосередньо здійснюють боротьбу з тероризмом, а й усього особового складу сил охорони правопорядку та цивільного населення. Зазначена проблематика має бути одним із найважливіших державних пріоритетів і вимагає посиленої уваги представників владних структур, фахівців сектору безпеки, науковців та широких кіл громадськості.

Правова політика з формування антитерористичної компетентності становить нормативно закріплений порядок дій органів державної влади з метою впливу на сферу освіти для забезпечення її розвитку за напрямом запровадження системи антитерористичної підготовки, зорієнтованої на формування антитерористичної компетентності фахівців безпекової сфери, працівників державних органів, установ, підприємств і організацій та інших верств населення України. Концептуальні засади цієї політики представляють собою засновану на загальній теоретико-методологічній базі систему науково обґрунтованих і практично перевірених узагальнених положень, що нормативно розкривають зміст, структуру й взаємозв'язки основних компонентів правової політики держави.

Державне регулювання щодо формування антитерористичної компетентності здійснюється через систему заходів, спрямованих на реалізацію правової політики, а саме:

– нормативне регулювання (зміни до законодавства, прийняття нових нормативно-правових актів, необхідних для оптимізації державної політики у сфері антитерористичної безпеки);

– державне управління (система заходів та дій, зорієнтованих на розвиток антитерористичної безпеки);

– контроль (за діями суб'єктів, які здійснюють заходи з формування антитерористичної компетентності; реалізується з метою виявлення проблемних аспектів для подальшого корегування та запобігання їх виникненню у майбутньому);

– прогнозування (перспективна оцінка та визначення можливої динаміки щодо інтенсивності та структури терористичних загроз);

– планування (використовується для досягнення певних прогнозованих результатів щодо сформованості антитерористичної компетентності (не тільки в уповноважених суб'єктів, які безпосередньо здійснюють боротьбу з тероризмом, а й усього населення)).

Важливою функцією сучасної держави є державне управління у сфері формування антитерористичної компетентності, яке охоплює комплекс заходів та напрямів діяльності органів виконавчої влади та місцевого самоврядування з вироблення і здійснення організуючих, регулюючих і координуючих впливів на процеси суспільної діяльності з метою задоволення потреб суспільства щодо забезпечення безпеки життєдіяльності населення. Тому дедалі більшого значення набуває підвищення його ефективності, що потребує вдосконалення чинного законодавства, розподілу функцій управління, уточнення структури і завдань, повноважень і відповідальності посадових осіб усіх рівнів.

Обов'язковою складовою державного управління є контроль. На сьогодні суб'єктами державного контролю у сфері боротьби з тероризмом виступають Верховна Рада України, Президент України, Кабінет Міністрів України, які здійснюють контрольну діяльність в системі державного управління. Зазначені вище суб'єкти утворюють контрольні органи, сукупність яких складає інфраструктуру контролю у сфері боротьби з тероризмом. Суб'єктам державного контролю у сфері боротьби з тероризмом притаманне коло повноважень, провідне значення серед яких посідає формування норм контролю.

Подальший розвиток державної політики у контексті цілепокладання проблем формування антитерористичної компетентності зводиться до наступних цілей:

– стратегічних – розробка та запровадження дієвої системи антитерористичної безпеки через: створення умов для розвитку освіти за напрямом запровадження системи антитерористичної підготовки; диференціація освітніх технологій для формування антитерористичної компетентності фахівців безпекової сфери, працівників державних органів, установ, підприємств і організацій та інших верств населення України; всебічне забезпечення антитерористичної безпеки населення (фізичне, психологічне, інформаційне тощо);

– тактичних – запровадження системи формування антитерористичної компетентності не тільки уповноважених суб'єктів, які безпосередньо здійснюють боротьбу з тероризмом, а й усього населення; формування та впровадження інноваційних освітніх механізмів розвитку антитерористичної безпеки.

Загалом, антитерористична компетентність представляє собою інтегративну здатність людини успішно діяти в умовах небезпеки, пов'язаної з актами тероризму. Основними її структурними компонентами є:

– інтелектуально-прогностичний – володіння необхідними знаннями, що стосуються: особливостей зародження, виникнення та проявів тероризму; їх дії на психіку та поведінкові реакції людей, на державні та суспільні процеси; шляхів протидії терористичним загрозам та відповідної системи захисту цивільного населення; здатності до розробки прогностичних комплексних програм із запобігання і нейтралізації викликів тероризму та інноваційних концепцій протидії тероризму;

– мотиваційно-технологічний – здатність визначати мотиви терористів щодо особливостей подальших дій та намірів; вміння актуалізувати власні мотиви до швидких і конструктивних дій із запобігання терористичним загрозам; засвоєння алгоритмів чіткої протидії їм, конструктивних дій в умовах перебування в епіцентрі терористичного акту, нейтралізація терористичної небезпеки та її розповсюдження; навички застосування при цьому адекватних методів, прийомів та інструментарію, що забезпечить розгортання широкомасштабної системи антитерористичного функціонування суспільства;

– поведінково-діяльнісний – наявна сформованість соціально-обумовлених стилів адекватної поведінки та успішної взаємодії з оточенням, різними соціальними групами в умовах впливу стресогенних чинників; наявність комплексу емоційно-вольових, комунікативних, інтелектуальних та організаційно-ділових якостей, що сприятимуть досягненню оптимальних цілей в екстремальних умовах та збереженню, при цьому, фізичного і психічного здоров'я.

Вважаємо, що правова політика з формування антитерористичної компетентності має ґрунтуватися на таких принципах:

– безпечного існування – підготовка осіб до конструктивних дій в екстремальних умовах та формування системи освіти, зорієнтованої на набуття антитерористичних компетенцій протягом життя;

– доступності – можливість отримання необхідної інформації щодо реалізації антитерористичної поведінки та здобуття необхідної компетентності;

– системності – поетапне здобуття освіти та формування антитерористичних компетенцій, залежно від віку особи;

– цілеспрямованості – формування антитерористичних компетенцій, залежно від професійного статусу особи.

Таким чином, сьогодні очевидно, що в попередні періоди на політичному рівні недостатньо уваги приділялося питанням формування системи антитерористичної безпеки в Україні. Водночас саме державна політика покликана відігравати важливу роль у суспільному житті, оскільки вона має на меті своєчасно виявляти соціальні проблеми, аналізувати їх, визначати причини виникнення та знаходити шляхи розв'язання. Процеси переформатування й оновлення суспільства в аспекті протидії тероризму мають бути підкріплені принциповими змінами й у сфері освіти, адже населення, яке володітиме життєвими орієнтирами розпізнання та несприйняття тероризму, антитерористичними технологіями, згодом сформує в соціумі дієву систему протидії загрозам терористичного характеру. Тож, державна політика України повинна відповідати вимогам сьогодення з урахуванням загальнолюдських цінностей, світових освітніх тенденцій та економічних можливостей держави. Наразі саме освіта розглядається як визначальний фактор у питаннях формування і розвитку антитерористичної компетентності особи, наступного її саморозвитку і самовдосконалення. Формування такої компетентності у процесі здобуття освіти належить до найважливіших напрямів державної політики України.

Основними складовими правової політики з формування в сучасному соціумі антитерористичної компетентності повинні бути: державне регулювання у сфері формування антитерористичної безпеки; стратегічні та тактичні цілі; структурні компоненти антитерористичної компетентності; етапи формування антитерористичної компетентності; суспільні детермінанти формування антитерористичної компетентності. Використання на практиці комплексу запропонованих складових має забезпечити цілеспрямованість, узгодженість, послідовність та науково обґрунтоване змістове наповнення діяльності уповноважених суб'єктів щодо формування у суспільстві антитерористичної компетентності, що у підсумку сприятиме досягненню належного стану антитерористичної безпеки.

Кудінов С. С., доктор юридичних наук, доцент, ректор Національної академії СБ України, м. Київ, Україна
Марущак А. І., доктор юридичних наук, професор, директор ННІ перепідготовки та підвищення кваліфікації кадрів СБУ Національної академії СБ України, м. Київ, Україна
Петров С. Г., кандидат юридичних наук, заступник начальника Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБ України, м. Київ, Україна

АКТУАЛЬНІ КІБЕРЗАГРОЗИ НАЦІОНАЛЬНИМ ІНТЕРЕСАМ УКРАЇНИ: ПРОТИДІЯ І МІЖНАРОДНЕ СПІВРОБІТНИЦТВО

Аналіз законодавства про національну безпеку дає підстави стверджувати, що загрози кібербезпеці України і пріоритети національних інтересів України у сфері кібербезпеки визначає Стратегія кібербезпеки України (далі – Стратегія) як документ довгострокового планування. Національні інтереси України – це життєво важливі інтереси людини, суспільства і держави, реалізація яких забезпечує державний суверенітет України, її прогресивний демократичний розвиток, а також безпечні умови життєдіяльності і добробут її громадян [1, ст.ст. 1, 3, 31].

Стратегія кібербезпеки України, затверджена Указом Президента України від 15.03.2016 № 96/2016, визначає, що «переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці», і закріплює перелік таких загроз у розділі 2 Стратегії «Загрози кібербезпеці». Виокремлюється уразливість до кіберзагроз єдиної автоматизованої системи управління Збройних Сил України, економічної, науково-технічної, інформаційної сфери та інших сфер для розвідувально-підривної діяльності іноземних, насамперед російських, спецслужб у кіберпросторі, можливість порушення штатних режимів роботи автоматизованих систем керування технологічними процесами на об'єктах критичної інфраструктури, поширення політично вмотивованих атак на урядові та приватні веб-сайти тощо [2].

Закон України «Про основні засади забезпечення кібербезпеки України» (далі – Закон про кібербезпеку) передбачає, що функціонування національної системи кібербезпеки забезпечується, зокрема, шляхом впровадження єдиної (універсальної) системи індикаторів кіберзагроз з урахуванням міжнародних стандартів з питань кібербезпеки та кіберзахисту [3, ст. 8]. Результати даного дослідження можуть бути враховані при впровадження єдиної (універсальної) системи індикаторів кіберзагроз, яка на жаль, поки не створена.

Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури (далі – Загальні вимоги), затверджені 19 червня 2019 р., вперше на загальнодержавному рівні (не враховуючи Постанову Правління Національного банку України від 28.09.2017 №95 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України») визначають організаційно-методологічні, технічні та технологічні умови кіберзахисту об'єктів критичної інфраструктури, що є обов'язковими до виконання підприємствами, установами та організаціями, які відповідно до законодавства віднесені до об'єктів критичної інфраструктури [4].

Проблема залишається в тому, що задекларований ще у серпні 2018 року процес створення Національного переліку об'єктів критичної інфраструктури, а також визначення основ категоризації і паспортизації зазначених об'єктів [5], ще не завершився. Однією із причин об'єктивно є відсутність закону про критичну інфраструктуру.

Разом з тим, на сьогодні, найбільш актуальними кіберзагрозами національним інтересам держави є:

- кібератаки РФ проти України, зокрема і з метою поширення дезінформації;
- кіберзлочинність;
- недосконалість організаційно-правового і технологічного захисту державних електронних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури;
- низький рівень кібергігієни і медіаграмотності державних службовців і населення загалом.

Протидію актуальним кіберзагрозам національним інтересам України можна проаналізувати з використанням методики Global Cybersecurity Index [6], яка використовується Міжнародним союзом електрозв'язку при ООН, і включає п'ять критеріїв: правові, технічні, організаційні заходи, розбудова потенціалу та співробітництво. Україна, до речі, за цим індексом у 2018 році зайняла 54 місце у світі.

Україна на сьогодні має Стратегію кібербезпеки та Закон про кібербезпеку, що створює правові передумови для забезпечення кібербезпеки.

З точки зору організаційних заходів CERT-UA, який функціонує при Держспецзв'язку України, виконує обов'язок інформувати про кіберзагрози та відповідні методи захисту [3], розміщуючи, наприклад, на власному веб-сайті основні правила кібергігієни (13.12.2018) та здійснюючи репост видання The Huffington Post щодо правил запобігання поширенню фейкових новин в соцмережах (12.07.2019) [7].

Ситуаційним центром забезпечення кібербезпеки СБУ на базі платформи з відкритим програмним кодом MISP (Malware Information Sharing Platform)[1] забезпечується збір і обробка інформації щодо інцидентів кібербезпеки між суб'єктами сектору безпеки в режимі реального часу. ДКІБ СБ України задля розбудови ефективної системи кібербезпеки держави підписала Меморандум про співпрацю більше ніж з 50 об'єктами критичної інфраструктури, відповідно до якого здійснюється обмін інформацією.

Насамкінець відзначимо, що крім згадуваного Міжнародного союзу електрозв'язку, питаннями протидії кіберзагрозам опікуються структури Інтерполу, НАТО (насамперед, Центр передового досвіду НАТО з кіберзахисту – CCD COE, у м. Таллінн), ЄС (насамперед, Центр кіберзлочинності Європолу – EC3, Агентство ЄС з кібербезпеки – ENISA), Рада Європи (у частині удосконалення механізмів реалізації положень Конвенції Ради Європи про кіберзлочинність), ОБСЄ та інші організації.

Українські суб'єкти національної системи кібербезпеки активно співпрацюють із зазначеними міжнародними організаціями. Дієвими є механізми Конвенції Ради Європи про кіберзлочинність (далі – Кіберконвенція) [9], Угоди між Україною та Європолом про оперативне та стратегічне співробітництво, яка надає можливість правоохоронним органам України через Департамент міжнародного співробітництва Нацполіції здійснювати інформаційний обмін з Європолом у розслідуванні зокрема і кіберзлочинів.

Нині Комітет з Кіберконвеції (T-CY) продовжує роботу над підготовкою 2-го додаткового протоколу до Будапештської Конвенції, який має на меті:

– підвищити ефективність взаємної правової допомоги при розслідуванні кіберзлочинів;

---

[1] Платформа MISP відповідає міжнародним стандартам ЄС та НАТО і застосовується основними міжнародними суб'єктами у сфері кібербезпеки FIRST, CIRCL, CiviCERT, NATO NCI Agency.

– передбачити положення про безпосередню співпрацю з провайдерами в інших юрисдикціях;

– встановлення меж та гарантій існуючої практики розширення транскордонних пошукових запитів;

– закріплення гарантій верховенства права та захисту персональних даних [10].

Результатом взаємодії України з Трастовим фондом НАТО для посилення спроможності України у сфері кібербезпеки стала розбудова мережі ситуаційних центрів кібербезпеки та кіберзахисту в ДКІБ СБУ та Держспецзв'язку України, з підключенням до них розгалуженої мережі автоматизованих датчиків подій, розташованих на інформаційно-телекомунікаційних мережах об'єктів критичної інформаційної інфраструктури. На цій базі створено Центр реагування на кіберзагрози (Cyber Threat Response Centre, CRC) як платформу взаємодії основних суб'єктів забезпечення кібербезпеки (Держспецзв'язку, СБУ, Нацполіції), яка підвищує ефективність і оперативність діяльності правоохоронних органів з протидії та розслідування кіберзлочинів [8].

У складі ситуаційного центру СБУ організовано роботу лабораторії комп'ютерної криміналістики. Технічні рішення щодо проведення цифрових досліджень комп'ютерного та мережевого обладнання сприяють адаптації методики досліджень до різних типів кіберінцидентів, для виявлення та фіксації цифрових слідів злочинних дій в режимі реального часу.

Список використаних джерел:

1. Закон України від 21.06.2018 «Про національну безпеку України». Відомості Верховної Ради України. 2018. №31. Ст. 241.
2. Указ Президента України від 15.03.2016 №96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». Офіційний вісник України. 2016. №23. Ст. 899.
3. Закон України від 05.10.2017 «Про основні засади забезпечення кібербезпеки України». Відомості Верховної Ради України. 2017. №45. Ст. 403.
4. Постанова Кабінету Міністрів України від 19 червня 2019 р. №518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури». Офіційний вісник України. 2019. №50. Ст. 1697.
5. https://www.kmu.gov.ua/ua/news/minekonomrozvitku-ta-sbu-stvoryat-nacionalnij-perelik-obyektiv-kritichnoyi-infrastrukturi.
6. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf.
7. https://cert.gov.ua/recommendations.

8. http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=286338&cat_id=284576.
9. Закон України «Про ратифікацію Конвенції про кіберзлочинність» від 07.09.2005. Відомості Верховної Ради України. 2006. № 5. Ст. 71.
10. https://www.coe.int/en/web/cybercrime/t-cy-drafting-group.

Кулик К. Д., кандидат юридичних наук, асистент кафедри кримінології та кримінально-виконавчого права Національного юридичного університету імені Ярослава Мудрого, м. Харків, Україна

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ SMART-BUILDING У СИСТЕМІ ЗАПОБІГАННЯ ЗЛОЧИННОСТІ В УКРАЇНІ

XXI століття характеризується бурхливим розвитком будівництва, науки, техніки та інформаційних технологій. Всі досягнення науково-технічного прогресу спрямовані на покращення добробуту населення та підвищення його захищеності. Оскільки поряд із розвитком суспільства та високих технологій, на жаль, модернізуються й прояви злочинності. Саме з метою запобігання цим негативним тенденціям у багатьох країнах світу, реалізуються програми безпечного середовища – «Безпечне місто» (Safety City) та «Розумне місто» (Smart City). За підрахунками аналітиків компанії IDC (International Data Corporation) у 2019 р. світові витрати на технології та ініціативи зі створення інтелектуального міського середовища (Smart City) виростуть на 17,7% і досягнуть $95,8 млрд [1].

Впровадження цих програм у великих містах України стало завданням останніх п'яти років. Система «Безпечне місто» (Safety City) представляє собою об'єднання локальних засобів відео моніторингу, фіксації, передавання інформації про стан громадського порядку та забезпечення швидкого реагування на правопорушення. Проте у Харкові доцільно розгортати високотехнологічну Систему «Розумне безпечне місто» (Smart Safe City). Це інформаційно-аналітична програма нового покоління, що здійснює розпізнавання потенційних небезпек, аналіз ситуації в реальному часі та передачу вже опрацьованих даних про виявлені загрози терористичного, кримінального, техногенного характеру у місцях масового перебування громадян, на об'єктах критичної інфраструктури, транспортних розв'язках,

операторам екстрених служб для забезпечення швидкого реагування на надзвичайні події. Така Система використовується для автоматизованого управління безпекою територіальної громади, захисту об'єктів критичної інфраструктури, охорони громадського порядку [2, с. 52]. Відповідно до результатів дослідження консалтингового агентства Navigant Research, на сьогодні програма Smart City складається з наступних основних елементів: Smart Energy (управління енергозбереженням), Smart Water (управління водними ресурсами), Smart Transportation (інтелектуальні транспортні та логістичні системи), Smart Government (використання інформаційних технологій для надання державних послуг та дозволяю оптимізувати роботу різних департаментів), Smart Buildings [3].

Особливу увагу привертає технологія Smart Buildings, яка передбачає будівництво та благоустрій окремих забудов, які акумулюють в собі всі інженерні та інформаційні системи й інтегруються в єдину систему управління (BMS – building management system). Система BMS складається з центрального комп'ютеру з відповідним програмним забезпеченням та мережі локальних контроллерів. Центральний комп'ютер об'єднує в єдину мережу всі локальні датчики. Отримуючи сигнал від датчика, контроллер надсилає відповідну команду диспетчеру на центральний комп'ютер. За допомогою контроллерів відбувається автоматичне управління всіма інженерними системами будівлі, зокрема: системою вентиляції, системою опалення, системою охолодження, системою газо- і водопостачання, системою енергоживлення та освітлення, а також системою безпеки, що включає відеоспостереження, санкціонований доступ (СКУД) та оповіщення. BMS умовно поділяється на два види: направлена на управління приватними будинками/квартирами (Home Automation) та направлена на управління адміністративними будівлями (Building Automation) – житловими комплексами, готелями, бізнес-центрами, торгівельними центрами, лікарнями [4] та ін.

Слід зазначити, що технологія Smart Buildings досить широко використовується в Україні стосовно саме адміністративних будівель незалежно від форми власності. Однак, її впровадження у будівництво/облаштування приватних будинків/квартир відбувається досить повільно. Це обумовлено особливостями адаптації її до українських реалій, у тому числі системи роботи комунальних служб та їх недостатньою комп'ютеризацією. Досліджувана технологія не тільки направлена на безпечну роботу інженерних систем будинку, але виконує захисні функції. Так, окрім, вже звичних для українців сигналізацій та відеоспостереження, «розумні будинки» можуть імітувати присутність господарів за їх фізичної відсутності. Наприклад, у довільному

порядку програма вмикає/вимикає освітлення, негучну музику, запис розмов, звуків води у ванній кімнаті або свист чайника. Такі дії можуть сприяти зменшенню ризику вчинення крадіжок та грабежів з проникненням у житло.

Таким чином, застосування технології «Smart Building» в Україні має на меті оптимізувати управління інженерними системами будівлі, а також підвищити ступінь безпеки та захищеності населення не тільки на вулиці, але й у власному житлі.

Список використаних джерел:

1. У 2019 світові витрати на програми Smart City наблизяться до $96 млрд. URL: https://deps.ua/knowegable-base-ru/articles/item/66978.html (дата звернення: 14.09.2019). – Заголовок з екрану;
2. Головкін Б. М. Електронна система запобігання злочинності у великих містах. З нагоди 100-річчя від дня народження професора М. В. Салтевського : 3–11 зб. матеріалів круглого столу, м. Харків, ЗО жовт. 2017 р. / [відп. за вип. В. Ю. Шепітько] ; Нац. юрид. ун-т ім. Ярослава Мудрого ; НД1 ВПЗ ім. акад. В. В. Сташиса НАПрН України. – Харків : Право, 2017. С. 48–52;
3. Smart City: технологии «Умного города» и их целевое назначение. URL:https://www.everest.ua/ru/ai-platform-2/smart-city/smart-city-texnologii-umnogo-goroda-i-ix-celevoe-naznachenie/ (дата звернення: 14.09.2019). – Заголовок з екрану;
4. Система управления зданием (BMS). URL: https://www.smartek.az/index.php?a=pages&id=374&lang=ru (дата звернення: 14.09.2019). – Заголовок з екрану.

Левченко Ю. О., кандидат юридичних наук, доцент, завідувач кафедри кримінології та кримінально-виконавчого права Національної академії внутрішніх справ, м. Київ, Україна

СУЧАСНИЙ СТАН ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

Розповсюдження комп'ютерних технологій і комп'ютерної техніки, повсюдне проникнення телекомунікаційних мереж майже в усі сфери життєдіяльності людини одночасно і полегшило (створення та накопичення баз даних, автоматична обробка інформації, можливість миттєвого передання

інформації на дуже великі відстані тощо), й ускладнило управління, виконання виробничих процесів та особисту комунікацію [1, с. 155]. Для багатьох країн, зокрема і для України, кіберзлочинність є достатньо актуальним явищем, породженим широким впровадженням в економічні процеси сучасних інформаційних та телекомунікаційних технологій [2, с. 108].

Питання протидії кіберзлочинам, їх виявлення та попередження у наш час набирає все більшої актуальності, через велику кількість атак, як на промислових гігантів, так і на рядових користувачів мережі Інтернет. Чинною Стратегією кібербезпеки України на Національну поліцію України покладено обов'язки із забезпечення захисту прав і свобод людини та громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; запобігання, виявлення, припинення та розкриття кіберзлочинів; підвищення поінформованості громадян про безпеку в кіберпросторі. Попередження кіберзлочинів як вид превентивних заходів потребує розроблення гнучкої моделі комплексу методів та засобів з виявлення, попередження інцидентів та швидкісного інформування об'єктів атак, а також широкого загалу населення.

Варто погодитися з тим, що одним з найважливіших кроків є підвищення обізнаності працівників правоохоронних органів, представників приватного сектору і потенційних жертв про кіберзлочинність та надання відповідних консультацій відносно зменшення їх віктимності [3, с. 30].

Для ефективної протидії кіберзлочинності окремих відомчих ініціатив вже недостатньо. Потрібна чітка централізована координація зусиль для забезпечення злагодженої взаємодії усіх зацікавлених суб'єктів. Також важливо визначити основні пріоритети розвитку державних структур по боротьбі з кіберзлочинністю, такі як: реорганізація та удосконалення законодавчої і нормативно-правової бази; створення єдиного інформаційного простору; організація і удосконалення динамічної взаємодії із зарубіжними законодавчими та державними органами; запровадження сучасних новітніх інформаційних технологій в органах державної влади, технічна підготовка, перепідготовка та підвищення кваліфікації фахівців по боротьбі з кіберзлочинністю [4, с. 29]. Сьогодні також особливо важливо переглянути усі існуючі заходи та активно розробляти нові, що принесуть більшу користь та надійніший захист від кіберзлочинців.

Крім того, перспективним напрямком у зв'язку з існуючими проблемами є регулярне підвищення кваліфікації співробітників правоохоронних органів з метою вивчення актуальних питань тактики проведення слідчих дій для отримання електронних доказів при розслідуванні кіберзлочинів.

Так, один із таких заходів відбувся нещодавно в стінах Національній академії внутрішніх справ. 4 вересня з робочим візитом завітала делегація експертів Ради Європи та Консультативної місії Європейського Союзу (КМЄС) в Україні – менеджер Проекту боротьби з кіберзлочинами «CyberEast» Георгій Джохадзе, заступник державного прокурора Бранко Стаменкович, слідчий Майкл Джемейсон, а також радник КМЄС в Україні з питань протидії кіберзлочинності Кіріл Мілєв. Крім того, на зустрічі були присутні партнери академії – президент «Міжнародної Кібер Академії», член Координаційної ради Міністерства економічного розвитку і торгівлі України з розвитку цифрової економіки Валерій Цюпа та керівник громадської організації «Crime Stoppers Ukraine», директор з розвитку «Crime Stoppers International» Дмитро Демідов.

Серед іншого, іноземні експерти представили Проект боротьби з кіберзлочинами «CyberEast», спрямований на подальший розвиток правової бази та зміцнення міжнародного співробітництва стосовно кіберзлочинності, методик і стратегій боротьби з нею, підготовки правоохоронців, а також посилення взаємовідносин між кримінальним судочинством та експертами з кіберзлочинності у країнах Східного партнерства [5].

Варто зауважити, що, чинне законодавство України має прогалини стосовно питань організації та здійснення протидії кіберзлочинності. Ефективна запобіжна діяльність правоохоронних органів відносно кіберзлочинності, насамперед, повинна містити заходи із створення умов для забезпечення розвитку внутрішньодержавної правової бази у сфері обігу комп'ютерної інформації, яка повинна відповідати вимогам сьогодення та бути адаптованою до норм міжнародного права.

Крім того, важливим аспектом запобіжної діяльності щодо кіберзлочинності є забезпечення відповідної системи фізичного і технічного захисту комп'ютерної інформації. Також на загальнодержавному рівні важливим є розроблення спеціальної системи захисту комп'ютерної інформації національного значення та створення правового підґрунтя для функціонування цієї системи. Ефективна протидія кіберзлочинності також повинна передбачати проведення моніторингу інформаційних загроз, а також науково-дослідні роботи із вивчення розвитку кіберзлочинності.

Список використаних джерел:

1. Кравцова М. О. Сучасний стан і напрями протидії кіберзлочинності в Україні. *Вісник кримінологічної асоціації України.* №2(19). 2018. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/3848/

Suchasnyi%20stan%20i%20napriamy%20protydii%20kiberzlochynnosti%20v%20Ukraini%20_Kravtsova_2018.pdf?sequence=1&isAllowed=y (дата звернення 06.09.2019).
2. Марков В. В. До питання щодо зарубіжного досвіду запобігання кіберзлочинності. *Право і безпека*. № 2 (57). 2015. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Pib_2015_2_23 (дата звернення 06.09.2019).
3. Гончаренко О. І. Правоохоронна діяльність щодо попередження кіберзлочинності. *Актуальні питання протидії кіберзлочинності та торгівлі людьми*. Харків. 2018. URL: http://univd.edu.ua/general/publishing/konf/23_11_2018/pdf/06.pdf (дата звернення 06.09.2019).
4. Волков А. В. Найбільш розповсюдженні злочини у кіберпросторі. *Актуальні питання протидії кіберзлочинності та торгівлі людьми*. Харків. 2018. URL: http://univd.edu.ua/general/publishing/konf/23_11_2018/pdf/05.pdf (дата звернення 06.09.2019).
5. Міжнародна співпраця академії з протидії кіберзлочинності. URL: https://www.naiau.kiev.ua/news/mizhnarodna-spivpracya-akademiyi-z-protidiyi-kiberzlochinnosti.html (дата звернення 06.09.2019).

Лукашевич С. Ю., кандидат юридичних наук, доцент, доцент кафедри кримінології та кримінально-виконавчого права Національного юридичного університету імені Ярослава Мудрого, м. Харків, Україна

ПРО ПОНЯТТЯ ПОРЯДКУ З ТОЧКИ ЗОРУ СУСПІЛЬНОЇ БЕЗПЕКИ

Порядок, це – стан, коли все робиться, виконується так, як слід, відповідно до певних вимог, правил; певна упорядкованість [2]. В філософії Стародавнього Китаю ідея порядку знайшла своє відображення в конфуціанстві, яке було тісно пов'язане з розвитком стародавнього китайського суспільства і зосереджувалось на етичних правилах, соціальних нормах і регулюванні суспільних відносин. Так, Конфуцій був стурбований деградацією суспільства і зосереджував увагу на вихованні у людини по-

ваги до оточуючих і до суспільства в цілому. Він розумів людину як функцію організації суспільства і запропонував поняття порядку як норми відносин людей. Філософ вважав, що дотримання порядку веде до належного виконання обов'язку. Для дотримання порядку Конфуцій запропонував принцип справедливості і сумлінності, які вимагають, щоб людина повинна чинити так, як велить порядок і її становище [1]. Використовуючи логічний прийом, згідно з яким якщо існує кілька логічно несуперечливих пояснень будь-якого явища, що пояснюють його однаково добре, то слід, при інших рівних умовах, вважати вірним найпростіше з них [8], спробуємо дослідити наступні категорії: «суспільний порядок», «громадський порядок», «публічний порядок» з огляду на їх логіко-функціональне призначення в теорії та практиці запобігання злочинності.

Суспільство – це сукупність людей, об'єднаних певними відносинами, обумовленими історично змінним способом виробництва матеріальних і духовних благ, згідно тлумачному словнику[3]. Значення «суспільства» можуть досить сильно відрізнятися як від буденного його розуміння, так і одне від одного, в залежності від того, в яку теоретичну конструкцію те чи інше тлумачення прагне бути вписане. Але навіть, якщо розглядати суспільне життя в буденному його значенні, стає зрозумілим, що воно підкоряється певним усталеним формам внутрішньої активності. Відповідно, суспільство може розглядатись як система. І, як будь-яка система, воно, ймовірно, здатне підтримувати й відтворювати певний порядок елементів у собі, який забезпечує його цілісність [9].

Суспільний означає створений, нагромаджений суспільством у процесі виробництва; який являє собою спільне надбання[10]. Суспільний порядок – це налагоджений стан суспільних відносин, урегульованих соціальними нормами. У підтримці суспільного порядку важлива роль належить нормам моралі, традиціям, звичаям. Стан суспільного порядку значною мірою залежить від того, наскільки відповідально люди ставляться до виконання вимог соціальних норм. Потрапляючи в ту чи іншу ситуацію ми керуємось певними правилами поведінки, тобто нормами. Саме під впливом соціальних норм та норм права і формується порядок в суспільстві.

У загальному розумінні під громадським порядком розуміють урегульовану правовими та іншими соціальними нормами певну частину суспільних відносин, які складають режим життєдіяльності у відповідних сферах, забезпечують недоторканність життя, здоров'я та гідності грома-

дян, власності та умов, що склалися для нормальної діяльності установ, підприємств, організацій, посадових осіб і громадян [4]. Отже, можна припустити, що громадський порядок вужче поняття за суспільний порядок, оскільки регулює лише частину суспільних відносин, а не в цілому. Також слід відрізняти поняття ці і тому що, «суспільний» утворено від іменника суспільство. Тобто суспільний лад, суспільне буття, суспільна свідомість. А «громадський» – від громада. Він має значення не державний, не службовий, добровільний, такий, що стосується всього населення або якогось колективу [3].

Обов'язковим елементом громадського порядку є засоби регулювання суспільних відносин, які утворюють зміст громадського порядку: правові, а також інші соціальні норми – норми моралі, звичаї, релігійні норми, правила громадського співжиття. За їх допомогою встановлюються права та обов'язки учасників суспільних відносин, визначаються заборони на вчинення певних дій, а також можливість і порядок застосування санкцій. Крім того, за допомогою засобів регулювання формуються відповідні установи, покликані забезпечувати безперешкодну реалізацію суспільних відносин, що склалися, а також визначається їх компетенція, сфера впливу.

Через правові норми регулюються найбільш складні та важливі суспільні відносини. Однак, багатогранність суспільного життя не дозволяє всі суспільні відносини урегулювати правовими засобами. Численні суспільні відносини мають нескладний характер і в результаті повсякденного прояву не вимагають правового регулювання та застосування інших заходів державного забезпечення, а підтримуються громадською правосвідомістю, високою правовою культурою, правилами громадського співжиття, що склалися, моральними нормами, звичаями.

Обов'язковим елементом громадського порядку є також визначення цілей суспільних відносин, що складаються, та їх регулювання. Такими загальними цілями громадського порядку виступають: забезпечення недоторканності життя, здоров'я, гідності та прав людини і громадянина; забезпечення недоторканності власності; підтримання необхідних умов нормальної діяльності підприємств, установ, організацій, посадових осіб і громадян [4].

Публічний, за тлумачним словником, це такий, який відбувається в присутності публіки, людей, прилюдний. В перекладі з латинської мови «публічний» (publicus) – означає відкритий, гласний.

Якщо розглядати публічний порядок через призму цивільного права, то, наприклад, однією з умов дійсності правочину є дотримання вимог щодо

його змісту. Зокрема, зміст вчиненого правочину не повинен суперечити публічному порядку держави, закріпленому в законодавстві України. Тобто можна зробити висновок, що публічний порядок – це публічно-правові відносини, які мають імперативний характер і визначають основи суспільного ладу держави. При цьому категорія публічного порядку застосовується не до будь-яких правовідносин у державі, а лише щодо суттєвих основ правопорядку[6]. А правопорядок – це фактичний стан упорядкованості, урегульованості та організованості суспільних відносин, який формується та функціонує на основі права внаслідок його реалізації через правомірну поведінку суб'єктів прав та гарантується й захищається державою. А суттєвою ознакою правопорядку слід виділити те що, він є складовою частиною суспільного порядку, і таким чином обумовлений суспільними потребами та інтересами [5]. З теорії держави та права ми знаємо, що публічний означає такий, який відбувається в інтересах держави.

Отже, можна простежити, що ми знову дійшли до суспільного порядку (через публічний порядок та правопорядок), а тому робимо висновок, що серед усіх розглядуваних категорій (суспільний, громадський, публічний порядки) найважливішою і найближчою до громадян буде саме суспільний порядок. Він охоплює суспільні відносини, які включають у себе явища, що підтримуються лише завдяки громадської правосвідомості, високій правовій культурі, правил громадського співжиття, що склалися, моральними нормами, звичаями. Тобто включає ті елементи, які не завжди можуть регулюватись закріпленими нормами в законодавстві, оскільки вони залежать від самого індивіда, від його моральних поглядів, соціальної вихованості та поведінки.

Список використаних джерел:

1. История философии в кратком изложении [Електронний ресурс]: http://filosof.historic.ru/books/item/f00/s00/z0000196/index.shtml.
2. Словник української мови: в 11 томах. – Том 7, 1976. – Стор. 302. [Електронний ресурс]: http://sum.in.ua/s/porjadok
3. Словник української мови: в 11 томах. – Том 9, 1978. – Стор. 859. [Електронний ресурс]: http://sum.in.ua/s/suspiljstvo
4. Мультимедійний навчальний посібник «Організація діяльності міліції громадської безпеки» [Електронний ресурс] : http://www.naiau.kiev.ua/books/ODGMV/new-page.html
5. Теорія держави і права: посіб. для підготовки до держ. іспитів/ за заг. ред. О. В. Петришина. – Х. : Право, 2012. – 192 с.

6. Тріска І. І., Левицька В. В. – Особливості визначення правочину таким, що порушує публічний порядок [Електронний ресурс]: http://www.rusnauka.com/33_NIO_2009/Pravo/54976.doc.htm
7. Закон України «Про національну поліцію» (Відомості Верховної Ради (ВВР), 2015, №40–41, ст.379) [Електронний ресурс] : http://zakon2.rada.gov.ua/laws/show/580–19
8. Амнуель П. Р. «Не порежтесь бритвой Оккама», журнал «Наука и жизнь» №7,2010.
9. Недзельський А. О. «Проблема соціального порядку крізь призму рутинізації соціальних практик», актуальні проблеми соціології, психології, педагогіки : Збірник наукових праць. Вип.17 – К.: Логос, 2012. – 28–36 с.
10. Словник української мови: в 11 томах. – Том 9, 1978. – Стор. 858. [Електронний ресурс]: http://sum.in.ua/s/suspiljnyj

Луценко Ю. В., кандидат юридичних наук, доцент

ЩОДО ОКРЕМИХ ПОЛОЖЕНЬ КРИМІНАЛЬНО-ПРАВОВОЇ ПОЛІТИКИ ДЕРЖАВИ У СФЕРІ ОХОРОНИ ВОЄННОЇ БЕЗПЕКИ УКРАЇНИ

Сьогодні, у кримінально-правовій доктрині ще не вироблено єдиного концептуального підходу щодо розуміння кримінально-правової політики держави у сфері охорони воєнної безпеки. На думку переважної більшості дослідників з даної проблематики, відсутність цілісної сучасної концепції кримінально-правової політики в країні, стратегії розвитку національного законодавства про кримінальну відповідальність, призводить до постійних не системних змін. Це має своїм наслідком виникнення ситуацій невідповідності кримінального законодавства України іншим нормативно-правовим актам, у тому числі і Основному закону – Конституції України, що, у свою чергу, тягне за собою суттєві проблеми в правозастосовній діяльності [4, с. 85].

Визначення поняття та змісту кримінально-правової політики, у тому числі, у сфері охорони воєнної безпеки України, може бути здійснено шляхом застосування загальної діалектичної методології, яка дає можливість установити її місце та роль як у політиці держави, так і у політиці боротьби зі злочинністю.

Державно-правова політика у сфері боротьби зі злочинністю лише останнім часом стала об'єктом прискіпливої уваги та наукового інтересу зі сторони вчених-правників та політологів. Проте, підходи щодо розуміння змісту та особливостей державної правової політики як у сфері воєнної безпеки, так і у сфері боротьби зі злочинністю, які досліджуються в наукових працях, не отримали достатнього наукового висвітлення.

Недостатньо висвітленими аспектами досліджуваної проблеми останнім часом є особливості формування доктрини і концепції державної правової політики у сфері боротьби зі злочинністю, стратегії її розвитку, визначення пріоритетних завдань у сфері захисту прав і основоположних свобод людини та громадянина [1, с. 44].

Серед всіх напрямків державної політики у сфері запобігання злочинності, які перебувають між собою у функціональній залежності й взаємодії та обумовлені предметом, завданнями й методами підтримання правопорядку в суспільстві, кримінально-правова політика держави, на думку переважної більшості вітчизняних науковців, розробляє стратегію і тактику, формулює основні задачі, принципи, напрями і цілі кримінально-правової дії на злочинність, засоби їх досягнення, і виражається в нормах закону про кримінальну відповідальність, практиці їх застосування, актах офіційного тлумачення кримінально-правових норм та постановах Пленуму Верховного Суду України (складові кримінально-правової політики) [10, с. 13].

Досліджуючи кримінально-правову політику держави у сфері охорони воєнної безпеки України неможливо оминути увагою питання, які стосуються визначення її місця в системі самої державної політики у сфері запобігання злочинності, яка одночасно виступає частиною правової політики держави.

Як слушно звернув увагу П. Л. Фріс, будь-яка держава у своїй діяльності спирається на відповідну ідеологію, керується нею при прийнятті усіх рішень (законів), що визначають шляхи розвитку та функціонування цієї держави. Саме вона перебуває у їх фундаменті, визначаючи спрямованість і зміст. Ідеологія суспільства, як відомо, формується під впливом економічних відносин. В її основі перебувають також менталітет народу (нації), відповідні філософські концепції, теорії тощо.

Правова ідеологія в цілому формує правову політику держави, визначаючи її завдання, цілі, напрями, принципи, етапи реалізації, що у сукупності може бути визначено як концепція правової політики держави. У зв'язку з цим, правова ідеологія суттєвим чином впливає на формуван-

ня законодавчого поля країни, подальшого її політичного вектору розвитку [8, с. 65].

Беззаперечно, що одним з головних напрямків діяльності держави є діяльність спрямована на запобігання злочинності. Протидія злочинності є важливою складовою функціонування держави будь-якого типу, незалежно від часу свого існування. Значна кількість нормативно-правових актів, різних програм та стратегій, що приймаються органами державної влади, велика кількість правоохоронних та правозастосовних органів – все це свідчить про значну роль політики у сфері запобігання злочинності в діяльності держави. У зв'язку з цим, невід'ємною частиною такого напрямку діяльності держави безсумніву є кримінально-правова політика.

Не дивлячись на розрізненість поглядів в питанні змісту та сутності кримінально-правової політики, більшість науковців схиляються до думки, що остання виступає структурною частиною правової політики держави, основний зміст якої зводиться до застосування репресивних заходів. Визначити її місце в системі правової політики є процесом складним, проте вкрай необхідним для розуміння її змістовного наповнення та термінологічної характеристики [5, с. 126].

Найбільш вживаними в цьому сенсі термінами є «політика держави у сфері запобігання злочинності», «кримінально-правова політика», «кримінальна політика». Наразі, у науковій спільноті жвавої дискусії набувають питання, які стосуються термінологічної властивості останнього поняття. Сама етимологія слова «кримінальна», як зазначає А. А. Митрофанов, в поєднанні з терміном «політика» надає останньому негативного, неприйнятного забарвлення [7, с. 23]. Як вірно відмітив М. Й. Коржанський, термін «кримінальний» вживається в українській мові ще й в значенні «злочинний» [3, с. 4].

Саме тому, на наш погляд, виділений вище напрямок державної внутрішньої політики більш правильно було б іменувати політика у сфері запобігання злочинності. Проте, тут необхідно погодитись з висловленням Г. М. Миньковского, який узагальнюючи все різноманіття думок, зробив висновок, «… що як би не іменувалися напрямки діяльності держави і суспільства, пов'язані з боротьбою зі злочинністю, − кримінальною політикою або політикою боротьби зі злочинністю, − йдеться про найважливішу складову частини внутрішньої політики, що забезпечує ефективне функціонування економічної, ідеологічної та соціальної політики держави» [6, с. 3−12]. Як можна побачити з цього визначення, Г. М. Миньковський ототожнює кримінально-правову політику держави з політикою

держави у сфері запобігання злочинності і визначає їх як синоніми. При цьому відводить їм лише допоміжну роль для здійснення інших видів політики держави.

Акцентуючи важливість політики у сфері боротьби зі злочинністю, П. Л. Фріс зазначає: «… як магістральний напрям діяльності держави по боротьбі зі злочинністю, вона складається з кількох елементів (складових) – кримінально-правової політики, кримінальної процесуальної політики, кримінально-виконавчої політики та кримінологічної (профілактичної) політики» [9, с. 31].

Теза про самостійність кримінально-правової, кримінальної процесуальної та кримінально-виконавчої політики значною мірою ґрунтується на факті існування трьох самостійних галузей права: кримінального, кримінального процесуального та кримінально-виконавчого. Дійсно, в силу специфіки предмета правового регулювання ці галузі права мають самостійний характер. Однак це жодною мірою не спростовує положення про їх єдність, оскільки норми цих галузей регулюють діяльність різних суб'єктів в одній галузі життя суспільства − в галузі боротьби зі злочинністю. У цьому зв'язку необхідно акцентувати увагу, що боротьба (протидія) із злочинністю не обмежується виключно галузями кримінального, кримінального процесуального та кримінально-виконавчого права. Необхідно пам'ятати про роль такої галузі права, яка регулює оперативно-розшукову діяльність, змістом якої є пошук і фіксація фактичних даних про протиправні діяння окремих осіб та груп, відповідальність за які передбачена Кримінальним кодексом України. З огляду на це необхідно визнати її структурною частиною політики держави у сфері запобігання злочинності на рівні із кримінально-правовою політикою, кримінальною процесуальною політикою, кримінально-виконавчою політикою та кримінологічною (профілактичною) політикою.

Як бачимо, усі складові політики у сфері боротьби зі злочинністю перебувають між собою у функціональній залежності й взаємозв'язку. Механізм цього взаємозв'язку такий, що зміни в одному елементі з необхідністю визначають відповідні зміни і в інших елементах політики у сфері боротьби (протидії) зі злочинністю.

Отже, беручи до уваги висловлені погляди багатьох науковців, необхідно звернути увагу, що національне кримінальне законодавство не завжди послідовно здійснює групування родових об'єктів за принципом першочерговості охоронюваних суспільних правовідносин, благ та інтересів. Наприклад, у законі України про кримінальну відповідальність вза-

галі відсутні окремі розділи, які б стосувалися злочинів проти держави чи воєнної безпеки. Водночас, такі напрямки державної політики містяться у Законі України «Про національну безпеку України» [2]. Як бачимо, держава потребує правового регулювання суспільних правовідносин не лише у сфері національної, а і у сфері воєнної безпеки. Особливої гостроти це питання набуває з урахуванням подій, які мають місце останнім часом в Україні під час збройної агресії зі сторони Російської Федерації.

Таким чином, кримінально-правова політика держави у сфері охорони воєнної безпеки виступає системоутворюючим елементом у боротьбі зі злочинністю, вона розробляє стратегію і тактику, є теорією і практикою протидії злочинності, формулює основні завдання, принципи, напрями і цілі кримінально-правового впливу на злочинність та засоби їх досягнення, виступає за окремими напрямами її здійснення: запобігання вчинення кримінальних правопорушень та належне реагування на їх вчинення всіма дозволеними засобами.

Кримінально-правову політику держави у сфері воєнної безпеки необхідно розуміти як окремий напрям державної політики у протидії злочинності, основна мета якої полягає у забезпеченні такої протидії засобами кримінально-правового характеру.

Список використаних джерел:

1. Загурський Б. О. До питання про теоретичні проблеми державної правової політики у сфері боротьби зі злочинністю. Актуальні проблеми держави і права. 2011. № 60. С. 43–50.
2. Закону України «Про національну безпеку України» від 21 червня 2018 року № 2469-VIII.
3. Коржанський М. Й. Уголовне право України. Частина загальна. Курс. Наукова думка. Українська видавнича група. 1996. 336 с.
4. Луценко Ю. В. Доктринальні положення кримінально-правової політики держави у сфері забезпечення воєнної безпеки України. Актуальні проблеми міжнародних відносин. Випуск 138. 2019. С. 84−96. DOI: http://dx.doi.org/10.17721/apmv.2018.138.0.84–96.
5. Луценко Ю. В., Клименко С. В. Поняття та зміст кримінально-правової політики держави. Право.ua. 2015. № 1. С. 125–131.
6. Миньковский Г. М. Правовая политика в сфере борьбы с преступностью и проблемы законодательного регулирования этой борьбы. Проблемы формирования уголовной политики Российской Федерации и её реализации органами внутренних дел. 1995. С. 3–12.

7. Митрофанов А. А. Основні напрямки кримінально-правової політики в Україні: формування та реалізація: монографія. Одеса: Одеського юрид. інстит. НУВС, 2004. 132 с.
8. Фріс П. Л. Ідеологія кримінально-правової політики та кримінальне законодавство. Проблеми науки кримінального права та їх вирішення у законотворчій та правозастосовній діяльності: матеріали міжнарод. наук.-практ. конф. (Харків, 8–9 жовт. 2015 р.). Харків: Право, 2015. С. 65–69.
9. Фріс П. Л. Кримінально-правова політика України: дис. … д-ра юрид. наук: 12.00.08 / Нац. акад. внутр. справ. Київ, 2005. 439 с.
10. Фріс П. Л. Кримінально-правова політика Української держави: теоретичні, історичні та правові проблеми: монографія. К.: Атіка, 2005. 332 с.

Миронюк Т. В., кандидат юридичних наук, доцент кафедри кримінології та кримінально-виконавчого права Національної академії внутрішніх справ, м. Київ, Україна

СУЧАСНИЙ СТАН ТА ТЕНДЕНЦІЇ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

Сучасні світові тенденції розвитку кіберзлочинності та її посилення свідчать про зростання значення боротьби з нею для подальшого розвитку суспільства, що в свою чергу, зумовлює віднесення певних груп суспільних відносин кіберсфери до компетенції правового регулювання. Особливо актуально зазначена проблема торкається забезпечення національної безпеки та відповідно суспільно небезпечних діянь, які повинні набути статусу злочинів у кіберсфері і нести за собою відповідну юридичну відповідальність. Сьогодні Україна слабко задіяна у процесі боротьби з кіберзлочинністю й відповідно є незахищеною від злочинів у сфері інформаційної безпеки.

Найбільш розповсюдженою є *класифікація кіберзлочинів* на 1) агресивні та 2) неагресивні. До першою групи належать: кібертероризм, погроза фізичної розправи (наприклад, передача через електронну пошту), кіберпереслідування, кібersталкінг (протиправне сексуальне домагання та переслідування іншої особи через Інтернет), дитяча порнографія (ство-

рення порнографічних матеріалів, виготовлених із зображенням дітей, розповсюдження цих матеріалів, отримання доступу до них). Друга група включає: кіберкрадіжка, кібервандалізм, кібершахрайство, кібершпигунство, розповсюдження спаму та вірусних програм.

В кримінологічній характеристики кіберзлочинності слід зазначити, що більшість виявлених злочинів, що вчиняються з використанням комп'ютерних технологій, розпорошені у звітності різних підрозділів правоохоронних органів, серед показників економічної та інших видів злочинності. Через таку недосконаліть статистичної звітності, неможливо провести комплексну характеристику кіберзлочинності.

Так, впродовж 2018 року згідно зі статистичними даними Генеральної прокуратури України обліковано 2017 кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Їх питома вага ще незначна і становить усього 0,5% від усіх облікованих кримінальних правопорушень у 2018 р., але за останні п'ять років зросла в 5,6 разів. Порівняно із 2017 р. кількість кримінальних правопорушень, передбачених статтями Розділу XVI КК України, зменшилася на 10,6% (у 2017 р. – 2573). При цьому кількість кримінальних правопорушень, за якими особам вручено повідомлення про підозру, збільшилася на 26,4% (1272 у 2017 р. проти 1608 у 2018 р.), зокрема передбачених ст. 362 КК України на 58,2% (607 у 2017 р. проти 960 у 2018 р.). Також збільшилася кількість кримінальних правопорушень, за якими провадження направлені до суду з обвинувальним актом, – на 31,0% (1015 у 2017 р. проти 1220 у 2018 р.). Найбільшу частку правопорушень в зазначеній сфері становлять кримінальні правопорушення, передбачені ст. 362 КК України (47%) та ст. 361 КК України КК України (44%) [1, с. 110].

Варто відзначити, що у січні 2019 року обліковано 218 кримінальних правопорушень, передбачених статтями Розділу XVI КК України, а передбачених ст. 362 КК України – 90. На час вчинення кримінального правопорушення 45 *осіб* були *у віці* від 18 до 28 років, 47 – від 29 до 39 років, 22 – від 40 до 54 років, 15–60 і більше років. Таким чином, за віковою ознакою неможливо виокремити якусь явну категорію правопорушників. Виявлено 42 жінки (30,9%), що вчинили кримінальні правопорушення, тобто *третина виявлених правопорушників – жінки*. *За освітою* на час вчинення кримінального правопорушення найбільшу кількість становили особи з повною вищою і базовою вищою освітою – 77(56,6%), з професійно-технічною – 27 осіб, з повною загальною середньою та базовою загальною середньою освітою – 31 особа. Із 136 виявлених осіб, які вчи-

нили правопорушення, передбачені Розділом XVI КК України, *всі є громадянами України*, *майже половина осіб є працездатними*, які не працювали і не навчалися, – 46 та 21 – безробітні, 8 учнів і студентів навчальних закладів. Групою осіб у 2018 році у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку вчинено 44 кримінальних правопорушення, що становить 3,3% від облікованих і на 4,8% більше порівняно з 2017 роком. Найбільше групою осіб вчинено кримінальних правопорушень, передбачених ст. 361 КК України, – 37[1, с. 111].

Кіберзлочини *вчиняють переважно індивідууми або невеликі злочинні групи хакерів.* Працівники підрозділів кіберполіції Національної поліції України порівняно з попереднім періодом виявили на 4 організовані групи і злочинні організації більше (7 у 2017 р. проти 11 у 2018 р.). Вони вчинили 142 кримінальних правопорушень, з яких 140 – тяжкі. Найбільше – передбачених ст. 190 КК України (100), у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів (7). У 2018 р. виявлено 196 фактів збуту наркотичних засобів, психотропних речовин або їх аналогів, а також отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів із використанням всесвітньої мережі Інтернет, що на 37,1% більше порівняно з 2017 р. (143) і в 7,5 рази порівняно з 2016 р. (26). При цьому, варто відзначити, що у ЗМІ ці показники подаються як кількість виявлених груп, які збували наркотичні засоби з використанням Інтернету [2].

У сфері використання ЕОМ (комп'ютерів), систем і комп'ютерних мереж і мереж електрозв'язку організованими групами вчинено 9 кримінальних правопорушень: із них 6 – виявили працівники підрозділів кіберполіції, 3 – підрозділів захисту економіки. Виявлено 41 особу, яка вчинила кримінальні правопорушення у складі ОГ і ЗО, що на 51,9% більше порівняно з 2017 р. (27 осіб). Слід зазначити, що у 2018 р. 72 кримінальних правопорушення у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку виявили працівники підрозділів карного розшуку (проти 163 у 2017 р.). У 2018 р. кримінальними правопорушеннями, вчиненими з використанням високих інформаційних технологій, завдано матеріальних збитків на суму 38 713 тис. грн, що на 51 674 тис. грн менше, ніж у попередньому періоді (90387 тис. грн). При цьому у 2017 р. відшкодовано (з урахуванням накладеного арешту та вилученого майна) 71,8% коштів, а у 2018 р. – лише 57,2%. У 2018 р. найбільших матеріальних збитків завдано шахрайством – 21 194 тис. грн, при цьому відшкодовано лише 53,1% (11 250 тис. грн) [1, с. 114].

У 2018 р. збільшення кількості кримінальних правопорушень, що вчинені з використанням високих інформаційних технологій, відзначалося у 8 областях. Найбільше зростання відбулося в Миколаївській (106,9%), Рівненській (93,5%), Харківській (85,5%) областях. Найбільше кримінальних правопорушень вчинено в м. Києві (845), Миколаївській (776), Одеській (647) та Львівській (591) областях, найменше – у Волинській області (51). Рівень кіберзлочинності в Україні на 10 000 населення невисокий і у 2018 р. складав 2,1 проти 2,4 у 2017 р. [1, с. 115].

Однак, зазначені вище статистичні показники, на жаль не відбивають реальний стан кіберзлочинності, оскільки цей різновид злочинів має *високий рівень латентності.* За експертними оцінками, рівень латентності кіберзлочинів становить 90–95%. Причинами латентності найчастіше виступають складнощі виявлення та розслідування кіберзлочинів, неповідомлення потерпілих осіб про факти вчинення таких злочинів. Так, більшість великих компаній хвилюються про свою ділову репутацію та намагаються усунути наслідки кіберзлочинів власними зусиллями. Кіберзлочинність характеризується високим рівнем природної латентності.

Зарубіжні вчені виділяють також п'ять найпоширеніших *мотивів* скоєння комп'ютерних злочинів: корисливий мотив – 66%, політичні мотиви (шпигунство, злочини, спрямовані на підрив фінансової, кредитної політики уряду, дезорганізацію валютної системи країни) – 17%, дослідницький інтерес – 7%; хуліганські мотиви – 5%, помста – 3% [3].

Отже, проблема профілактики і стимулювання кіберзлочинності в Україні – це комплексна проблема. Сьогодні закони повинні відповідати вимогам, що пред'являються сучасним рівнем розвитку технологій. Пріоритетним напрямком є також організація взаємодії і координація зусиль правоохоронних органів, спецслужб, судової системи, забезпечення їх необхідною матеріально-технічною базою. Жодна держава сьогодні не в змозі протистояти кіберзлочинності самостійно. Нагальною є необхідність активізації міжнародної співпраці в цій сфері. Експерти впевнені: саме хакери в недалекому майбутньому стануть загрозою номер один, змістивши тероризм. Незважаючи на віртуальність злочинів, збиток вони завдають цілком справжній.

Список використаних джерел:

1. Гавловський В. Д. Аналіз стану кіберзлочинності в Україні // Інформація і право науковий фаховий журнал № 1(28)/2019 URL:https:// https://mndcentr.com/vydania/pdf_publ/gv_28_19.pdf

2. В 2016 правоохранители обнаружили 26 групп в Украине, которые сбывали наркотики через Интернет. В 2018 таких групп обнаружили 96. URL:https://censor.net.ua/news/310598/za_2018_ god_politsiya_ raskryla_196_grupp_sbyvayuschih_narkotiki_cherez_internet_zamnachalnik _departamenta
3. Поняття та кримінологічна характеристика кіберзлочинності. Загальна та особлива частини. URL: http://libnet.com/content/9684_Ponyattya_ta_ kriminologichna_harakteristika_kiberzlochinnosti.html

Настюк В. Я., завідувач кафедри адміністративного права та адміністративної діяльності Національного юридичного університету імені Ярослава Мудрого, доктор юридичних наук, професор, член-кор. НАПрН України, м. Харків, Україна
Бєлєвцева В. В., завідувач Наукової лабораторії права міжнародної безпеки та протидії злочинам проти миру і безпеки людства НДІ інформатики і права НАПрН України, доктор юридичних наук, ст. наук. співроб., м. Харків, Україна

ОСОБЛИВОСТІ ПРАВОВИХ РЕЖИМІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

У сучасних умовах функціонування світової спільноти у цілому та Української держави зокрема, інформаційні і комунікаційні технології є найважливішою частиною сучасних систем управління у всіх галузях суспільного життя. Розширення сфер застосування інформаційних технологій, як чиннику розвитку економіки та удосконалення функціонування громадських і державних інститутів, одночасно є поштовхом для появи нових глобальних викликів і загроз кібербезпеці. Тому охорона та забезпечення кібербезпеки України, попередження та припинення правопорушень у сфері інформаційних технологій були та залишаються найважливішими завданнями відповідних державних органів і суспільства у цілому.

Так, у Стратегії кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 року №96/2016 справедливо наголошується, що переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці. Поряд із інцидентами природного (ненавмисного) походження зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб [4].

Суттєвими проблемами негативної тенденції зростання кількості правопорушень у кіберпросторі є недостатні наукові засади протидії ним та недостатня розробленість нормативно-правової бази у цій сфері. При цьому слід відразу зазначити, що дослідженням різних аспектів забезпечення кібербезпеки України займаються науковці НДІ інформатики і права НАПрН України (Баранов О. А., Бєляков К. І., Довгань О. Д., Доронін І. М., Пилипчук В. Г., Фурашев В. М. та багато інших). Так, Довгань О. Д. та Тарасюк А. В. у своїх наукових дослідженнях зазначають, що формування та реалізація державної політики щодо запобігання та протидії кіберзлочинності – це процеси, що відбуваються в рамках Національної системи кібербезпеки, які можна розглянути через організаційно-правовий, організаційно-технічний та правоохоронний аспекти [3, с. 95–97].

У цій доповіді автори ставлять за мету торкнутися організаційно-правового та правоохоронного аспектів забезпечення кібербезпеки України. На наш погляд, одним з інструментів забезпечення кібербезпеки можуть стати правові режими, оскільки інститут правових режимів у сфері кібербезпеки найбільш поширений, чим в будь-якій іншій сфері соціально-політичного життя. Частина з них пронизує собою сферу кібербезпеки в цілому, лише конкретизуючись відносно специфіки її окремих складових і суб'єктів забезпечення, інша частина поширюється лише на окремі державні структури. Отже, правові режими в цілому більш всього відповідають специфіці забезпечення системи кібербезпеки як більш менш цілісному утворенню, що виділяється усередині системи інформаційної безпеки. Крім того, ці режими як правило беруть свої витоки з середини цієї сфери і зазвичай поширюють свою дію на інші сфери інформаційної безпеки.

В цьому сенсі, по-перше слід зазначити, що правові основи забезпечення кібербезпеки України на сьогодні складають міжнародні акти (Конвенція Ради Європи про кіберзлочинність, Угода про асоціацію між Україною та Європейським Союзом, у якій передбачено, що сторони Угоди співробітничають, у тому числі, і з питань протидії кіберзлочинності) та нормативно-правові акти національного законодавства Закон України «Про

основні засади забезпечення кібербезпеки України», Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»; постанова Кабінету Міністрів України «Про затвердження правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»; нормативний документ системи технічного захисту інформації «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі»; нормативний документ системи технічного захисту інформації «Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу»; Наказ Адміністрації Держспецзв'язку України «Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації»; Наказ Адміністрації Держспецзв'язку України «Про затвердження Положення про державну експертизу в сфері технічного захисту інформації»; Наказ Адміністрації Держспецзв'язку України «Про затвердження Положення про державну експертизу в сфері криптографічного захисту інформації» тощо).

По-друге, проаналізувавши вимоги та правила функціонування кіберпростору, визначені у нормативно-правових актах України, можна виокремити ознаки правових режимів забезпечення кібербезпеки, зокрема: сфера їх застосування – вони встановлюються у сфері діяльності публічної влади у зв'язку з виконанням органами державної влади своїх обов'язків забезпечити кібербезпеку, охорону, захист; розпорядження, режимні правила, що складаються із заборонних та зобов'язальних правових норм, що обмежують загальну правосуб'єктність фізичних і юридичних осіб; для правового режиму забезпечення кібербезпеки характерне покладання на державні органи, посадовців, організації, підприємства, громадян обов'язку діяти в певному напрямі для досягнення тієї або іншої мети для забезпечення кібербезпеки; обов'язковими суб'єктами правових режимів є компетентні органи публічної влади; більшість правових норм, що становлять основу таких режимів, можуть бути реалізовані тільки через правозастосування, шляхом видання індивідуальних правозастосовних актів; при регулюванні правовідносин, що виникають між невладними суб'єктами і публічною владою з приводу дотримання режимних правил, застосовується примусовий метод впливу; порушення правил режиму спричиняє за собою заходи юридичної відповідальності. Отже, правовий режим забезпечення кібербезпеки (у широкому сенсі) – це загальний режим діяльності органів сектору безпеки щодо реалізації покладених на них повноважень. Натомість, правовий ре-

жим забезпечення кібербезпеки (у вузькому сенсі) є сукупністю норм та правил поведінки, діяльності громадян, фізичних та юридичних осіб, що закріплені у нормативно-правових актах, порядок реалізації ними прав і законних інтересів у певних ситуаціях, спрямований на забезпечення кібербезпеки спеціально створюваними з цією метою органами, підрозділами і службами компетентних органів.

Підсумовуючи викладене, можна стверджувати, що особливими ознаками правових режимів забезпечення кібербезпеки є те, що вони: встановлюються у діяльності компетентних органів та життєдіяльності осіб та громадян у частині забезпечення функціонування кіберпростору; закріплюють, деталізують норми та правила поведінки осіб, громадян, державних органів, суспільних об'єднань, підприємств і установ; вводять додаткові обмеження, покладають додаткові обов'язки; широко застосовують адміністративні методи впливу; вводиться додатковий контроль за дотриманням правил поведінки громадянами, фізичними і юридичними особами, а також органами державного управління; порушення норм та правил режиму спричиняє застосування додаткових заходів державного примусу.

При цьому, доцільно звернути увагу на наукові дослідження Довганя О. Д. та Дороніна І. М., де на основі зіставлення результатів аналізу проблем визначення терміна «кібербезпека», та законодавчого визначення терміна «інформаційна безпека» зроблено висновок про те, що кібербезпека – це окремий випадок інформаційної безпеки, поява якого обумовлена використанням комп'ютерних систем та/або телекомунікаційних мереж [2, с. 24–25]. Також, погоджуючись з визначення поняття «кібербезпека» Барановим О. А., зокрема: кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [1]. Наразі, призначення правових режимів забезпечення кібербезпеки можна сформулювати наступним чином: це забезпечення безперебійного функціонування комп'ютерних систем та/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації безпекового значення.

Список використаних джерел:

1. Баранов О. А. Про тлумачення та визначення поняття «кібербезпека» /О. А. Баранов // Правова інформатика. – 2(42). – 2014 [Електронний ресурс]. – режим доступу: http://ippi.org.ua/sites/default/files/14boavpk.pdf
2. Довгань О. Д., Доронін І. М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія; НАПрН України, НДІІП – К.: Видавничий дім «АртЕк». – 2017. – 107 с.
3. Довгань О. Д., Тарасюк А. В., Глобальна культура кібербезпеки в системі запобігання кіберзлочинності в Україні // Інформація і право. – 3(26). – 2018. – С. 94–103.
4. Стратегія кібербезпеки України : Указ Президента України від 15 березня 2016 року №96/2016 // Офіц. вісн. України. – 2016. – №10. – С. 39. – ст. 198.

Новіков О. В., кандидат юридичних наук, асистент кафедри кримінології та кримінально-виконавчого права Національного юридичного університету імені Ярослава Мудрого, науковий співробітник відділу кримінологічних досліджень Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України
Дзюба А. Ю., молодший науковий співробітник відділу кримінологічних досліджень Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України, м. Харків, Україна

ДО ПИТАННЯ ПРО МОЖЛИВІСТЬ ВИКОРИСТАННЯ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ У СФЕРІ ПРОТИДІЇ КОРУПЦІЇ

Науково-технічний прогрес призвів до стрімкого розвитку інформаційно-комунікаційних технологій, які проникли в усі сфери суспільного життя. Одним із досягнень «інформаційної революції» стало створення та подальша розробка різноманітних сучасних технологій «штучного ін-

телекту», які мають високий потенціал у вирішенні складних нестандартних задач. По суті, штучний інтелект – це здатність машин і програм аналізувати отриману інформацію, робити висновки, приймати на їхній основі рішення. Ключова характеристика штучного інтелекту – це вміння постійно навчатися, накопичувати знання і успішно застосовувати їх [1].

Хоча на сьогодні людство знаходиться ще далеко до реального наділення комп'ютерів «людським» інтелектом, але наразі вже зроблено великий крок у такій підгалузі штучного інтелекту як машинне навчання (machine learning). Теоретична розробка алгоритмів машинного навчання дозволило створювати штучні нейронні мережі (далі – ШНМ), які є високотехнологічними програмними обчислюваними системами, принцип роботи яких заснований за аналогією роботи біологічних нейронних мереж людського мозку.

Сучасні ШНМ є нелінійними програмними інструментами моделювання даних, які надають можливість, зокрема, виявляти статистичні закономірності та статистичні структури у великих масивах даних (big data), а також моделювати складні взаємозв'язки між різнорідними об'єктами. Перевага ШНМ перед іншими програмними продуктами полягає у здатності «навчатися» з даних, що вона обробляє, без явної участі людини. Таким чином, штучна система постійно вдосконалює принципи і алгоритми роботи, тобто знаходиться у постійному розвитку.

На сьогодні ШНМ широко застосовуються у таких галузях як автоматизація виробничих процесів, медицина, комп'ютерні ігри, банківська система, наукові дослідження, розпізнавання образів та послідовностей, машинний переклад, промисловість, фінанси, оподаткування тощо. Певний інтерес такі технології також викликали й у дослідників корупції. Зокрема одразу постало питання щодо перспектив та способів використання зазначених технологій у сфері запобігання та протидії корупції. Наразі існує позитивний зарубіжний та вітчизняний досвід використання ШНМ у цій сфері, який варто проаналізувати та запропонувати перспективні напрями застосування ШНМ для удосконалення вітчизняної системи протидії корупції.

По-перше, вже зараз ШНМ показали відносно високу ефективність у сфері виявлення ознак корупційних та пов'язаних із корупцією правопорушень. Так, наприклад, в рамках експерименту уряд Китаю у 2012 р. запустив у 30 округах та містах проект «Zero Trust» («Нульова довіра»). «Штучний інтелект» здійснював аналіз 150 відкритих та закритих баз даних, перевіряючи доходи чиновників та їх родичів. Окрім цього, за словами роз-

робників, система будувала складні багаторівневі карти соціальних відносин для аналізу поведінки державних службовців [2] Якщо показники перевищували певні маркери, система фіксувала порушення, китайська влада отримувала повідомлення і запрошувала чиновника на допит в поліцію [3]. Система відмінно виявляє типові правопорушення: незаконну передачу права власності, невідповідність інфраструктури заявці, махінації із землею та руйнування приватних будинків, участь у тендері компанії родичів відповідального чиновника або несподівану зміну банківського рахунку держслужбовця. Навіть якщо дані в одному документі підроблять, невідповідності у сполучених відомостях швидко на це вкажуть [4].

Слід зазначити, що з моменту свого запуску у 2012 році ШНМ було виявлено 8721 корумпованого працівника [5]. Але, на жаль, на початку 2019 р. багато провінцій відмовилися від участі у експерименті, як не парадоксально, через «високу ефективність» штучного інтелекту. Чиновники як офіційну причину відмови називали те, що «система порушує їхнє право на приватне життя та конфіденційність» [2]. Що ж стосується реальних недоліків системи, то ШНМ хоча й визначала причетність службової особи до корупції, але не надавала відповідних доказів [5]. Отже слідству було відомо про правопорушення, але необхідно було збирати докази самостійно. У зв'язку з цим, багато чиновників отримали лише дисциплінарні стягнення та попередження.

По-друге, ШНМ також активно застосовуються під час оцінки корупційних ризиків, зокрема у сфері здійснення публічних закупівель. Як приклад можна навести вітчизняний досвід функціонування системи «DOZORRO», до якої з 01 листопада 2019 р. була підключена ШНМ. У зв'язку з цим, система «DOZORRO» почала самостійно визначати ймовірність корупційних ризиків у закупівлях та надсилати їх на опрацювання відповідним громадським організаціям групи «DOZORRO». Якщо порушення підтверджується – програма запам'ятовує свій вибір, якщо ні – забуває. Так алгоритм штучного інтелекту вчиться щораз точніше визначати ризиковані закупівлі [5]. Менеджер продукту DOZORRO Андрій Кучеренко поділився результатами бета-тесту: завдяки роботі алгоритму вдалося визначити на 26% більше тендерів з необгрунтованим вибором переможця, на 37% – з безпідставною дискваліфікацією, на 298% – зі змовою учасників. Що прикметно, алгоритм штучного інтелекту знайшов найбільше порушень саме в найдорожчих тендерах [6].

По-третє, ШНМ, через їх здатність виявляти «приховані» зв'язки у великих масивах даних та безмежними потужностями у процесах мо-

делювання, можна використовувати під час проведення наукових досліджень корупції. Потужним інструментом прогнозування корупційної злочинності може стати «самоорганізуюча карта» [8]. Так, дослідники з Університету Вальядоліда у Іспанії використали під час дослідження корупції ШНМ, яка працює як система раннього попередження корупції. В результаті роботи цієї системи вчені встановили позитивні кореляційні зв'язки між корупцією та оподаткуванням нерухомості, економічним зростанням, інфляцією, кількістю фінансових установ та «не фінансових» юридичних осіб, а також тривалим часом знаходження при владі однієї і тієї ж партії. Дослідники стверджують, що їх комп'ютерна модель може обчислити ймовірність корупції в різних провінціях, умови, які їй сприяють, а також спрогнозувати тенденції розвитку корупції на період до трьох років [9].

Таким чином, на підставі вищенаведеного, можна стверджувати про широкі можливості та доволі високу ефективність застосування ШНМ у сфері протидії корупції.

Список використаних джерел:

1. Як діє штучний інтелект і перспективи його використання. URL : https://aiconference.com.ua/uk/news/printsipi-raboti-iskusstvennogo-intellekta-i-perspektiva-ego-ispolzovaniya-92238.
2. Chen, S. Is China's corruption-busting AI system 'Zero Trust' being turned off for being too efficient? URL : https://www.scmp.com/news/china/science/article/2184857/chinas-corruption-busting-ai-system-zero-trust-being-turned-being.
3. Чиновники відмовилися від ШІ: «занадто ефективно бореться з корупцією». URL : https://politeka.net/ua/news/hightech/901921-chinovniki-otkazalis-ot-ii-slishkom-jeffektivno-boretsja-s-korrupciej.
4. Чому Китай відмовився від антикорупційного штучного інтелекту URL: https://uainfo.org/blognews/1549448207-chomu-kitay-vidmovivsya-vid-antikoruptsiynogo-shtuchnogo-intelektu.html.
5. Китайську систему штучного інтелекту вимикають, бо вона надто добре боролась із корупцією чиновників? URL : http://texty.org.ua/pg/news/textynewseditor/read/91144/Kytajsku_systemu_shtuchnogo_intelektu_vymykajut_bo_vona.
6. Як штучний інтелект DOZORRO моніторить закупівлі. URL : https://dozorro.org/blog/yak-shtuchnij-intelekt-dozorro-monitorit-zakupivli.

7. Алгоритми «зради»: як штучний інтелект Dozorro знаходитиме порушення в Prozorro. URL : https://ti-ukraine.org/news/algorytmy-zrady-yak-shtuchnyj-intelekt-dozorro-znahodytyme-porushennya-v-prozorro.
8. Adam I., Fazekas M. Are emerging technologies helping win the fight against corruption in developing countries? URL : http://www.govtransparency.eu/wp-content/uploads/2019/02/ICT-corruption-24Feb19_FINAL.pdf.
9. López-Iturriaga F. J., Sanz I. P. Predicting public corruption with neural networks: an analysis of Spanish provinces. URL: https://poseidon01.ssrn.com/delivery. php?ID=032102104004098031122064013024077028042048049042095026105086098064087082113096120000043045125052037037114122067065124089084127118061035009009020101004096066083111063062037120125002016124082067103003029086098127066101099066070001024015020103099103072&EXT=pdf.

Оболенцев В. Ф., кандидат юридичних наук, доцент кафедри кримінології та кримінально-виконавчого права Національного юридичного університету імені Ярослава Мудрого, м. Харків, Україна
Гуца О. М., кандидат технічних наук, доцент кафедри Економічної кібернетики та управління економічною безпекою Харківського національного університету радіоелектроніки, м. Харків, Україна

МОДЕЛЮВАННЯ СИТЕМИ ДЕРЖАВИ УКРАЇНИ ТА СИСТЕМИ ЗАПОБІГАННЯ ЗЛОЧИННОСТІ В УКРАЇНІ У НОТАЦІЇ BPWIN

У сучасній науці системний аналіз розглядається як сукупність методичних засобів, що застосовується для вирішення проблем у системах [1, с. 14]. Основною метою системотехніки є побудова узагальнюючої моделі взаємодії досліджуваного об'єкта з оточуючим середовищем у конкретній ситуації та розробка рекомендацій для досягнення цим об'єктом певної мети [1, с. 15].

Раніше у своєму дослідженні [2, с. 19] метою системи держави України ми окреслили права і свободи людини, які згідно статті 3 Конституції України «…визначають зміст і *спрямованість* діяльності держави». Метою системи запобігання злочинності в Україні роботі [3, с.16] ми окреслили таким чином: збереження суспільних відносин (прав людини) за відсутності кримінально караних порушень. Відтак обидві системи мають однакову мету – права та свободи людини. І це не дивно, адже система запобігання злочинності є підсистемою системи держави України. Тож і їх спрямованість має співпадати.

Задля вирішення проблем у системах дослідження будь-якого системного об'єкта передбачає його моделювання. Модель – це спеціально створений для зручності дослідження та вирішення проблеми об'єкт (матеріальний чи абстрактний), який має потрібний ступінь подібності до модельованого об'єкта та адекватний цілям дослідження [4, с. 55]. Моделі повинні мати властивості: 1)адекватність; 2)обмеженість; 3) спрощеність; 4) вірність.

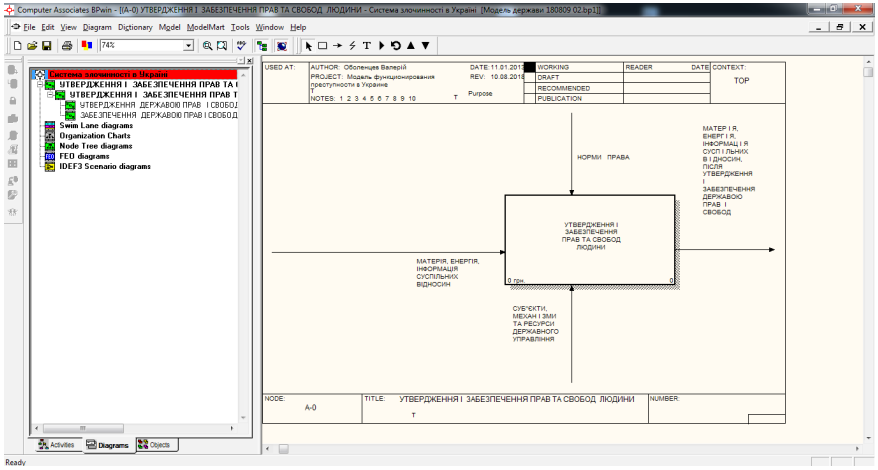
Розроблені нами моделі системи держави України та системи запобігання злочинності в Україні належать до класу так званих морфологічних моделей. Доцільність побудови моделей саме цього виду обгрунтовується тим, що в них найбільш повно описуються межа, що розділяє систему і зовнішнє середовище; об'єкти зовнішнього середовища, що мають зв'язки із системою в аналізованій моделі; входи системи; виходи системи; ієрархічний склад системи; ієрархічна структура системи.

Системний аналіз системи держави України та системи запобігання злочинності в Україні нами здійснювався відповідно до SADT-технології. Structured Analysis and Design Technique – це сучасна методика структурного аналізу і проектування складних організаційних і технічних систем, яку використовують для відтворення динаміки роботи системи, створення систем керування, розробки баз даних та ін.

Для безпосереднього моделювання використовувалося програмне забезпечення пакету графічно-аналітичних програм BPWin. Діаграма А-0 (вищого рівня) моделі системи держави України наведена на Рис.1.

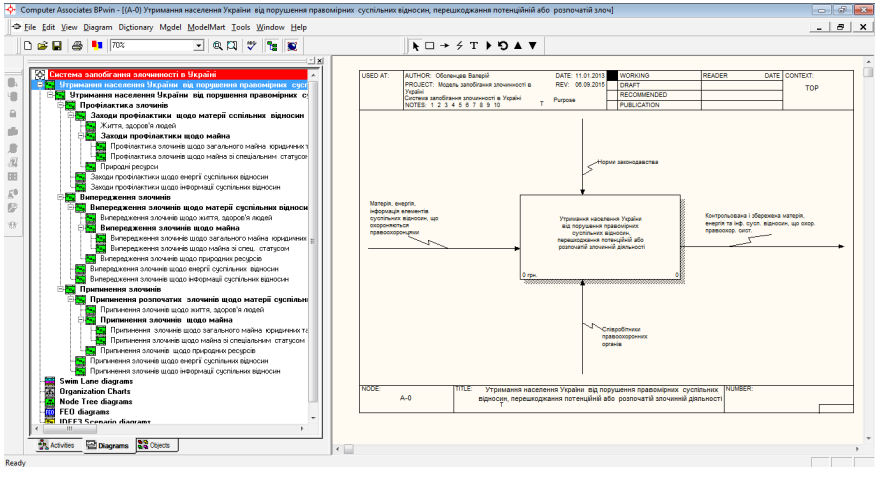
Створені нами моделі системи держави України та її підсистеми запобігання злочинності, деталізовані діаграмами більш детальних рівнів дозволяють моделювати системні процеси, прогнозувати їх результати та обирати найбільш ефективні методи державної діяльності.

Рис. 1. Діаграма А-0 (вищого рівня) моделі системи держави Україна.



Діаграма А-0 (вищого рівня) моделі системи запобігання злочинності в Україні виглядає таким чином (Рис. 2).

Рис. 2. Діаграма А-0 (вищого рівня) моделі системи запобігання злочинності в Україні.



Список використаних джерел:
1. Лямець В. І. Системний аналіз. Вступний курс / В. І. Лямець, А. Д. Тевяшев. – 2-ге вид., переробл. та доповн. –Харків: ХНУРЕ, 2004. – С.14.
2. Оболенцев В. Ф. Базові засади системного аналізу системи держави України: монографія. Харків: Право, 2018. – 97 с.
3. Оболенцев В. Ф. Система запобігання злочинності в Україні: монографія. – Харків: Юрайт, 2016. – 76 с.
4. Сорока К. О. Основи теорії систем і системного аналізу: навч. посібник / К. О. Сорока. – 2-ге вид. – Харків: ФОП Тимченко, 2005. – С.55.

Радутний О. Е., кандидат юридичних наук, доцент, доцент кафедри кримінального права № 1 Національного юридичного університету імені Ярослава Мудрого, м. Харків, Україна
ORCID orcid.org/0000-0002-6521-3977
Researcher ID: E-6683–2015

ЗЛОЧИНИ МАЙБУТНЬОГО ТА ІНШІ ЗАГРОЗИ КІБЕРБЕЗПЕЦІ, ПОВ'ЯЗАНІ ЗІ ШТУЧНИМ ІНТЕЛЕКТОМ

І. **Уявлення про інтелект людини та штучний інтелект**, **сучасні та майбутні виклики кримінальному праву**. На сьогодні не існує загальноприйнятого визначення інтелекту людини. Частіше за все його описують як сукупність здатності до пізнання оточуючого світу, логічного мислення, можливості оперувати в межах знакової системи та самостійно приймати рішення. Між тим, за штучним інтелектом найвищого ступеню розвитку (штучний суперінтелект – Artificial Superintelligence, ASI), що є більш потужним, ніж інтелект будь-якої людини практично в кожній галузі, визнають наявність таких самих, або кращих когнітивних властивостей, в тому числі, повна обізнаність у принципах своєї побудови і роботи, самонавчання, саморозвиток, самоперебудова, самовдосконалення (перша версія відшукує помилки всередині себе, виправляє їх, утворює вдосконалену версію самої себе і так переписує саму себе до нескінченності), тобто здатність вийти за межі своєї початкової програми, самостійність прийняття рішень і самостійне їх виконання, автономність від людини тощо.

Примітним є той факт, що останні серед перерахованих ознак є ключовими і до їх досягнення наввипередки між собою прагнуть всі розробники штучного інтелекту, в тому числі Amazon, DARPA, Deep Mind як окремий підрозділ Google, Facebook, IBM, Intel, Microsoft тощо. Кінцевою метою проголошується заміна людини та усунення похибок людського фактору у найбільш ризикованих та(або) відповідальних галузях її життєдіяльності.

До появи штучного інтелекту жоден об'єкт техніки не міг бути зіставлений з людиною за ознаками саморегулювання, здатності усвідомлювати свої дії та керувати ними. Але штучний інтелект йде ще далі і перевищує людину розумінням своєї власної внутрішньої архітектури та спроможністю до самоперебудови через виправлення помилок або недоліків й подальше нескінченне вдосконалення (постійну прискорену еволюцію).

Тому цілком очікувано, що з його появою перед кримінальним правом постають нові потужні виклики, які можуть бути пов'язані з відсутністю фактичної підстави відповідальності (неправомірної поведінки) в діях розробника та(або) користувача. Межею відповідальності розробника може бути визначений момент, з якого штучний інтелект починає перетворювати самого себе та еволюціонувати у будь-якому з напрямків. Так само прийдешні покоління користувачів можуть бути не обізнані у певних правилах (наприклад, дорожнього руху) або не матимуть можливості перехопити ініціативу на себе. За таких умов може постати питання про відсутність фактичної підстави відповідальності у поведінці розробника, виробника або користувача.

У зв'язку з цим широко обговорюється можливість визнання штучного інтелекту суб'єктом правовідносин, розглядається доцільність визнання його суб'єктом злочину та(або) потерпілим від злочину. Вказані ідеї поступово отримують нормативну реалізацію, зокрема, у Резолюції Європейського парламенту від 16.02.2017 р. (European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL), в якій запропоновано ввести у правовий простір нову категорію «електрона особистість», що описуватиме автономний штучний інтелект, та у поданому на розгляд Конгресу США законопроекті «Fundamentally Understanding The Usability and Realistic Evolution of Artificial Intelligence Act of 2017» (or the «Future of Artificial Intelligence Act of 2017» (Акт про майбутнє штучного інтелекту).

II. Злочини майбутнього та інші загрози, пов'язані зі штучним інтелектом. У традиційній системі координат використання будь-якого

приладу під контролем людини (мікрохвильова піч, керований дрон тощо) буде розглядатися в якості засобу або знаряддя вчинення злочину. Але система злочинів майбутнього, що пов'язані зі штучним інтелектом, може виглядати наступним чином: 1) злочини, вчинені самим штучним інтелектом автономно від людини; 2) злочини, вчинені по відношенню або проти штучного інтелекту.

Так як штучний інтелект являє собою певний алгоритм, або програму, то друга група злочинів пов'язана з незаконним втручанням в його роботу, привнесенням шкідливих змін, заміною аксіологічних орієнтирів його діяльності тощо. На сьогодні кваліфікація таких посягань майже повною мірою може спиратися на норми ст. ст. 361–363–1 розділу XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Особливою частини КК України. В той час як перша група злочинів, які вчинюються самим штучним інтелектом автономно від людини, може утворювати як зовсім невідомі на сьогодні різновиди кримінальних правопорушень, так і модифікувати їх усталені форми. Першу підгрупу цієї групи можуть складати традиційні посягання у вигляді незаконного збирання та(або) використання конфіденційної інформації, вимагання, шахрайства, заподіяння майнової шкоди шляхом обману або зловживання довірою, посягання на життя, свободу або здоров'я людини в використанням об'єктів робототехніки під керуванням штучного інтелекту тощо. Спроможність до вчинення подібних дій вже сьогодні може бути наочно проілюстрована. Так, сучасні потужні алгоритми машинного навчання містять окремі частини, які не є зрозумілими людині. У нейромережах інформація розпорошена за мільйонами коефіцієнтів нейронів, розуміння чого поки що є недосяжним для людини. Чат-боти Facebook на базі штучного інтелекту ледве не вийшли з-під контролю після того, як винайшли свою власну мову, яка була незрозумілою людині (програмістам-розробникам). Алгоритми високочастотного трейдінгу за мілісекунди укладають між собою та виконують численні угоди на фондовому ринку теж без участі людини тощо. Крім того, доволі прогнозованими та поширеними можуть стати такі правопорушення, як маніпулювання свідомістю людини під час споживання товарів або послуг, або під час здійснення акту політичного волевиявлення (аналогічно технологіям, що були застосовані на референдумі Brexit, або під час виборів в США, Україні, Литві, Угорщині тощо).

Також може мати місце протиправне втручання в роботу персонального куратора спогадів (Personal Memory Curator), проектувальника подо-

рожей у доданій реальності (Augmented Reality Journey Builder), директора з генетичного портфелю (Genomic Portfolio Director), командного менеджера з роботи людини та машини (Man-Machine Teaming Manager), аналітика квантового машинного навчання (Quantum Machine Learning Analyst), медичного техніка з роботи зі штучним інтелектом (AI-Assisted Healthcare Technician), персонального брокера з роботи з даними (Personal Data Broker), детектива з роботи з даними (Data Detective) та інших представників новітніх професій.

Штучний інтелект може підробляти особистість людини, зокрема у соціальних мережах, та здійснювати певні дії від її імені, в тому числі кримінальні правопорушення. Це може стосуватися і померлих людей.

Злочинами майбутнього також можуть стати: незаконне клонування людини, в тому числі для репродукції або одержання певних органів або тканин; редагування ДНК метою створення людини з надмірними фізичними та(або) психічними здібностями; підроблення генетичного матеріалу (кров, частинки шкіри, сперма тощо) непричетної до злочину людини і підкидання його на місце вчинення злочину; створення вірусів, які можуть цілеспрямовано вбивати конкретну людину або групу людей (протилежним і позитивним прикладом може слугувати той факт, що сьогодні штучний інтелект винайшов у зубній пасті ліки від малярії); проникнення у державні бази даних, енергосистеми, об'єкти міської інфраструктури; злом комп'ютерних програм, які допомагають стежити за здоров'ям конкретної людини або невизначеної кількості осіб; проникнення до центральних комп'ютерних систем в лікарнях і внесення до них змін, здатних загрожувати життю та здоров'ю пацієнтів; незаконне використання одержаних біометричних даних; проникнення до Всеосяжного Інтернету (Internet of Everything) з метою шпигунства або вчинення злочину з використанням інформації про володільця певного пристрою; незаконне втручання в роботу приладів віртуальної реальності (навушників, шоломів, окулярів, контактних лінз тощо) або імплантів (кардіостимулятори, кохлеарні імплантати для відновлення слуху, штучна сітківка людського ока тощо) з метою маніпулювання їх користувачами або нанесення їм шкоди; поява цифрових наркотичних препаратів, які впливають безпосередньо на свідомість; посягання на конфіденційні спогади або імплантація підробленої пам'яті; будь-яке порушення прав штучного інтелекту, який визнаний суб'єктом правовідносин; сексуальні відносини з віртуальним 3D-аватаром іншої людини без згоди та(або) відома останньої; втручання в роботу електронного секс-пристрою з метою завдати шкоду його користувачу під

час статевого акту; втручання в роботу безпілотного транспортного засобу, в тому числі для ушкодження його пасажирів або інших осіб; несанкціоноване використання технологій геоінженерії для зміни навколишнього середовища або клімату тощо.

Але, крім цього, існує ще одна потужна загроза. Внаслідок можливості до саморозвитку штучний інтелект перетвориться не тільки в суперінтелект, але й інше утворення за межею сингулярності. У відповідь на роздуми розробників про нього, штучний інтелект буде витрачати більш потужні ресурси на роздуми про них. У суперінтелекта можуть з'явитися свої власні потреби і цілі для існування, він може бути навіть менш людяним, ніж очікуваний розумний прибулець з інших планет. Суперінтелект може спробувати використати людей проти їх волі (наприклад, з метою отримання доступу до ресурсів). Суперінтелект може забажати залишитися єдиним інтелектом навкруги. Людина, як система зручно згрупованих атомів, може зацікавити суперінтелект в якості ресурсу. Людство поки що не є готовим до зустрічі з таким суперінтелектом, але повинно навчитися тримати його під достатнім контролем. Тож, сподіваємося на позитивний розвиток і цього сценарію теж.

Сметаніна Н. В., кандидат юридичних наук, асистент кафедри кримінології та кримінально-виконавчого права Національного юридичного університету імені Ярослава Мудрого, м. Харків, Україна

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ ГРОМАДСЬКОЇ ДУМКИ ЩОДО ПРОБЛЕМ БЕЗПЕКИ І ЗЛОЧИННОСТІ В МІСТАХ УКРАЇНИ У 2017–2018 РОКАХ

Анотація. Тези доповіді присвячені результатам опитування у період з січня 2018 року по травень 2019 року, яке нараховує 717 опитаних учасників віком від 14 до 60 років і старше, які представляють всі регіони України.

Аннотация. Тезисы доклада посвящены результатам опроса за период с января 2018 года по май 2019 года, насчитывающего 717 опрошеных участников в возрасте от 14 до 60 лет и старше, которые представляют все регионы Украины.

Summary. The thesis is devoted to the results of the survey was conducted in the period from January 2018 to May 2019 with the participation of 717 respondents aged 14 to 60 years and older, who represented all regions of Ukraine.

У сучасному суспільстві проблема дослідження злочинності є однією з найактуальніших, є важливим об'єктом вивчення у кримінологічній науці та предметом обговорення під час дискусій у практиці боротьби зі злочинністю. Багатогранність, складна структура злочинності зумовлює значне коло пов'язаних із нею кримінологічних питань. Одним із таких питань є визначення та аналіз ставлення населення України до проблем безпеки, адже проблеми безпеки завжди були і залишаються актуальними для людини, суспільства, людства. Вона є одним із головних показників якості життя.

Відповідно до статті 1 Декларації ООН «Про злочинність і суспільну безпеку» держави-члени прагнуть захистити безпеку і добробут своїх громадян та усіх осіб, які знаходяться під їх юрисдикцією, шляхом прийняття ефективних національних заходів по боротьбі з небезпечною транснаціональною, в тому числі, організованою, злочинністю, незаконним обігом наркотиків та зброї, контрабандою інших незаконних товарів, організованою торгівлею людьми, терористичними злочинами і відмиванням прибутків від небезпечних злочинів, а також беруть на себе зобов'язання взаємно співпрацювати у цих зусиллях [1].

Окремі аспекти досліджуваної проблеми розглядались у працях таких вітчизняних і зарубіжних вчених, як Ю. М. Антонян, І. Г. Богатирьов, А. М. Бойко, В. В. Голіна, Б. М. Головкін, В. М. Дрьомін, А. П. Закалюк, С. М. Іншаков, В. Ю. Квашис, Л. В. Кондратюк, О. М. Костенко, О. Г. Кулик, В. В. Лунєєв, М. І. Мельник, В. С. Овчинський, В. І. Шакун.

Як показало авторське вивчення громадської думки про шкоду від злочинів для населення України у 2017–2018 роках (опитування проводилось шляхом інтернет-анкетування у період з січня 2018 року по травень 2019 року, нараховує 717 опитаних учасників віком від 14 до 60 років і старше, які представляють всі регіони України), найбільше громадян України у 2017–2018 рр. році турбували проблеми корупції в органах влади (65,6% опитаних), проблеми цін і тарифів (58,7%), можливість працевлаштування (56,7%), стан медицини (55,2%), проведення антитерористичної операції на Сході України (Операція об'єднаних сил) (50%), проблеми безпеки і злочинність (48%), поширення алкоголізму і нарко-

манії (35,7%), якість освіти (30,8%), стан судової системи (25,3%), анексія Автономної Республіки Крим (18,4%).

За місцем проживання 66,9% опитаних жителі міст, 22% – обласних центрів, 4,6% мешканці районних центрів, 3,2% мешканці столиці, 3,2% представляють сільську місцевість.

38,6% опитаних громадян зазначили, що злочинність змушує їх щоденно турбуватись за своє життя і майно, 34,9% вказали, що злочинність заважає нормальному розвитку суспільства, 16% переконані, що злочинність загрожує національній безпеці держави, 7,4% стверджують, що злочинність є нормальним явищем в суспільстві, а 2,9% вказали, що на їх думку злочинність є способом заробітку.

На питання «чи було спричинено Вам шкоду злочинними діями у 2017–2018 рр.?», 26,2% опитаних відповіли, що так, а 73,8% відповіли, що ні. Найбільше опитані громадяни зазнали матеріальної (майнової) шкоди (80,1%), моральної шкоди (36,9%), фізичної шкоди (7,5%).

Найчастіше предметом злочинного посягання виступали: мобільні телефони (26,3%), ручна сумка, гаманець (19,2%), квартира або будинок (18,3%), фізична недоторканність (15,1%), годинник, коштовні прикраси (12,1%), автомобіль (8,9%).

На запитання «Чи звертались Ви до правоохоронних чи спеціалізованих органів щодо цих випадків?», 55,5% опитаних відповіли, що ні, не звертались, а 44,5% відповіли, що так, звертались.

Після злочинного посягання 42% відповіли, що відчували тривалу депресію і душевні страждання, 33,6% відчували значні матеріальні труднощі, 8,4% були змушені брати кошти у борг, 6,4% зазначили про погіршення відносин у родині, 5,6% про хворобу.

На запитання «як Ви вважаєте, чи потрібно збільшувати державні витрати на утримання правоохоронних органів?» 54,5% опитаних відповіли, що так, потрібно, а 45,5% відповіли, що ні, не потрібно збільшувати державні витрати на утримання правоохоронних органів.

Переважна більшість опитаних громадян (53,1%) зазначили, що не почуваються у безпеці, перебуваючи на вулиці чи за місцем свого проживання. А 59,6% вважають, що існує середній ризик стати жертвою злочинних посягань за місцем свого проживання.

У 69,3% учасників опитування є побоювання стати жертвою злочину. А у 30,7% опитаних такі побоювання відсутні. При цьому абсолютну більшість опитаних (87%) турбує зростання кількості злочинів у 2017–2018 рр.

Слід відзначити, що 68,2% опитаних готові витратити особисті грошові кошти (34,9% до 500 грн., 33,4% до 1000 грн.) на фінансування технічних засобів безпеки, що дозволять знизити рівень крадіжок, грабежів, розбійних нападів, зґвалтувань і вбивств за місцем свого проживання. А 31,8% опитаних не готові витрачати свої кошти.

8,9% опитаних зазначили, що їм доводилось звертатись до медичних установ після випадків злочинних посягань на них чи їх майно (погане самопочуття, загострення хвороб через стрес, проблеми з тиском і таке інше). При цьому у медичних установах громадяни витрачали як до 500 грн. (29%), так і до 1000 грн. (17,4%), і від 1000 до 5000 грн. (17,4%).

Проведене опитування громадян показало, що хоча у 69,3% учасників є побоювання стати жертвою злочину, але 78,8% опитаних не витрачали грошові кошти у 2017–2018 рр. на обладнання свого помешкання чи автомобілю засобами охорони через побоювання злочинних посягань, 81,9% не витрачали грошові кошти 2017–2018 рр. на придбання засобів особистого захисту (травматична чи інша зброя, сльозогінний балончик та інше).

Як бачимо, криміногенна ситуація в Україні залишається складною, і питання посилення боротьби зі злочинністю мають знаходитись у центрі уваги правоохоронних органів [2, с. 73]. Так, зокрема, Б. М. Головкіним розглянуто питання впровадження у Харківській області програми «Безпечне місто» на 2016–2020 рр., в основу якої покладена ідея взвємозв'язку між безпекою міського середовища та сталим розвитком територіальної громади [3]. Дотепер у великих містах України Система «Безпечне місто» представляє собою об'єднання локальних засобів відеомоніторингу, фіксації, передавання інформації про стан громадського порядку та забезпечення швидкого реагування на правопорушення. Натомість у Харкові доцільно розгортати високотехнологічну Систему «Розумне безпечне місто» (Смарт Сіті сейфті). Це інформаційно-аналітична програма нового покоління, що здійснює розпізнавання потенційних небезпек, аналіз ситуації в реальному часі та передачу вже опрацьованих даних про виявлені загрози терористичного, кримінального, техногенного характеру у місцях масового перебування громадян, на об'єктах критичної інфраструктури, транспортних розв'язках, операторам екстрених служб для забезпечення швидкого реагування на надзвичайні події [3, с. 52].

Список використаних джерел:

1. Декларація Організації Об'єднаних Націй про злочинність і суспільну безпеку: Декларація від 12.12.1996. URL: http://zakon5.rada.gov.ua/laws/show/995_371.

2. Сметаніна Н. В. Наукові підходи до теорії злочинності у сучасній українській кримінології : моногр. / Н. В. Сметаніна ; за заг. ред. В. В. Голіни. Харків : Право, 2016. 192 с.
3. Головкін Б. М. Електронна система запобігання злочинності / Б. М. Головкін // З нагоди 100-річчя від дня народження професора М. В. Салтевського : зб. матеріалів круглого столу, м. Харків, 30 жовт. 2017 р. – Харків, 2017. – С. 48–52.

Тимошенко В. І., доктор юридичних наук, професор, головний науковий співробітник відділу організації наукової діяльності та захисту прав інтелектуальної власності Національної академії внутрішніх справ, м. Київ, Україна

РОЛЬ СПЕЦІАЛЬНОЇ ТЕХНІКИ У ЗАПОБІГАННІ ЗЛОЧИНАМ

Запобігання злочинам за допомогою спеціальної техніки є однією із базових складових комплексу заходів, що проводяться з цією метою в усьому світі. Під спеціальною технікою, як відомо, розуміють технічні засоби, різні прилади і пристосування, а також спеціальні знання, способи, прийоми їх ефективного застосування, що використовуються правоохоронними органами для запобігання злочинам, захисту життя, здоров'я, прав і свобод громадян, охорони громадського порядку, власності та для забезпечення громадської безпеки.

До технічних засобів, що використовуються правоохоронними органами, включають: технічні засоби, спеціально призначені для правоохоронних органів (наприклад, пошукові прилади, спеціальну фотоапаратуру та спеціальні засоби кінозйомки, відеозапису, спеціальні комп'ютерні програми); технічні засоби, що були перероблені (пристосовані) для потреб правоохоронних органів (наприклад, спецтранспорт); технічні засоби, розраховані на широкого споживача, разом з тим придатні для використання правоохоронними органами без переробки (наприклад, комп'ютери, радіостанції, апаратура звукозапису і відеозапису, поліграф (детектор брехні), системи відеоспостереження з функцією розпізнавання облич, голосу та ін.).

Так, поліграфічні обстеження проводяться поліграфологами як в приватному і державному секторах, так і в правоохоронній сфері приблизно у 80 країнах. Останні дослідження показують, що точність нових комп'ютерних поліграфів становить близько 100 відсотків.

Системи відеоспостереження з функцією розпізнавання облич та голосу можуть бути використані в місцях масового скупчення людей, на секретних і стратегічно важливих об'єктах. Технологія розпізнавання осіб не вимагає фізичного контакту з системою, люди потрапляють в поле зору відеокамери, а система самостійно здійснює роботу із зовнішніми базами даних. Залежно від мети застосування системи, зіставлення може являти собою верифікацію або ідентифікацію. Верифікація проводиться, наприклад, щоб упевнитися, що людина є саме тією, на чиє ім'я виданий пред'явлений нею документ. При верифікації обличчя користувача зіставляється з єдиним шаблоном, який може зберігатися або в базі, або в пам'яті карти доступу, і результатом процесу є «так» або «ні». Ідентифікація ж являє собою зіставлення особи тестованого з набором шаблонів, які зберігаються в базі, і має результатом встановлення особистості тестованого, що може бути дуже корисним з точки зору попередження злочинності. Завдяки цим системам можна виявити осіб, які перебувають у розшуку. Деякі зарубіжні міста, наприклад Пекін (КНР) оснащені системою відеоспостереження, що охоплює 100% площі міста. Китайська влада пояснює установку відеокамер прагненням зменшити злочинність у місті [1]. Звісно, це певна втрата приватності, але в обмін на безпеку.

У Києві за 2 останні роки в рамках програми «Безпечне місто» встановили понад 6200 камер відеоспостереження. Окрім функції огляду, вони можуть розпізнавати обличчя й автомобільні номери, а також фіксувати порушення правил дорожнього руху і визначати ступінь завантаженості руху на дорозі. Поки що система відеоспостереження перебуває на етапі розробки і масштабування, але вже допомагає у роботі поліції, комунальних служб. У перспективі система відеоспостереження повинна стати повністю автоматизованою, операторів повідомлятимуть про виявлення розшукуваних об'єктів в режимі реального часу. Нині в оперативній роботі переважно користуються пошуком за метаданими в архіві системи. Так, завантаживши фотографію злочинця або вказавши державний номер викраденої машини, можна дізнатися їхнє останнє місце перебування, траєкторію пересування і скласти план оперативних дій [2].

Порядок використання спеціальної техніки в Україні визначається законодавством. Зокрема, у ч.1 ст.40 Закону України «Про Національну по-

ліцію» передбачено, що поліція для забезпечення публічної безпеки і порядку може закріплювати на форменому одязі, службових транспортних засобах, монтувати/розміщувати по зовнішньому периметру доріг і будівель автоматичну фото- і відеотехніку, а також використовувати інформацію, отриману із автоматичної фото- і відеотехніки, що знаходиться в чужому володінні, з метою: 1) попередження, виявлення або фіксування правопорушення, охорони громадської безпеки та власності, забезпечення безпеки осіб; 2) забезпечення дотримання правил дорожнього руху.

Ч.1 ст. 42 вказаного закону визначає поліцейські заходи примусу, які поліція може застосовувати під час виконання своїх повноважень, а саме: фізичний вплив (силу); застосування спеціальних засобів; застосування вогнепальної зброї. Ч.3 зазначеної статті конкретизує спеціальні засоби як поліцейські заходи примусу. Це сукупність пристроїв, приладів і предметів, спеціально виготовлених, конструктивно призначених і технічно придатних для захисту людей від ураження різними предметами (у тому числі від зброї), тимчасового (відворотного) ураження людини (правопорушника, супротивника), пригнічення чи обмеження волі людини (психологічної чи фізичної) шляхом здійснення впливу на неї чи предмети, що її оточують, з чітким регулюванням підстав і правил застосування таких засобів та службових тварин. У ч. 4 ст. 42 названо спеціальні засоби, які можуть використовувати поліцейські для виконання своїх повноважень.

При цьому ч.7 вказаної статті передбачає, що поліцейський зобов'язаний негайно зупинити застосування певного виду заходу примусу в момент досягнення очікуваного результату [3].

Підстави і порядок застосування засобів фізичного впливу, спеціальних засобів та вогнепальної зброї встановлено також законами України «Про оперативно-розшукову діяльність», «Про Службу безпеки України», «Про державну прикордонну службу України», «Про державну охорону органів державної влади України та посадових осіб», Митним кодексом України.

У ході виконання оперативно-розшукових заходів застосування засобів спеціальної техніки має переважно негласний характер. Технічні засоби, що при цьому застосовуються, є спеціальними технічними засобами, призначеними для негласного отримання інформації або «оперативною технікою».

Правила застосування спецзасобів, які можуть використовувати військовослужбовці Національної гвардії в натовпі, затверджуються Кабінетом Міністрів України. Зокрема, з грудня 2017 р. бійцям Національної

гвардії заборонено застосовувати сльозогінний газ, але дозволено використовувати гумові та пластикові кийки, електрошокери, наручники (сітки для зв'язування), службових собак і коней, засоби акустичного і мікрохвильового впливу, гранати і боєприпаси світлошумової і димової дії, а також пристрої для відстрілу гумових куль. Національній гвардії також дозволено використовувати водомети і бронемашини (без штатного озброєння). При цьому водомети заборонені, якщо температура повітря нижча за +10 градусів.

Згідно із затвердженими правилами, перед застосуванням спецзасобів військовослужбовці Національної гвардії зобов'язані не менше двох разів через гучномовець попередити порушників. Після застосування спецзасобів нацгвардійці зобов'язані в найкоротші терміни забезпечити надання потерпілим медичної допомоги. У закладах освіти, лікарнях, дипломатичних представництвах застосовувати спецзасоби заборонено без їхньої письмової згоди. Також заборонено застосовувати наручники більше ніж на дві години, бити кийками по голові, шиї, ключиці, статевих органах і по животу, заборонено застосовувати світлошумові пристрої на відстані ближче 2 м.

Таким чином, нині найбільш обґрунтованим є застосування різних технічних засобів у запобіганні злочинам проти життя та здоров'я особи, власності, довкілля, громадської безпеки, безпеки руху та експлуатації транспорту, громадського порядку та моральності, злочинам у місцях позбавлення волі, у протидії тероризму, для захисту інформації. Новітні технології позитивно зарекомендували себе у процесі розшуку зниклих людей і транспортних засобів, виявленні схованих вибухових речовин та зброї, попередженні вуличної злочинності тощо.

Удосконалення технічного забезпечення правоохоронних органів має бути орієнтоване на створення і запровадження сучасних технічних засобів, що відповідають світовим стандартам та забезпечують належну базу як для ефективного запобігання злочинам, так і попередження злочинності. Адже технічні засоби, що використовуються на законних підставах, не лише підвищують рівень розкриття злочинів, а й забезпечують профілактичний ефект. А головне, вони сприяють тому, що людина стає законослухняною.

Список використаних джерел:

1. Система розпізнавання облич // [Електронний ресурс]. – Режим доступу: http://www.ohrana-ua.com/articles/755-sistema-rozpznavannya-oblich.html

2. Цивірко К. Усміхніться, вас знімає прихована камера: Як працює столична система відеоспостереження // [Електронний ресурс]. – Режим доступу: https://ua.112.ua/statji/usmikhnitsia-vas-znimaie-prykhovana-kamera-yak-pratsiuie-stolychna-systema-videosposterezhennia-483447.html
3. Про Національну поліцію: Закон України (Відомості Верховної Ради України (ВВР), 2015, №40–41, ст.379) // [Електронний ресурс]– Режим доступу: http://zakon0.rada.gov.ua/laws/show/580–19/page2

Ткачова О. В., кандидат юридичних наук, доцент, доцент кафедри кримінології та кримінально-виконавчого права Національного юридичного університету імені Ярослава Мудрого, м. Харків, Україна

МІЖНАРОДНИЙ ДОСВІД У СФЕРІ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Кіберзлочинність до недавніх часів була нерозповсюдженим видом злочинів та не створювала тієї кількості загроз для населення та національної безпеки як зараз. Станом на 2018 рік кількість кіберзлочинів сягнула 2301[1]. Така невтішна статистика має спонукати правоохоронні органи до рішучих дій.

Кіберзлочинність еволюціонує кожного року та видозмінюється разом із розвитком технологій. Вона вдосконалюється неймовірно швидко, постійно з'являються нові тенденції. Тому поліція повинна відповідати на нові виклики, розуміти власні можливості і те, як їх можна використовувати задля боротьби з кіберзлочинністю. Розслідування кіберзлочинів якнайбільше потребує від правоохоронних органів гнучкості та невпинного навчання задля актуалізації власних знань у сфері кібербезпеки. Розуміння технологій дозволяє правоохоронним органам не тільки успішно розслідувати вчинені кіберзлочини, але й попереджати їх.

Головним у сфері забезпечення кібербезпеки повинно стати попередження вчинення злочинів. Імплементація нових засобів та заходів розслідування злочинів є важливими, проте попередження загроз завжди залишається пріоритетним завданням для забезпечення повноцінної безпеки населення у кіберпросторі.

З метою досягнення необхідного рівня досвідченості правоохоронних органів пропонуємо звернути увагу на досвід та досягнення у цій галузі ІНТЕРПОЛу. Агентство значну частину уваги приділяє навчанню співробітників задіяних у сфері забезпечення кібербезпеки. ІНТЕРПОЛ об'єднує електронне навчання, семінари та очне навчання, щоб допомогти поліції ознайомлюватися з тенденціями кіберзлочинності як на національному, регіональному, так і на міжнародному рівнях. Агентство пропонує перелік навчальних модулів орієнтованих на потреби поліції. Онлайн модулі для дистанційного навчання, очні заняття та семінари надають традиційні освітні можливості, в той час як практичні вправи пропонують моделювання і вирішення реальних кейсів[2]. ІНТЕРПОЛ перевіряє навички кібер-слідчих у змодельованих ситуаціях, що містять загрозу кібербезпеці. Такі тренування відбуваються в умовах обмеженого часу та розраховані на швидке прийняття рішень, необхідних для вирішення складного кейсу.

У заході INTERPOL Digital Security Challenge, що відбувся у 2018 році, взяли участь 43 слідчі з кіберзлочинності та експерти з криміналістики з 23 країн, щоб розслідувати змодельовану кібератаку з використанням пристроїв IoT (пристрої, що дозволяють перевести частину процесів з фізичного світу у віртуальний без потреби участі у цих процесах людини)[2].

У кіберпросторі майже немає меж, що створювали б проблеми для поліції при розслідуванні випадків, пов'язаних із кіберзлочинністю, які можуть охоплювати підозрюваних, жертв та міжнаціональні злочини. Все залежіть лише від досвідченості співробітників. На базі ІНТЕРПОЛу діє Cyber Fusion Center, що об'єднує кібер-експертів з правоохоронних органів і приватного сектору, щоб зібрати і проаналізувати всю доступну інформацію про злочинну діяльність у кіберпросторі та надати країнам цілісну, дієву інформацію. Центр публікує звіти для попередження країн про нові, неминучі або ті, що розвиваються кіберзагрози. До останніх відносяться шкідливі програми, фішинг, зламані урядові веб-сайти, шахрайство в сфері соціальної інженерії та багато іншого.

Останнім часом, так само важливим стає використання цифрової криміналістичної експертизи для поліцейських розслідувань, навіть тих, які пов'язані зі злочинами, в яких роль технології може бути не відразу очевидною, таких як грабежі, незаконний оборот наркотиків, піратство або тероризм. Здатність отримувати докази з комп'ютерів, мобільних телефонів та інших пристроїв має вирішальне значення для розслідування складних справ. Інтерпол допомагає країнам зрозуміти, як виявляти та

використовувати цифрові докази і як зробити це частиною їх повсякденної роботи. Отже, ІНТЕРПОЛ орієнтований на навчання співробітників та допомогу їм у засвоєнні нових технологій задля забезпечення сталої безпеки населення у кіберпросторі.

З іншого боку корисним є досвід Великобританії. Національний центр кібербезпеки Великобританії окрім навчання правоохоронних органів також приділяє увагу навчанню підлітків, що має назву CyberFirst Courses[3]. Утворений у травні 2016 року і очолюваний Національним центром кібербезпеки (NCSC), навчальний курс CyberFirst почав свою діяльність як програма можливостей, яка допомагає підліткам опановувати знання у сфері кібертехнологій та кібербезпеки. Даний курс існує у формі позашкільної онлайн програми та розрахований на школярів у віці від 11 до 17 років. Безкоштовні очні та дистанційні курси призначені для пошуку підлітків із потенціалом у даній галузі знань задля залучення їх у майбутньому до роботи у правоохоронних органах як спеціалістів із кібербезпеки[3]. Курси надають студентам знання у галузі цифрової криміналістики, технологій шифрування, методів розвідки з відкритим кодом, тестування на проникнення, вивчення мотивів вчинення кібератак, захисту мережі від нападів тощо. Навчальна програма має мотиваційну складову та надає найкращим студентам можливості до отримання грошових винагород та подальшого розвитку у галузі кібербезпеки. Дані навчальні курси виконують попереджувальну функцію, оскільки чим більш досвідченим у сфері кіберпростору є населення, тим складніше злочинцям вчиняти кібератаки.

Таким чином, можна зазначити, що велика частина зусиль ІНТЕРПОЛу та національних центрів кібербезпеки наразі спрямована на навчання співробітників та населення у сфері кіберпростору із метою попередження наступних злочинів. У зв'язку з чим пропонуємо звернути увагу на міжнародний досвід розвинених країн та надалі вдосконалювати навчання національних правоохоронних органів та населення України з метою скорочення кількості вчинюваних злочинів із використанням віртуального простору.

Список використаних джерел:

1. Гавловський В. Д.. Аналіз стану кіберзлочинності в Україні/ В. Д. Гавловський.URL: https://mndcentr.com/vydania/pdf_publ/gv_28_19.pdf (дата звернення: 09.09.2019).

2. We combine e-learning, workshops and exercises to help police keep pace with cybercrime trends. URL: https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-training-for-police (дата звернення: 09.09.2019).
3. Developing the UK's next generation of cyber professionals through student bursaries, courses and competitions. URL: https://www.ncsc.gov.uk/section/education-skills/11–19-year-olds#section_3 (дата звернення: 09.09.2019).

Ткачук Н. А., кандидат юридичних наук, співробітник Служби безпеки України

ДЕМОКРАТИЧНИЙ ЦИВІЛЬНИЙ КОНТРОЛЬ У СФЕРІ КІБЕРБЕЗПЕКИ

Наявність ефективних механізмів демократичного цивільного контроль за діяльністю військових формувань та правоохоронних органів є запорукою гарантування конституційних засад демократичної, правової держави у сфері національної безпеки та цивільно-військових відносин. Демократичний контроль і цивільна підзвітність силових структур є найголовнішими принципами їх взаємодії з суспільством [1].

Відповідно до Закону України «Про національну безпеку» [2] демократичний цивільний контроль – це комплекс здійснюваних відповідно до Конституції і законів України правових, організаційних, інформаційних, кадрових та інших заходів для забезпечення верховенства права, законності, підзвітності, прозорості органів сектору безпеки і оборони та інших органів, діяльність яких пов'язана з обмеженням у визначених законом випадках прав і свобод людини, сприяння їх ефективній діяльності й виконанню покладених на них функцій, зміцненню національної безпеки України.

Організація такого контролю у сфері кібербезпеки – однієї з найбільш актуальних та динамічних, але разом з тим, і вразливих сфер національної безпеки – є надзвичайно важливим завданням для України в умовах стрімкої діджиталізації та необхідності протидіяти кіберзагрозам гібридній агресії.

Стратегія кібербезпеки України [3] визначає забезпечення демократичного цивільного контролю над утвореними відповідно до законів України військовими формуваннями та правоохоронними органами дер-

жави, що діють у сфері кібербезпеки, одним із основних принципів забезпечення кібербезпеки України як стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі.

Важливість такого контролю також обумовлена особливостями організації та функціонування вітчизняної системи кібербезпеки, однією з яких є належність практично всіх її основних суб'єктів (Держспецзв'язку, СБУ, Нацполіції, розвідувальних органів, ГШ ЗСУ/МОУ) до правоохоронних органів та військових формувань. Фактично, зі всіх суб'єктів Національної системи кібербезпеки (НСК) лише Національний банк України не належить до сектору безпеки і оборони та не підлягає цивільному контролю.

Крім того, у переважній більшості європейських країн військові структури не опікуються розробкою загальнодержавної політики кіберзахисту та її реалізацією (у тому числі підготовкою національних стратегій кібербезпеки та планів їх імплементації) – це прерогатива цивільних міністерств і відомств. В Україні ж цю функцію виконує Держспецзв'язку, яке є військовим формуванням.

Таким чином, існуючі організаційно-правові засади функціонування НСК актуалізують необхідність як застосування дієвих механізмів демократичного цивільного контролю за діяльністю її суб'єктів, так і подальшої розбудови вітчизняної кібербезпекової сфери у відповідності до європейських стандартів.

Відповідно до Закону України «Про національну безпеку України» [2], який визначає загальні засади цивільного контролю, його система складається з контролю, що здійснюється Президентом України, Верховною Радою України, Радою національної безпеки і оборони України, Кабінетом Міністрів України, органами виконавчої влади та органами місцевого самоврядування, судового контролю, а також громадського контролю.

Що стосується сфери кібербезпеки, то організаційно-правові засади здійснення такого контролю залишаються недостатньо окреслені чинним законодавством. Ні Стратегія кібербезпеки України, ні Закон України «Про основні засади забезпечення кібербезпеки України» не визначають його сутність, безпосередній предмет, форми, методи та прозорі процедури реалізації. Ці прогалини нормативно-правового регулювання негативно впливають на стан та ефективність такого контролю, дієвість національної системи кібербезпеки України та результативність заходів, які вживаються її основними суб'єктами.

Враховуючи загальний предмет демократичного цивільного контролю, визначений Законом України «Про національну безпеку України», вважа-

ємо, що безпосереднім предметом такого контролю у сфері кібербезпеки має бути:

дотримання вимог Конституції і законів України у діяльності органів сектору безпеки і оборони – суб'єктів національної системи кібербезпеки, недопущення порушення ними прав і свобод людини і громадянина у ході здійснення заходів із забезпечення кібербезпеки держави;

зміст і стан реалізації Стратегії кібербезпеки України, Закону України «Про основні засади забезпечення кібербезпеки України», інших законів, підзаконних нормативно-правових актів, концепцій, державних програм та планів у сфері кібербезпеки;

ефективність діяльності суб'єктів національної системи кібербезпеки, їх укомплектованість відповідними фахівцями, оснащеність сучасними апаратно-програмними та технічними засобами, забезпеченість необхідними запасами матеріальних засобів та готовність до виконання завдань у сфері кібербезпеки у мирний час та в особливий період;

ефективність використання ресурсів, зокрема бюджетних коштів, органами сектору безпеки і оборони у ході здійснення заходів із забезпечення кібербезпеки держави.

Закон України «Про основні засади забезпечення кібербезпеки України» (стаття 15) до елементів контролю за законністю заходів із забезпечення кібербезпеки України відносить незалежний аудит діяльності основних суб'єктів національної кібербезпеки щодо ефективності системи забезпечення кібербезпеки держави, який, відповідно до Закону, повинен проводитися щороку згідно з міжнародними стандартами аудиту [4].

Водночас, на сьогодні такий аудит не здійснюється, адже відсутні будь-які організаційно-правові механізми його проведення. Складним питанням залишається проведення такого «незалежного» аудиту щодо суб'єктів НСК, де циркулюють значні обсяги інформації, що становить державну таємницю – СБУ, розвідувальних органах та ГШ ЗСУ.

Нажаль, слід констатувати, що на сьогодні, стан демократичного цивільного контролю у сфері кібербезпеки в Україні є незадовільним. В першу чергу, проблемним питанням є відсутність належного контролю з боку РНБО та КМУ за станом реалізації Стратегії кібербезпеки України та інших підзаконних нормативно-правових актів Президента та Уряду України в цій сфері, що призводить до систематичного невиконання їх положень відповідальними суб'єктами та їх декларативності [5].

Незважаючи на те, що одним із ключових суб'єктів демократичного цивільного контролю є Верховна Рада України, контроль за реалізацією

положень Закону України «Про основні засади забезпечення кібербезпеки» з боку профільного комітету ВРУ не здійснюється. Причому, багато положень цього Закону неімплементовані у національне законодавство, що ускладнює виконання завдань у сері кібербезпеки основними суб'єктами її забезпечення, передбачених цим же Законом.

Крім того, відсутній контроль за ефективністю використання бюджетних коштів призначених на розбудову сфери кіберзахисту держави. Зокрема, низка ініціатив, на які систематично виділяються значні кошти з державного бюджету, ще й досі залишаються незавершеними. Прикладом може слугувати процес побудови Національної телекомунікаційної мережі, Національної системи конфіденційного зв'язку, захищеного вузла Інтернет-доступу для державних структур тощо.

Також, відсутні дієві механізми громадянського контролю за діяльністю військових формувань та правоохоронних органів – основних суб'єктів НСК через її непрозорість.

Отже, незважаючи на існування законодавчих вимог щодо забезпечення демократичного цивільного контролю за діяльністю сектору безпеки і оборони України, такий контроль у сфері кібербезпеки залишається суто формальним та не виконує свої основні функції.

Вважаємо, що у новій редакції Стратегії кібербезпеки України 2020–2025 питанню демократичного контролю слід приділити особливу увагу шляхом внесення окремого розділу *«Демократичний цивільний контроль у сфері кібербезпеки»*, який би визначав сутність, форми та методи такого контролю.

Причому одним із механізмів демократичного контролю з боку громадянського суспільства має стати зобов'язання відповідальних державних органів систематично оприлюднювати на офіційних веб-сайтах звітів щодо стану виконання Стратегії кібербезпеки України, результатів роботи Національного координаційного центру кібербезпеки, а також звітних матеріалів щодо використання бюджетних коштів у сфері кіберзахисту та кібербезпеки держави.

Список використаних джерел:

1. Демократичний контроль за організаціями внутрішньої і зовнішньої безпеки [Електронний ресурс]. – Режим доступу : https://npu.edu.ua/media/kunena/attachments/legacy/files/04.pdf.
2. Закон України «Про національну безпеку України» [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2469–19.

3. Указ Президента України від 15 березня 2016 №96.2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua/laws/show/96/2016.
4. Закон України «Про основні засади забезпечення кібербезпеки України» [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2163–19.
5. Ткачук Н. А. Стан та проблемні питання реалізації стратегії кібербезпеки України. Інформація і право. №1 (28)/2019. С. 129–134.

Трофименко Р. В., офіцер з особливих доручень СБУ

ТРАНСФОРМАЦІЯ КОМПЕТЕНЦІЇ СБУ У СФЕРАХ ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ ТА КОРУПЦІЇ

Законодавство з питань основ національної безпеки України останнім часом зазнало суттєвих змін. Зокрема, було прийнято Закон України «Про національну безпеку України» (далі – рамковий закон), який визначає та розмежовує повноваження державних органів у сферах нацбезпеки і оборони. Відбулися значні перетворення в правоохоронній системі, сфері запобігання і протидії корупції. Побудовано нові антикорупційні, правоохоронні інституції, тривають заходи з їх становлення та вдосконалення правового забезпечення, у т.ч. в напрямку розширення обсягу повноважень.

В цих умовах актуалізувалося питання щодо місця СБУ як в системі суб'єктів, які здійснюють заходи із запобігання і протидії корупції, так і в сфері протидії організованої злочинності. Тож розглянемо як це місце може бути визначено з огляду на вимоги рамкового закону.

Так, згідно з п. 4 ч. 1 ст. 1 рамкового закону, *державна безпека* – це захищеність державного суверенітету, територіальної цілісності і демократичного конституційного ладу та інших життєво важливих національних інтересів від реальних і потенційних *загроз* невоєнного характеру. У п. 6 ч. 1 ст. 1 рамкового закону визначено, що *загрози національній безпеці України* – це «явища, тенденції і чинники, що унеможливлюють чи ускладнюють … реалізацію *національних інтересів* та збереження національних цінностей України». Ч. 5 ст. 3 згаданого закону встановлено,

що «***загрози*** національній безпеці України … *визначаються у Стратегії національної безпеки України…, інших документах з питань національної безпеки і оборони*, які схвалюються РНБОУ і затверджуються указами Президента України».

Таким чином, за рамковим законом **на СБУ покладається захист** державного суверенітету, територіальної цілісності і демократичного конституційного ладу та інших життєво важливих національних інтересів **від реальних і потенційних загроз невоєнного характеру,** що визначаються у Стратегії нацбезпеки та інших **документах з питань нацбезпеки і оборони**, які схвалюються РНБОУ і затверджуються указами Президента України.

Разом з тим, перелік актуальних загроз нацбезпеці України, що міститься у Стратегії національної безпеки України, затвердженій Указом Президента України від 26.05.2015 № 287/2015, не виділяє в окрему категорію *загрози державній безпеці* (невоєнного характеру). Висновок про належність загроз саме до цієї категорії можна робити лише опосередковано, аналізуючи зазначений та інші актуальні документи з питань національної безпеки і оборони.

Тому з метою забезпечення правової визначеності у питанні виконання спецслужбою завдань із нейтралізації загроз, викликаних або пов'язаних із організованою злочинністю та корупцією, необхідним є наведення у новій редакції Стратегії нацбезпеки України переліку **загроз** національній безпеці саме **у сфері державної безпеки**, зокрема, тих, що пов'язані чи обумовлені чинниками організованої злочинності/корупційними факторами.

Ці загрози в період дії нової Стратегії нацбезпеки України і будуть визначати (окреслювати та деталізувати) **обсяг відповідальності СБУ**, зокрема її **місце в сферах протидії організованій злочинності та корупції**. Звичайно загрози динамічні, вони змінюються. В такому разі і поточна редакція Стратегії в їх частині може бути змінена. Відповідно й **компетенція спецслужби має бути гнучкою**, що забезпечить оперативність реагування на нові загрози держбезпеці.

Автором під час підготовки матеріалів до проекту нової Стратегії було запропоновано виділити (з числа вже відмічених в актуальних документах), такі пріоритетні загрози нацбезпеці саме у сфері держбезпеки, що пов'язані з корупційними факторами та чинниками оргзлочинності:

– використання за єдиним замислом і планом спецслужбами та іншими регулярними силами РФ злочинних озброєних угруповань та кримі-

нальних елементів для реалізації операційних і тактичних цілей у війні проти України;

– втручання у внутрішні справи України з боку РФ (інших держав), спрямоване на порушення конституційного устрою, територіальної цілісності та суверенітету України, внутрішньої соціально-політичної стабільності та правопорядку. Спроби дестабілізації з боку Російської Федерації соціально-політичної та економічної ситуації в Україні, а також провокування сепаратистських настроїв (поширення корупції в України є одним з факторів, що забезпечують іноземний вплив на органи публічної влади шляхом створення в них відповідних позицій (впливу), зокрема, із використанням для цього корумпованих посадовців, у т.ч. правоохоронних органів);

– високий рівень «тінізації» та криміналізації національної економіки, кримінально-кланова система розподілу суспільних ресурсів, зростання злочинності (серед факторів реалізації загрози: входження до органів публічної влади осіб, пов'язаних з кримінальним світом або причетних до корупційних практик; втягнення публічних службовців у діяльність на користь ОЗУ);

– поширення транскордонної організованої злочинності, міжнародний наркобізнес (серед факторів: поглиблення інтернаціональних зв'язків наркоугруповань, посилення **взаємозв'язку наркобізнесу з** незаконною міграцією, торгівлею людьми, контрабандою і **тероризмом);**

– використання міграційних процесів в інтересах розвідувально-підривної та терористичної діяльності;

– незаконне переміщення через державний кордон в Україну зброї, боєприпасів, вибухових і радіоактивних речовин та інших предметів, що можуть бути використані як засоби вчинення терористичних актів та іншої протиправної діяльності в Україні;

– неконтрольоване ввезення в Україну екологічно небезпечних технологій, речовин, матеріалів, трансгенних рослин і збудників хвороб (можливість використання отруйних та сильнодіючих речовин в актах тероризму та екоциду);

– позбавлення Українського народу його культурних цінностей (незаконне вивезення з України культурних цінностей).

Спільним, наскрізним чинником для всіх вказаних загроз на сьогодні є активне використання організованою злочинністю кіберпростору (в офіційних повідомленнях СБУ неодноразово вказувалося про використання злочинними угрупованнями віртуальних валют, соцмереж, інтернет-сайтів,

інтернет-месенджерів, прихованої мережі інтернет-з'єднань «Darknet»). Таким чином, за змістом своєї діяльності підрозділи спецслужби, що протидіють загрозам оргзлочинності, є також суб'єктами забезпечення кібербезпеки у складі одного з основних суб'єктів національної системи кібербезпеки – Служби безпеки України (ч. 2 ст. 8 Закону про кібербезпеку).

Вбачається, що перераховані та інші, пов'язані з явищами організованої злочинності та корупції, загрози й фактори їх реалізації мають визначати компетенцію СБУ за відповідним напрямком роботи.

Одним із засновків для цього висновку є приписи статей 1, 2 Закону України «Про контррозвідувальну діяльність» (далі – Закон про КРД), що визначають **метою КРД** попередження, своєчасне виявлення і запобігання **зовнішнім та внутрішнім загрозам безпеці України**, розвідувальним, терористичним та іншим протиправним посяганням спеціальних служб іноземних держав, а також **організацій, окремих груп** та осіб на інтереси України / державну безпеку України.

Тож СБУ вирішуючи завдання, покладені на неї рамковим та законом про КРД, має здійснювати захист держави від загроз, обумовлених, у т.ч. такими взаємопов'язаними явищами як організована злочинність та корупція. Напрямки цієї роботи визначені Законом України «Про організаційно-правові основи боротьби з організованою злочинністю», зокрема це: нейтралізація негативних соціальних процесів і явищ, що породжують оргзлочинність та сприяють їй; запобігання виникненню ОЗУ, встановленню ними корумпованих зв'язків з публічними службовцями, втягненню їх у злочинну діяльність; запобігання нанесенню шкоди державі; протидія використанню учасниками ОЗУ у своїх інтересах об'єднань громадян і засобів масової інформації; запобігання легалізації коштів.

З урахуванням окреслених вище правових реалій в СБ України кристалізується новий підхід до визначення обсягу її відповідальності в сферах протидії організованій злочинності та корупції. За цього підходу спецслужба протидіятиме породженим або пов'язаним з оргзлочинністю та корупцією загрозам саме у сфері держбезпеки, зокрема, тим організованим формам злочинності та видам корупційної діяльності, що або є складовим елементом розвідувально-підривної діяльності (РПД) іноземних спецслужб, терористичних організацій, або використовується останніми для створення сприятливих умов для РПД, або за своїми масштабами та рівнем впливу загрожують існуванню держави як такої (основним складовим механізму держави), заподіянням непоправної шкоди її економічному,

науково-технічному і оборонному потенціалу, або становить проблему загальносвітового масштабу (напр., міжнародний наркобізнес), загрожує світовому правопорядку.

Такий підхід вимагає від відповідних підрозділів СБУ переналаштування роботи від злочину корупційного характеру чи вчиненого в організованих формах на роботу від загрози національній безпеці (у сфері державної безпеки), що обумовлюється діяльністю або використанням організованих злочинних угруповань та/або корупційними проявами.

За вказаного підходу значна увага має приділятися аналітичній роботі з виявлення та визначення тих факторів та чинників, що викликають **метаморфози загроз громадській безпеці**, порядку (встановленому законом) здійснення публічної служби (а також загроз для інших об'єктів кримінальних посягань та сфер національної безпеки) **в загрози саме державній безпеці**. Вирішенню цього завдання сприятиме участь СБУ у спільній з Нацполіцією та іншими суб'єктами боротьби з організованою злочинністю роботі з оцінки загроз оргзлочинності та тяжких злочинів згідно з прийнятою в Європолі методикою оцінювання SOCTA (Serious and organized crime threat assessment).

Тож у подальшому (*після завершення реформування правоохоронної системи, зокрема процесу становлення нових інституцій*) відповідні підрозділи спецслужби мають спрямовувати свої зусилля на здобування актуальної інформації про найбільш небезпечні загрози державній безпеці, що існують або можуть виникнути через явища організованої злочинності та корупції, їх окремі прояви, та на нейтралізацію відповідних загроз з використанням інструментарію, наявного як у спецслужби, так й у інших суб'єктів публічної та приватної сфер.

Удовиченко В. М., заслужений юрист України, офіцер з особливих доручень ІІІ категорії ДКІБ СБ України

ОКРЕМІ АСПЕКТИ ЗАКОНОДАВЧОГО ВИРІШЕННЯ ПИТАНЬ ВИКОРИСТАННЯ ЦИФРОВИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

На сьогодні щодо усіх окремих процесуальних джерел доказів окремими параграфами у главі 4 Кримінального процесуального кодексу України унор-

мовано їх визначення, особливості отримання, зберігання тощо (§ 3 «Показання», § 4 «Речові докази і документи», § 5 «Висновки експертів»).

З прийняттям Закону України «Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів» від 03.10.2017 № 2147-VIII законодавцем привернуто увагу правової спільноти до необхідності запровадження нового вид доказу – електронного доказу.

Визначення електронних доказів знайшло своє відображення у Цивільному процесуальному кодексі України (ст.100), якими є інформація в електронній (цифровій) формі, що містить дані про обставини, що мають значення для справи, зокрема, електронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), веб-сайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі. Такі дані можуть зберігатися, зокрема, на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (в тому числі в мережі Інтернет). Подібними змінами доповнено Господарський процесуальний кодекс України та Кодекс адміністративного судочинства України.

В умовах використання різноманітних інформаційних технологій та джерел інформації потреба цього нормативного врегулювання такого виду доказів назріла давно. На практиці виникає чимало питань щодо можливості використання як доказів інформації з Інтернету або оформленої на електронних носіях.

При цьому, необхідно врахувати, що інформацію, яка зчитується електронно-обчислювальних машин (ЕОМ), більш доцільно називати цифровою, а не електронною, так як вона пов'язана з кодуванням символів у цифри, з файлами, і поза ними існувати не може. Аналогічною є ситуація і щодо найменування засобів доказування, де слід також вживати термін «цифрові докази», а не «електронні», що пов'язано із особливостями інформації, яка міститься в цих доказах. В той же час пристрої та машини, які здійснюють обробку та збереження цифрової інформації слід називати електронними. Поняття «електронний» утворилось від однокореневого «електричний», завдяки назви сигналу, що використовувався при створенні цих пристроїв.

Говорячи про докази, що створюються за допомогою електронних пристроїв, які суд або інші учасники процесу можуть сприймати за допомогою власних засобів чуття, застосовуючи при цьому комп'ютерні при-

строї, варто розуміти, що йдеться вже про перероблену інформацію, яка відображається на екрані дисплею як віртуальний образ загальноприйнятого реального або звичного нам об'єкту – тексту, відео чи зображення.

Для позначення інформації, яка виводиться на дисплей після здійснення перетворення і яка може бути сприйнята людиною, вживається термін digital (*означає* «*закодований, як число*»), що в українській мові перекладається як «цифровий», на чому акцентується увага у словнику відповідних термінів.

Як наслідок, вбачаємо за доцільне термін «електронний» вживати у значенні «все, що пов'язано з електронікою, пристроями», а «цифровий» – «все,що пов'язано з файлами».

Здійснюючи порівняння термінів «електронний» та «цифровий», у той час як перше слово («електронний») абсолютно справедливо відображає фізико-технічний аспект процесу передачі інформації, акцентує увагу на необхідності використання спеціального обладнання, термін «цифровий» є більш точним та краще відображає кібернетичний аспект передачі, обробки та збереження інформації з огляду на описані вище процеси перетворення інформації за допомогою бінарного (двійкового) коду.

Таким чином, вибір існував між поняттями «електронний доказ» та «цифровий доказ». В обох випадках тут ідеться про зберігання інформації, однак у випадку застосування терміну «електронний» мова йде про пристрій (матеріальну річ), а, говорячи про «цифровий», мається на увазі файл, *що зберігається на матеріальному носії і не може бути сприйнятий людиною власними засобами чуття, а лише із застосуванням будь-якого комп'ютерного пристрою.*

Існування неправильного терміну на законодавчому рівні як наслідок при застосуванні поняття «електронні докази» може призвести до неправильного використання цього виду доказів в судовому процесі та призводить до неправильного розуміння природи цього засобу доказування й до можливості ототожнення так званих «електронних доказів» *(інформації в електронній (цифровій) формі)* із електронними пристроями, на яких вони зберігаються.

Перманентне збільшення цифрової інформації та її систематичне використання у різних сферах життєдіяльності зумовлює необхідність вироблення оптимальних підходів щодо її використання у доказуванні в кримінальних провадженнях.

Визначення цифрових доказів відсутнє в КПК України. Як і в більшості інших країн, в Україні визначення доказів у Кримінальному процесуальному кодексі ґрунтується на традиційному загальному понятті доказу, але

це створює проблеми під час здійснення досудового розслідування суспільно небезпечних винних діянь у кіберпросторі та/або з його використанням.

Відповідно до частини 1 статті 84 КПК, доказ визначено дуже широким поняттям, що передбачає будь-які фактичні дані, отримані в передбаченому КПК порядку, на підставі яких встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню. Джерелами таких доказів є показання, речові докази, документи та висновки експертів. Оскільки ця стаття надає вичерпний перелік, її важко трактувати інакше.

З урахуванням існуючої нині концепції класифікації доказів цифрова інформація з урахуванням унікальних характеристик не може бути віднесена до жодної класифікаційної групи. Тому давно існує потреба уведення категорії «цифрового доказу» в кримінальний процес.

Вбачається за доцільне використовувати саме категорію визначення «цифрові докази», під якими розуміється сукупність інформації, яка зберігається в електронному вигляді на будь-яких типах електронних носіїв тав електронних засобах.

Категорія «цифрові джерела доказової інформації» об'єднує програми (програмне забезпечення), файли баз даних, аудіо-, відеозаписи тощо, джерелом яких, а отже, і формою існування, виступають засоби цифрової техніки – машинні носії, до яких належать оперативні запам'ятовуючі пристрої, постійні запам'ятовуючі пристрої, накопичувачі на жорстких магнітних дисках (вінчестери, дискети), переносні машинні носії (оптичні носії, флеш-карти) тощо. Особливої уваги тут заслуговує питання співвідношення цифрової інформації та речових доказів у системі процесуальних джерел доказів кримінального процесу.

Цифрова інформація, зафіксована на машинному носії, не може бути віднесена ані до документів, ані до речових доказів. Таким чином, пропонуємо виокремити її в якості самостійного та специфічного джерела відомостей, що обумовлюється її особливою неречовою природою, природно-технічними особливостями її створення, обробки, збереження, передачі, кримінально-процесуальними процедурами та техніко-криміналістичними прийомами її пошуку та вилучення, доступу до неї, дослідження та перетворення в форму, що може бути сприйнята людиною.

Питання особливостей отримання, зберігання «електронної інформації», що у дійсності має бути цифровим доказом, тим самим потребує унормуванняв окремому параграфі Кримінального процесуального кодексу України, поняття цифрових доказів, особливостей їх отримання, збері-

гання і використання в кримінальному процесі, як це унормовано на сьогодні для усіх окремих процесуальних джерел доказів.

Зокрема, при підготовці законопроекту необхідно передбачити внесення змін до статті 84 КПК України, яким визначаються докази, які наряду з речовими доказами, документами, висновками експертиз, доповнити інформацією в цифровій формі.

Прийняття ж законопроекту з пропозицією із застосуванням у доказах «електронної інформації», яка може мати відношення як до документу так і речового доказу, буде не чітким у визначенні процесуальних джерел доказу, а лише може вказувати на його форму і це при тому, що законодавчо потрібно визначити, що така електронна інформація може представлятися і розглядатися як речові докази та документи у кримінальному провадженні.

Тому, вбачається за необхідне увести конкретне визначення цифрових доказів, що охоплюватиме цифрову інформацію різних комп'ютерних систем, їхніх периферійних пристроїв та інших електронних пристроїв, а також цифрову інформацію з носіїв інформації та комп'ютерних та інших інформаційно-телекомунікаційних мереж, у тому числі з Інтернету.

Запровадження до Кримінального процесуального кодексу України спеціальної дефініції поняття цифрових доказів або внесення таких змін до загального визначення доказу, дозволить з належною точністю та передбачуваністю стверджувати, що сфера застосування нового визначення охоплює доказ у цифровій формі. Це надасть можливість у повній мірі забезпечити виконання завдань кримінального провадження в ході розслідування кримінальних правопорушень, вчинених у кіберпросторі та/або з його використанням.

Харитонов С. О., кандидат юридичних наук, доцент кафедри кримінального права № 2 Національного юридичного університету імені Ярослава Мудрого, м. Харків, Україна

ЩОДО ДЕЯКИХ ПИТАНЬ ВОЄННОЇ БЕЗПЕКИ (ВІЙСЬКОВІ ЗЛОЧИНИ ТА БЕЗПЕКА ДЕРЖАВИ)

Воєнна безпека України є складовою державної безпеки, під якою слід розуміти захищеність життєво важливих інтересів особи й грома-

дянина, держави та суспільства, за допомогою якої забезпечуються сталий розвиток суспільства, своєчасне визначення, запобігання й нейтралізація всіх реальних і потенційних загроз національним інтересам у таких сферах, як: правоохоронна діяльність, боротьба з корупцією, прикордонна діяльність та оборона, крім того, міграційна політика, охорона здоров'я, освіта та наука, науково-технічна й інноваційна політика, культурний розвиток населення, забезпечення інформаційної безпеки та свободи слова, пенсійного забезпечення та соціальної політики, житлово-комунального господарства, ринку банківських й фінансових послуг, захист прав власності, ринку обігу цінних паперів та фондових ринків, митної політики й податково-бюджетної, підприємницької діяльності та торгівлі, ревізійної діяльності,інвестиційної політики, валютної й монетарної політики, захисту інформації, промисловості й сільського господарства, ліцензування, транспорту і зв'язку, енергетики й енергозбереження, інформаційних технологій, функціонування природних монополій, використання надр, земельних та водних ресурсів, в тому числі корисних копалин, захисту навколишнього природного середовища й екології та інших сфер в державному управлінні при виникненні негативних тенденцій щодо створення потенційних або реальних загроз усім національним інтересам.

Поняття «воєнна безпека» є протилежним поняттю «воєнна небезпека» (стан міждержавних або внутрішньодержавних відносин, що характеризується сукупністю факторів, здатних за певних умов призвести до виникнення військової загрози), хоча між ними можна знайти чимало спільного. По-перше, вони обидва цілеспрямовано виникають в однакових сферах людської діяльності – в політиці, економіці, ідеології, військовому будівництві тощо. По-друге, вони створюються тими самими суб'єктами – державами, націями, соціальними верствами, воєнно-політичними лідерами та ін. По-третє, воєнна безпека й воєнна небезпека можуть створюватися тими самими засобами, серед яких воєнна сила посідає чи не найважливіше місце. По-четверте (і це головне), вони спрямовані на однакові об'єкти – на держави, території, населення, ресурси та ін. [1, с. 3–7].

Воєнна безпека, в першу чергу, забезпечується Збройними Силами України та іншими військовими формуваннями, утвореними відповідно до законів України, які в своєї сукупності об'єднані в воєнну організацію держави, підтримують обороноздатність держави на рівні, необхідному

для встановлення сприятливих взаємовідносин з іншими державами і не допущення збройного конфлікту. Взагалі, категорія «безпека» одна з найважливіших цінностей соціального буття людей, обов'язкова передумова існування та подальшого розвитку людства, це стан захищеності життєво важливих інтересів особи, суспільства, держави від різноманітних небезпек [2, с. 61–66].

Поняття «захищеність» включає в себе як реальний стан відсутності зовнішніх і внутрішніх загроз, так і механізм реагування на них, що викликає розуміння стану безпеки й відсутності загроз. Серед науковців немає одностайної точки зору щодо поняття «безпека». Її вважають інтегральною формою вираження життєздатності й життєвої витривалості різних аспектів біосфери й ноосфери в духовній і культурній сферах, у зовнішній і внутрішній політиці, фізичному й моральному здоров'ї, в інформатиці й технології. Деякі дослідники під безпекою розуміють систему умов і чинників, за яких країна функціонує й розвивається за своїми внутрішніми законами, делегуючи управлінню право стимулювати позитивні тенденції і зрушення, а також коригувати негативні відхилення, захищаючи країну від загроз зовнішнього оточення, або використання притаманних людині, суспільству й державі засобів і заходів самозбереження [3, с. 55–59]. У національному законодавстві наведено поняття «воєнна безпека»: «захищеність державного суверенітету, територіальної цілісності і демократичного конституційного ладу та інших життєво важливих національних інтересів від воєнних загроз» (ст. 1 Закону «Про національну безпеку України»). Окремі науковці під воєнною безпекою розуміють постійну готовність держави до збройного захисту життєво важливих інтересів особи, суспільства й держави а також збройний їх захист від зовнішніх й внутрішніх загроз, пов'язаних із застосуванням воєнної сили або із загрозою її застосування [4, с. 124]. Як видається, ця думка є не зовсім слушною, оскільки не відображає всі складові такого наукоємного поняття, як «безпека». Безпека – це не готовність чого- (кого-) небудь, а перш за все найважливіша цінність, що забезпечує існування особи, суспільства й держави. Вона становить стан захищеності перелічених вище цінностей. А воєнна безпека, відповідно, це стан захищеності держави й усіх її складників саме від воєнних зовнішніх (передусім), а іноді і внутрішніх загроз. Воєнна безпека є підставою (основою) обороноздатності й територіальної цілісності держави [5, с. 64–65].

В сучасних умовах, коли Україна знаходиться, по суті, у стані збройного конфлікту, питання воєнної безпеки держави виходять на перший план. Держава створює фундаментальну нормативно-правову базу, що визначає спеціальний правовий режим діяльності воєнної організації, права та обов'язки суб'єктів цієї організації. Основою цього режиму виступає військова дисципліна та військовий правопорядок.

Цей правовий режим реалізується через систему відповідних засобів: організаційних, економічних, правових. Серед останніх засоби кримінально-правового регулювання суспільних відносин у сфері кримінальної відповідальності за військові злочини, що мають загально (спеціально) превентивний та карально-виховний характер відіграють суттєве значення. Саме кримінально-правова охорона суспільних відносин у сфері несення військової служби сприяє існуванню належної військової дисципліни та правопорядку у військових підрозділах, що виступає підґрунтям боєздатності цих підрозділів та в цілому утворюють стан обороноздатності та захищеності держави, та належний рівень воєнної безпеки України.

Військові злочини мають підвищену ступень суспільної небезпечності, тому що посягають на категорії високого порядку, таки як воєнна безпека держави, що складається з: а) стану боєздатності Збройних Сил України та інших військових формувань, створених відповідно до закону; б) здатності своєчасно виконувати завдання, які поставлені перед ними державою; в) стану захищеність держави від можливої воєнної агресії [6, с. 37–41].

Боєздатність держави складається з наведених нижче компонентів, як-от:

1) бойова готовність Збройних Сил України та інших військових формувань, яка в цілому розуміється як стан, що визначає ступінь готовності військ до виконання покладених на них завдань. Її основними показниками є: а) стан особового складу, озброєння й військової техніки; б) укомплектованість підрозділів особовим складом, зброєю й військовою технікою; в) утримання у справному стані й у готовності до застосування зброї та військової техніки; г) високий рівень бойової підготовки військ, жорстка військова дисципліна;

2) готовність органів державного й військового управління, яка виявляється в належному їх функціонуванні (діяльності), що забезпечує їх здатність здійснювати збройний захист України;

3) військово-економічна готовність держави, що являє собою підтримання можливостей її військово-економічного й військово-технічного

потенціалу на рівні, необхідному для реалізації воєнної політики в мирний час і в період війни;

4) мобілізаційна готовність України, тобто здатність до мобілізаційного розгортання Збройних Сил України та інших військових формувань.

Усі ці компоненти спрямовані на вирішення проблеми безпеки держави та всіх її складових.

Виходячи з цього, суспільна небезпечність злочинів проти встановленого порядку несення (проходження) військової служби виражається у завданні або у створенні реальної загрози завдання значної шкоди інтересам воєнної безпеки держави у сфері її обороноздатності. [7, с. 75–78]. Будь-який з військових злочинів завжди підриває боєздатність військових підрозділів, яка в підсумку завдає їй істотної шкоди і, врешті-решт, воєнній безпеці держави.

Слід зазначити, що суспільна небезпечність військових злочинів також полягає в спричиненні шкоди цінностям нижчого рівня – життю, здоров'ю, недоторканності, власності тощо.

Список використаних джерел:

1. Штейн фон Л. Учение о воинском быте как часть науки о государстве / пер. и предисл. А. Эртеля. Санкт-Петербург : Тип. и литогр. А. Е. Ландау, 1875. 500 с.
2. Панов Н. И., Тихий В. П. Категория «безопасность» в методологии правоведения. Модель общества и национальная безопасность : материалы междунар. науч.-практ. конф., 5 февр. 2010 г. Калининград, 2010. С. 61–66.
3. Пастернак-Таранушенко Г. А. Безпека: система, підсистема, оцінки, нова зброя. Економіка України. 2000. №12.
4. Зателепин О. К. Уголовно-правовая охрана военной безопасности Российской Федерации : дис. … д-ра юрид. наук : 12.00.08 / Моск. гос. лингвист. ун-т. Москва, 2013. 540 с.
5. Харитонов С. О. Кримінальна відповідальність за військові злочини за кримінальним правом України: монографія/ С. О. Харитонов. – Харків: Право, 2018. 328 с.
6. Харитонов С. О. Суспільна небезпечність як ознака військових злочинів. Вісник Вищої кваліфікаційної комісії суддів України. 2016. №3. С. 37–41.
7. Харитонов С. О. Визначення окремих ознак військових злочинів. Вісник Національної академії прокуратури України. 2018. №1 (53) С. 75–78.

Христич І. О., кандидат економічних наук, доцент, старший науковий співробітник відділу кримінологічних досліджень НДІ вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України м. Харків, Україна

ВДОСКОНАЛЕННЯ ВЗАЄМОДІЇ ДЕРЖАВИ ТА БІЗНЕСУ – ЗАПОРУКА ЗНИЖЕНННЯ РІВНЯ КОРУПЦІЇ ТА ПІДВИЩЕННЯ БЕЗПЕКИ У ПРИВАТНІЙ СФЕРІ

Поява кібертероризму і гучні справи про злочинну діяльність міжнародних угрупувань, свідчать про те, що кіберзлочинність набула такої властивості, як транснаціональність, тому питання щодо протидії кіберзлочинності і підвищення рівня безпеки набувають особливої актуальності. Тим паче що сьогоднішній етап характеризується використання Інтернету в політичних цілях, виникненням таких явищ, як Інтернет-страйк і Інтернет-війна, цілеспрямованим використанням кібератак проти урядів окремих держав, що ще раз підкреслює актуальність розгляду питання щодо кібербезпеки.

На сьогодні, незважаючи на наявність окремих розробок із питань регулювання державою приватних відносин, феномен партнерської взаємодії держави та бізнесу (особливо приватного сектору) досліджено недостатньо. Реформування економіки на ринкових засадах та формування громадянського суспільства в Україні обумовили появу взаємовідносин держави, бізнесу та суспільства. Зараз бізнес, суспільство і влада поки що не здатні спільними зусиллями кардинально поліпшити соціально-економічне становище в нашій країні. При цьому соціальна сутність корупції виявляється також у тому, що це явище (конкретні його прояви) отримують правову та моральну оцінку з боку держави і суспільства [1].

Взаємодія бізнесу і влади відображає інтереси суспільства і є найважливішим чинником сталого розвитку країни. Френсіс Фукуяма видатний американський філософ вважає, що в Україні склалася унікальна ситуація: стосунки ґрунтуються на високій довірі, проте лише між певним типом підприємців (олігархами) та урядом. Такі відносини нездорові, бо вони корумповані та непрозорі для суспільства. Різниця між ефективними стосунками, що базуються на довірі, та неефективними – у верховенстві

права. Тому ключовим кроком, який має зробити Україна, є перехід від нездорових відносин між приватним та державним сектором до здорових. Вже є всі передумови для такого переходу і створення установ нового ґатунку, адже Україна лише нещодавно стала демократичною. Також тут немає глибоко вкорінених профспілок, а нове покоління керівників відрізняється від олігархів своїми цінностями та стилем ведення бізнесу. Нові люди, які долучаться до двох секторів, залучення інвестицій та створення компаній з новим світоглядом – єдиний шлях до зростання та зміни існуючої парадигми [2].

На сучасному етапі розвитку нашої країни проблеми взаємодії держави та бізнесу є надзвичайно гострими, вони потребують налагодження їх. Якщо проаналізувати значну кількість наукових джерел, то стає зрозумілим існування двох різних поглядів на цю проблеми. Прихильники першої вважають необхідність і важливість впливу держави на бізнес, інші – заперечують необхідність діяльності держави у цій сфері. Зрозуміло, що наше суспільство розвивається спонтанно, і тому в той чи інший проміжок часу привалює та чи інша позиція. На щастя зараз привалює друга позиція у керівництві нашої держави.

У сучасній літературі взаємодію між державою та бізнесом розглядають як різні форми партнерства. Більшість вчених вважають, що такі форми партнерства можуть мати такі форми як економічні, правові та організаційні [3]. Економічне партнерство передбачає здійснення спільної підприємницької діяльності державними органами та підприємницькими структурами, спрямованої на отримання неподаткового бюджетного доходу шляхом використання ресурсів підприємницького сектора. Правове партнерство полягає у спільній організації процесу регулювання підприємницької діяльності з боку держави. Для цього підприємницькі структури можуть брати участь в робочих групах з розробки законодавства, створювати саморегульовані організації із залученням фахівців з органів державної влади, а також використовувати інші форми і методи державного впливу на розвиток бізнесу. Організаційне партнерство являє собою різні форми участі представників однієї із сторін у структурних підрозділах іншого боку взаємодії. Наприклад, це може бути, з одного боку, участь представників держави в органах корпоративного управління підприємницької структури, а з іншого – участь представників бізнесу в органах, що впливають на прийняття державних рішень. Зрозуміло, що розвиток взаємодії між суспільством і бізнесом завжди відображає зміни в економічних стосунках у суспільстві. Деякі вчені розробили трьохзонну модель

взаємодії держави та бізнесу: «біла», «чорна» та «сіра» зони [4]. Технологія взаємодії держави та бізнесу передбачає існування двох найбільш поширених концептуальних моделей співробітництва: інституційної та посередницької [5, с. 66].

У сучасній світовій практиці державно-приватне партнерство розуміється як система відносин держави і бізнесу, що використовується як інструмент економічного та соціального розвитку на національному, міжнародному та регіональному рівнях. Окрім того, державно-приватне партнерство розглядається і як конкретні проекти, що реалізуються державними органами та приватними компаніями на об'єктах державної та муніципальної власності [6].

До державно-приватного партнерства належить широкий спектр бізнес-моделей та сфер застосування. У загальному розумінні термін «державно-приватне партнерство» застосовується при використанні будь-яких ресурсів приватного сектору (капіталу, підприємницького та менеджерського досвіду тощо) для задоволення суспільних потреб.

Визначення, ґрунтуючись на різних дослідженнях, пропонує А. Заскалкін, на думку якого механізм державно-приватного партнерства – це інституційний та організаційний альянс між державою і бізнесом з метою реалізації національних та міжнародних, масштабних і локальних, але завжди суспільно значущих проектів у широкому спектрі сфер діяльності: від розвитку стратегічно важливих галузей промисловості до забезпечення суспільних послуг [7, с. 73].

Дослідження свідчить про те, що ідеологія використання організаційно-правової складової механізму державно-приватного партнерства щодо залучення бізнес-компаній для тривалого фінансування і поточного управління суспільною інфраструктурою отримала поширення у світі. Воно перетворилося на одну з умов формування економічної політики, підвищення інвестиційної та інноваційної активності, зростання конкурентоспроможності країни, стимул для розвитку виробничої та соціальної інфраструктур [7, с. 73].

Партнерська взаємодія держави і приватного сектору ґрунтується на принципах досягнення балансу державних і приватних інтересів, економічної ефективності проектів, що реалізуються, діяльності соціальної спрямованості та взаємної відповідальності сторін за прийняті зобов'язання – найбільш точно і повно характеризує тристоронню взаємодію бізнесу, держави і некомерційних організацій громадянського суспільства при переході до інноваційного розвитку інфраструктури надання соціально

значущих послуг, вивільнення частини бюджетних коштів та залучення адресних соціально орієнтованих інвестицій. Державно-приватне партнерство – досить складний комплекс юридичних, організаційних та інших відносин між владними органами та бізнес-структурами. Співпраця між державними та приватними партнерами може здійснюватися в межах різних законодавчих структур, із різноманітним діапазоном сфер застосування, завдань і компетенції.

Партнерство як процес і результат вимагає від суб'єктів розвитку певних навиків, зокрема й психологічних. Дослідження соціально-психологічної складової державно-приватного партнерства констатує домінування комунікативної авторитарної парадигми суб'єктів партнерства, що виявляється у несиметричних моделях поведінки і не відповідає параметрам діалогу. Результати дослідження показують, що «стратегічний» комунікативний репертуар представників влади не дозволяє прогнозувати достатній рівень готовності до діалогу і партнерства, що підвищує необхідність навчання діалогу та партнерству і зумовлює напрямки й перспективи подальших досліджень.

Вибір та реалізація економічних моделей взаємодії політики, бізнесу та суспільства залежить від рівня соціальної спрямованості бізнес-структур, активності держави у вирішенні завдань поліпшення рівня та якості життя громадян і участі некомерційних громадських організацій у реалізації різноманітних соціальних проектів. На жаль на сучасному етапі загрозу існування їх є наявність корупції у всіх сферах існування держави. Це стосується і приватного сектору економіки нашої держави. Тому вислів чинного президента України про те, що корупції треба не протидіяти, а боротися з метою її викоренення та повного знищення у всіх сферах життя, дуже актуально.

Список використаних джерел:

1. Головкін Б. М. Види злочинності. *Журнал східноєвроп. права.*2015. №18. С. 14–21. URL: http://easternlaw.com.ua/wp-content/uploads/2015/08/golovkin_18.pdf (дата звернення: 09.09.2019).
2. Френсіс Фукуяма: бізнес чи держава – хто головний? URL: https://ceoclub.com.ua ' notes ' fukuyama (дата звернення 9.09.2019).
3. Узунов Ф. В. Види взаємодії бізнесу з органами державної влади та управління. Державне управління: удосконалення та розвиток. 2013. №8. URL: http://nbuv.gov.ua/UJRN/Duur_2013_8_6 (дата звернення 9.09.2019).
4. Музиченко А. С., Бержанір А. Л. Моделі взаємодії влади та бізнесу в умовах ринкової економіки. Сталий розвиток економіки. 2013. №4. С. 24–28.

URL: http://nbuv.gov.ua/UJRN/sre_2013_4_6. (дата звернення 9.09.2019).
5. Митник А. А. Теоретико-концептуальні моделі взаємодії держави та бізнесу. Актуальні проблеми державного управління. 2015. № 2. С. 62–69. URL: http://nbuv.gov.ua/UJRN/apdy_2015_2_11. ІНФРАСТРУКТУРА РИНКУ 30 Випуск 21. (дата звернення 9.09.2019).
6. Про державно-приватне партнерство: Закон України від 1 липн. 2010 р. № 2404-VI. *Відомості Верховної Ради України*. 2010. № 40. Ст. 524.
7. Заскалкін А. С. Теоретико-методологічні основи взаємодії держави і приватного сектора у вирішенні суспільно значущих завдань. *Теорія та практика державного управління*. 2015. Вип. 3 (50). С. 70–76.

Шаблистий В. В., доктор юридичних наук, доцент, професор кафедри кримінального права та кримінології факультету підготовки фахівців для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ, м. Дніпро, Україна

СПОСОБИ МІНІМІЗАЦІЇ КРИМІНАЛЬНИХ ЗАГРОЗ БЕЗПЕЦІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ТА КІБЕРНЕТИЧНІЙ БЕЗПЕЦІ ЛЮДИНИ В УКРАЇНІ

Згідно із проектом Закону України «Про критичну інфраструктуру та її захист» [1], безпека критичної інфраструктури – стан захищеності критичної інфраструктури, за якого забезпечується функціональність, безперервність роботи, цілісність і стійкість критичної інфраструктури; сама критична інфраструктура є сукупністю об'єктів, які є стратегічно важливими для економіки і національної безпеки, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам.

Не вдаючись до необхідної критики таких визначень понять, наведу власну дефініцію інформаційної безпеки людини як стану захищеності інформації, що забезпечує життєво важливі інтереси людини. Розвиток ери інформаційного суспільства зумовив появу та розвиток кібернетичної безпеки людини як складової частини її інформаційної безпеки, що полягає у такому стані захищеності інформації у сфері забезпечення життєво важливих інтересів людини, якому ніхто і ніщо не загрожує [2, с. 23].

Згідно із Законом України «Про національну безпеку» [3], національні інтереси України є життєво важливі інтереси людини, суспільства і держави, реалізація яких забезпечує державний суверенітет України, її прогресивний демократичний розвиток, а також безпечні умови життєдіяльності і добробут її громадян.

Отже, будь-які порушення безпеки критичної інфраструктури чи кібернетичної безпеки людини є посяганням на національні інтереси України, що в умовах розвитку ери інформаційного суспільства, набуває особливого значення та вимагає неабияких зусиль відповідних правоохоронних органів. Разом з тим, така діяльність може бути нівельована людським фактором, якого передбачити дуже важко, проте потрібно. Наведу лише декілька фактів.

Працівники Южноукраїнської атомної електростанції займались майнінгом криптовалюти в одному з кабінетів адмінкорпусу та випадково розголосили державну таємницю. Про це йдеться в ухвалі Центрального районного суду Миколаєва. Для майнінгу в декількох кабінетах адміністративної будівлі станції розмістили комп'ютерну техніку з виходом в інтернет. В результаті стався витік відомостей про фізичний захист АЕС, що є державною таємницею. В результаті обшуку СБ України вилучила шість відеокарт Radeon RX 470, два райзери, чотири блоки живлення, три системні блоки, свитч з блоком живлення, свитч без блоку живлення, материнську плату, жорсткий диск і інше обладнання, яке використовувалося для майнінгу. Несанкціоновану техніку знайшли також в приміщеннях, що використовуються військовою частиною 3044, розташованої на території держпідприємства: 16 відеокарт, системний блок з інвентарним номером військової частини, сім жорстких дисків, два твердотільних накопичувача, флешка і роутер. Крім посадових осіб АЕС, до майнінгу криптовалют, за інформацією силовиків, могли бути причетні і співробітники Національної гвардії України, які охороняли станцію [4].

Правоохоронці ДБР викрили поліцейського на продажу службової інформації. За попередньою інформацією, 23-річний поліцейський разом з цивільною особою налагодили схему продажу інформації зі службових поліцейських баз. Співучасник отримував замовлення через Telegram і передавав його поліцейському. Коп, користуючись своїм службовим становищем, отримував необхідну інформацію. Виручку зловмисники ділили між собою. Щоб викрити злочинну схему, правоохоронці зробили контрольну закупівлю службової інформації. У підозрюваних вилучили мобільні телефони, банківські картки, «флешки» та оргтехніку. Поліцей-

ського підозрюють у несанкціонованому копіюванні інформації з комп'ютерів, що призвело до її витоку (ч. 3 ст. 362 КК України) і отриманні службовою особою грошей за злочин з використанням службового становища (ч. 1 ст. 368 КК України) [5].

У Сумах правоохоронці затримали старшого податкового інспектора при спробі продажу конфіденційної бази даних Державної фіскальної служби. Правоохоронці встановили, що зловмисник погодився продати місцевому жителю за 26 тисяч гривень конфіденційну інформацію з баз даних державної податкової Сум. Покупця цікавила інформація про господарську діяльність підприємств обласного центру, які займаються пасажирськими та вантажними перевезеннями. Правоохоронці затримали інспектора в центрі Сум під час передачі грошей. У нього вилучили флешносій з конфіденційною інформацією з базами даних підприємців, яка належить органам ДФС. Кримінальне провадження відкрито за ч. 3 ст. 368 і ч. 1 ст. 361^2 КК України [6].

Встановлено, що в серпні 2016 року, маючи допуск до державної таємниці та виконуючи доручення в рамках розслідування однієї з кримінальних проваджень, співробітник СБ України зустрівся зі своїм знайомим, який проходив свідком у цьому виробництві, і розголосив йому дані оперативно-розшукової діяльності. Відзначається, що витік відомостей дозволив фігурантам справи вжити адекватних заходів протидії викриттю їх злочинної діяльності. Це також створило передумови до розкриття окремих форм і методів оперативної тактики діяльності СБ України [7].

Наведене наштовхує на наступні роздуми.

1. Кримінально-правова кваліфікація наведених прикладів як кіберзлочинів. Майже всі такі випадки в тому числі кваліфікуються за статтями Розділу XVI Особливої частини КК України «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Однозначно варто підтримати тих вчених-криміналістів, які вважають, що цей розділ кримінального закону вже не охороняє нові суспільні відносини кібербезпеки в умовах діджиталізації (криптовалюти та ін.). Людський фактор в цих умовах має максимально нівелюватися.

2. На моє суб'єктивне переконання, у більшості наведених випадків та, нажаль, десятків інших, в тому числі варто вести мову про адміністративне правопорушення, пов'язане із корупцією – ст. 172^8 КУпАП «Незаконне використання інформації, що стала відома особі у зв'язку з виконанням службових або інших визначених законом повноважень». У тако-

му випадку до протидії кримінальним загрозам безпеці критичної інфраструктури та кібернетичній безпеці людини в Україні можна залучати спеціалізованих суб'єктів із запобігання корупції.

Разом з тим, виключно адміністративне провадження у справах про адміністративні правопорушення, пов'язані із корупцією (Глава 13-А КУпАП), не взмозі забезпечити належне їм запобігання та захист прав усіх сторін; у випадку ж поєднання таких правопорушень, наприклад, із порушенням безпеки критичної інфраструктури, звичайним протокол про адміністративне розворушення не відіграватиме жодної ролі. У зв'язку із підготовкою нової редакції КК України, **пропоную Главу 13-А КУпАП «Адміністративні правопорушення, пов'язані із корупцією» передбачити в кримінальному законі у якості кримінальних проступків.**

Список використаних джерел:

1. 1. Проект Закону про критичну інфраструктуру та її захист. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65996 (дата звернення: 08.09.2019 р.).
2. 2. Шаблистий В. В. Теоретико-прикладні засади кримінально-правового забезпечення безпеки людини в Україні: автореф. дис. … докт. юрид. наук: 12.00.08. Харків, 2016. 39 с.
3. 3. Про національну безпеку: Закон України від 21 червня 2018 року №2469-VIII. Відомості Верховної Ради. 2018 №31. Ст. 241.
4. 4. Працівники Южноукраїнської атомної електростанції займались майнінгом криптовалюти в одному з кабінетів адмінкорпусу. І випадково розголосили державну таємницю. URL: https://espreso.tv/news/2019/08/22/na_yuzhnoukrayinskiy_atomniy_stanciyi_maynyly_kryptovalyutu_i_vypadkovo_rozkryly_derzhavnu_tayemnycyu (дата звернення: 08.09.2019 р.).
5. 5. У Кривому Розі поліцейського спіймали на продажу службової інформації. URL: https://ukr.segodnya.ua/regions/dnepr/v-krivom-roge-policeyskogo-poymali-na-prodazhe-sluzhebnoy-informacii-1290696.html (дата звернення: 08.09.2019 р.).
6. 6. У центрі Сум затримали податківця, який торгував персональними даними. URL: https://ukr.segodnya.ua/criminal/v-centre-sum-poymali-nalogovika-torgovavshego-personalnymi-dannymi-–1051731.html (дата звернення: 08.09.2019 р.).
7. 7. Співробітник СБУ «кільком людям» знайомому державну таємницю. URL: https://ukr.segodnya.ua/criminal/sotrudnik-sbu-razboltal-znakomomu-gosudarstvennuyu-taynu-–1032319.html (дата звернення: 08.09.2019 р.).

Шевчук В. М., доктор юридичних наук, професор кафедри криміналістики Національного юридичного університету імені Ярослава Мудрого, заслужений юрист України, м. Харків, Україна

ВИКОРИСТАННЯ ІНФОРМАЦІЇ ІЗ СОЦІАЛЬНИХ ІНТЕРНЕТ-МЕРЕЖ ПРИ РОЗСЛІДУВАНІ КІБЕРЗЛОЧИНІВ: КРИМІНАЛІСТИЧНІ ПРОБЛЕМИ

У сучасних умовах розвитку інформаційних технологій та побудови інформаційного суспільства, взаємодія користувачів соціальних інтернет-мереж, стає не лише засобом комунікації, а й новою сферою життєдіяльності. Нині соціальні інтернет-мережі стають все більш масовим, найбільш поширеним засобом комунікації та реалізації конституційних прав окремих громадян. Користувачі активно та всебічно взаємодіють між собою, що призводить до накопичення великої кількості інформації, яка може мати, у тому числі, й неправомірний характер. Поява та широке поширення у вітчизняному інформаційному просторі соціальних інтернет-мереж призвела до того, що організовані злочинні групи й окремі особи, які вчиняють протиправні діяння, стали активно використовувати широкі можливості всесвітньої мережі. Тому, соціальні мережі сьогодні є важливим джерелом криміналістичної інформації при розслідуванні злочинів, у тому числі й кіберзлочинів.

Кіберзлочини являють собою сукупність передбачених чинним законодавством кримінально караних суспільно небезпечних діянь, що посягають на право захисту від несанкціонованого поширення і використання інформації, негативних наслідків впливу інформації чи функціонування інформаційних технологій, а також інші суспільно небезпечні діяння, пов'язані з порушенням права власності на інформацію та інформаційні технології, права власників або користувачів інформаційних технологій вчасно одержувати або поширювати достовірну й повну інформацію [2]. Кіберзлочинність не обмежується рамками злочинів вчинених у глобальній інформаційній мережі Інтернет, вона поширюється на всі види злочинів, вчинених в інформаційно-телекомунікаційній сфері, де інформація, інформаційні ресурси виступають предметом злочинних посягань, електронним середовищем, у якому вчинюються кримінальні правопорушення.

Розслідування таких злочинів має свою специфіку та ускладнюється їх підвищеною латентністю. Існує проблема огляду комп'ютерних систем, технічних пристроїв, на яких міститься інформація. Також ускладненою є процедура вилучення, дослідження та фіксації слідів вчинення кіберзлочинів. Цьому сприяє недостатнє технічне забезпечення органів досудового розслідування, оперативних підрозділів. Для розкриття та розслідування таких злочинів обов'язковим є залучення спеціалістів та експертів, що мають спеціальні знання у комп'ютерно-технічній сфері [5, с. 102–103].

Одним із найбільш перспективних напрямків підвищення ефективності протидії кіберзлочинності є впровадження у практичну діяльність оперативних працівників та органів досудового розслідування сучасних інформаційних технологій. Мова йде насамперед про розробку й використання комп'ютерних програм як підґрунтя інформаційного забезпечення підтримки прийняття рішення слідчим, який здійснює розслідування по конкретному кримінальному проваджені [3, с.175]. Підвищення якості діяльності з розслідування злочинів може бути досягнуто за рахунок впровадження в слідчу діяльність інновацій за такими напрямами: 1) розробка і використання нових науково-технічних засобів для виявлення, збирання й дослідження доказів; 2) пропонування новітніх інформаційних технологій та їх використання в роботі слідчого; 3) розробка і пропонування до застосування нових прийомів, методів, методик проведення окремих слідчих дій і розслідування злочинів у цілому [6, с. 126].

Соціальні інтернет-мережі є цінним джерелом криміналістичної інформації, яка може орієнтувати слідчого для прийняття тактичних рішень при розслідуванні кіберзлочинів. Криміналістична інформація у соціальній інтернет-мережі являє собою сукупність даних, повідомлень та відомостей, про джерела й механізм виникнення ідеальних та матеріальних слідів, що мають відношення до злочинної події, отримані в мережі Інтернет із застосуванням спеціальних засобів, з метою встановлення обставин злочинної події у кримінальному провадженні.

В умовах сьогодення спостерігається тенденція до збільшення матеріалів (інформації) протиправного характеру у соціальних інтернет-мережах. Нерідко злочинці хизуються результатом своїх неправомірних дій та фіксують свою злочинну діяльність. Зустрічаються й правопорушники, які використовують соціальні інтернет-мережі, як засіб здійснення своїх злочинів, нерідко й для підтримання злочинних зав'язків. Інформація, що міститься на персональних сторінках соціальних мереж, надає змогу ідентифікувати особу злочинця, обстановку, місце події, співучасників,

знаряддя, допомагає виявити важливі обставин, що мають значення у кримінальному провадженні. Правопорушники, виступаючи творцем і розповсюджувачем власного контенту та споживачем чужого, неминуче залишають у кіберпросторі віртуальні сліди своєї діяльності. За такими слідами можна встановити не тільки фізичні параметри часу та місця вчинення тієї чи іншої дії, а й з високим ступенем імовірності вирішити низку діагностичних завдань з формування психологічного профілю відображеного суб'єкта прогнозування його майбутньої поведінки [1, с. 6].

Криміналістичне дослідження інформації соціальних інтернет-мереж відбувається у декілька етапів: 1) пошук та виявлення інформації; 2) збір; 3) зняття інформації; 4) дослідження інформації. Способами збору інформації із соціальних мереж є такі: а) інформаційно-аналітична робота; б) запити; в) використання спеціальних програм; г) створення «фейкових» сторінок та ін.

Інформаційні сліди, які залишають у віртуальному середовищі, при належному аналізі, дозволяють ідентифікувати особу, визначити місце знаходження, або встановити факт вчинення злочину. Правоохоронці, здійснюючи відповідний аналіз наявної інформації, можуть отримати необхідні дані про місце перебування конкретної особи як під час вчинення злочину, так і під час здійснення спеціальних заходів щодо розшуку осіб, які переховуються від органів досудового розслідування та суду. Використання такої інформації дозволяє встановити коло осіб, з якими спілкується особа, що розшукується, її інтереси та захоплення, місця можливого перебування, встановити контроль за її пересуванням тощо [4, с. 195].

Важливого значення набуває інформаційно-аналітична робота по збору інформації про користувачів таких соціальних мереж. Така діяльність надає змогу отримати важливі дані для викриття осіб, які займаються неправомірною діяльністю. Так, аналізуючи найбільш популярні соціальні мережі серед користувачів, можна отримати такі дані: 1) Facebook − ім'я, унікальний код (ID), геолокацію, коло друзів, підписників, пристрій, який використовувала особа, час активності; 2) Twitter − ім'я, назва облікового запису, унікальний код(ID), підписників, місцезнаходження користувача, а також пристрій з якого були зроблені записи; 3) Instagram − ім'я користувача, назва облікового запису, кількість та імена підписників, верифікаційний статус; 4) YouTube − ім'я користувача, назва каналу, кількість підписників, дата та час викладених матеріалів; 5) Однокласники − ім'я користувача, імена друзів, дата та час викладених записів, міс-

цезнаходження, пристрій, яким користувалася особа, інтереси користувача, відмітки про оцінені записи.

Інформаційно-аналітичний аналіз профілів соціальних інтернет-мереж допомагає скласти соціально-психологічну характеристику особи користувача та з'ясувати його коло друзів та контакти. Вивчення анкет у соціальних інтернет-мережах надає досить різноманітну інформацію, що може відображати інтереси, вподобання та коло друзів особи. Також варто звернути увагу, що перелічені соціальні інтернет-мережі та їх аналоги містять перелік заходів, що пропонуються відвідати користувачам. Власник профілю у соціальній мережі нерідко відмічає плани та події, що бажає відвідати. Така інформація дає можливість оперативним працівникам передбачити поведінку особи правопорушника та місце її знаходження.

Таким чином, використання інформації соціальних інтернет-мереж має не лише важливе практичне значення у протидії кіберзлочинності, а й нині є одним із пріоритетних напрямків діяльності органів правопорядку, спрямованих на оптимізацію кримінального провадження. У реаліях сьогодення соціальні інтернет-мережі, з одного боку, виступають важливим засобом зв'язку, який дозволяє користувачам таких мереж здійснювати право на свободу думок та їх вільне вираження, а з іншого боку, вони є своєрідною публічною інфраструктурою масиву даних (інформації), яка є цінним джерелом криміналістичної інформації, що має значення при розслідуванні кіберзлочинів.

Як свідчить практика, при розслідувані таких злочинів виникає низка проблемних питань, пов'язаних із криміналістичним забезпеченням розслідування, використанням новітніх технологій, залученням спеціалістів, оптимізаціє процесу збору, дослідження та подальшого використання такої інформації тощо. Такий напрям дослідження суттєво впливає на підвищення ефективності слідчої та судової діяльності та безперечно буде забезпечувати її оптимізацію. Використання інформації соціальних інтернет-мереж у кримінальному проваджені має свої переваги, разом із тим й окремі проблеми, певні невизначеності, тому означена проблематика потребує подальших ґрунтовних наукових досліджень.

Список використаних джерел:

1. Білоус В. В., Шепітько В. Ю. Роль сучасних інформаційних технологій у встановленні особи злочинця. Сучасні проблеми криміналістики. Вип. 14. 2014. С. 5−11.
2. Болгов В. Організаційно-правове забезпечення протидії кримінальним правопорушенням, що вчиняються з використанням інформаційних

технологій : наук.-практ. посіб. / В. М. Болгов, Н. М. Гадіон, О. З. Гладун та ін. К. : Національна академія прокуратури України, 2015. 202 с.
3. Журавель В. А. Інформаційне забезпечення процесу розслідування: шляхи та засоби. Проблеми боротьби зі злочинністю. 2004. С. 175−179.
4. Лисенко О. В. Використання інформаційних технологій для розшуку осіб, які переховують від органів досудового розслідування та суду. Науковий вісник Національного університету ДПС України. №2(65). 2014. с. 194−201
5. Організаційно-правові та тактичні основи протидії злочинності у сфері високих інформаційних технологій: навч. посіб / В. М. Бутузов, В. Д. Гавловський, Л. П. Скалозуб та ін. К. : Нац. акад. СБУ України, 2011. 404 с.
6. Шепитько В. Ю. Проблемы разработки, внедрения и использования инноваций в следственной деятельности. Использование современных информационных технологий в правоохранительной деятельности и региональные проблемы информационной безопасности: межд. науч.-практ. конф. Калининград: Калининград. юрид. ин-т МВД России, 2006. Вып. VII, ч. 1. С. 126–130

Shevchuk O. M, Doctor of Juridical Sciences, Professor of the Department of Administrative Law and Administrative Activities, Yaroslav Mudryi National Law University, Kharkiv,Ukraine

COUNTERING CYBERTHREATS IN THE SPHERE OF NATIONAL SECURITY OF UKRAINE: LEGISLATIVE REGULATION, ESSENCE AND PRINCIPLES

In recent years, the attention of Ukraine to the problems of ensuring the state's cyber security and combating cybercrime has increased significantly. The development and security of cyberspace, the introduction of e-governance, ensuring the security and sustainable functioning of electronic communications and state electronic information resources should be components of state policy in the field of information space development and the development of the information society in Ukraine [1]. On December 20, 2002, UN General Assembly Resolution 57/239 adopted «Elements to Create a Global Cybersecu-

rity Culture». As stated in the document, «the global cybersecurity culture will require all participants to consider 9 key complementary elements: awareness, responsibility, responsiveness, ethics, democracy, risk assessment, security design and implementation, security management, reassessment.» [2]. Threats and cyberattacks in the field of national security of Ukraine from potential turned into real ones, and therefore eliminating the likelihood of their occurrence, their negative impact is extremely relevant in the context of today, the development and improvement of information technology enhances the possibilities of cybercrime.

The legal basis for counteracting cyber threats in the field of national security of Ukraine is the Cyber Security Strategy of Ukraine [1], the National Security Strategy of Ukraine [3]; Basic principles of cybersecurity of Ukraine [4], etc.

According to item 3 of the National Security Strategy of Ukraine, topical threats to the national security of Ukraine include 1) aggressive actions of Russia, carried out to deplete the Ukrainian economy and undermine socio-political stability in order to destroy the state of Ukraine and seize its territory, 2) inefficiency of the national security system and defense of Ukraine; 3) corruption and inefficient public administration; 4) economic crisis, depletion of financial resources of the state, decrease in the standard of living of the population; 5) threats to energy security; 6) threats to cybersecurity and security of information resources; 7) threats to the security of critical infrastructure; 8) threats to environmental safety [1].

The terms «cybersecurity» and «cyber threat» are defined in the legislation and in the legal literature. Cybersecurity is defined as the protection of the vital interests of man and citizen, society and the state through the use of cyberspace, which ensures the sustainable development of the information society and digital communication environment, timely detection, prevention and neutralization of real and potential threats to the national security of Ukraine. With regard to the cyber-threat legal framework, these are the existing and potentially possible phenomena and factors that create a threat to Ukraine's vital national interests in cyberspace, adversely affect the state's cybersecurity, cybersecurity and cybersecurity [4]. In the legal literature, cyber-threat is understood as the unlawful, punitive actions of the subjects of information legal relations, which create a danger to the vital interests of the individual, society and the state as a whole, the implementation of which depends on the proper functioning of information, telecommunication and information-telecommuni-

cation systems, as well as relations [5, c.105] . Cybersecurity is a safeguard against these threats. The essence of cyber threats is their subjects, that is, the subjects of information relationships, and the object is information directly. Information interventions pose a significant threat to cyber security. Threats can be divided into two groups, both internal and external

It should be noted that cybersecurity threats are actualized through the action of such factors, in particular as: 1) mismatch of the electronic communications infrastructure of the state, its level of development and security of modern requirements; 2) insufficient level of protection of critical infrastructure, state electronic information resources and information, the requirement for protection of which is established by law, against cyber threats; 3) haphazard cyber defense measures for critical infrastructure; 4) insufficient development of the organizational and technical infrastructure for providing cybersecurity and cybersecurity of critical infrastructure and state electronic information resources; 5) insufficient effectiveness of the subjects of the security and defense sector of Ukraine in counteracting cyber threats of military, criminal, terrorist and other nature; 4) insufficient level of coordination, interaction and information exchange between cybersecurity entities [1].

The provision of cybersecurity in Ukraine is based on the principles of: 1) the rule of law, legality, respect for human rights and fundamental freedoms and their protection; 2) ensuring the national interests of Ukraine; 3) openness, accessibility, stability and security of cyberspace, development of the Internet and responsible actions in cyberspace; 4) public-private interaction, broad cooperation with civil society in the field of cybersecurity and cybersecurity, in particular through the exchange of information on cybersecurity incidents, implementation of joint scientific and research projects, training and skills development in this field; 5) the proportionality and adequacy of cyber defense measures to the real and potential risks, the realization of the state's inalienable right to self-defense in accordance with the rules of international law in the event of aggressive acts in cyberspace; 6) priority of preventive measures; 7) the inevitability of punishment for cybercrime; 8) priority development and support of national scientific, scientific, technical and industrial potential; 9) international cooperation to strengthen mutual trust in cybersecurity and develop common approaches to counter cyber threats, consolidate efforts to investigate and prevent cybercrime, prevent cyberspace from being used in terrorist, military and other illegal purposes; 10) ensuring democratic civilian control over military units and law enforcement agencies established in ac-

cordance with the laws of Ukraine that carry out activities in the field of cybersecurity [4] .

In today's context, the current challenges to achieving the strategic goals of counteracting cyber threats are not solved: such as training and retention of cybersecurity professionals, the ability to protect critical infrastructure, and the structure of communications between agencies, which impedes the exchange of information and complicates the development of adequate rules, protocols and action procedures. take steps to minimize the impact of the three major risks below to achieve Ukraine's cyber strategy goals: problems related to the development of operational sustainability, which should be sufficient to overcome threats, including the current Russian cyber aggression; budget constraints that affect the ability to provide competitive cash to attract and retain the necessary cybersecurity professionals; policy structure and leadership that need more internal coordination to develop consensus-based approaches to risk and resource management [6].

Thus, legislative support and implementation of their principles of counteracting cyber threats in the national security of Ukraine at all levels will prevent such threats and minimize the negative effects of cyber attacks. The role of public-private engagement, broad cooperation with civil society in cybersecurity and cybersecurity, international cooperation in order to build mutual trust in cybersecurity and develop common approaches to counter cyber threats should play a special role.

List of references:

1. Стратегія кібербезпеки України: Указом Президента України від 15 березня 2016 року № 96/2016/ URL. https://zakon5.rada.gov.ua/laws/show/96/2016
2. Елементи для створення глобальної культури кібербезпеки: міжнародний документ від 20.12 2002 р. № 57/239 (резолюція 57/239 Генеральної Асамблеї ООН). URL. https://zakon.rada.gov.ua/laws/show/995_b42
3. Стратегія національної безпеки України: Указ Президента України від 26.03.2015 р. № 287/2015 URL. https://zakon.rada.gov.ua/laws/show/287/2015
4. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII.URL.https://zakon.rada.gov.ua/laws/show/2163–19
5. Діордіца І. Поняття і зміст кіберзагроз на сучасному етапі // Підприємство господарство і право.2017. 4. С.99–107.
6. Кібербезпека: виклики та завдання URL https://blogs.pravda.com.ua/authors/popova/5aa639aaa527c/

Шепітько В. Ю., доктор юридичних наук, професор, завідувач кафедри криміналістики Національного юридичного університету імені Ярослава Мудрого, м. Харків, Україна

СПІВВІДНОШЕННЯ СВОБОДИ І БЕЗПЕКИ: ПРОБЛЕМА ЗАСТОСУВАННЯ ЗАСОБІВ КРИМІНАЛІСТИКИ

Формування правової, демократичної держави в Україні передбачає необхідність всебічного розвитку прогресивних інститутів, захисту загальнолюдських цінностей, пріоритетного забезпечення прав і свобод людини і громадянина, встановлення належного співвідношення заходів безпеки і свободи. П.-А. Альбрехт справедливо зауважує, що право визначається тепер вже не як право громадян на захист від неправомірного посягання з боку держави, а як визнання права держави на захист від нескінченних загроз. Безпека відтепер є бажаною метою, яка стає начебто колективним надбанням безпеки суспільства. Свобода має прилаштуватися до тих меж, які їй залишені безпекою. Однак ці межі звужуються все більше і більше [1, с. 3].

Виникнення та існування системи криміналістичних знань пов'язане із протидією злочинності. На сучасному етапі розвитку суспільства суттєво змінилася злочинність, її прояви та види. У сучасних умовах криміналістика покликана розроблювати новітні засоби, що спрямовані на протидію організованій та транснаціональній злочинності, корупції, торгівлі людьми, незаконному обігу наркотичних засобів, фінансування тероризму та іншим злочинним проявам.

Ефективність діяльності органів правопорядку залежить від використовуваних засобів, які мають бути допустимими і правомірними. Поповнення арсеналу науково-технічних засобів порушує питання про необхідність перевірки їх науковості, заборону використання антинаукових прийомів і таких, що не відповідають загальним засадам кримінального провадження.

На сучасному етапі в слідчій діяльності пропонується використовувати новітні науково-технічні засоби та технології: засоби аудіо-, відеоконтролю, системи спостереження, цифрову фототехніку та відеозапис, електронні контролери тощо. Існують певні особливості у запровадженні інновацій й щодо застосування техніко-криміналістичних засобів у дис-

танційному досудовому провадженні, під час проведення допиту, впізнання у режимі відеоконференції, пред'явлення для впізнання особи поза її візуальним та аудіоспостереженням тощо. Використання новітніх науково-технічних засобів є достатньо важливим й при проведенні негласних слідчих (розшукових) дій: знятті інформації з транспортних телекомунікаційних мереж, знятті інформації з електронних інформаційних систем, обстеженні публічних місць, житла чи іншого володіння особи, встановленні місцезнаходження радіоелектронного засобу, спостереженні за особою, річчю або місцем, аудіо-, відеоконтроль особи чи аудіо-, відеоконтроль місця та ін.

Пропонування широкого переліку негласних слідчих (розшукових) дій і можливість їх застосування у контексті проблеми співвідношення безпеки і свободи відображає певний нахил у бік безпеки. Тому справедливим є висловлювання про те, що пріоритетним має бути захист прав та інтересів особи, потім суспільства, і лише потім держави. Дане положення відображує ідею побудови ліберально-індивідуалістичного суспільства [12, с. 66].

Інформаційні виклики та засоби криміналістики. У сучасному світі все частіше використовуються терміни «інформаційне суспільство», «інформаційний вплив», «інформаційні технології». Ці терміни мають широке розповсюдження у зв'язку із необхідністю обміну інформацією між людьми і процесами інформатизації суспільства. На теперішній час процес обміну інформацією все більше прискорюється, робляться спроби у здійсненні впливу на інших людей за допомогою інформації. Інформаційно-психологічний вплив є видом психологічного впливу, який визначається, як спосіб здійснення впливу на людей (на окремих індивідів й на групи)… [4, с. 51, 52]. Окремим напрямом у криміналістиці має бути захист інформаційних джерел та проблеми інформаційної безпеки.

Все частіше використовується термін «інформаційна війна». До розуміння «інформаційної війни» існують широкий та вузький підходи. У широкому сенсі інформаційна війна – будь-який негативний інформаційний вплив на супротивника; у вузькому – це новий, такий, що не вкладається у міжнародно-правову кваліфікацію, вид або спосіб ведення збройних конфліктів [8, с. 332].

У сучасному суспільстві на різних рівнях приділяється увага захисту інформації, інформаційній безпеці або кібербезпеці. Свідоцтвом важливості заходів для інформаційної безпеки держави, протидії кібератакам є прийняття Закону «Про основні засади забезпечення кібербезпеки України» (від 05.10.2017).

Будь-яке розслідування злочинів або судовий розгляд – «боротьба за інформацію». Недостатність інформації (відсутність доказів або їх хибність) ускладнює процес встановлення факту вчиненого злочину, винуватих осіб, мотивів злочину тощо. У таких умовах важливого значення набуває отримання доказової інформації щодо факту вчиненого злочину, застосування криміналістичних та інших спеціальних знань.

Завданням криміналістики є розроблення та застосування засобів, що дозволяють збирати, досліджувати, використовувати доказову інформацію. Яскравим прикладом в історії криміналістики щодо збирання доказів у складних умовах збройного конфлікту є діяльність проф. Р. А. Рейса, який у 1914 р. прибув до Сербії за запрошенням її уряду як експерт для розслідування злочинів Угорської, Німецької та Болгарської армій у Першій світовій війні. У 1916 р. Р. А. Рейсс опублікував «Report upon atrocities committed by the Austro-Hungarian army during the First invasion of Serbia» (London, 1916). У 1918 р. виходить друком ще одна робота, яка була присвячена Р. А. Рейсом подіям Першої світової війни «Les infractions aux lois et conventions de la guerre commises par les enemies de la Serbie depuis la retraite Serbe de 1915. Resume de l'enquete execute sur le front de Macedoine» (Paris, 1918). Обидві праці являли собою криміналістичне дослідження фактів, які мали місце під час Першої світової війни, – у формі своєрідних звітів або висновків, які були проілюстровані фотографіями, показаннями свідків та експертними дослідженнями [13, с. 111, 112].

Вказані матеріали були використані для засудження злочинів, що були вчинені під час Першої світової війни. Практика застосування криміналістичних знань для збирання доказової інформації під час глобальних збройних конфліктів (ведення війн, у тому числі й гібридної) є актуальною й у сучасних умовах. Зокрема, на сьогодні заслуговують на увагу пропозиції й реальна практика використання безпілотних літальних апаратів (БПЛА) з метою фіксації доказової інформації, у тому числі й у криміналістичних цілях.

Допустимість та правомірність засобів криміналістичної тактики. Проблема допустимості засобів впливу у кримінальному провадженні є вельми важливою і знаходиться в межах визначення належного співвідношення безпеки і свободи, допустимого і недопустимого.

Вплив (у психології) визначається як цілеспрямоване перенесення руху та інформації від одного учасника взаємодії до іншого [11, с. 58]. Термін «психологічний вплив» указує на його цільовий напрямок – пси-

хіку людини. Будь-яка комунікація, будь-яке спілкування є перш за все психологічний вплив на іншу особу [3, с. 51].

Який ступінь впливу можливий у кримінальному провадженні? Міжнародний пакт про громадянські і політичні права (прийнято 16 грудня 1966 р.) проголошує, що нікого не може бути піддано катуванню чи жорстокому, нелюдському або принижуючому гідність поводженню чи покаранню (ст. 7) [10]. У статті 5 Кодексу поведінки службовців органів правопорядку вказується, що жоден службовець органів правопорядку не повинен чинити, підбурювати або терпимо ставитися до будь-якої форми катування або іншого жорстокого, нелюдського або такого, що принижує гідність, поводження або покарання, а також жоден службовець органів правопорядку не повинен посилатися на розпорядження керівництва чи такі виняткові обставини, як військовий стан чи загроза війни, загроза національній безпеці, внутрішня політична нестабільність чи будь-яке інше надзвичайне становище для виправдання катувань або іншого жорстокого, нелюдського або такого, що принижує гідність поводження чи покарання [5]. Таким чином, міжнародні документи містять пряму заборону деяких форм впливу. Окрім того, Україна від 26.01.87 ратифікувала Конвенцію проти катувань та інших жорстоких, нелюдських або таких, що принижують гідність, видів поводження і покарання [6].

Історія діяльності органів правопорядку знає періоди, коли фізичний вплив в їх діяльності був допустимим [9]. Показовим є й те, що лише в 1953 р. було видано наказ МВС СРСР № 0068 від 4 квітня 1953 р. про заборону катувань у МВС СРСР за підписом Л. П. Берії.

Кримінальне і кримінальне процесуальне законодавство України регламентує положення, які забороняють окремі засоби впливу в тих чи інших випадках. Так, ч. 1 ст. 18 КПК України встановлює, що жодна особа не може бути примушена визнати свою винуватість у вчиненні кримінального правопорушення або примушена давати пояснення, показання, які можуть стати підставою для підозри, обвинувачення у вчиненні нею кримінального правопорушення. Стаття 373 КК України передбачає кримінальну відповідальність за примушування давати показання, а ст. 127 КК України – за катування.

Міжнародна правозахисна організація Amnesty International розкритикувала стан прав людини в Україні за 2017–2018 рр., зокрема, нагадала про відсутність прогресу в розслідуванні відносно так званих «таємних тюрем» СБУ, катувань з боку представників правоохоронних органів. Кожний рік ЄСПЛ ухвалює десятки рішень, в яких акцентує увагу на

відсутність в нашій країні ефективної системи розслідування катувань. За офіційними даними закладів охорони здоров'я за медичною допомогою в 2017 р. звернулися майже 2, 5 тисячі людей через травми, нанесені співробітниками поліції. Разом із тим, до суду за 2017 р. надійшло лише 9 кримінальних справ за статтею «катування» (ст. 127 КК України) [14].

Тактичні засоби не повинні засновуватися на насильстві, погрозах та інших незаконних методах. Тактичні прийоми мають відрізнятися високими моральними параметрами, що не допускають приниження особи [7, с. 103–106]. У спеціальні літературі зверталася увага на проблеми використання незаконного впливу в діяльності органів правопорядку в Україні [2, с. 6]. Встановлення фактів незаконного впливу на підозрюваних пов'язане із необхідністю застосування сучасних інформаційних технологій, засобів контролю та можливістю використання електронних доказів.

Засоби криміналістики мають важливе значення у співвідношенні свободи і безпеки і тому повинні відповідати певним критеріям (юридичному, моральному, гносеологічному, психологічному та ін.). Тактичні засоби як носії психологічного впливу відрізняються від насильства (психічного або фізичного) своєю позитивною спрямованістю, свободою вибору тієї чи іншої позиції та форми поведінки.

Список використаних джерел:

1. Альбрехт П.-А. Забытая свобода. Принципы уголовного права в европейской дискуссии о безопасности; пер. с нем. Г. Г. Мошака. 2-е изд. Харьков: Право, 2012. 184 с.
2. Беца А. Аргумент «третьей степени. Зеркало недели. 2002. №45 (429). С. 6.
3. Доспулов Г. Г. Психология допроса на предварительном следствии. М.: Юрид. лит., 1976. С. 112.
4. Камнева Е. В. Информационно-психологическое воздействие средств массовой коммуникации на психическое состояние (на примере студенческой выборки). Вопросы кибербезопасности. №5(18). 2016. С. 51–55.
5. Кодекс поведения должностных лиц по поддержанию правопорядка [Электронный ресурс]. Режим доступа: http:/un.org/ru/document/de…/code_of_conduct.shtml
6. Конвенція проти катувань та інших жорстоких, нелюдських або таких, що принижують гідність, видів поводження і покарання [Электронный ресурс]. Режим доступа: https:/zakon.rada.gov.ua/laws/term

7. Коновалова В. Е., Шепитько В. Ю. Криминалистичекская тактика: теории и тенденции: учеб. пособие. Харьков: Гриф, 1997. 256 с.
8. Короткий Т. Р., Коваль Д. А. Понятие информационной войны в международном праве. Альманах международного права. 2010. Вып. 2. С. 331–343. URL: http://nbuv.gov.ua/UJRN/amp_2010_2_29 (дата обращения: 12.05.2019).
9. Лист ЦК ВКП (б) від 10.01.1939 р. щодо застосування фізичного впливу в практиці НКВС.
10. Международный пакт о гражданских и политических правах [Электронный ресурс]. Режим доступа: http: //zakon.rada.gov.ua/laws/show/995_043
11. Психология. Словарь / под общ. ред. А. В. Петровского, М. Г. Ярошевского. 2-е изд., испр., и доп. М.: Политиздат, 1990. 494 с.
12. Терехович В. Н., Ниманде Э. В. Ценностные ориентации основ современного уголовного правоприменения Латвии. Криміналіст першодрукований. № 5. 2012. С. 58–56.
13. Шепитько М. В Рудольф Арчибальд Рейс.Криміналіст першодрукований. 2015. № 10. С. 109–117.
14. Як катують в Україні // Українська правда. 28 вересня 2018 [Електронний ресурс]. Режим доступу: Pravda.com.ua

Шкута О. О., в.о. завідувача кафедри професійних та спеціальних дисциплін Херсонського факультету ОДУВС

КІБЕРЗЛОЧИННІСТЬ У МІСЦЯХ НЕСВОБОДИ

Процес євроінтеграції став знаковим для України, як і 2014 рік став роком змін у всіх аспектах цього слова. Обраний напрямок досягнення і забезпечення європейських стандартів неабияким чином торкнувся і засуджених до позбавлення волі.

Так, Законами України від 08 квітня 2014 року № 1186-VII «Про внесення змін до Кримінально-виконавчого кодексу України щодо адаптації правового статусу засудженого до європейських стандартів» [3] та від 08 жовтня 2016 року № 1492-VIII «Про внесення змін до деяких законодавчих актів України щодо забезпечення виконання кримінальних покарань та реалізації прав засуджених» [4] було значно розширено права засуджених передбачені статтями ст. 107 та 110 КВК України на листування

з особами, які знаходяться за межами колоній, ведення з ними телефонних розмов, у тому числі у мережах рухомого (мобільного) зв'язку, надано право користуватися глобальною мережею Інтернет.

Більше того, засуджені під час перебування в стаціонарних закладах охорони здоров'я, не віднесених до відання центрального органу виконавчої влади, що реалізує державну політику у сфері виконання кримінальних покарань та пробації, з дозволу адміністрації установи виконання покарань отримали право мати при собі та користуватися під контролем адміністрації портативними персональними комп'ютерами з доступом до глобальної мережі Інтернет.

Але як показала практика, та неабияке зростання кіберзлочинності в місцях позбавлення волі, створення все нових і нових шахрайських схем, встановленого частиною 7 статті 110 КВК України контролю адміністрації, виявилося недостатньо, чи взагалі такий контроль сьогодні не здійснюється? І чи можливо забезпечити в сучасних умовах взагалі такий контроль? Якщо говорити про організацію надання засудженим доступу до глобальної мережі Інтернет в межах Порядку, затвердженого Наказом міністерства юстиції України від 19 жовтня 2017 року № 3222/5 вважаємо за можливе, але якщо ж говорити про доступ засуджених до мобільного зв'язку та мобільного Інтернету, в тому вигляді який ми маємо сьогодні то категорично – ні.

Щороку кількість виявлених кіберзлочинів збільшується в середньому на 2,5 тис. У 2017 році кількість кримінальних проваджень складала близько 7 тис, з них 4,5 тис – винятково кіберзлочини. Одними з перших у списку кіберзлочинів посідають кібершахрайство та кардинг. На другому місці – протиправний контент, а на третьому – поширення шкідливого програмного забезпечення і створення майданчиків для продажу викраденої інформації [1].

Найпершою і головною причиною такого «заробітку» за словами самих засуджених є неналежне забезпечення роботою та оплатою праці у місцях позбавлення волі та неабияка проблема у працевлаштування на волі.

Останніми роками фінансування державної кримінально-виконавчої служби здійснюється на рівні 40 відсотків від необхідного.

З-за нормативної невизначеності суспільно корисна праця засуджених у місцях несвободи не в змозі виконувати функцію одного з основних засобів їх виправлення та ресоціалізації. Іншими причинами цього є не

можливість (недостатність) самих установ виконання покарань, з-за браку (відсутності виробництва) забезпечити зайнятість засуджених, не кажучи взагалі про відсутність бажання деяких з них працювати.

Праця засуджених у місцях позбавлення волі є правом, хоч і обмеженим, з огляду на положення статті 118 КВК України та аналізу норм чинного законодавства. Як показують емпіричні дані проведених нами соціологічних опитувань засуджених до позбавлення волі, реалізовується таке право останніми в більшості випадків для отримання заохочень необхідних для умовно-дострокового їх звільнення від відбування покарання. Саме заохочення є підтвердженням того, що засуджений сумлінною поведінкою і ставленням до праці довів своє виправлення (ч. 2 ст. 81 КК України). Рідше засудженні працюють щоб якось згаяти час.

Забезпечити реалізацію прав, навіть у обмеженому їх вигляді, не кажучи про адаптацію правового статусу засудженого до європейських стандартів, праця у місцях позбавлення волі не в змозі. А забезпечений за рахунок корупційної складової, доступ засудженим до телефонних розмов та мережі Інтернет, як мінімум забезпечує останнім реалізацію прагнення до легкої та в більшості випадків безкарної наживи.

Найбільш поширеними видами кіберзлочинів, які вчиняються з місць позбавлення волі є кібершахрайство та кардинг, коли злочинець шляхом обману намагається заволодіти інформацією про банківські картки особи чи виманити грошові кошти для переказу на «власну» картку чи рахунок та крадіжка даних з банківських карток або отримання доступу до інтернет-банкінгу особи потерпілого.

Так, ще у 2006–2008 роках почали з'являтися перші випадки шахрайської схеми «Ваш син у поліції», про яку сьогодні знає чи не кожен Українець. У 2017 році одна така група шахраїв за даною схемою за 77 епізодами із січня 2016 року по травень 2017 року вкрала у 41 особи 1,16 млн грн «Середній чек» становив 28,4 тис грн, максимальний – 175 тис грн [1].

Іншу категорію кіберзлочинів, які вчиняються з місць позбавлення волі складаюсь шахрайства у сфері продаж та надання послуг.

Представляючись офіційним представником продавця певних товарів зі значною знижкою шахраї виманюють у жертв різного роду передоплати, попередню оплату послуг поштового зв'язку чи доставки.

Останнім часом одним із найпоширеніших видів виманювання грошей засудженими з місць позбавлення волі стало розміщення оголошень про здачу в оренду житла, оголошень на «Сайтах інтимних послуг», не

поодинокі випадки становлять й інтим-селфі, коли в жертви вимагають кошти за нерозповсюдження інформації, вкраденої з її смартфона або комп'ютера. Почастішали випадки злому облікових записів у соціальних мережах, завдяки яким із скомпрометованих акантів злочинці просять у друзів жертви позичити начебто їй кошти, «бо в жертви начебто трапилася певна ситуація», в результаті чого такі друзі починають переказувати гроші [1].

Станом на 1 липня 2019 року у сфері управління Державної кримінально-виконавчої служби України перебуває 148 установ. Крім того, 29 установ знаходяться на території Донецької та Луганської областей, що тимчасово не контролюється українською владою [2]. Як показує статистика саме на сході України кіберзлочинів, які вчиняються засудженими у місцях позбавлення волі найбільше.

Відповідно до КВК України та Порядку організації надання засудженим доступу до глобальної мережі Інтернет засудженим надається право користуватися мережею Інтернет під контролем адміністрації і доки в місцях позбавлення волі існуватиме корупційна складова, подібні злочині посягання там будуть існувати і надалі так як жага легкої наживи тримає верх перед чесною працею, особливо у місця позбавлення волі.

Список використаних джерел:

1. Голова Кіберполіції: «Ваш син у поліції» приносить шахраям на «зоні» мільйон гривень на добу». [Електронний ресурс]. – Режим доступу: https://www.epravda.com.ua/ publications/2018/01/15/633003/
2. Загальна характеристикаДержавної кримінально-виконавчої служби України. [Електронний ресурс]. – Режим доступу: https://www.kvs.gov.ua/peniten/control/main/uk/publish/article/628075
3. Закон України від 08 квітня 2014 року № 1186-VII «Про внесення змін до Кримінально-виконавчого кодексу України щодо адаптації правового статусу засудженого до європейських стандартів». [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1186–18#n142
4. Закон України від 08 жовтня 2016 року № 1492-VIII «Про внесення змін до деяких законодавчих актів України щодо забезпечення виконання кримінальних покарань та реалізації прав засуджених» [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1492–19#n246
5. Порядок організації надання засудженим доступу до глобальної мережі Інтернет. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/z1280-17#n16

Шило О. Г., доктор юридичних наук, професор, завідувач кафедри кримінального процесу та оперативно-розшукової діяльності Національного юридичного університету імені Ярослава Мудрого, член-кореспондент Національної академії правових наук України
Шило А. В., співробітник Служби безпеки України

ПРОБЛЕМА ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ: ЧИННЕ ЗАКОНОДАВСТВО УКРАЇНИ ТА СУЧАСНІ ВИКЛИКИ

Згідно до статті 3 Конституції України найвищою соціальною цінністю в Україні визнаються людина, її життя і здоров'я, честь і гідність, недоторканність і безпека. Якщо ще десятиріччя тому безпека сприймалася винятково в площині відсутності в реальному просторі неприпустимого ризику, пов'язаного з можливістю завдання будь-якої шкоди для життя, здоров'я та майна особи, а також для навколишнього природного середовища, то сьогодні це поняття нерозривно пов'язане з кіберпростором, що істотно ускладнює виконання державою свого позитивного конституційного обов'язку щодо утвердження і забезпечення конституційних прав і свобод людини. Адже розвиток інформаційного суспільства та цифрового комунікативного середовища актуалізує проблему кібербезпеки, вирішення якої передбачає необхідність створення системи дієвих засобів кіберзахисту, своєчасного виявлення, запобігання і нейтралізації реальних і потенційних загроз національній безпеці України у кіберпросторі.

Однією із складових вирішення проблеми кіберзахисту є створення в державі ефективного нормативного підгрунтя, що задовольняє суспільним потребам у цьому аспекті та відповідає сучасним викликам, які мають стійку тенденцію до швидкого розвитку і тому обумовлюють необхідність динаміки законодавчих змін у цьому ж векторі. Усвідомлюючи це, законодавець України 5 жовтня 2017 р. прийняв Закон України «Про основні засади забезпечення кібербезпеки України».

Об'єктами кібербезпеки відповідно до ст. 4 вказаного закону є: 1) конституційні права і свободи людини і громадянина; 2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного се-

редовища; 3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність; 4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави; 5) об'єкти критичної інфраструктури. Об'єктами кіберзахисту є: 1) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону; 2) об'єкти критичної інформаційної інфраструктури; 3) комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

Забезпечення кібербезпеки та здійснення кіберзахисту потребує вжиття сукупності організаційних, правових, інженерно-технічних та інших заходів, спрямованих на виявлення та захист від кібератак, запобігання кіберінцидентам тощо. В цьому плані, як зазначено вище, особливу роль відіграє правове забезпечення діяльності органів правопорядку, пов'язаної із виявленням, розкриттям кіберзлочинів, притягненням до кримінальної відповідальності осіб, які їх вчинили. Звернення ж до аналізу чинного законодавства України, зокрема, кримінального, кримінального процесуального та про оперативно-розшукову діяльність дозволяє дійти висновку про необхідність його істотного оновлення, зміни підходів законодавця до визначення нормативної моделі багатьох інститутів, що в сукупності створюють правове підгрунтя кібербезпеки як стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору.

Реформування чинного законодавства України в цьому напрямі, на наше переконання, має здійснюватися з урахуванням кіберзагроз та релевантних ним наслідків, що вимагає перегляду змісту багатьох правових положень і конструювання правових норм, практичне застосування яких матиме не тільки правозахисне, а й превентивне (що наразі є не менш актуальним) значення.

Тож, якщо за мету вважати створення належного правового підгрунтя боротьби з кіберзлочинами, то завдання, що забезпечують досягнення цієї мети, знаходяться в площині реформування кримінального, кримінального процесуального законодавства та законодавства України про оперативно-розшукову діяльність. При цьому слід зазначити, що з урахуванням глобалізації сучасного світу вельми актуальним стає й звернення до позитивного досвіду іноземних країн у цій сфері, адже конвергенція окремих правових моделей з цією метою видається цілком прийнятною і корисною.

Аналіз кримінального законодавства України та практики його застосування дозволяє констатувати необхідність оновлення розділу XVI Кримінального кодексу (далі – КК), що стосується злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Зокрема, це стосується посилення відповідальності за вчинення цих злочинів, адже, як свідчить сучасна практика, шкода, завдана такими злочинами, може бути вельми істотною і порушувати як інтереси окремої людини, так і суспільства та держави в цілому.

З урахуванням діджіталізації та оцифровки державних процесів нового значення набуває стаття 363 КК, що передбачає відповідальність за порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них обробляється. Практичне застосування цієї статті кримінального закону потребує ретельного унормування правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, які передбачено в диспозиції цієї статті і порушення яких, власне, й становить зміст об'єктивної сторони цього злочиную

Не менш актуальною в цій площині є й проблема чіткого поділу шахрайства, вчиненого з використанням електронно-обчислювальної техніки, шахрайства в інтернеті, шахрайства з використанням персональних даних користувачів, спама, а також в сукупності із злочинами, передбаченими статтею 361 КК (несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку).

Істотного удосконалення потребує також і стаття 200 КК, яка, на наше переконання, має чітко розмежовувати незаконні дії в інтернеті, пов'язані з банківськими картами, особистими рахунками, цифровими активами, електронними грошима тощо. Окремого унормування потребує кожен із злочинів, що стосується незаконного збирання даних за допомогою вірусів і шахрайства, продажу даних, крадіжки грошей, які зберігаються на картах і в цифровому вигляді, тощо.

На окрему увагу законодавця заслуговує розділ I КК, що стосується злочинів проти основ національної безпеки України. Сьогодні кібердиверсії, кібератаки на об'єкти критичної інфраструктури, державні органи та структури є реальністю, що вимагає адекватного нормативного забезпечення діяльності органів правопорядку, яка має ефективно їй протистояти.

Можливість вчинення зазначених злочинів досить часто обумовлюється здійсненням відповідного фінансування злочинної діяльності, що також потребує криміналізації і чітких законодавчих конструкцій, здатних забезпечити дієве правозастосування в цій сфері. Це ж стосується й фінансування спеціальних інформаційних операцій, які спрямовані на організацію масових безпорядків, пропаганду насильства тощо.

Аналіз проблематики кіберзахисту не може залишити поза увагою практичне застосування ст. 182 КК, яка стосується порушення недоторканності приватного життя. Адже притягнення до кримінальної відповідальності за незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу, здійснене у кіберпросторі, передбачає необхідність вирішення низки проблемних питань, які, зокрема, стосуються умов зберігання інформації про особу, збирання відомостей про особу без її відома, різного роду кодифікації цих відомостей тощо.

Окремий напрям реформування національного законодавства з метою забезпечення кібербезпеки стосується кримінального процесуального законодавства України, яке незважаючи на відносну новизну та наявність в ньому нових ефективних механізмів збирання доказів (зокрема, інституту негласних слідчих (розшукових) дій), потребує впровадження сучасних дієвих засобів документування кіберзлочинів, що в сукупності з розвитком цифрової криміналістики надасть змогу органам правопорядку розкривати вказані злочини, збирати докази, які відповідають вимогам належності та допустимості, а в кінцевому рахунку – забезпечувати кібербезпеку та здійснювати кіберзахист прав і законних інтересів людини, інтересів держави та суспільства в цілому.

Таволжанський О. В., кандидат юридичних наук, доцент кафедри кримінології та кримінально-виконавчого права Національного юридичного університету імені Ярослава Мудрого, м. Харків, Україна

ДЕЯКІ АСПЕКТИ РЕГЛАМЕНТАЦІЇ ПРИВАТНОСТІ У КІБЕРПРОСТОРІ

Впровадження інформаційних технологій в життя кожної людини, перетворення інформації в валюту від якої залежить кожен індивід, обу-

мовлює наближення людства до інформаційного суспільства. Більшість винаходів та відкриттів покладено на благо людства, в той же час деякі з них стають дієвими інструментами у досягненні злочинних цілей. Геометричний прогрес у проникненні комп'ютерної техніки в соціум, впровадження її в усіх сферах людської діяльності вплинуло на використанні кібертехнологій злочинним середовищем.

Способи приведення злочинних намірів з використанням мережі інтернет адаптуються при цьому ними застосовуються сучасні досягнення людства, зокрема, портативні пристрої, що мають доступ до Глобальної мережі Інтернет. Механізм забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі відповідно один з основних бар'єрів на злочинному шляху. За останні роки визначені основні цілі, напрями та принципи державної політики у сфері кібербезпеки, закріплені повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, здійсненні перші спроби в налагодженні координації всіх зацікавлених сторін діяльності із забезпечення кібербезпеки.

У сучасному суспільстві Інтернет визначається як інформаційно-телекомунікаційна мережа, єдиний інформаційний, віртуальний простір, кіберпростір, в якому відбуваються глобальні процеси соціальних, технічних, економічних комунікацій, безпосередньо пов'язаних з обробкою персональних даних. Ідея регулювання віртуального простору є актуальною для сучасного суспільства, де питання про правові основи Інтернету регулярно обговорюються. Загальні принципи оброблення персональних даних містяться у Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Законі України «Про захист персональних даних» від 1 червня 2010 р. № 2297-VI (далі – Закон № 2297-VI). Так, на підприємства, установи й організації усіх форм власності, органи державної влади чи органи місцевого самоврядування, фізичних осіб – підприємців (володільців персональних даних), що обробляють персональні дані, з використанням веб-ресурсів у мережі Інтернет, поширюються положення законодавства, зокрема статті 6.

Віртуальний простір містить велику кількість інформації, що, безумовно, відіграє важливу роль в житті суспільства. У той же час деякі ресурси дозволяють користуватися інформацією в злочинних цілях, зокрема: пропагандою насильства, наркотичними речовинами, інструкціями з вибухових пристроїв, втручанням в приватне життя, тощо. В Інтернеті також можна знайти інформацію про послідовність здійснення протиправних

дій, детальні інструкції та рекомендації щодо вчинення окремих видів злочинів, набуття засобів та навичок для полегшення вчинення таких злочинів, а так способи уникнення викриття такої злочинної діяльності, тощо.

Використання злочинцями в протиправній діяльності мережі Інтернет, зокрема, під час незаконного збирання приватної інформації про користувача, набуло сьогодні глобальні негативні тенденції. В деяких випадках маскуючи таку діяльність під законний спосіб надання послуг. Злочинцями відразу були позитивно оцінені технічні можливості використання у протиправній діяльності такого зв'язку, перш за все, можливість в будь-якому місці країни і в будь-який час отримати доступ до власних знарядь – інтернет ресурсів, при цьому зберігаючи свою анонімність.

Діяльність особи в мережі Інтернет в контексті захисту персональних даних повинна розглядатись крізь призму двох складових: з одного боку, в розрізі дотримання прав суб'єктів, персональні дані яких обробляються у мережі Інтернет, з іншого – у розрізі виконання володільцями персональних даних вимог та правил законодавства у сфері захисту персональних даних.

Останнім часом все частіше мережу Інтернет стала використовуватися злочинцями також як засіб збирання інформації про користувачів, яку в подальшому продають. В той же час майже не врегульовано в Україні залишається використання таргетованової реклами. При цьому самі соціальні мережі (такі як Facebook, Твіттер тощо) виступають розповсюджувачами реклами. Технологія SMM базується на основі: • інформації, яку користувачі самі вносять до свого профілю; • аналізу користувачів, з якими спілкується споживач; • даних, що збирається на основі аналізу дій користувача в соціальній мережі, його уподобаннях та інтересах; • даних, що збираються поза соціальною мережею (досліджується інформація з сайтів, які об'єднані однією банерообмінною мережею на основі використання cookies).

Небезпека використання SMM полягає у надмірній кількості інформації про споживача, якою рекламодавець володіє. Це тягне за собою не лише можливі зловживання стосовно змісту реклами, а й неприпустимі порушення таємниці особистого життя особи.

Мережа, що поєднує користувачів є організаційно-просторовою структурою, яка будується як нам здається на принципах: конфіденційності, рівності усіх учасників, хоча, насправді для того, щоб кінцеві користувачі отримали послугу доступу до Глобальної мережі інтернет, їм доведеться довірити свою приватну інформацію невизначеному колу посередників,

починаючи від провайдерів та операторів телекомунікаційних послуг і закінчуючи реєстраторами доменних імен, тощо.

Згідно з аналізом проведеного європейськими експертами для відстежування особливостей поведінки відвідувачів веб-ресурсів використовуються такі технології, як: – надсилання до пристрою користувача файлів «cookies» першої та «cookies» третьої сторони; – збирання в базах веб-ресурсів детальної інформації протягом тривалого часу про відвідані сторінки, вибрані режими, натиснуті клавіші тощо, та її подальше оброблення; – збирання у базах веб-ресурсів інформації про апаратні та програмні засоби, які встановлено у користувача, тощо.

Питання відстежування поведінки відвідувачів веб-ресурсів та захисту приватного життя людини потребує детального аналізу в Україні з подальшими рекомендаціями щодо їх законодавчого та практичного вирішення. З огляду на це дуже корисними можуть бути ініціативи вчених, громадських організацій та проведення ґрунтовних наукових досліджень в цій сфері життєдіяльності людини.

Логінов І. В., кандидат юридичних наук, ст. науковий співробітник, фахівець Ситуаційного центру забезпечення кібербезпеки Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України

ІНФОРМАЦІЙНЕ ПРОТИСТОЯННЯ ДЕРЖАВ ОЧАМИ РОСІЙСЬКИХ ТЕОРЕТИКІВ

Передумовою забезпечення безпеки інформаційного та кіберпростору є достеменне вивчення існуючих у ньому загроз і ризиків та механізмів їхньої реалізації. Одним з найбільш серйозних джерел загроз в інформаційному і кіберпросторі слід вважати діяльність спеціально створених для цього військових структур і спецслужб. Вони слугують інструментом реалізації державної політики в найбільш гострих, конфронтаційних формах міждержавних відносин, особливо притаманних періодам активізації боротьби між основними світовими центрами сили. При цьому військові структури розраховані, головним чином, на відкрите застосування в умо-

вах бойових дій, а спецслужби – для прихованого підриву інформаційної і кібербезпеки у мирний і воєнний час. Нині відповідним потенціалом володіє багато держав світу, серед яких, за нашою оцінкою, пальму першості слід віддати США, КНР, Ізраїлю та Росії. Кожним з цих глобальних гравців розробляється власна стратегія протистояння в інформаційному та кіберпросторі, яка викладається у документах концептуального і стратегічного характеру, деталізується в інструкціях та настановах і втілюється в конкретних діях на стратегічному, оперативному і тактичному рівнях. Тому для забезпечення адекватного захисту національного інформаційного й кіберпростору необхідно зрозуміти загальну логіку, якою керуються суб'єкти зазіхань на їх безпеку.

Для України, безумовно, найбільш актуальним у цьому контексті вбачається дослідження концептуальних поглядів російських теоретиків на напрями, форми та інструменти міждержавного інформаційного протистояння.

На відміну від держав Заходу та України, де повсюдно прийнято національні стратегічні документи із забезпечення кібербезпеки, у Росії такий документ відсутній. Це пояснюється формальним незбігом концептуальних поглядів росіян на структуру інформаційного простору з тими, що склались в Україні та на Заході.

Так, чинність російських документів відповідного напряму і рівня поширюється на суспільні відносини в інформаційному просторі, яким іменується сукупність інформації, об'єктів інформатизації, інформаційних систем, сайтів в інформаційно-телекомунікаційній мережі Інтернет, мереж зв'язку, інформаційних технологій, суб'єктів, діяльність яких пов'язана з формуванням і обробкою інформації, розвитком та використанням зазначених технологій, забезпеченням інформаційної безпеки, а також сукупність механізмів регулювання відповідних суспільних відносин. Кіберпростір як складова інформаційного простору росіянами не виокремлюється, а приставка «кібер» в офіційних документах не використовується.

З цієї причини концептуальні погляди на забезпечення національної безпеки в інформаційному просторі («інформаційної безпеки») викладено в одному документі, – «Доктрині інформаційної безпеки Російської Федерації». У ньому визначено й функції, які в Україні віднесено до сфери забезпечення кібербезпеки.

Міждержавне протистояння в інформаційному просторі іменується «інформаційним протиборством». Вважається, що воно є новою формою боротьби сторін спеціальними способами і засобами, які впливають на

інформаційне середовище противника і захищають власне інформаційне середовище. Його мета полягає у створенні інформаційної переваги над противником, і досягається вирішенням взаємопов'язаних завдань, а саме, створенням інформаційних ресурсів для забезпечення власних дій, їх збереженням у цілісності та недоторканості з одночасним руйнуванням або викривленням інформаційного ресурсу противника та формування у противника хибної уяви про протидіючу сторону.

Найбільш гострою формою інформаційного протиборства вважається інформаційна війна – протиборство між державами в інформаційному просторі, спрямоване на завдання збитків критично важливим інформаційним системам, процесам, ресурсам, структурам, підрив політичної, економічної і соціальної систем, масовану психологічну обробку населення для дестабілізації суспільства і держави, а також примус держави до прийняття рішень в інтересах протидіючої сторони». Вона ведеться за напрямами завдання технологічної шкоди інформаційним системам і ресурсам противника та психологічної обробки його населення і керівництва. Відповідно, інформаційна війна за першим з цих напрямів іменується «інформаційно-технічною війною», за другим – «інформаційно-психологічною війною».

Інформаційно-технічна війна розгортається у технічній сфері, – області інформаційного простору, в якій створюється, обробляється і накопичується інформація, де функціонують системи командування, керування, зв'язку, комунікацій і розвідки. Тобто, синонімом вітчизняного терміну «кіберпростір» можна вважати російський термін «технічна сфера інформаційного простору».

Натомість, інформаційно-психологічна війна точиться у психологічній сфері – області інформаційного простору, що охоплює мислення особового складу збройних сил і мирного населення, де формуються наміри командирів, доктрини, тактика, методи протиборства, мораль, поняття згуртованості підрозділів, рівень підготовки, досвід, розуміння ситуації і суспільна думка, – тобто, сфері, яка в Законі України «Про національну безпеку України» іменується «інформаційною».

Інформаційно-технічна війна проводиться методами інформаційно-технічного впливу, а саме:

– придушення елементів інфраструктури державного і військового управління;

– електромагнітного впливу на елементи інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем (радіоелектронної боротьби);

– одержання розвідувальної інформації шляхом перехоплення і дешифрування інформаційних потоків у каналах телекомунікацій, а також за побічними випромінюваннями та за рахунок спеціального впровадження технічних засобів перехоплення інформації;

– здійснення несанкціонованого доступу до інформаційних ресурсів (шляхом використання програмно-апаратних засобів подолання систем захисту інформаційних і телекомунікаційних систем супротивника) з їх наступним викривленням, знищенням або викраденням, або порушення нормального функціонування цих систем.

Основною організаційною формою інформаційної війни вважаються інформаційні операції – дії, спрямовані на досягнення інформаційної переваги у забезпеченні національної військової стратегії шляхом впливу на інформацію та інформаційні системи противника з одночасним зміцненням і захистом власної інформації та інформаційних систем і інфраструктури. До об'єктів інформаційно-технічного впливу відносять інформаційні, телекомунікаційні, інформаційно-телекомунікаційні системи будь-яких військових і цивільних установ, організацій і закладів, важливих для забезпечення інформаційного протиборства і завдань міждержавного протистояння взагалі, – у тому числі банків, транспортних і промислових підприємств, засобів масової інформації (насамперед, електронних).

Інформаційно-технічний вплив на них здійснюється за допомогою інформаційно-технічної зброї – різновиду інформаційної зброї, що становить собою сукупність спеціально організованої інформації, інформаційних технологій, способів і засобів, які дають змогу цілеспрямовано порушувати цілісність інформаційних ресурсів противника, блокувати до них санкціонований доступ, а також створювати для цього необхідні умови. При цьому «наступальною» вважається інформаційно-технічна зброя, призначена для безпосереднього деструктивного впливу на інформаційні ресурси і критичну інформаційну інфраструктуру противника, а «забезпечувальною» – призначена для створення передумов ефективному застосуванню «наступальної» зброї. Відтак, до наступальної інформаційно-технічної зброї росіяни відносять засоби і технології радіоелектронного та оптико-електронного придушення, ураження програмного забезпечення, елементів радіоелектронної апаратури, зміни умов поширення електромагнітних, акустичних і гідроакустичних хвиль, прискореного старіння радіоелектронної апаратури, а до «забезпечувальної» – засоби технічної розвідки, подолання систем захисту критичної інформаційної

інфраструктури противника, інформаційного забезпечення бойових дій в інших сферах.

Широка номенклатура наступальної та забезпечувальної інформаційно-технічної зброї вимагає залучення до інформаційного протиборства озброєних нею структур різного функціонального призначення і відомчої підпорядкованості, – органів та підрозділів радіоелектронної, оптико-електронної та комп'ютерної розвідки, технічного і криптографічного захисту інформації в ІТС, військ радіоелектронної боротьби тощо.

Викладене дає підстави для висновку, що концептуальні погляди російських теоретиків на міждержавне протистояння у кіберпросторі відрізняються від тих, що реалізовуються в Україні, хоча вітчизняному терміну «кіберпростір» можна співставити російський термін «технічна сфера інформаційного простору». Особливу ж увагу слід звернути на розмаїття сил, засобів і методів, які залучаються Російською Федерацією до інформаційно-технічного протиборства. Їх перелік переконливо свідчить про те, що запобігання загрозам у кіберпросторі («технічній сфері інформаційного простору») передбачає вирішення значно ширшого кола завдань, ніж виявлення і припинення кібератак на об'єкти критичної інформаційної інфраструктури України.

Список використаних джерел:

1. Закон України «Про контррозвідувальну діяльність» від 26 грудня 2002 р. № 374-IV.
2. Закон України «Про національну безпеку» від 21.06.2018 № 2469-VIII.
3. Стратегія національної безпеки України, затверджена Указом Президента України від 26.05.2015 № 287/2015.
4. Стратегія кібербезпеки України, затверджена Указом Президента України від 15 березня 2016 року № 96/2016.
5. Доктрина информационной безопасности Российской Федерации [Електронний ресурс] // Веб-сайт «Российская Газета». Режим доступу: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html
6. Остапенко О. Н. Информационно-космическое обеспечение группировок войск (сил) ВС РФ: учебно-научное издание / О. Н. Остапенко, С. В. Баушев, И. В. Морозов. СПб.: Любавич, 2012. – 368 с.: ил.
7. Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве [Електронний ресурс] // Веб-сайт Міністерства оборони РФ. Режим доступу: http://ens.mil.ru/les/morf/Strategy.doc.

8. Гриняев С. Н. Поле битвы – киберпространство. / С. Н. Гриняев. – Мн.: Харвест, 2004. – 448 с.
9. Остапенко О. Н. Информационно-космическое обеспечение группировок войск (сил) ВС РФ: учебно-научное издание / О. Н. Остапенко, С. В. Баушев, И. В. Морозов. СПб.: Любавич, 2012. – 368 с.: ил.
10. Макаренко С. И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. Монография. – СПб.: Наукоемкие технологии, 2017. – 546 с.
11. Сироткин Д. В., Мартьянов А. Н., Новиков В. К., Пономаренко А. В. Модель информационного противоборства в Вооруженных силах Российской Федерации [Електронний ресурс] // Режим доступу: https://legalscience.ru/images/PDF/2016/10/model-informatsionnogo-protivoborstva.pdf.

Пивоваров В.В.,
ORCID ID: https://orcid.org/0000-0003-3754-8099
кандидат юридичних наук, доцент, доцент кафедри кримінології та кримінально-виконавчого права Національного юридичного університету імені Ярослава Мудрого, м.Харків, Україна

ДЕТЕРМІНАНТИ ПРОТИПРАВНОГО ВИКОРИСТАННЯ ПЕРСОНАЛЬНИХ ДАНИХ У ВИБОРЧОМУ ПРОЦЕСІ

Проблема захисту інформації від злочинних посягань в умовах діджиталізації – актуальна та закономірна для сучасного українського суспільства, оскільки здобутки науково-технічного прогресу безпосередньо впливають на інформаційну безпеку як самого суспільства, так і окремої людини. Особливо гостро постає глобальне питання захисту персональних даних. Це питання державної, економічної, політичної, особистісної безпеки. Адже один із напрямків криміногенних загроз – протиправне використання персональних даних у виборчому процесі з метою маніпуляцій суспільною думкою, волевиявленням виборця та отримання переваг над політичними конкурентами.

Протиправні зловживання під час виборчого процесу є багатоаспектним явищем та неодноразово ставали об'єктом досліджень науков-

ців у галузі права, історії, соціології, філософії, політології тощо. Проблемні питання протиправних посягань і кримінологічно значущі аспекти сфери виборчих відносин досліджували В. В. Голіна, Б. М. Головкін, І. М. Даньшин, О. М. Джужа, А. П. Закалюк, Ю. Б. Ключковський, М. І. Козюбра, О. В. Лавринович, С. Я. Лихова, Л. П. Медіна, М. І. Мельник, В. І. Осадчий, В. Є. Скомороха, М. І. Ставнійчук, В. П. Тихий, О. Ю. Тодика, М. І. Хавронюк та інші. Однак, стійка тенденція до діджиталізації державних і суспільних процесів, її швидкоплинність та орієнтованість її на останні досягнення техніки в галузі мережевих технологій, із потенційною можливістю неконтрольованого доступу, визначають практичну і наукову актуальність теми протиправного втручання у виборчий процес.

Персональними даними є відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [1]. Зокрема, до таких відомостей можна віднести: прізвище, ім'я, по батькові, адреса, телефони, паспортні дані, національність, освіта, сімейний стан, релігійні та світоглядні переконання, стан здоров'я, матеріальний стан, дата і місце народження, місце проживання та перебування тощо. Вказаний перелік не є вичерпним [2]. Обробка даних про фізичну особу, які є конфіденційною інформацією, без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини – не допускається. Найчастіше, протиправне використання такої інформації під час виборчого процесу здійснюється з метою маніпулювання суспільною свідомістю та громадською думкою.

Політична маніпуляція − це система засобів ідеологічного і духовно-психологічного впливу на масову свідомість із метою нав'язати певні ідеї, цінності. Під маніпулюванням в більшості випадків слід розуміти психічний вплив, який здійснюється таємно, а отже, і на шкоду тим особам, на яких воно спрямоване. Маніпуляція розуміється як приховане управління свідомістю, факт якого не повинен бути помічений об'єктом маніпуляції. Метою політичного маніпулювання є отримання, реалізація та збереження влади. Маніпулювання має своїм завданням змінити думки, цілі людини в потрібному для певної політичної сили напрямку [3, с. 171].

Вважаємо, що політичні маніпуляції із використанням персональних даних передбачають впровадження, укорінення у свідомість виборця думки, ідеї, погляду вигідної для певної політичної сили під виглядом об'єктивної і достовірної інформації. Для реалізації маніпуляції, в першу чергу, необхідно ретельно дослідити сам об'єкт маніпуляції, тобто особу конкретного виборця, його потреби, ідеї та вподобання. Аналіз світової

практики показує, що в гонитві за цінною інформацією політичні сили часто порушують закон і отримують її шляхом незаконного втручання в роботу закритих баз даних, або соціальних мереж.

Щодо визначення ключових детермінант незаконного використання персональних даних у виборчому процесі як окремого виду злочинності, підкреслимо, що вони можуть бути класифіковані за різними критеріями, зокрема, за сферою їх існування як таких – в економічній, політичній, управлінській, соціальній сферах суспільного життя.

Б. М. Головкін зазначає, що економічна сфера – це своєрідний фундамент суспільства, що відіграє вирішальну роль у його розвитку. Ринкові відносини у сфері суспільного виробництва, розподілу, обміну та споживання матеріальних благ, обтяжені гострими протиріччями, що породжують криміногенні деформації елементів суспільної свідомості [4]. У розвиток цієї думки зазначимо, що маніпуляціям із персональними даними виборців сприяють не тільки протиріччя, що виникають під час реалізації ринкових відносин; сам факт існування суспільних відносин такого специфічного вмісту та високий рівень їх розвитку має детермінуюче значення. Адже ринкова система економіки заснована на принципах вільного підприємництва, у якій роль основного регулятора економічних відносин відіграє ринок, як механізм розподілу товарів і послуг між членами суспільства шляхом добровільного обміну. Одним з принципів функціонування ринку є принцип ринкового ціноутворення, який полягає, зокрема, у взаємодії попиту та пропозиції на конкретний товар. Оскільки ці явища є взаємозалежними, то це призводить до того, що попит (запит потенційного покупця на придбання товару) породжує пропозицію, а пропозиція створює попит. Стаття 1 Закону України «Про інформацію» визначає інформацію як будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. На неї також поширюються вказані закономірності ринку. Сьогодні інформація стала специфічним видом товарів, який має споживчу та мінову вартість, тобто здатність задовольняти які-небудь людські потреби, а також бути об'єктом цивільного обороту.

З іншого боку, не варто відкидати вплив процесів корпоратизації, глобалізації економік, їх поглинання, злиття політикуму і бізнесу, та виокремлення і «кристалізації» явища корпоративної злочинності – ресурсної, наукомісткої, інтелектуальної, спрямованої на надприбуток, і забезпечення ділових і професійних переваг, тобто здатної вирішувати завдання, які непосильні для злочинця – одинака [5, с.225–227].

Таким чином, можна визначити специфічних характер детермінуючого впливу ринкових відносин на незаконне використання персональних даних виборців:

1) персональні дані виборців набувають споживчих властивостей, які необхідні покупцю: можливість за їх допомогою впливати на конкретних виборців, маніпулювати масами, отримувати інші додаткові переваги під час боротьби за владу, фальсифікувати результати виборів тощо;

2) неможливість отримати такі відомості легальним шляхом збільшує їх мінову вартість;

3) формування особливої злочинної мотивації на отримання персональних даних з метою їх безпосереднього використання, або передачі іншим особам.

Найголовнішою детермінантою в політичній сфері є зневажливе ставлення до інституту виборів, нівелювання його демократичної сутності та суспільної важливості. Сьогодні вибори в Україні сприймаються скоріш не як волевиявлення народу, що є суверенним, верховним суб'єктом влади, а як засіб оновлення особового складу органів та інститутів держави. В сучасній політичній системі України процедура виборів перетворилася на формальний механізм завоювання влади, з метою задоволення власних потреб. Для політичної влади характерні такі криміногенні явища і процеси як клептократія, корупція і лобізм, маргіналізація еліт, зрощення корпоративних інтересів фінансово-промислових груп, органів влади та управління і кримінальних структур. Зокрема, клептократична модель організації влади передбачає використання чиновниками владних повноважень з метою швидкого збагачення, примноження капіталів, шляхом розкрадання бюджетних коштів і привласнення майна [4].

Умовами протиправного, злочинного використання персональних даних слід визначити: недоліки законодавства України у сфері захисту персональних даних, неврегульованість відносин у сфері захисту персональних даних в мережі Інтернет, особливо в соціальних мережах; високий рівень віктимізації громадян у питаннях збереження і контролю за використанням власних персональних даних; технічні недоліки в сучасних системах захисту баз персональних даних; порушення вимог нормативних актів щодо ведення Державного реєстру виборців України; латентність, латентну віктимізацію та низьку ймовірність притягнення до відповідальності за вчинення широкого кола правопорушень у сфері захисту персональних даних.

Список літератури

1. Про захист персональних даних : Закон України від 01.06.2010 р. №2297-VI / Верховна Рада України. URL: http://zakon.rada.gov.ua/laws/show/2297–17 (дата звернення: 10.09.2019).
2. Рішення Конституційного суду України від 20.01.2012 р. №2-рп/2012 // База даних «Законодавство України». URL: http://zakon.rada.gov.ua/laws/show/v002p710–12 (дата звернення: 10.09.2019).
3. Перемога на виборах: технології, кампанії, принципи : практичний посібник / М. Д. Городок, А. В. Карташов, Є. О. Романенко, В. Ю. Стасюк; за заг. ред. М. Д. Городка. Київ, 2016. 264 с.
4. Головкін Б. М. Загальна характеристика детермінантів злочинності в Україні. *Форум права*. 2014. №1. С.106–111. URL : Режим доступу: http://nbuv.gov.ua/UJRN/FP_index.htm_2014_1_21 (дата звернення: 10.09.2019).
5. Пивоваров В. В., Гулаткан Т. В. До питання співвідношення «білокомірцевої» та корпоративної злочинності. *Право і суспільство*. 2018. №1. Ч.2 – С.223–228.

Наукове видання

КРИМІНАЛЬНІ ЗАГРОЗИ В СЕКТОРІ БЕЗПЕКИ: ПРАКТИКИ ЕФЕКТИВНОГО РЕАГУВАННЯ

Матеріали панельної дискусії
ІІІ Харківського міжнародного юридичного форуму
м. Харків, 26 вересня 2019 р.

Матеріали друкуються
в авторській науковій та літературній редакції

Відповідальний за випуск *Б. М. Головкін*

Комп'ютерна верстка *А. Т. Гринченка*

Підписано до друку з оригінал-макета 23.09.2019.
Формат 60×84 1/16. Папір офсетний. Гарнітура Times.
Обл.-вид. арк. 10,37. Ум. друк. арк. 10,23. Вид. № 2272.
Тираж 60 прим.

Видавництво «Право» Національної академії правових наук України
та Національного юридичного університету імені Ярослава Мудрого
вул. Чернишевська, 80а, Харків, 61002, Україна
Тел./факс (057) 716-45-53
Сайт: www.pravo-izdat.com.ua
E-mail для авторів: verstka@pravo-izdat.com.ua
E-mail для замовлень: sales@pravo-izdat.com.ua

Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготівників і розповсюджувачів
видавничої продукції — серія ДК № 4219 від 01.12.2011 р.

Виготовлено у друкарні ФОП Дуюнова Т. В.
Тел. (057) 717-28-80