БЕРЕЗДЕЦЬКИЙ Юрій Миронович
ПАЛЬЧИК Максим Леонідович

ОКРЕМІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ДОСВІД ДЛЯ УКРАЇНИ

Постановка проблеми. Останні кілька років стали періодом надзвичайно стрімких та масштабних змін у сфері інформаційно-комунікаційних технологій. Для нашої держави цей період виявився сповненим нових викликів та загроз кібербезпеці, які актуалізувались через низку зовнішніх і внутрішніх чинників. При цьому сформована за попередні періоди недостатність та невідповідність національної системи захисту безпеки держави у кіберпросторі призвела до того, що Україна досить повно відчула на собі наслідки реалізації загроз кібернетичній безпеці, а успішні кібератаки, вмотивованих інтересами окремих держав-суб'єктів, призвели до завдання значної шкоди численним комунікаційним системам та об'єктам критичної інфраструктури.

За повідомленням Державної служби спеціального зв'язку та захисту інформації України (далі – ДССЗЗІ), протягом останніх п'яти років на інформаційно-телекомунікаційні системи деяких об'єктів, які за своїм значенням і роллю для життєдіяльності суспільства є об'єктами критичної інфраструктури, здійснено низку масштабних кібератак, зокрема: злом сайту ЦВК під час президентських виборів (2014 р.), знеструмлення підстанцій Прикарпаттяобленерго за допомогою троянської програми BlackEnergy3 (2015 р.), хакерська атака на внутрішні телекомунікаційні мережі Мінфіну, Держказначейства, Пенсійного фонду (2016 р.), DDOS-атака на сайт АТ «Укрзалізниця» (2016 р.), застосування віруса-шифрувальника файлів PetyaRansomware (2017) та ін. [1].

Вважаємо, що вчинені кібератаки стали своєрідним каталізатором розвитку правового регулювання на національному рівні. Як наслідок, за останній час розроблено та прийнято низку нормативно-правових актів, що створюють правові передумови для розв'язання існуючих проблем у сфері забезпечення кібербезпеки та захисту критичної інфраструктури.

Окремим блоком у формуванні нормативно-правового регулювання на національному рівні стоять питання створення дієвої системи реагування на виклики та загрози, що виникають у кіберпросторі, та остаточного закріплення завдань основних суб'єктів системи забезпечення кібербезпеки держави. Одним із таких завдань, що, на наш погляд, потребує додаткового вивчення, є завдання по здійсненню перевірки готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів.

Аналіз останніх досліджень і публікацій. Проблемам забезпечення кібербезпеки приділяли увагу такі науковці, як В. М. Бутузов, В. Д. Гавловський, В. О. Голубєв, Д. В. Дубов, О. О. Климчук, В. А. Номоконов, Н. А. Ожеван, В. М. Панченко, М. А. Погорецький, Е. В. Рижков, К. В. Тітуніна, Н. А. Ткачук, Т. Л. Тропіна, В. П. Шеломенцев та ін.

Актуальні питання забезпечення безпеки об'єктів критичної інфраструктури вивчали також дослідники Д. С. Бірюков, І. Д. Бондаренко, В. М. Гребенюк, Ю. А. Іванов, С. І. Кондратов, І. М. Павлов, О. М. Суходоля та ін. Водночас окремого дослідження проблем організації й правового регулювання перевірки готовності об'єктів критичної інфраструктури до кібератак та кіберінцидентів з урахуванням іноземного досвіду до сьогодні здійснено не було.

Метою статті є дослідження іноземного досвіду перевірки готовності об'єктів критичної інфраструктури до кібератак і вивчення особливостей правового регулювання та організації діяльності уповноважених суб'єктів за цим напрямом в Україні.

Виклад основного матеріалу. Аналіз існуючого іноземного досвіду свідчить про те, що в окремих державах здійснення перевірки готовності інфраструктурних об'єктів до кібератак і кіберінцидентів є усталеною практикою та невід'ємною складовою національної системи забезпечення кібербезпеки. При чому до вказаної діяльності поряд із державними органами активно залучаються представники приватного сектору.

Так, у США для пошуку уразливостей кіберзахисту на об'єктах сектору безпеки і оборони ініційовано кілька успішних державно-приватних програм та проєктів. Зокрема, за ініціативи Міністерства оборони в 2016 році, у межах перевірки стану кібербезпеки, реалізовано проєкт «Зламай Пентагон» («Hack the Pentagon»). Метою проєкту було знаходження проблем та уразливостей у системі кіберзахисту оборонного відомства за допомогою добровольців з числа представників приватного сектору, які спеціалізуються на питаннях кібербезпеки. Фахівцями для тестування були обрані громадяни США, які пройшли процедуру реєстрації та щодо яких було здійснено перевірку біографії. У 2016 році участь у проєкті взяли понад 1,4 тисячі «хакерів». Для тестування, у межах діючої ініціативи, спеціалістам були відкриті окремі комп'ютерні мережі на визначений період [2].

Проект тривав з 18-го квітня по 12-те травня 2016 року. Та за інформацією керівників оборонного відомства перевершив усі очікування. Вже через 13 хвилин після запуску програми було повідомлено про першу уразливість. А протягом перших шести годин подано близько 200 звітів про уразливості. За увесь час реалізації проєкту спеціалістам вдалось виявити 1 189 уразливостей, з яких 138 визнано найбільш небезпечними для системи безпеки сайтів Пентагону [3].

За кожну виявлену та повідомлену уразливість спеціалістам виплачувалась відповідна грошова винагорода, так званий «bug bounty». Індивідуальні виплати за цим проєктом складали від 100 дол. до 15 тис. дол. Розмір виплат залежав від типу та небезпечності виявленої уразливості, а також від того чи зміг «хакер» нею скористатися чи ні. Загальна сума виплат за програмою склала близько 75 тис. дол. за подані в установленому порядку звіти про уразливість.

За словами колишнього міністра оборони США Еша Картера, запровадити таку ініціативу змусив той факт, що військові на сьогодні не володіють достатніми знаннями в індустрії інформаційної безпеки, саме тому дії по залученню кращих представників були усвідомленою необхідністю забезпечення кібербезпеки. При цьому, за інформацією керівництва оборонного відомства, програма дозволить у майбутньому зробити інформаційні системи більш безпечними при відносно незначних витратах [2].

Подібною ініціативою в США є програма «Зламай Військово-повітряні сили» («Hack the Air Force»). Останню таку програму було реалізовано у період з 19 жовтня по 22 листопада 2018 року. За час програми було виявлено і усунено понад 120 уразливостей кіберзахисту Військово-повітряних сил США, здійснено виплати на загальну суму 130 тис. дол. Це була сьома подібна ініціатива за участі оборонного відомства США та третя за участі Військово-повітряних сил США [4].

Ще одним прикладом залучення приватного сектору є спільна програма платформи HackerOne та Європейської комісії, що стала можливою завдяки проєкту EU-FOSSA (EU-Free and Open Source Software Auditing). Саме цей проєкт має допомогти установам ЄС краще захистити критичну інформаційну інфраструктуру. Проєкт EU-FOSSA було започатковано після інциденту «Heartbleed», який засвідчив наявність уразливостей у програмному забезпеченні, що досить широко використовувалось Європейською комісією [5].

Як бачимо, в США та Європі вже сформовано позитивну практику перевірки готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів, у тому числі із залученням фахівців приватного сектору. Подібні ініціативи офіційно санкціонуються на певний проміжок часу, для визначених категорій осіб, що одночасно виключає несанкціонованість доступу до інформаційних ресурсів, а

також дозволяє обмежити доступ до них забезпечивши залучення максимальної кількості кваліфікованих експертів.

Варто зазначити, що проблеми організації та правового регулювання перевірки готовності об'єктів критичної інфраструктури до кібератак та кіберінцидентів в Україні поступово стають актуальним напрямом наукових досліджень. І хоча сьогодні не існує єдиного погляду на вирішення наявних проблем за цим напрямом, дослідники справедливо наголошують на необхідності створення належної правової основи регулювання суспільних відносин, що виникають у вказаній сфері [6; 7].

У сформованій практиці забезпечення інформаційної безпеки перевірка готовності об'єктів до кібератак та кіберінцидентів здійснюється шляхом моделювання дій зловмисників з проникнення до інформаційних систем чи мереж та отримання доступу до інформації так званого тестування на проникнення.

Під час тестування на проникнення здійснюється пошук уразливостей, використання яких дозволить у подальшому проникнути на сервер ззовні та отримати несанкціонований доступ до критичної інформації. При цьому здійснюється пошук можливих уразливостей програмного забезпечення, недоліків парольної політки, недоліків налаштувань інформаційної системи та подальше їх використання. Здійснюючи тестування на проникнення, спеціаліст влаштовує псевдоатаку на мережу чи інфраструктуру, інсценуючи при цьому дії реальних зловмисників або атаку, що реалізується за допомогою шкідливого програмного забезпечення. Тобто метою тестування на проникнення є виявлення слабких місць у захисті інформаційних систем від кібератак та подальше їх усунення.

Зауважимо, що при здійсненні перевірки готовності об'єктів критичної інфраструктури шляхом тестування на проникнення відбувається фактичне втручання в роботу комп'ютерних мереж, електронно-обчислювальних машин, автоматизованих систем тощо. У той час як несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку відповідно до ст. 361 КК України є злочином.

Про це також зазначають у своїх працях такі дослідники, як Д. Дубов [6] та Н. Ткачук [7]. При цьому, на думку Д. Дубова, формулювання зазначеної статті КК України практично унеможливлює діяльність некомерційних пентестерів, якщо ці тести заздалегідь не погоджені з об'єктами атаки [6, с. 66].

Пропонуючи вирішення існуючої проблеми, Д. Дубов висловлює думку про легалізацію пентестінгу через застосування правового інституту звільнення від кримінальної відповідальності. При цьому науковець пропонує доповнити статтю 361 КК України наступним пунктом: «звільняється від кримінальної відповідальності громадянин України, якщо таке втручання здійснювалось за погодженням із суб'єктами національної системи кібербезпеки…» [6, с. 79].

Дещо іншу позицію висловлює Н. Ткачук. На її думку, залучення Службою безпеки України осіб до негласної перевірки стану кіберзахисту об'єктів критичної інфраструктури необхідно відносити до обставин, що виключають злочинність діяння. При цьому дослідниця пропонує доповнити статтю 361 КК України наступним пунктом: «Не є злочином дії особи, передбачені частиною першою цієї статті, яка відповідно до закону виконувала спеціальне завдання органів державної безпеки із негласної перевірки готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів». На думку вченої, подібні зміни дозволять створити правове поле для розвитку державно-приватної взаємодії СБ України за вказаним напрямом [7].

Підтримуємо тезу про можливість віднесення залучення Службою безпеки України осіб до негласної перевірки стану кіберзахисту об'єктів критичної інфраструктури до обставин, що виключають злочинність діяння. Водночас дещо дискусійними вбачаються запропоновані дослідницею зміни до положень КК України. Так, ми вважаємо не зовсім

коректним пропонувати обставину, що виключає злочинність діяння для певного злочину, із включенням до диспозиції статті Особливої частини, у нашому випадку ст. 361 КК України, у той час як у розділі VIII загальної частини КК України вже закріплено вичерпний перелік обставин, що виключають злочинність діяння, та які можуть бути застосовані до кожного злочину у кожному конкретному випадку. Серед таких обставин, визначених Кримінальним кодексом України, є: необхідна оборона (ст. 36), уявна оборона (ст. 37), затримання особи, що вчинила злочин (ст. 38), крайня необхідність (ст. 39), фізичний або психічний примус (ст. 40), виконання наказу або розпорядження (ст. 41), діяння, пов'язане з ризиком (ст. 42), виконання спеціального завдання з попередження чи розкриття злочинної діяльності організованої групи чи злочинної організації (ст. 43).

При цьому, якщо вести мову про заподіяння шкоди, залученими СБ України особами, під час здійснення негласної перевірки стану кіберзахисту об'єктів критичної інфраструктури в контексті обставин, що виключають злочинність діяння, на наш погляд, доцільніше говорити про діяння, пов'язане з ризиком (ст. 42 КК України). Тобто діяння, яке заподіяло шкоду правоохоронюваним інтересам, якщо це діяння було вчинене в умовах виправданого ризику для досягнення значної суспільно корисної мети.

Ми, у свою чергу, пропонуємо поглянути на вказану проблему дещо під іншим кутом. Так, суспільна небезпечність діяння, відповідальність за яке передбачена ст. 361 КК України, полягає саме у несанкціонованому втручанні у роботу електронно-обчислювальних машин, систем чи комп'ютерних мереж, а також мереж електрозв'язку. Саме несанкціоноване втручання є фактично формою об'єктивної сторони складу цього злочину. У той час, якщо втручання буде санкціоновано уповноваженими суб'єктами, можемо говорити про відсутність об'єктивної сторони та, відповідно, складу злочину, передбаченого ст. 361 КК України.

М. І. Мельник, М. І. Хавронюк визначають несанкціоноване втручання в роботу ЕОМ, їх систем чи комп'ютерних мереж як проникнення до цих машин, їх систем чи мереж і вчинення дій, які змінюють режим роботи машин, їх систем чи комп'ютерних мереж, або ж повністю чи частково припиняють їх роботу, без дозволу (згоди) відповідного власника або уповноважених ним осіб, а так само вплив на роботу АЕОМ за допомогою різних технічних пристроїв, здатних зашкодити роботі машин [8, с. 986].

При цьому варто зауважити, що на сьогодні законодавством не визначені категорії «несанкціоноване втручання…» та «незаконне втручання у роботу» [9]. Водночас ст. 1 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» сформульовано термін «несанкціоновані дії щодо інформації у системі», під якими розуміються дії, що проводяться з порушенням порядку доступу до інформації, встановленого відповідно до законодавства. «Порядок доступу до інформації в системі», у свою чергу, – це умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації. Відповідно до ст. 4 порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються володільцем інформації, яким може бути фізична або юридична особа, якій належать права на інформацію [10].

Захист же інформації в системі, відповідно до ст. 5 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», здійснюється власником системи в порядку та на умовах, визначених у договорі, який укладається ним із володільцем інформації, якщо інше не передбачено законом [10].

Таким чином, при здійсненні перевірки готовності об'єктів критичної інфраструктури до кібератак та кіберінцидентів та з метою недопущення вчинення злочину, передбаченого ст. 361 КК України, необхідно вирішувати питання про санкціонованість втручання в роботу інформаційних систем вказаних об'єктів з боку власників відповідних систем, на яких покладено обов'язок по захисту інформації у системах об'єктів критичної інфраструктури. При цьому актуальним є визначення

суб'єктів, що уповноважені на здійснення перевірки готовності об'єктів критичної інфраструктури до кібератак та кіберінцидентів.

Відповідно до ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України» основними суб'єктами, на які покладено виконання вказаного завдання, є СБ України в частині здійснення негласної перевірки готовності до кібератак та кіберінцидентів (ст. 8), а також Державна служба спеціального зв'язку та захисту інформації України, яка відповідно до ст. 8 закону здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків; інформує про кіберзагрози та відповідні методи захисту від них; забезпечує впровадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури [11]. Таким чином, СБ України здійснює негласну перевірку, у той час як ДССЗЗІ фактично здійснює гласну перевірку готовності об'єктів критичної інфраструктури до кібератак та кіберінцидентів.

Враховуючи викладене, вважаємо, що на сьогодні існує об'єктивна необхідність подальшого унормування та наукового вивчення особливостей здійснення гласної та негласної перевірок готовності об'єктів критичної інфраструктури з метою їх чіткого розмежування між собою та уникнення дублювання виконуваних функцій різними відомствами.

Крім того, варто зазначити, що основною складовою здійснення негласної перевірки готовності об'єктів критичної інфраструктури до кібератак та кіберінцидентів, що покладено на Службу безпеки України, науковці визначають здійснення тестування на проникнення [6; 7]. У той же час тестування на проникнення є одночасно одним із завдань, що вирішується у ході проведення незалежного аудиту інформаційної безпеки [12, с. 20], впровадження якого покладено на Державну службу спеціального зв'язку та захисту інформації України. Вказане додатково підтверджує необхідність подальшого наукового вивчення таких нормативно закріплених завдань.

Висновки. Підсумовуючи викладене, варто зауважити, що виконання завдання з перевірки готовності об'єктів критичної інфраструктури до кібератак та кіберінцидентів може бути ефективним інструментом попередження кібератак на важливі інфраструктурні об'єкти.

Також необхідно зазначити, що в умовах обмеженості у власних ресурсах, використання державними органами та органами безпеки нашої держави існуючого іноземного досвіду та апробованих підходів із залучення фахівців приватного сектору до перевірки готовності об'єктів критичної інфраструктури до кібератак та кіберінцидентів може значно допомогти у формуванні дієвої системи реагування на виклики та загрози, що виникають у кіберпросторі.

Водночас для імплементації наявного іноземного досвіду та повноцінної реалізації законодавчо закріплених механізмів потребують подальшого наукового дослідження питання здійснення перевірки готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів в контексті законності та санкціонованості втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, а також розмежування завдань з негласної перевірки готовності об'єктів та інших організаційно-технічних заходів із запобігання, виявлення та реагування на кіберінциденти і кібератаки та інформаційного аудиту, які є фактично заходами гласної перевірки таких об'єктів.

Список використаних джерел

1. Кібератака на об'єкти критичної інфраструктури України [Електронний ресурс]. – Режим доступу : www.dsszzi. gov.ua.

2. Програма «Зламай Пентагон» успішно завершилась [Електронний ресурс]. – Режим доступу : http://fainaidea.com.

3. Hack the Pentagon [Електронний ресурс]. – Режим доступу : https://www.hackerone.com/resources/hack-the-pentagon.
4. «Hack the Air Force» bug hunting challenge uncovers 120 flaws in websites and services [Електронний ресурс]. – Режим доступу : https://www.zdnet.com/ article/hack-the-air-force-bug-hunting-challenge-uncovers-120-flaws-in-websites-and-services.
5. The European Commission's first-ever bug bounty program, Dec13 2017 [Електронний ресурс]. – Режим доступу : https://www.hackerone.com/blog/the-european-commissions-first-ever-bug-bounty-program.
6. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України : аналіт. доп. / за заг. ред. Д. Дубова. – Київ : НІСД, 2018. – 84 с.
7. Ткачук Н. А. Правове регулювання взаємодії Служби безпеки України з приватним сектором у сфері забезпечення кібербезпеки / Н. А. Ткачук // Інформація і право. – 2018. – № 4(27). – С. 104–111.
8. Науково-практичний коментар Кримінального кодексу України / за ред. М. І. Мельника, М. І. Хавронюка. – 6-те вид., переробл. та доповн. – К. : Юридична думка, 2009. – 1236 с.
9. Курман О. В. Криміналістична характеристика несанкціонованого втручання у роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку / О. В. Курман // Науковий вісник Херсонського державного університету. – 2017. – Вип. 4. – Т. 2. – С. 127–130.
10. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 5 липня 1994 р. № 80/94 // Відомості Верховної Ради України. – 1994. – № 31. – Ст. 286.
11. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163-VIII // Відомості Верховної Ради України. – 2017. – № 45. – Ст. 403
12. Аудит та управління інцидентами інформаційної безпеки : навч. посіб. / [Корченко О. Г., Гнатюк С. О., Казмірчук С. В. та ін.]. – К. : Центр навч.-наук. та наук.-практ. видань НА СБ України, 2014. – 190 с.

Рецензенти:
доктор юридичних наук
В. Гребенюк,
доктор юридичних наук,
старший науковий співробітник
І. Авдошин

Аннотация. В статье исследованы проблемы правового регулирования и практики проверки готовности объектов критической инфраструктуры к кибератакам и киберинцидентам в иностранных юрисдикциях. Предложены пути решения существующих проблем в этом направлении в Украине.
Ключевые слова: информационная безопасность, кибербезопасность, кибератаки, киберинциденты, критическая инфраструктура, незаконное вмешательство, информационный аудит.

Abstract. The article considers issues of legal regulation and ways aimed at controlling critical infrastructure objects preparedness for cyber attacks and cyber incidents under the foreign jurisdiction. The auther offered solutions of current issues which can be implemented in Ukraine.
Key words: information security, cybersecurity, cyber attacks, cyber incidents critical infrastructure, unlawful interference, information audit.