ПЕТРОВ Станіслав Геннадійович

МІЖНАРОДНИЙ ДОСВІД З ПРОТИДІЇ ПРОТИПРАВНИМ ПОСЯГАННЯМ НА ДЕРЖАВНІ ЕЛЕКТРОННІ ІНФОРМАЦІЙНІ РЕСУРСИ

Постановка проблеми. Чисельність посягань на державні інформаційні ресурси (далі – ДЕІР) невпинно зростає. Причому зазначена проблема стосується не тільки України, яка стала полігоном для проведення спецслужбами Росії кібератак, а й зарубіжних держав, у яких об'єкти критичної інформаційної інфраструктури, на яких обробляється ДЕІР, усе частіше стають предметом посягань злочинців. Однією із причин вразливостей є використання неліцензованого програмного забезпечення в системах, що обробляють ДЕІР, а також використання несанкціонованих додатків або іншого програмного забезпечення.

Крім того, Україна знаходиться в унікальному кіберсередовищі й напрацьовує власний досвід протидії гібридній війні Росії. І хоча за минулі декілька років кібератаки, спрямовані на ДЕІР та інші ресурси, спричинили низку негативних наслідків економічного характеру, система протидії кіберзагрозам динамічно розвивається. Задля продовження процесів впровадження платформ з обміну інформацією про кіберзагрози на рівні держави особливу увагу варто звернути на питання міжнародного досвіду щодо протидії протиправним посяганням на ДЕІР.

Аналіз останніх досліджень і публікацій свідчить про те, що питання міжнародного досвіду з протидії протиправним посяганням на ДЕІР були предметом досліджень лише частково. У вітчизняній юридичній літературі науковим розвідкам окремих питань цієї проблематики в різні часи приділяли увагу такі фахівці, як В. Бутузов, О. Довгань, А. Пазюк, В. Пилипчук, О. Ткаченко, К. Тітуніна, О. Юрченко та інші. Серед зарубіжних авторів виокремлюємо роботи таких вчених, як Я. Вільямсон, З. Недовіч-Будіч, А. Раябіфард, М. Фіні, П. Флетчер та інших.

Окремі дослідники обґрунтовують потребу в прийнятті на рівні ООН універсального міжнародно-правового акта, наприклад, Конвенції протидії кіберзлочинності, задля врегулювання міжнародно-правових питань взаємодії державних органів у процесі протидії кіберзагрозам. Інші стверджують, що достатньо дієвими є механізми, передбачені Конвенцією Ради Європи про кіберзлочинність (далі – Конвенція) від 23 листопада 2001 року, яка спрямована на підвищення ефективності кримінальних розслідувань і переслідувань, що стосуються кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними на надання можливості збирання доказів, що стосуються кримінального злочину, в електронній формі [1].

Метою статті є аналіз міжнародного досвіду з протидії протиправним посяганням на державні електронні інформаційні ресурси з метою його використання у діяльності державних, насамперед правоохоронних, органів України.

Виклад основного матеріалу. У попередніх дослідженнях сформульовано наступне визначення поняття «державні електронні інформаційні ресурси»: систематизована, закріплена на матеріальних носіях і/або відображена в електронному вигляді інформація, право на володіння, використання або розпорядження якою належить державі або яка обробляється
фізичними чи юридичними особами відповідно до наданих їм повноважень суб'єктами владних повноважень, призначена для задоволення потреб громадянина, суспільства, держави [2]. Воно, на нашу думку, найбільш повно відповідає як вітчизняному законодавству, так і міжнародно-правовим актам.

Виявлення і припинення протиправних посягань на ДЕІР неможливе без тісної співпраці між державними органами, насамперед правоохоронними, різних країн. Відповідна взаємодія ґрунтується на двосторонніх та багатосторонніх міжнародних договорах про взаємну правову допомогу, взаємне визнання іноземних судових рішень.

Серед універсальних міжнародно-правових документів, окрім згаданої Конвенції, вирізняємо Довідник ООН із запобігання і контролю злочинності, пов'язаної з комп'ютерами, 1995 рік; Десять принципів боротьби з високотехнологічними злочинами, прийняті на зустрічі міністрів внутрішніх справ та міністрів юстиції Великої Вісімки, 1997 рік; Конвенцію ООН проти транснаціональної організованої злочинності, 2000 рік. Одним із перших міжнародних документів у боротьбі з кіберзлочинністю є «Мінімальний список» правопорушень у цій сфері, прийнятий Європейським комітетом з проблем злочинності Ради Європи у 1990 році, який передбачав наступні злочини: комп'ютерне шахрайство, комп'ютерний підлог, пошкодження комп'ютерної інформації чи програм, комп'ютерний саботаж, несанкціонований доступ до комп'ютерних систем, несанкціоноване перехоплення інформації, несанкціоноване копіювання захищених комп'ютерних програм, незаконне виготовлення топографічних копій. Згодом ця класифікація злочинних посягань була скорегована Конвенцією 2001 року. З метою протидії міжнародній кіберзлочинності, а також для координації діяльності правоохоронних органів країн світу такі злочини класифікуються за кодифікатором міжнародної кримінальної поліції Генерального Секретаріату Інтерполу, який з 1991 року інтегровано в автоматизовану систему пошуку, і сьогодні він доступний підрозділам Національних центральних бюро Інтерполу більшості країн світу, зокрема, й НЦБ Інтерполу МВС України.

У Європейському Союзі нормативно-правовими актами, прийнятими для протидії протиправним посяганням на ДЕІР та інші ресурси, є Директива ЄС щодо протидії кібератакам на інформаційні системи, 2013 рік; Директива Єврокомісії щодо боротьби з шахрайством та іншими фінансовими злочинами в мережі Інтернет, 2017 рік.

У ЄС значна увага приділяється проблематиці раннього виявлення й оперативного реагування на кіберінциденти та кібератаки проти ДЕІР. Так, Стратегія кібербезпеки Європейського Союзу [3] у поняття «кіберзахист» додає виявлення і блокування кібератак, локалізацію їх наслідків незалежно від походження стосовно цивільних об'єктів усіх форм власності, а також встановлення і розслідування кіберзлочинів.

Європейська агенція мережевої та інформаційної безпеки (European Network and Information Security Agency, ENISA) забезпечує виконання функції виявлення і блокування кібератак, а також локалізації їх наслідків незалежно від походження стосовно цивільних об'єктів усіх форм власності. CERT-EU (Computer Emergency Response Team) – це структура, яка виявляє кібератаки за допомогою спеціалізованої технологічної системи датчиків, встановлених на абонентських лініях доступу до серверів. У разі здійснення кібератаки спрацьовує датчик, про що оперативно сповіщається CERT-EU. Якщо CERT-EU виявляє кібератаки з ознаками злочинних дій, то відповідна інформація передається до Європейського центру з розслідування кіберзлочинів (European Cybercrime Centre, ECC), який, у свою чергу, може поінформувати про них Європейську агенцію оборони (European Defence Agency) для організації кібероперацій або Європейську службу зовнішніх справ (European External Action Service) [4].

У США ще у 2007 році розпочато реалізацію програми Довірчих інтернет-з'єднань (TIC, Trusted Internet Connections), у межах якої планувалося забезпечити кіберзахист понад 5 тис. інформаційних систем органів і підрозділів федеральної влади США [5].

У США система протидії протиправним посяганням на ДЕІР та інші критичні інформаційні ресурси має більш розгалужений характер. Одним з основних суб'єктів такої системи є Національний центр кібербезпеки та інтеграції зв'язку (NCCIC, National Cybersecurity and Communication Integration Center), до складу якого входять група екстреного реагування на комп'ютерні події в США (US-CERT, U.S. Computer Emergency Response Team), група екстреного реагування на надзвичайні події у системах управління промисловістю (ICS-CERT, Industrial Control Systems Cyber Emergency Response Team) та Національний координаційний центр зв'язку (NCC, National Coordinating Center for Communications).

US-CERT виявляє кібератаки на об’єктах федеральних органів влади США, попереджає про них адміністраторів безпеки інформаційних систем та координує діяльність щодо відновлення федеральних інформаційних систем після кібератак або кіберінцидентів [6].

ICS-CERT попереджає і виявляє кібератаки на інформаційні системи об’єктів критичної інфраструктури в промисловості США [7]. У листопаді 2018 року указом президента США NCCIC передано у підпорядкування нового агентства з кібербезпеки та безпеки інфраструктури міністерства внутрішньої безпеки США [8].

В Україні переважно з урахуванням досвіду ЄС і США розбудовується мережа ситуаційних центрів кіберзахисту на об’єктах критичної інформаційної інфраструктури та система ситуаційних центрів кібербезпеки в основних суб’єктах системи забезпечення кібербезпеки (СБУ, Нацполіція, МОУ, СЗР, ГУР МОУ).

Порівняння міжнародного досвіду протидії протиправним посяганням на ДЕІР свідчить про низку проблемних питань, які потребують як нормативного, так і організаційного вирішення.

Так, наприклад, останнім часом існує тенденція щодо співпраці з країнами-учасниками Конвенції про кіберзлочинність, оскільки відсутні механізми практичної імплементації положень Конвенції в українському законодавстві, насамперед стосовно невідповідності системи збирання електронних доказів, і загалом співвідношення поняття «електронний доказ» за законодавством України та інших країн. Крім того, у процесуальному законодавстві більшості країн-учасниць Конвенції є положення про особливий порядок перехоплення і розкриття інформації про рух даних у комп’ютерних системах задля розслідування кіберзлочинів з метою оперативного припинення кіберзлочину та ліквідації його наслідків.

Однак відповідно до чинного Кримінального процесуального кодексу України [9] для отримання інформації від операторів і провайдерів, необхідної для припинення злочину або встановлення винних у його вчиненні, ліквідації негативних наслідків від кримінального правопорушення, зокрема, блокування (обмеження) ресурсу з протиправним контентом, правоохоронні органи витрачають значний час для одержання відповідного рішення суду в межах кримінального провадження.

Безумовно, зазначена проблема може бути вирішена виключно шляхом законодавчого закріплення механізму оперативного обмеження (блокування) певного інформаційного ресурсу (інформаційного сервісу) та впровадження особливих умов проведення обшуку і арешту електронних доказів, насамперед закріплення процесуально значимої можливості копіювання інформації.

На ефективність розслідувань кіберзлочинів позитивно вплине імплементація у вітчизняне законодавство статей 16–18 Конвенції про невідкладне фіксування і подальше зберігання даних операторами, провайдерами телекомунікацій, постачальниками послуг хостингу, власниками ресурсу (веб-сайту, веб-сторінки тощо) із забезпеченням їх цілісності.

Такі зміни, безперечно, позитивно вплинуть на ефективність співробітництва із спецслужбами та правоохоронними органами країн ЄС у частині надання інформації національними інтернет-провайдерами, оперативності виконання запитів щодо збереження електронних доказів, відповіді на запити про правову допомогу тощо.

Варто відзначити, що СБ України є учасником проекту «CybercrimeEAPIII» щодо налагодження державно-приватного партнерства в Україні, у межах якого задля взаємодії правоохоронних органів та спецслужб країни з ІТ-спільнотою розроблено проект змін до законодавства України, який дозволить повноцінно імплементувати Конвенцію з кіберзлочинності, а також типовий Меморандум про взаєморозуміння між інтернет-провайдерами та державними органами. Безумовно, існує потреба в удосконаленні співробітництва як СБ України, так і Національної поліції з приватним ІТ-сектором щодо протидії кіберзагрозам. Доцільно з урахуванням міжнародного досвіду створити в

Україні державно-приватну мережу з обміну інформацією загалом у сфері кібербезпеки та групу обміну знаннями за участю представників Держспецзв'язку України, СБ України, Національної поліції, а також приватного ІТ-сектору. До такої мережі доцільно включити сховище відкритих аналітичних, криміналістичних матеріалів та ресурсів, а також інструментів та ресурсів для захисту мереж для українських організацій з кібербезпеки, операторів телекомунікаційних мереж.

Корисним також є досвід США щодо функціонування Національного інституту наук та технологій США (NIST), який займає чільне місце у кібербезпековому середовищі цієї держави. Варто розглянути питання щодо створення подібної організації задля проведення форумів для публічно-приватного партнерства щодо розгляду технічних стандартів і стандартів кібербезпеки, а також методичних рекомендацій із кіберзахисту та кібербезпеки.

На рівні Держспецзв'язку України доцільно вводити у дію такі стандарти та методичні рекомендації для основних галузей об'єктів критичної інформаційної інфраструктури та державних органів. Такі рекомендації варто розробляти з урахуванням міжнародних практик та стандартів розвитку груп реагування на інциденти, що пов'язані з кібербезпекою (CERT та CSIRT/SOC). У методичних рекомендаціях доцільно закріплювати питання координації реагування на кіберінциденти, зокрема, процедури інформування суспільства, а також обов'язки державних суб'єктів системи кібербезпеки України щодо захисту критично важливої інфраструктури для запобігання ризикам, реагування на них, зменшення їх впливу та відновлення.

Організація, подібна до NIST, могла би формалізувати систему управління ризиками для державних органів та приватних суб'єктів, долучити їх до відкритої дискусії про загрози, вразливості, стійкість до ризиків, а також можливість їх зниження в кіберкомпонентах сфери національної безпеки України. За допомогою такої організації можна організовувати і впроваджувати програми навчання і підвищення кваліфікації, стажування та обміну між компаніями, що займаються кібербезпекою, і державними органами, а також налагодити співпрацю та обмін співробітниками між групою швидкого реагування (CERT-UA) та іншими групами швидкого реагування об'єктів критичної інформаційної інфраструктури.

З урахуванням міжнародного досвіду задля протидії протиправним посяганням на ДЕІР важливо удосконалювати співробітництво між СБ України та НП України з іноземними органами. Партнерські відносини між ФБР та СБ України і НП України призвели до багатьох арештів та судових процесів у сфері кібербезпеки. Доцільно розширювати співпрацю з правоохоронними органами з інших країни, зокрема, Францією, Німеччиною, Нідерландами, Фінляндією, Японією, Естонією, Сінгапуром та іншими.

Висновки. В Україні враховується досвід ЄС і США щодо розбудови мережі ситуаційних центрів кіберзахисту на об'єктах критичної інформаційної інфраструктури та системи ситуаційних центрів кібербезпеки.

Необхідними змінами законодавства задля протидії протиправним посяганням на ДЕІР має бути закріплення механізму оперативного обмеження (блокування) певного інформаційного ресурсу (інформаційного сервісу) та впровадження особливих умов проведення обшуку і арешту електронних доказів, насамперед закріплення процесуально значимої можливості копіювання інформації, а також імплементація статей 16–18 Конвенції про невідкладне фіксування і подальше зберігання даних операторами, провайдерами телекомунікацій, постачальниками послуг хостингу, власниками ресурсу (веб-сайту, веб-сторінки тощо) із забезпеченням їх цілісності.

У роботі обґрунтовано необхідність створення в Україні організації, подібної до Національного інституту наук та технологій США (NIST), задля проведення форумів для публічно-приватного партнерства щодо розгляду технічних стандартів та стандартів кібербезпеки, а також методичних рекомендацій із кіберзахисту та кібербезпеки.

Перспективами подальших наукових пошуків визначаємо питання охорони і захисту державних електронних інформаційних ресурсів від протиправних посягань.

Список використаних джерел

1. Конвенція про кіберзлочинність від 23 листопада 2001 року // Офіційний вісник України. – 2007. – № 65. – Ст. 253.
2. Петров С. Г. Зміст поняття «державні електронні інформаційні ресурси» // С. Г. Петров, А. І. Марущак // Інформація і право. – 2018. – № 4. – С. 15–21.
3. Cybersecurity Strategy of the European Union : An Open, Safe and Secure Cyberspace / European Comission. High representative of the European Union for foreign affairs and security policy. – Brussels, 7.2.2013. – Join (2013) 1 final.
4. Cybersecurity Strategy of the European Union : An Open, Safe and Secure Cyberspace / European Comission. High representative of the European Union for foreign affairs and security policy. – Brussels, 7.2.2013. – Join (2013) 1 final; An evaluation Framework for National Cyber Security Strategies [Електронний ресурс] / Веб-сайт «European Union Agency for Network and Information Security». – Режим доступу : http://www.enisa.europa.eu.
5. Milton Mueller, Andreas Kuehn. Einstein on the Breach: Surveillance Technology, Cybersecurity and Organizational Change. [Електронний ресурс]. – Режим доступу : https://www.econinfosec.org/archive/weis2013/ papers/MuellerKuehnWEIS2013.pdf.
6. National Infrastructure Protection Plan – NIPP [Електронний ресурс]. – Режим доступу : https://www.dhs.gov/national-infrastructure-protection-plan.
7. ICS-CERT. Industrial Control Systems Cyber Emergency Response Team [Електронний ресурс] // Офіційний веб-сайт ICS-CERT. – Режим доступу : https://ics-cert.us-cert.gov.
8. Cybersecurity and Infrasructure Security Agency [Електронний ресурс] // Офіційний веб-сайт МВБ США. – Режим доступу : https://www.dhs.gov/cybersecurity-and-infrasructure-security-agency.html.
9. Кримінальний процесуальний кодекс України від 13 квітня 2012 року // Офіційний вісник України. – 2012. – № 37. – Ст. 1370.

Рецензенти:
доктор філологічних наук, професор
Л. Компанцева,
доктор юридичних наук, професор
А. Марущак

Аннотация. В статье исследуется международный опыт по противодействию противоправным посягательствам на государственные электронные информационные ресурсы. Сформулированы выводы относительно использования международного опыта в развитии систем киберзащиты и кибербезопасности в Украине, усовершенствования полномочий правоохранительных органов по расследованию противоправных посягательств на государственные электронные информационные ресурсы.

Ключевые слова: информация, ресурс, государственные информационные ресурсы, государственные электронные информационные ресурсы.

Abstract. The article deals with international practices of counteracting the unlawful interference with the state digital information resources. Conclusions are formulated on applying international practices for the development of cyber defense and cyber security systems in Ukraine, improvement of law enforcement agencies powers in investigating cases of the unlawful interference with the state digital information resources.

Key words: information, resources, state information resources, state digital information resources.