СЕКЦІЯ 5
МІЖНАРОДНИЙ ДОСВІД ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

УДК 341:004.056.5

Андрій Васильович ВОЙЦІХОВСЬКИЙ,
кандидат юридичних наук, доцент,
професор кафедри конституційного і міжнародного права факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0001-5629-8852

ПИТАННЯ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ВІД КІБЕРЗАГРОЗ

У той час як можливості інформаційних і телекомунікаційних технологій добре відомі і в даний час широко використовуються, значимість їх взаємодії всередині критичної інфраструктури досі сприймається з недостатнім ступенем серйозності. Вже сьогодні складові елементи національної критичної інфраструктури стали відігравати вирішальну роль в обороноздатності країни, її економічному і соціальному розвитку, тому у більшості випадків атаки на такі об'єкти спрямовані, головним чином, на пошкодження саме цих елементів, що може заподіяти серйозної шкоди національній безпеці і економіці.

Значення терміну «критична інфраструктура» у кожній із країн дещо відрізняється, проте ці відмінності не є суттєвими. Зокрема, згідно з чинним законодавством США під критичною інфраструктурою розуміються «системи та об'єкти, фізичні чи віртуальні, настільки життєво важливі для держави, що недієздатність або знищення таких систем або об'єктів підриває національну безпеку, економіку, здоров'я або безпеку населення, або має своїм результатом будь-яку комбінацію з перерахованого вище».

У законодавстві Великобританії термін «критична інфраструктура» визначений як: «найважливіші елементи інфраструктури, а саме активи, об'єкти, системи, мережі, процеси і ключові посадові особи, втрата яких може привести до згубного впливу на: 1) доступність, цілісність або надання основних послуг, у тому числі тих, порушення цілісності яких може привести до втрати життя або виникнення нещасних випадків з урахуванням значних економічних і соціальних наслідків; 2) національну безпеку, національну оборону або функціонування держави» [1, с. 168].

Зазвичай до критичної інфраструктури відносять енергетичні та транспортні магістральні мережі, нафто- й газопроводи, морські порти, канали швидкісного та урядового зв'язку, системи життєзабезпечення

(водо- й теплопостачання) мегаполісів, утилізації відходів, служби екстреної допомоги населенню та служби реагування на надзвичайні ситуації, високотехнологічні підприємства і підприємства військово-промислового комплексу, а також центральні органи влади. Слід зауважити, що у США критичну інфраструктуру розглядають у більш широкому розумінні, включаючи до неї національні символи (пам'ятки культурної спадщини) [2, с. 3-4].

Запровадження системного підходу до розв'язання проблем захищеності критичної інфраструктури, звичайно, виходить далеко за межі лише введення відповідного терміна. На першому місці – створення дієвого механізму координації зусиль органів влади, спрямованих на недопущення втрати чи завдання невиправної шкоди вузловим елементам критичної інфраструктури внаслідок дії негативних чинників будь-якого походження: техногенного, природного, соціально-політичного або будь-якої їх комбінації.

Практично безмежні можливості використання Інтернету підкреслюють глобальну загрозу віртуальних злочинів, кібертероризму та ведення кібервійни. За останні декілька років по ключових сегментах інфраструктур розвинутих країн неодноразово завдавалися різні за характером і масштабами кібератаки.

Так, кібератака на одну з бразильських ГЕС у листопаді 2009 р. на три дні паралізувала в десяти містах (близько 60 млн. жителів) роботу громадського транспорту, світлофорів, ліфтів та мережі зв'язку. Була призупинена робота декількох тисяч заправок, банків, торговельних центрів і промислових об'єктів.

На початку 2010 р. глава американської контррозвідки підтвердив, що комп'ютерні злочинці отримали доступ до документації найдорожчого військового проекту Пентагону винищувача-бомбардувальника п'ятого покоління F-35 Lightning II. Представники Пентагону відмовилися давати коментарі щодо розмірів завданої шкоди.

Міністр внутрішніх справ Німеччини оголосив у 2010 р. про «значне зростання атак» на німецькі телефонні мережі, мережу Інтернет і, особливо, урядові мережі зв'язку. Міністерства, посольства і державна адміністрація Німеччини стали жертвами потужної і масштабної атаки.

Окремі напади на об'єкти певної критичної інфраструктури зазнавала й Україна. Так, 27 червня 2017 р. найбільшої хакерської атаки, яка поширювала вірус Petya.A, що блокує роботу комп'ютерних систем, зазнали українські державні установи (Кабінет Міністрів України, Національна поліція України та ін.), аеропорт «Бориспіль», «Укртелеком», «Укренерго», «Укрзалізниця», «Укрпошта», держпідприємство «Антонов», Чорнобильська атомна електростанція, державні інтернет-ресурси і локальні мережі, українські медіа і ряд інших великих підприємств. Ця кібератака також призвела до зараження комп'ютерів по всьому світу (США, Великобританія,

Німеччина, Польща, Індія, Литва та ін.), і завдала збитків приблизно на 8 млрд. доларів США. [3]

Останнім часом все більше й більше країн втягуються у «холодну війну» в кіберпросторі, накопичують «кіберможливості», шпигують і тестують комп'ютерні мережі, готуючись використовувати можливості Інтернету в кібервійнах. Деякі країни терміново підвищують свої кібернетичні можливості шляхом створення спеціальних підрозділів з питань протидії нападу в кіберпросторі (Ізраїль, КНР, Німеччина, Франція, Індія, Південна Корея, Естонія та ін.). Крім того, координація зусиль з даного питання на міжнародному рівні дуже активно розгортається в рамках НАТО та ЄС.

Останнім часом цілями кібератак стають критичні інфраструктури країн, що пов'язані з ядерною, хімічною чи будь-якою іншою промисловістю, системами життєзабезпечення великих мегаполісів, фінансовими, продовольчими, енергетичними національними системами, транспортними мережами, діяльністю урядів, правоохоронних органів, армії тощо). Удари завдаються через інформаційно-телекомунікаційні системи, особливо, автоматизовані системи управління, які необхідні для функціонування повсякденного життя людей, структур економіки чи органів влади.

Джерелами таких атак, як правило, є «недружні» держави, терористичні або радикальні організації, і невідомі угруповування або окремі фахівці з програмного забезпечення (так звані «хакери»).

Кібератака на життєво важливі об'єкти критичної інфраструктури може бути інструментом терору, помсти або навіть простого хуліганства. У разі акції недружньої держави такі дії є військовою акцією, у разі хакерської атаки це психологічний спосіб довести свою зверхність та розумову перевагу.

Безпека інформаційних та телекомунікаційних систем вже стала невід'ємною частиною національних оборонних стратегій провідних країн світу. Уже зараз кіберпростір стає п'ятою сферою ведення війни після землі, моря, повітря та космосу. Ті країни, які першими створять системи кіберзахисту, закладуть фундамент законодавчого врегулювання цього питання, зможуть отримати фундаментальну перевагу на початкових стадіях загострення проблеми кіберзахисту.

На сьогодні захист критичної інфраструктури ствердився як важливий напрям політики у сфері безпеки країн-членів ЄС і НАТО. На відміну від США, де було створено єдиний орган виконавчої влади – Міністерство внутрішньої безпеки, Німеччини – Федеральне міністерство внутрішніх справ, Польщі – Урядовий центр безпеки, на які покладено функції координації захисту національної критичної інфраструктури, в ЄС такого органу немає. Відповідні функції захисту критичної інфраструктури в ЄС виконують відповідні органи окремих країн-членів [1, с. 171].

У Євросоюзі загальноєвропейський підхід до захисту критичної інфраструктури задекларовано в Повідомленні Європейської Комісії

про європейську програму захисту основних інфраструктур № 786 від 2006 р. [4] і Директиві Ради ЄС № 114 від 2008 р. про ідентифікацію, призначення європейських критичних інфраструктур і необхідність покращення їх захисту. [5] До загальноєвропейської критичної інфраструктури належать ті елементи національних критичних інфраструктур країн-членів ЄС, відмова, інцидент або атака на які може мати значний вплив і на країну, в якій ця подія відбудеться, і хоча б на одну з інших країн-членів ЄС. Згаданим Повідомленням започатковано Європейську програму із захисту критичної інфраструктури, розроблену задля підвищення рівня захищеності останньої у спосіб створення спільного підходу до її захисту в країнах-членах ЄС і гармонізації національних законодавств у згаданій сфері.

Висновок. З огляду на реальність, яку ми спостерігаємо і в якій ми живемо, виникає нагальна необхідність щодо регулювання захисту критичної інфраструктури по відношенню до усього спектру загроз і ризиків, оскільки саме критична інфраструктура забезпечує життєво важливі для населення, суспільства та держави послуги та функції, без яких неможливі їх безпечне існування та благополуччя, а також належний рівень національної безпеки.

Захист критичної інфраструктури повинен здійснюватися не лише шляхом оновленням термінів в національних законодавствах країн, але й розробкою і впровадженням нових підходів забезпечення національної кібернетичної безпеки. Основними чинниками таких заходів повинні бути створення безпекового партнерства між усіма заінтересованими сторонами (державами і приватним сектором), організація комплексної оцінки загроз критичній інфраструктурі та їх впливу на рівень національної безпеки в окремих її складових, створення механізму моніторингу та попередження кризових ситуацій, що пов’язані із функціонуванням критичної інфраструктури.

Список бібліографічних посилань

1. Євсєєв В. О. Можливі шляхи удосконалення захисту критичної інфраструктури України з урахуванням світового досвіду // *Збірник наукових праць Харківського національного університету Повітряних Сил*. 2016, № 4(49). С. 168-172.

2. Бірюков Д. С. Кондратов С. І. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні. Київ : НІСД, 2012. 96 с.

3. Масова кібератака вірусом Petya досі не припинилася – Європол // УНІАН Інформаційне агентство: сайт / Новини науки та ІТ. 28.06.2017. URL: https://www.unian.ua/science/2000881-masova-kiberataka-virusom-petya-dosi-ne-pripinilasya-evropol.html (дата звернення: 30.10.2018).

4. Communication from the Commission on a European programme for critical infrastructure protection: adopted by Commission of the european communities on 12 December 2006 (COM/2006/786 final) / European Union. URL: http://ec.europa.eu/transparency/regdoc/rep/1/2006/EN/1-2006-786-EN-F1-1.Pdf (дата звернення: 30.10.2018).

5. Council directive on the identification and designation of european critical infrastructures and the assessment of the need to improve their protection: Directive 2008/114/EC of 8 December 2008 / Official Journal of the European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2008.345.01.0075.01.ENG (дата звернення: 30.10.2018).

Одержано 30.10.2018

УДК 343.43

Таміла Володимирівна ГЕРУЛА,
студентка юридичного факультету 4 курсу 452 групи
Чорноморського національного університету імені Петра Могили;
Олександра Сергіївна ТУНТУЛА,
кандидат юридичних наук,
доцент кафедри цивільного та кримінального права і процесу
Чорноморського національного університету імені Петра Могили

МІЖНАРОДНИЙ ДОСВІД ПРОТИДІЇ ТОРГІВЛІ ЛЮДЬМИ

Однією з проблем, що стоять сьогодні перед Україною та міжнародними організаціями, є торгівля людьми. Кожного року мільйони людей у світі стають жертвами відкритої чи таємної торгівлі. Це негативне явище може виявлятися у різних формах – від викрадення людей до їх продажу з використанням обману, шантажу чи уразливого стану особи. Жертви торгівлі людьми використовуються для примусової праці, у порнобізнесі, як донори для трансплантації тканин і органів тощо. Міжнародні уряди, організації спрямовують свою діяльність на створення програм, стратегій, законів та механізмів, які будуть протидіяти даній проблемі [1].

На даний час поняття «торгівля людьми» визначено низкою нормативно-правових актів. Базове, міжнародно-узгоджене визначення торгівлі людьми міститься в Протоколі про попередження і припинення торгівлі людьми, особливо жінками та дітьми, і покарання за неї, що доповнює Конвенцію ООН проти транснаціональної організованої злочинності (Палермський протокол), у підпункті (а) ст. 3: «Торгівля людьми – означає здійснювані з метою експлуатації вербування, перевезення, передачу, приховування або одержання людей шляхом загрози силою чи її застосування або інших форм примусу, викрадення, шахрайства, обману, зловживання владою або уразливістю становища, шляхом підкупу, у вигляді платежів, вигод для одержання згоди особи, яка контролює іншу особу»[2].

За даними Держдепартаменту США масштаби транснаціональної торгівлі людьми становлять від 600 до 800 тисяч осіб на рік. Центр безпеки людини в Канаді з урахуванням внутрішньої торгівлі людьми в різних країнах оцінює кількість жертв цього злочину в 4 млн. осіб.