УДК 343.2
DOI https://doi.org/10.24144/2307-3322.2024.81.2.51

ОСОБЛИВОСТІ ВІДПОВІДАЛЬНОСТІ ЗА КІБЕРАТАКИ В КРАЇНАХ ЄС

Салій А.Я.,
аспірант ПВНЗ «Європейський університет»
ORCID: https://orcid.org/0009-0002-9088-5879
e-mail: nauka.ta.robota@gmail.com

Салій А.Я. Особливості відповідальності за кібератаки в країнах ЄС.

Стаття присвячена особливостям відповідальності за кібератаки в країнах Європейського Союзу. Зазначено, що кібератаки на державні органи можуть бути складовою частиною кібервійни або гібридної війни і при цьому становити загрозу для національної та глобальної безпеки, оскільки вони можуть призвести до витоку важливої інформації, порушити роботу державних систем та призвести до різних негативних наслідків. Так, наприклад, в Європі основними цілями хакерів з 2022 року, окрім України, стали Польща, країни Балтії, Північної Європи та Німеччина. Частка кібератак на країни Європейського Союзу (далі – ЄС) зросла з близько 10% у першому кварталі 2022 року, до майже 50% у 2023 році. Загалом на Україну у 2022 році було здійснено 162 кібератаки; на Польщу – 114; Естонію, Литву та Латвію – 157; Швецію, Норвегію, Данію та Фінляндію – 95, Німеччину – 57.

Встановлено зростання активності кібератак на мережі енергетичного сектору, дипломатичний корпус, силові відомства, оборонний комплекс, державні підприємства та медіа-компанії. Основною метою цих атак є завдання шкоди критичній інфраструктурі країни. Глобально спостерігається стійка тенденція до зростання кількості цілеспрямованих кібератак на об'єкти критичної інфраструктури протягом останніх років. І тому, у зв'язку з можливими негативними наслідками в разі реалізації кібератак, важливо відзначити, що забезпечення ефективного функціонування системи кіберзахисту країни залишається високопріоритетним завданням. Кожен рік підкреслює актуальність цього завдання, оскільки загрози в кіберпросторі продовжують зростати та стають все більш високоспеціалізованими.

Зроблено висновок, що важливим для визначення можливої відповідальності в країнах Європейського Союзу за кібератаку виступатиме їх публічна атрибуція, яка включатиме ідентифікацію та публічне оголошення того, хто стоїть за конкретною кібератакою, яка впливає на державні, комерційні або інші об'єкти.

Ключові слова: кібератака, кіберзлочини, кримінальна відповідальність, кіберзагрози, Європейський Союз.

Saliy A.Ya. Features of liability for cyber-attacks in EU countries.

The article is devoted to the peculiarities of responsibility for cyber-attacks in the countries of the European Union. It is noted that cyber-attacks on state bodies can be a component of cyber war or hybrid war and at the same time pose a threat to national and global security, as they can lead to the leakage of important information, disrupt the operation of state systems and lead to various negative consequences. So, for example, in Europe, the main goals of hackers from 2022, in addition to Ukraine, became Poland, the Baltic countries, Northern Europe and Germany. The share of cyberattacks on European Union (EU) countries increased from about 10% in the first quarter of 2022 to almost 50% in 2023. In total, 162 cyber-attacks were carried out on Ukraine in 2022; to Poland – 114; Estonia, Lithuania and Latvia – 157; Sweden, Norway, Denmark and Finland – 95, Germany – 57.

An increase in the activity of cyber-attacks on the networks of the energy sector, the diplomatic corps, law enforcement agencies, the defense complex, state enterprises and media companies has been established. The main goal of these attacks is to damage the country's critical infrastructure. Globally, there has been a steady trend towards an increase in the number of targeted cyber-attacks on critical infrastructure facilities in recent years. And therefore, in connection with the possible negative

consequences in the case of the implementation of cyber-attacks, it is important to note that ensuring the effective functioning of the country's cyber defense system remains a high-priority task. Each year underscores the urgency of this challenge as threats in cyberspace continue to grow and become more highly specialized.

It was concluded that their public attribution will be important for determining possible responsibility in the countries of the European Union for a cyber-attack, which will include the identification and public announcement of who is behind a specific cyber-attack that affects state, commercial or other objects.

Key words: cyber-attack, cybercrimes, criminal responsibility, cyber threats, European Union.

Постановка проблеми. Кібератаки на державні органи можуть бути складовою частиною кібервійни або гібридної війни і при цьому становити загрозу для національної та глобальної безпеки, оскільки вони можуть призвести до витоку важливої інформації, порушити роботу державних систем та призвести до різних негативних наслідків. Так, наприклад, в Європі основними цілями хакерів з 2022 року, окрім України, стали Польща, країни Балтії, Північної Європи та Німеччина. Частка кібератак на країни Європейського Союзу (далі – ЄС) зросла з близько 10% у першому кварталі 2022 року, до майже 50% у 2023 році. Загалом на Україну у 2022 році було здійснено 162 кібератаки; на Польщу – 114; Естонію, Литву та Латвію – 157; Швецію, Норвегію, Данію та Фінляндію – 95, Німеччину – 57 [1].

Цілком зрозуміло, що державні органи зазвичай володіють ключовими частинами інфраструктури, такими як: енергетика, транспорт, телекомунікації тощо. А тому кібератаки, спрямовані саме на ці сектори, створюють найбільшу загрозу. А оскільки кіберзагрози можуть мати транснаціональний характер, дослідження відповідальності сприяє міжнародній співпраці у боротьбі з кіберзлочинами, а встановлення норм та міжнародних стандартів допомагає ефективніше реагувати на такі загрози.

Стан дослідження. Правові, технічні та інші аспекти здійснення кібератак досліджувало багато вчених, серед яких: С.А. Буяджи, Р.В. Грищук, О.І. Денькович, О.В. Кузьменко, Д.О. Маріц, М.І. Саєнко, О.О. Сурілова, О.Р. Ярема та інші.

Мета статті полягає у дослідженні особливості відповідальності за кібератаки в країнах Європейського Союзу.

Виклад основного матеріалу. Кібератака – це поняття, яке стало вже звичним явищем у сучасному суспільстві. Соціологи всього світу одностайно стверджують, що сучасне суспільство стало як ніколи раніше конфліктним. Кількість конфліктів у політичній, соціальній, трудовій, релігійній, а також особистісних сферах невпинно збільшується. В свою чергу, розвиток науки та новітніх технологій не завжди приносить користь, а навпаки – їх використання стає вдалим інструментарієм для винахідливих віртуальних злочинців [2, с. 105].

Д.О. Маріц вважає, що інформаційна війна 21 сторіччя відрізняється від «холодної війни» тим, що способів впливу на маси стало набагато більше. Якщо раніше більшість людей довіряли ЗМІ, як єдиному джерелу інформації, яке не могло збрехати, то зараз довіра до телебачення значно впала, і будь-яка інформація, яка надходить через екран, повинна підкріплюватись чимось дуже значним, яскравим і навіть лячним. Щоб належним чином надавати таку інформацію, ЗМІ була створена ціла система, яка спрямовується на те, щоб тримати увесь світ на «гачку». Інтернет став не просто інноваційним проривом, а як наслідок став використовуватись як інформаційний важіль. Мільйони людей витрачають більшу частину свого життя на теренах всесвітнього павутиння, і частина такого життя дуже особиста, навіть інтимна. І можливо, більшість вірить в те, що це його особистий віртуальний простір, який начебто залишиться секретним від інших. В такі ігри грають не тільки Android з Apple, але і антивірусні компанії, які із задоволенням запускають вірусні програми, проти яких потім і борються. Ось такий віртуальний театр відбувається повсякчас у кіберпросторі. Конфлікти, які виникають, не вирішуються, а натомість розробляються більш закручені стратегії, які дозволяють здійснювати більш ефективні кібератаки. Вони можуть вивести з ладу об'єкти оборонного призначення, та будь-які інші об'єкти, які представляють інтерес для кіберзлочинців [2, с. 107].

Дослідження доступної інформації свідчить про зростання активності кібератак на мережі енергетичного сектору, дипломатичний корпус, силові відомства, оборонний комплекс, державні підприємства та медіа-компанії. Основною метою цих атак є завдання шкоди критичній інфра-

структурі країни. Глобально спостерігається стійка тенденція до зростання кількості цілеспрямованих кібератак на об'єкти критичної інфраструктури протягом останніх років.

І тому, у зв'язку з можливими негативними наслідками в разі реалізації кібератак, важливо відзначити, що забезпечення ефективного функціонування системи кіберзахисту країни залишається високопріоритетним завданням. Кожен рік підкреслює актуальність цього завдання, оскільки загрози в кіберпросторі продовжують зростати та стають все більш високоспеціалізованими.

При цьому, варто розуміти, що у випадку успішної кібератаки на державні об'єкти настануть дуже серйозні наслідки. Наприклад, на думку С. Гончара та Г. Леоненка, будь-яка кібератака призведе до прямих та непрямих збитків. Прямі збитки є витратами, які пов'язані з заміною активів. Збитки можуть мати місце за причиною фізичного пошкодження активу, в результаті втрати цілісності або доступності, переривання точної послідовності або зміни характеру процесу. Активи можуть мати порівняно низькі прямі збитки по відношенню до їх корисності, оскільки носій, який використовується для зберігання активу, як правило, має низьку вартість. Незначні пошкодження людських активів з коротким часом відновлення можуть мати низькі прямі збитки для організації, навіть у випадку довгострокових наслідків для травмованої людини.

Непрямі збитки є збитками завданими внаслідок втрати активів. Вони можуть включати в себе збитки, пов'язані з процесом простою, переробки або інші виробничі витрати через втрату активів.

Для фізичних активів непрямі збитки, як правило, включають наслідки, які виникають через втрату компонентів. Непрямі збитки від пошкодження обладнання можуть призвести до ремонту, реінжинірингу або інших зусиль для відновлення контролю над промисловим процесом. Водночас непрямі збитки часто можуть бути дуже великими. Вони включають в себе втрату довіри громадськості, втрату ліцензії на діяльність, втрату конкурентних переваг від випуску інтелектуальної власності, як наприклад конфіденційний процес, нові технології тощо [3, с. 109-110].

Відповідно до Закону Королівства Іспанія «Про встановлення заходів щодо захисту критичної інфраструктури» негативними наслідками кібератак є:

– кількість залучених громадян (загиблі, поранені з тяжкими травмами та іншими серйозними наслідками для здоров'я);

– економічний ефект (економічні втрати та погіршення якості продукції та послуг);

– вплив на навколишнє середовище;

– політичні наслідки (довіра до органів державного управління) та соціальні наслідки (фізичні страждання, порушення повсякденного життя) [4, с. 219].

Концепція критичної інфраструктури у Словацькій Республіці, її захисту та оборони до основні критеріїв для визначення критичності інфраструктури відносить порушення системи, що призведе:

– до загибелі більш ніж 50 осіб;

– до впливу на здоров'я наслідком якого стане госпіталізація більш ніж 100 осіб терміном на тиждень;

– до ускладнення здійснення внутрішньої безпеки держави;

– втрат більш ніж 10 млн. євро на день;

– неможливості постачання питної води або їжі протягом тижня для 100 тис. осіб;

– неможливості постачання електроенергії протягом 3 діб або природного газу протягом тижня для населення більш ніж 100 тис. осіб;

– неможливості постачання нафтопродуктів протягом тижня для населення більш ніж 100 тис. осіб;

– зараження поверхні більш ніж 100 га;

– втрати систем зв'язку протягом доби, що може спричинити збої в підтримці роботи інших критичних систем [4, с. 219].

Крім того, в ЄС нормативно-правовими актами, прийнятими для протидії протиправним посяганням на електронні інформаційні ресурси є Директива ЄС щодо протидії кібератакам на інформаційні системи та Директива Єврокомісії щодо боротьби з шахрайством та іншими фінансовими злочинами в мережі Інтернет.

Саме в Директиві Єврокомісії зазначено масштаб наслідків кібератак (географічне охоплення території, для якої втрата елементу критичної інфраструктури завдає значної шкоди): міжнародний, національний, регіональний або територіальний. А також встановлено градацію важкості можливих наслідків за такими показниками, як:

– вплив на населення (число постраждалих, загиблих, осіб, які отримали значні травми, а також чисельність евакуйованого населення);

– економічна шкода (вплив на ВВП, розмір економічних втрат, як прямих, так і непрямих);

– екологічна шкода (вплив на населення та навколишнє природне середовище);

– взаємозв'язок з іншими елементами критичної інфраструктури;

– політичний ефект (втрата впевненості в дієздатності влади);

– тривалість впливу (як саме і коли проявлятимуться наслідки, пов'язані зі втратою чи відмовою об'єктів критичної інфраструктури) [4, с. 220].

Безкарність в кіберпросторі підштовхнула Європейський Союз та його держав-членів до максимізації зусиль, що спрямовані на ідентифікацію і встановлення відповідальності тих, хто стоїть за кібероперaціями. В результаті Європейський Союз прийшов до прийняття Рамок для спільного дипломатичного реагування ЄС на шкідливу кібердіяльність, що наразі представляють унікальний підхід до реагування на кібератаки.

Слід також зазначити, що 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) [5].

При цьому, результативний нагляд несприятливих явищ в кібепросторі, зокрема, таких, як протизаконність, закликає до значно більш активного інтернаціонального партнерства, чим наявні заходи по боротьбі з різними іншими формами міжнародної злочинності. Власне, отже, крім гармонізації кримінально-правових норм, необхідна гармонізація процесуальних важелів і формування нових елементів інтернаціонального партнерства. Важливу значимість у війні з кіберзлочинністю представляють інтернаціональні договори в належній сфері, подібні, так само як Конвенція Ради Європи про кіберзлочинність, рішення Ради Європейського Союзу, Модельний Закон Співдружності Націй про комп'ютерні злочини 2002 р., Модельний Закон країн Карибського Басейну про кіберзлочинність (проект HIPCAR), спільний проект Європейського союзу і Міжнародного Союзу Електрозв'язку для держав Тихоокеанського регіону (проект ICB4PAC), проект ООН з розробки законодавства в галузі кіберзлочинності для країн Африки (проект ESCWA) тощо [6, с. 389].

Крім того, на основі зібраних даних щодо здійснення кібератак можна констатувати наступне. До країн, які постраждали від кібератак відносяться Австрія, Польща, Італія, Німеччина, Литва, Латвія, Чехія, Норвегія, Франція, Бельгія, Люксембург, Нідерланди, Швейцарія, Болгарія, Туреччина, Данія, Швеція, Данія, Фінляндія, Угорщина, Іспанія. До країн-ініціаторів здійснення кібератак на території Європейського Союзу віднесено Росію, Китай, Північна Корея, В'єтнам, Ліван, Іран, Казахстан, США. Крім цього, виявлено наступні типи кібератак: шпіонаж, пошкодження або знищення інформації, дефейс, саботаж, доксинг, фінансова крадіжка, відмова в обслуговуванні. Дані кібератаки були здійснені на об'єкти різних сфер: публічний та приватний сектор, військовий сектор, громадянське суспільство [7, с. 98].

На нашу думку, важливим для визначення можливої відповідальності в країнах Європейського Союзу за кібератаку виступатиме їх публічна атрибуція, яка включатиме ідентифікацію та публічне оголошення того, хто стоїть за конкретною кібератакою, яка впливає на державні, комерційні або інші об'єкти.

Публічна атрибуція кібератак – це завжди реалізація суверенного права держави, тому держави (як постраждалі, так і треті), можуть публічно присвоїти кібератаку іншій державі або утриматись від таких дій. Така атрибуція здійснюється на підставі аналізу даних власної розвідки, оцінки політичних індикаторів, а також результатів роботи CERT-EU та INTCEN, які на рівні Союзу сприяють виробленню спільного розуміння. Враховуючи політичне забарвлення цього виду атрибуції і нерівні людські та технічні можливості, державам-членам ЄС досить складно прийти до спільного рішення. Внаслідок цього їх підходи до публічної атрибуції досить різні: одні за-

ймають активну позицію та навіть здійснюють політичну атрибуцію разом з державами, які не є членами ЄС (Нідерланди, Німеччина, Великобританія до виходу з ЄС), інші – утримуються від політичного присвоєння кібератак державам (Франція) [8, с. 210].

Саме тому, на нашу думку, доцільним було також відкриття Європейського центру компетенції у сфері кібербезпеки 09 травня 2023 року у Бухаресті. Необхідність у ньому стала актуальною після збільшення гібридних та кібератак на інфраструктуру Європи [9].

Висновки. Отже, з огляду на все вищезазначене, можемо зробити висновок, що безкарність у кіберпросторі стало стимулом для Європейського Союзу та його держав-членів активізувати зусилля з ідентифікації та встановлення відповідальності за кібератаки. У результаті, ЄС прийшов до прийняття Рамок для спільного дипломатичного реагування на кіберзлочинність, що представляє унікальний підхід до реагування на кібератаки.

Крім того, саме публічна атрибуція кібератак в ЄС є інструментом суверенного права держав, проте існує складність прийняття спільного рішення через політичні та технічні обмеження. Ініціатива створення Європейського центру компетенції у сфері кібербезпеки свідчить про необхідність координації та співпраці для зміцнення кіберзахисту в Європі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. 2022-2023: A year of cyber conflict in Ukraine. Summary of extensive analysis from the Thales Cyber Threat Intelligence Team. URL: https://bo-cyberthreat.thalesgroup. com/sites/default/files/2023-03/Brochure-resume-A5-WEB.pdf (дата звернення 07.02.2024).
2. Маріц Д.О. «Кібератака» – війна майбутнього. *Інформація і право*. 2015. № 3. С. 104–109.
3. Гончар С., Леоненко Г. Наслідки можливих кібератак на об'єкти критичної інфраструктури. *Information Technology and Security*. 2016. Vol. 4, № 1. С. 108–113.
4. Дрейс Ю.О. Аналіз базової термінології і негативних наслідків кібератак на інформаційно-телекомунікаційні системи об'єктів критичної інфраструктури держави. *Захист інформації*. 2017. Т. 19, № 3. С. 214–222.
5. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. URL: http://www.enisa.europa.eu. (дата звернення: 07.02.2024).
6. Саєнко М.І., Савела Є.А., Тополянський Ю.Ю. Міжнародний досвід протидії кіберзлочинності та кібершахрайству. *Науковий вісник Ужгородського Національного Університету. Серія: Право*. 2021. Вип. 64. С. 386–391.
7. Кузьменко О.В., Доценко Т.В., Боженко В.В., Світлична А.О. Закономірності здійснення кібератак в країнах єс на основі використання асоціативних правил. *Вісник Сумського державного університету. Серія: Економіка*. 2021. № 1. С. 95–103.
8. Сурілова О.О. Публічна атрибуція кібератак державами-членами ЄС та застосування кіберсанкцій союзом щодо кібератак, які становлять загрозу ЄС та його членам. *Правова держава*. 2021. № 43. С. 209–216.
9. У Бухаресті відкрили Європейський центр з кібербезпеки. URL: https://ms.detector.media/kiberbezpeka/post/31891/2023-05-09-u-bukharesti-vidkryly-ievropeyskyy-tsentr-z-kiberbezpeky/ (дата звернення: 07.02.2024).