УДК 343.9. 01
DOI 10.33244/2617-4154.3(16).2024.296-302

Я. П. Харченко,
аспірант,
Державний податковий університет
e-mail: ykharchenko90@gmail.com
ORCID ID 0009-0004-9997-7088

КРИМІНОЛОГІЧНЕ ЗАБЕЗПЕЧЕННЯ ОХОРОНИ КІБЕРПРОСТОРУ ВІД КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ У СФЕРІ ЕКСПЛУАТАЦІЇ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ

У цій статті вказується про постійний розвиток сучасних технологій, що зумовлює необхідність постійного оновлення кіберзахисту сфери кіберпростору. Зазначено, що відкрите вторгнення РФ пришвидшило вдосконалення чинного законодавства та гарантій безпеки в сучасному інформаційному ІТ просторі. Сучасний прогрес нікого не залишає осторонь, що й обумовило прояв такого явища, як кіберзлочинність. У всьому світі кримінальні правопорушення у сфері експлуатації електронно-обчислювальної техніки в кіберпросторі з року в рік завдають збитків на десятки мільярдів американських доларів як фізичним особам і приватним компаніям, так і державам загалом.

Звертається увага, що під час війни в зоні ризику перебувають державні органи, великі підприємства, підприємства оборонної та критичної інфраструктури, а також підприємства, які забезпечують населення та оборону всім необхідним в умовах війни. Є ризики й для місцевих жителів, які перебувають у зоні бойових дій. Під час воєнного стану кожному варто звернути увагу на декілька аспектів контролю: для компаній, органів влади та посадовців наявність залученого технічного спеціаліста зі спеціалізованої компанії суттєво підвищить рівень кіберзахисту. Професіонали здатні ускладнити роботу ворогу через запровадження в компанії необхідних механізмів захисту, зокрема організаційних.

Зазначено, що підґрунтя законодавчого забезпечення механізмів для ефективного кіберзахисту в умовах воєнного стану існує. І існує воно ще з початку двохтисячних років, коли Україна ратифікувала міжнародну конвенцію із запобігання кіберзлочинності від 23 листопада 2001 року. Акцентується увага на тому, що завданням кожного під час виявлення кібератаки залишається якнайшвидше активувати цей механізм, щоб у майбутньому подібних кібернападів та втручань і збитків від них ставало дедалі менше. А відсіч таких атак ставала ефективнішою.

Ключові слова: *запобігання, злочинність, кібератаки, кримінальні правопорушення, кіберзахист, кримінологія, електронно-обчислювальна техніка, кіберзлочин.*

Постановка проблеми. На сьогодні світ зазнав кардинальних реформацій. Так, наразі ми не можемо уявити свого життя без інтернету, комп'ютерів, смартфонів та інших сучасних технологій. Поряд з реальним світом розвивається віртуальний, який у майбутньому може вплинути на сфери нашого звичного життя. Такий розвиток подій є наслідком так званої цифрової революції, яка відбувається завдяки розвитку IT-технологій. Прогрес нікого не залишає осторонь, що й обумовило прояв такого явища, як кіберзлочинність. У всьому світі кримінальні правопорушення у сфері експлуатації електронно-обчислювальної техніки, або кіберзлочини, у кіберпросторі з року в рік завдають збитків на десятки мільярдів американських доларів як фізичним особам і приватним компаніям, та і державам загалом.

Аналіз останніх досліджень і публікацій. У сучасній кримінології все більше піднімаються теми для обговорення проблеми кіберзлочинності як загрози інформаційному простору та перебувають у сфері інтересів все більшої кількості науковців і практиків. Серед когорти знаних науковців М. В. Гуцалюк, Г. В. Дідківська, М. О. Кравцова, В. В. Марков, Ю. В. Нікітін, Є. Д. Скулиш, О. В. Таволжанський, інші. Незважаючи на це, все ще існує потреба в подальшому дослідженні саме кримінологічного забезпечення охорони кіберпростору від кримінальних правопорушень у сфері експлуатації електронно-обчислювальної техніки, що, на нашу думку, дасть змогу надати певне розуміння небезпеки кіберзлочинності для соціуму.

Виклад основного матеріалу. Кримінальні правопорушення у сфері експлуатації електронно-обчислювальної техніки визначають як кіберзлочини і дають визначення у фаховій літературі як «кримінальні правопорушення, вчинені в кіберпросторі за допомогою спеціальних пристроїв (комп'ютерів, смартфонів, планшетів, терміналів та інших), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, та пов'язані з протиправним, несанкціонованим створенням, зберіганням, обробленням, підробленням, блокуванням, знищенням об'єктів інформаційної інфраструктури» [1].

Відповідно до вищезазначеного, кіберзлочинність можна вважати такою, що охоплює різноманітні сфери життя в суспільстві та будь-хто може стати його жертвою такого правопорушення.

То чому ж такий вид кримінальних правопорушень так швидко поширюється на всі сфери нашого життя. Відповідь, як вбачається, дуже проста, великий відсоток того, що діяння залишиться поза увагою правоохоронних органів. Кримінальні правопорушення у сфері експлуатації електронно-обчислювальної техніки є досить латентними.

В умовах війни, в яких перебуває Україна, такі кримінальні правопорушення можуть вчинятися з метою дестабілізації ситуації на неокупованих територіях, крадіжки конфіденційної інформації, диверсії на державних підприємствах, завдання інших тяжких наслідків.

Латентність кримінальних правопорушень у сфері експлуатації електронно-обчислювальної техніки / кіберзлочини у фаховій літературі пояснюється такими ознаками: здійснення такого кримінального правопорушення вимагає певного набору знань; кіберзлочини, на відміну від інших інтелектуальних злочинів, доступні людям невисоких соціальних і вікових можливостей; для здійснення кіберзлочинів не треба

займати високе соціальне положення, досить мати доступ до мережі Інтернет та електронну обчислювальну техніку; анонімність і неперсоніфікованість кіберзлочинів – механізми ідентифікації кіберпростору дають змогу особі здійснювати користування анонімно або видавати себе за іншу особу, змінювати біографічні дані або соціальний статус.

В умовах війни такий кіберзлочинець стає бойовою одиницею, а його основна діяльність – кібератаки і злами. Крім того, під час воєнного стану атаки можливі як зі сторони ворога, який використовує інфопростір для шкоди обороноздатності України, так і зі сторони тих, хто вирішив скористатися ситуацією, перевантаженістю правоохоронних органів для власного збагачення. Тож сьогодні війна в інформаційному просторі може завдати не меншої шкоди, аніж війна на полі бою. Розуміючи це, у перший місяць війни парламент оперативно оптимізував кримінальне та кримінально-процесуальне законодавство, удосконаливши підстави та процесуальні механізми притягнення до кримінальної відповідальності кіберзлочинців [2].

Наразі в Україні спостерігається тенденція збільшення кібератак, тому в умовах війни постає потреба посилити кримінальну відповідальність.

Президент України Указом від 01.02.2022 № 37/2022 ввів у дію рішення РНБО «Про План реалізації Стратегії кібербезпеки України». Правоохоронні органи мають мінімізувати кіберзлочинність.

Кримінальний кодекс не узгоджувався з законодавством у сфері кібербезпеки та не забезпечував повноту і всебічність розслідування кіберзлочинів, а відповідальність була неспівмірною зі шкодою державі та суспільству.

Тому парламентарі оптимізували для протидії кіберзагрозам: 1) ст. 361 КК України – кібератака; 2) ст. 361-1 КК України – створення, розповсюдження та збут шкідливих програм чи техніки для кібератак. Закон України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» 03.04.2022 набув чинності (опублікований у «Голос України» 02.03.2022), за яким: стст. 361 та 361-1 КК України узгоджені із законодавством у сфері кібербезпеки; у ст. 361 КК України розмежована суворість покарання за кібератаку залежно від наслідків та посилив покарання – від штрафу до 15 років в'язниці; пошук та виявлення вразливостей – не кібератака (ч. 6 ст. 361 КК України); посилено покарання за ст. 361-1 КК України – від штрафу до 5 років в'язниці [3].

Також, відповідно до Закону України «Про електронні комунікації» та вимог іншого законодавства України у сфері кібербезпеки, термін «електронно-обчислювальні машини (комп'ютери), автоматизовані системи, комп'ютерні мережі чи мережі електрозв'язку» замінено на «інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні системи, електронні комунікаційні мережі».

Сучасний стан речей вимагає від кожної сучасної соціально активної людини в Україні використовувати мобільні пристрої та користуватися інтернетом, державні органи впроваджують електронний документообіг, стабільна діяльність фінансових установ, залізниці й авіатранспорту, великих підприємств залежить і від стабільності кіберпростору, з яким вони вимушені працювати, та забезпечується комунікація за допомогою електронних засобів зв'язку.

Досліджуючи історію розвитку злочинності, варто звернути увагу на одну закономірність: де розвиваються нові суспільні відносини, там з'являється й злочинність. Відповідно до офіційної статистики Офісу Генерального прокурора України, останнім часом кількість виявлених кримінальних правопорушень у сфері експлуатації електронно-обчислювальної техніки збільшилась майже в 7,5 раза (і це не враховуючи класичних правопорушень з використанням комп'ютерної техніки, а також рівня латентності такої злочинності).

Варто згадати невдалу спробу атаки хакерського угруповання Strontium, які намагалися отримати доступ до комп'ютерних мереж в Україні, США та ЄС, щоб забезпечити тактичну підтримку фізичного вторгнення росії в Україну та викрасти конфіденційну інформацію.

На початку повномасштабного вторгнення РФ Держспецзв'язку повідомило про отримання українськими користувачами нових небезпечних електронних листів з темою «№ 1275 від 07.04.2022», відкриття яких призводить до отримання хакерами повного контролю над вашим комп'ютером та загрожує крадіжкою та пошкодженням комп'ютерних даних.

Раніше Держспецзв'язку попереджало про розповсюдження електронних листів з назвою «Військові злочинці РФ.htm», активація яких призводить до того, що хакери отримують віддалений доступ до комп'ютера будь-кого.

Під прицілом перебувають також об'єкти критичної інфраструктури. Український провайдер Укртелеком зазнав потужної атаки 28 березня 2022 року, під час якої хакери намагались проаналізувати, як влаштована IT-інфраструктура, вивести з ладу обладнання та сервіси, а також отримати контроль над мережею та обладнанням компаній усіх форм власності.

23 березня того ж року ворог намагався здійснити кібератаку на державні установи України з використанням шкідливої програми Cobalt Strike Beacon, яка дестабілізує роботу комп'ютера у випадку її відкриття. Це приклади лише масованих атак. Щодо атак меншого значення та окремі випадки персональних зламів просто не повідомляються.

Враховуючи постійний розвиток сучасних технологій, виникає необхідність постійного оновлення кіберзахисту сфери кіберпростору. Відкрите вторгнення РФ пришвидшило вдосконалення чинного законодавства та гарантій безпеки в сучасному інформаційному IT-просторі.

Наразі під час війни в зоні ризику перебувають державні органи, великі підприємства, підприємства оборонної та критичної інфраструктури, а також підприємства, які забезпечують населення та оборону всім необхідним в умовах війни. Є ризики й для місцевих жителів, які перебувають у зоні бойових дій. Під час воєнного стану кожному варто звернути увагу на декілька аспектів контролю: для компаній, органів влади та посадовців наявність залученого технічного спеціаліста зі спеціалізованої компанії суттєво підвищить рівень кіберзахисту. Професіонали здатні ускладнити роботу ворогу через запровадження в компанії необхідних алгоритмів захисту, зокрема організаційних.

Виникає необхідність проводити інструктажі для працівників, які виконують роботу, пов'язану з відповідними системами та мережами, адже багато атак досягають мети зламу через непродумані й необережні дії саме працівників.

Тим, хто перебуває в зоні кіберризику, мають надаватися рекомендації щодо відслідковування за відповідними повідомленнями на офіційних ресурсах Держспецзв'язку та CERT-UA. Такі ресурси публікують офіційні попередження для отримання інформації про можливі кіберзагрози та про те, які є можливості мінімізувати ті чи інші ризики.

У разі здійснення кібератаки пропонується відразу повідомляти тих, на кого така атака може ще поширитися. Для фізичних осіб, це контакти тих, з ким здійснюється активний зв'язок. Для компаній та органів влади можуть бути співробітники, клієнти, контрагенти та ділові партнери. Також важливим є інформування офіційних суб'єктів охорони кібербезпеки України, CERT-UA та Кіберполіцію. Це дасть змогу вжити оперативних заходів і заблокувати шкідливі вебресурси.

Зі свого боку хто проводить кібератаки на ворога або займається багхантингом, пропонують у цілях удосконалення української кібербезпеки в умовах війни для уникнення непорозумінь із правоохоронними органами бути готовими підтвердити направленість своєї діяльності саме інтересам України [4].

Висновки. Як бачимо, підґрунтя законодавчого забезпечення механізмів для ефективного кіберзахисту в умовах воєнного стану існує. І існує воно ще з початку двохтисячних років, коли Україна ратифікувала міжнародну конвенцію із запобігання кіберзлочинності від 23 листопада 2001 року. Наразі завданням кожного в разі виявлення кібератаки залишається як найшвидше активувати цей механізм, щоб у майбутньому подібних кібернападів та втручань і збитків від них ставало дедалі менше. А відсіч таких атак ставала все більш ефективною.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кривенко К. Є. Кіберзлочинність: актуальна судова практика / ЛІГА ЗАКОН, 2022. URL : https://biz.ligazakon.net/analitycs/209283_kberzlochinnst-aktualna-sudova-praktika (дата звернення: 03.06.2024).

2. Кримінальна відповідальність за кіберзлочини. URL : https://wiki.legalaid.gov.ua/index.php/%D0%9A%D1%80%D0%B8%D0%BC%D1%96%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0_%D0%B2%D1%96%D0%B4%D0%BF%D0%BE%D0%B2%D1%96%D0%B4%D0%B0%D0%BB%D1%8C%D0%BD%D1%96%D1%81%D1%82%D1%8C_%D0%B7%D0%B0_%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B7%D0%BB%D0%BE%D1%87%D0%B8%D0%BD%D0%B8 (дата звернення: 03.06.2024).

3. Посилено кримінальну відповідальність за кіберзлочини / Юридична компанія «Капітал». Київ, 2022. URL : https://capital-ukraine.com/posyleno-kryminalnu-vidpovidalnist-za-kiberzlochyny/ (дата звернення: 03.06.2024).

4. Єрема М. Боротьба з кіберзлочинністю в умовах дії воєнного стану : Закон 2149-IX / ЛІГА ЗАКОН. 2022. URL : https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix (дата звернення: 03.06.2024).

REFERENCES

1. Kryvenko K. Ye. Kiberzlochynnist: aktualna sudova praktyka / LIHA ZAKON. 2022. URL : https://biz.ligazakon.net/analitycs/209283_kberzlochinnst-aktualna-sudova-praktika (data zvernennia: 03.06.2024).

2. Kryminalna vidpovidalnist za kiberzlochyny. URL : https://wiki.legalaid.gov.ua/index.php/%D0%9A%D1%80%D0%B8%D0%BC%D1%96%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0_%D0%B2%D1%96%D0%B4%D0%BF%D0%BE%D0%B2%D1%96%D0%B4%D0%B0%D0%BB%D1%8C%D0%BD%D1%96%D1%81%D1%82%D1%8C_%D0%B7%D0%B0_%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B7%D0%BB%D0%BE%D1%87%D0%B8%D0%BD%D0%B8 (data zvernennia: 03.06.2024).

3. Posyleno kryminalnu vidpovidalnist za kiberzlochyny / Yurydychna kompaniia «Kapital». Kyiv, 2022. URL : https://capital-ukraine.com/posyleno-kryminalnu-vidpovidalnist-za-kiberzlochyny/ (data zvernennia: 03.06.2024).

4. Yerema M. Borotba z kiberzlochynnistiu v umovakh dii voiennoho stanu : Zakon 2149-IX / LIHA ZAKON. 2022. URL : https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix (data zvernennia: 03.06.2024).

Ya. P. Kharchenko. CRIMINOLOGICAL PROTECTION OF CYBERSPACE AGAINST CRIMINAL OFFENSES IN THE FIELD OF EXPLOITATION OF ELECTRONIC COMPUTING EQUIPMENT

This article indicates the constant development of modern technologies, which creates the need for constant updating of cyber protection in the sphere of cyberspace. It is noted that the open invasion of the Russian Federation accelerated the improvement of current legislation and security guarantees in the modern information IT space. Modern progress does not leave anyone behind, which led to the appearance of such a phenomenon as cybercrime. All over the world, criminal offenses in the field of exploitation of electronic computing equipment in cyberspace from year to year cause losses of tens of billions of US dollars both to individuals and private companies, and to states as a whole.

Attention is drawn to the fact that during a war, state bodies, large enterprises, defense and critical infrastructure enterprises, as well as enterprises that provide the population and defense with everything necessary in war conditions are at risk. There are also risks for local residents who are in the war zone. During martial law, everyone should pay attention to several aspects of control: for companies, authorities and officials, the presence of a technical specialist from a specialized company will significantly increase the level of cyber protection. Professionals are able to complicate the enemy's work by introducing the necessary protection mechanisms in the company, including organizational ones.

It is noted that the basis for the legislative provision of mechanisms for effective cyber protection in the conditions of martial law exists.And it has existed since the beginning of the 2000s, when Ukraine ratified the international convention on the prevention of cybercrime dated November 23, 2001. Attention is focused on the fact that the task of everyone, when a

cyber attack is detected, remains to activate this mechanism as soon as possible, so that in the future such cyber attacks and interventions and losses from them become less and less. And repelling such attacks became more and more effective.

Keywords: *prevention, crime, cyber attacks, criminal offenses, cyber defense, criminology, electronic computing, cyber crime.*

Стаття надійшла до редколегії 1 серпня 2024 року