

*М. Авдотьєв О. Туровський, д.т.н., проф.
(Національний авіаційний університет, Україна)*

Актуальність кіберзлочинності під час воєнного стану в Україні

Боротьба з кіберзлочинністю є важливою задачею для всіх, хто працює з інформацією та використовує комп'ютерні мережі та системи.

Кіберзлочинність є актуальною проблемою у будь-який час, але під час воєнного стану вона стає ще більш небезпечною. Саме зараз – переломний етап для України, так після повномасштабного вторгнення ворога 24 лютого 2022 року у нашої державі бої відбуваються не тільки на полі бою, але і в інформаційному просторі це можуть бути як медіа сервіси або ж мережа інтернет. Загибель близьких, втрата домівки, постійної роботи, введення воєнного стану – всі ці моменти вплинули не свідомість та поведінку людей, яка у більшості випадків стала антиправовою.

Кібератаки можуть призвести до розколу та дестабілізації суспільства, порушення функціонування критично важливих інфраструктур, таких як енергетика, транспорт, медицина, фінанси тощо. Крім того, кіберзлочинці можуть використовувати соціальні мережі та інші онлайн-ресурси для поширення дезінформації та пропаганди, що може призвести до збільшення напруженості у суспільстві та погіршення ситуації на фронті. Тому важливо забезпечити захист критично важливих інфраструктур та збереження кібербезпеки в цілому. Для цього необхідно проводити регулярні аудити та оновлення систем захисту від кібератак, забезпечувати своєчасне виявлення та реагування на кібернапади, а також проводити інформаційну роботу з населенням щодо кібербезпеки та уникнення шахрайства в інтернеті.

У процесі реагування на швидке зростання рівня кіберзлочинності Верховна Рада України провела оптимізацію кримінального та кримінально-процесуального законодавства, удосконаливши процесуальні механізми та підстави притягнення до кримінальної відповідальності кіберзлочинців.

Кіберзлочинність - це злочинні дії, які виконуються за допомогою комп'ютерних мереж та інтернету. Такі дії можуть бути спрямовані на отримання конфіденційної інформації, порушення правил користування мережею, шахрайство та інші злочини.

Під час воєнного стану в Україні кіберзлочинність може бути особливо небезпечною, оскільки вона може бути спрямована на порушення безпеки держави та громадян. Наприклад, хакерські атаки на важливі інфраструктурні об'єкти (електростанції, водозабори тощо) можуть призвести до серйозних наслідків для населення та економіки країни.

Крім того, кібершпиунство може бути використане для отримання конфіденційної інформації про військові плани та дії, що може призвести до небезпеки для життя та здоров'я військовослужбовців. Існує кілька способів боротьби з кіберзлочинністю. Основні з них:

1. Захист мереж та систем. Це включає в себе захист від вірусів, шпигунського програмного забезпечення та інших загроз, а також захист від хакерських атак.
2. Шифрування даних. Шифрування може допомогти захистити конфіденційну інформацію від несанкціонованого доступу.
3. Організація резервних копій. Резервні копії можуть допомогти відновити дані в разі їх втрати або пошкодження.
4. Підвищення обізнаності користувачів. Важливо навчати користувачів, як попереджати кіберзлочинність та уникати пасток.
5. Співпраця з правоохоронними органами. Правоохоронні органи можуть допомогти виявити та покарати кіберзлочинців.
6. Розробка законодавства. Законодавство може встановлювати правила та стандарти для захисту інформації та покарання кіберзлочинців.

Тому, під час воєнного стану в Україні, необхідно звертати особливу увагу на захист комп'ютерних мереж та інформації від кіберзлочинців. Для цього можуть бути використані різноманітні заходи, такі як шифрування даних, захист мережевих пристроїв та програмного забезпечення, організація резервних копій тощо.

Список літератури

1. Бусель В. Т. Великий тлумачний словник сучасної української мови / Уклад. і го- лов. ред. К. Ірпінь: ВТФ «Перун», 2001. С. 1391.
2. Чернишов Г. М. Кіберзлочинність як виклик глобалізації та загроза світовій безпеці: теоретичні основи дослідження.
URL: http://www.pjv.nuova.od.ua/v3_2018/2018_3 (дата звернення: 11.11.2022).
3. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовт. 2017 No 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 20.11.2022).
4. еліканов С. В., Волобуєв А. Ф., Журавель В. А., та ін. Криміналістична профілактика економічних злочинів: науково-практичний посібник. Харків : «Харків юридичний», 2006. 236 с.
5. Левківська Я. І. Вплив воєнного стану на трансформувannya та розвиток інтернет-шахрайства в Україні. URL: <http://dspace.onua.edu.ua/handle/11300/19993> (дата звернення: 20.11.2022).
6. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану від 24.02.2022 No 2149-IX. URL: <https://zakon.rada.gov.ua/laws/show/2149-20#Text> (дата звернення: 20.11.2022).
7. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану : Закон України від 24 берез. 2022 No 2149- IX : URL: <https://zakon.rada.gov.ua/laws/show/2149-20#Text> (дата звернення: 20.11.2022).

8. Офіційний сайт Національного банку України. URL: <https://bank.gov.ua/ua/news/all/startuye-informatsiyna-kampaniya-natsionalnogobanku-z-platijnoyi-bezpeki-shahraygudbay> (дата звернення 21.11.2022).

9. Лист Національного банку України «Рекомендації для зниження ризику шахрайських операцій» від 4 липня 2018 р. URL: https://vk24.ua/regulations_and_jurisprudence/listi/oplata-praci/list-nacionalnogo-banku-ukraini-rekomendacii-dlya-znizhennya-riziku-shakhrayskikhoperaciuj

10. Офіційний сайт Національного банку України. Проект «#ШахрайГудбай». URL: <https://promo.bank.gov.ua/stopfraud/#section-35>

11. Стережіться «виplat»: ПриватБанк попереджає про нову схему шахрайства. УНІАН. URL: <https://www.unian.ua/economics/finance/shahraystvo-z-bankivskimi-kartkami-privatbank-poperedzhaye-pro-novu-shemu-mahinaciy-novini-ukrajina-11895471.html>

12. Положення «Про запобігання шахрайству»: затв. рішенням Правління банку «ПриватБанк» від 28.09.2017 р. URL: <https://static.privatbank.ua/fles/politika-zapobigannya-shaxrajstva-ta-korupcii.pdf>

13. Захист від шахрайства. Офіційний сайт ПриватБанк. URL: <https://privatbank.ua/strahovaniye/zakhyst-vid-shakhraystva>

14. Сметаніна Н. В. Національний і міжнародний досвід визначення та розрахунку ціни кіберзлочинності. Міжнародні стандарти з кібербезпеки та їх застосування в Україні : матеріали «круглого столу» (м. Харків, 19 квіт. 2016 р.). Харків, 2016. С. 59–61.

15. Nizovtsev, Yuriy; Parfylo, Oleg; Barabash, Olha; Kyrenko, Sergij; Smetanina, Nataliia. Mechanisms of money laundering obtained from cybercrime: the legal aspect. *Journal of Money Laundering Control*. Volume 25, Issue 2, Pages 297–305. 21 April 2022. <https://www.emerald.com/insight/content/doi/10.1108/JMLC-02-2021-0015/full/html>.