Список використаних джерел:

1. Кіберзлочинність як виклик глобалізації та загроза світовій безпеці: теоретичні основи дослідження. Г. М. Чернишов URL : http://www.pjv.nuoua.od.ua/v3_2018/2018_3
2. Криміналістична профілактика економічних злочинів: Науково-практичний посібник / Кол. авт.: С. В. Веліканов, А. Ф. Волобуєв, В. А. Журавель та ін. Х. : «Харків юридичний», 2006. 236 с.
3. Секреты хакеров. Безопасность сетей – готовые решения, 3-е издание. : Пер. с англ. – М. : Издательский дом «Вильяме», 2002. – 736 с.
4. Шахрайство під час війни: топ-4 схеми і нові тенденції URL : https://minfin.com.ua/ua/2022/03/15/82162508/

Ключові слова: шахрайство під час воєнного стану, шахрайство в мережі Інтернет, фішинг, фейк, персональні дані, схема вчинення інтернет-шахрайства.

Key words: martial law fraud, Internet fraud, phishing, fake, personal data, scheme of Internet fraud.

ФЛЮНТ МАР'ЯНА ОРЕСТІВНА

Національний університет «Одеська юридична академія», аспірантка кафедри кримінального процесу, детективної та оперативно-розшукової діяльності

КІБЕРБЕЗПЕКА ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ПРАВОВІ ВИМОГИ ДО ОРГАНІЗАЦІЇ ТА РЕАЛІЗАЦІЇ

Забезпечення національної безпеки завжди було та залишається однією з основних функцій будь-якої держави та ключовим напрямом її політики.

Так, Закон України «Про національну безпеку України» [1] декларує: «державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, кібербезпеки України тощо». Водночас, у Стратегії кібербезпеки України 2021 р. [2] зазначено, що кіберпростір разом з іншими фізичними просторами визнано одним з можливих театрів воєнних дій.

В сучасних умовах глобальної діджиталізації, збільшення випадків кібератак на державний та приватний сектор, існування та появи нових кіберризиків і кіберзагроз, росту рівня кіберзлочинності та «удосконалення» способів вчинення кіберзлочинів, а також в контексті ведення повномасштабної війни, кібербезпекова політика є не просто складовою національної безпеки України, а й одним з найактуальніших напрямів її реалізації.

Так, у 2016 році було вперше прийнято Стратегію кібербезпеки України [3], метою якої було створення умов для безпечного функціонування

кіберпростору, його використання в інтересах особи, суспільства і держави. Для досягнення цієї мети необхідним є, зокрема, забезпечення кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також інформаційної інфраструктури, яка знаходиться під юрисдикцією України, та порушення сталого функціонування якої матиме негативний вплив на стан національної безпеки і оборони України (критична інформаційна інфраструктура).

Керуючись зазначеним, – Закон України «Про основні засади забезпечення кібербезпеки України» 2017 р. [4] встановлює, що об'єкти критичної інфраструктури є об'єктами кібербезпеки, а об'єкти критичної інформаційної інфраструктури є об'єктами кіберзахисту. Так, Закон [4] визначає *критично важливі об'єкти інфраструктури* як підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей; а *об'єкт критичної інформаційної інфраструктури* як комунікаційну або технологічну систему об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури.

Крім того, у Статегії кібербезпеки України 2021 р. [2] зазначено, що набирає сили тенденція зі створення кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, що включає виведення з ладу критично важливих об'єктів інфраструктури противника шляхом руйнування інформаційних систем, які управляють такими об'єктами.

Положення Стратегії кібербезпеки України та Закону України «Про основні засади забезпечення кібербезпеки України», в контексті захисту критичної інфраструктури, загалом відповідають вимогам Директиви (EU) 2016/1148 [5]. Варто зазначити, що не будучи країною-членом ЄС Україна приєдналась до виконання основних положень Директиви та розпочала розбудову власної системи кібербезпеки, відповідно до стандартів та рекомендацій Європейського співтовариства.

В подальшому лише у листопаді 2021 р. було прийнято Закон України «Про критичну інфраструктуру» [6], який визначає правові та організаційні засади створення та функціювання національної системи захисту критичної інфраструктури і є складовою законодавства у сфері національної безпеки. Так, Закон [6] тлумачить *об'єкти критичної інфраструктури* як об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди

життєвоважливим національним інтересам; а сукупність об'єктів критичної інфраструктури називає «критичною інфраструктурою».

Окрім тлумачення термінології, Закон [6], зокрема: (1) визначає основні засади державної політики у сфері захисту критичної інфраструктури, зокрема декларує основні принципи функціонування та встановлює рівні управління національною системою захисту критичної інфраструктури, (2) перелічує сектори критичної інфраструктури та описує критерії віднесення об'єктів до критичної інфраструктури, здійснює категоризацію об'єктів критичної інфраструктури, (3) встановлює загальні процедури формування та реалізації державної політики у сфері захисту критичної інфраструктури, перелічує суб'єктів національної системи захисту критичної інфраструктури, (4) визначає організаційні засади національної системи захисту критичної інфраструктури, зокрема щодо планування, моніторингу, взаємодії з іншими системами захисту у сфері національної безпеки та державно-приватного партнерства.

Станом на сьогодні, вимоги щодо заходів забезпечення кібербезпеки об'єктів критичної інфраструктури містяться у значній кількості підзаконних нормативно-правових актів, у відомчих інструкціях, рекомендаціях, технічних вимогах, а також міжнародних стандартах інформаційної безпеки серії 2700х тощо.

Так, наприклад, організація кіберзахисту в банківській системі України здійснюється на основі [7]: Законів України «Про Національний банк України», «Про основні засади забезпечення кібербезпеки України», з урахуванням Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 року № 447/2021, національних стандартів України ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги» (ISO/IEC 27001:2013, IDT), прийнятого наказом Державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 18 грудня 2015 року № 193, ДСТУ ISO/IEC 27010:2018 «Інформаційні технології. Методи захисту. Керування інформаційною безпекою для міжгалузевих та міжорганізаційних комунікацій» (ISO/IEC 27010:2015, IDT), прийнятого наказом Державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 10 грудня 2018 року № 470.

Крім того, Національним банком України було розроблено та запропоновано для обговорення проект постанови «Про затвердження Положення про організацію кіберзахисту в банківській системі України» [7]. Вважаємо, що подальше прийняття зазначеного документу дозволить більш ефективно реалізовувати кіберзахист банківської системи нашої держави, як одного з секторів критичної інфрастуктури, та є показником реалізації державної політики у сфері захисту критичної інфраструктури та дотримання кібербезпекової політики загалом.

Актуальним вбачається оновлення вже існуючих та/або створення та подальша реалізація аналогічних за суттю документів й для інших

секторів критичної інфраструктури, що стане доказом функціонування національної системи захисту критичної інфраструктури та показником позитивної динаміки на шляху до побудови ефективної системи кібербезпеки України.

Враховуючи зазначене, сформовано наступні висновки:

– правові вимоги щодо організації та реалізації кібербезпеки об'єктів критичної інфраструктури в Україні містяться у низці нормативно-правових актів різної юридичної сили та галузевої спрямованості;

– наслідком широкого переліку документів, що врегульовують окремі питання кібербезпеки є розшарованість, неоднорідність, колізійність, а подекуди, й відсутність вимог до кібербезпеки окремих секторів критичної інфраструктури, що, в свою чергу, зумовлено низкою обставин, зокрема, (1) широким переліком сфер/секторів критичної інфраструктури, (2) відсутністю протягом тривалого періоду часу спеціалізованого законодавства та вимог щодо заходів кіберзахисту критичної інфраструктури, а також чіткого переліку уповноважених суб'єктів, переліку їх компетенцій та завдань у сфері захисту критичної інфраструктури, (3) неналагодженістю взаємодії та координації державних органів, низьким рівнем реалізації державно-приватної взаємодії тощо;

– суб'єктами національної системи захисту критичної інфрастуктури розпочато роботу з розробки та уніфікації вимог, а також застосування затверджених заходів забезпечення кібербезпеки об'єктів критичної інфраструктури, в т.ч. з врахуванням міжнародних практик та стандартів.

Список використаних джерел:

1. Про національну безпеку : Закон України від 21 червня 2018 року № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text
2. Стратегія кібербезпеки України : Безпечний кіберпростір – запорука успішного розвитку країни : Затверджено Указом президента України від 26 серпня 2021 року № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013
3. Стратегія кібербезпеки України : Затверджено Указом Президента України від 15 березня 2016 р. № 96/2016. URL: https://www.president.gov.ua/documents/962016-19836
4. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
5. DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. URL: https://eur-lex.europa.eu/eli/dir/2016/1148/oj
6. Про критичну інфраструктуру : Закон України від 16 листопада 2021 року № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text

7. Про затвердження Положення про організацію кіберзахисту в банківській системі України : Проект постанови. URL: https://bank.gov.ua/ua/news/all/kiberzahist-bankivskoyi-sistemi-ukrayini-maye-posilitisya-12738

Ключові слова: кібербезпека, критична інфраструктура, політика кібербезпеки, національна система захисту критичної інфраструктури, кібервійна.

Key words: cyber security, critical infrastructure, cybersecurity policy, national system of critical infrastructure protection, cyberwar.

OSADCHYI BOGDAN

National University "Odesa Law Academy",
graduate student of the Department of Criminal Procedure,
Detective and Operational Investigation

THEORETICAL AND DOCTRINAL APPROACHES TO CRIMINOLOGICAL STUDY OF CRIMES PROVIDED FOR BY ARTICLE 191 OF THE CC OF UKRAINE

Modern changes in Ukrainian society, the lack of systematic work in law-making and law enforcement necessitate the solution of a number of issues related to the criminological study of corruption crime and develop measures to counteract it, improve prevention mechanisms and strengthen precautionary measures. Corruption crime is now a specific phenomenon of criminal activity, and the problems of counteracting corruption have become key value in the state's reforms and policymaking in general. To this end, systematic reforms of criminal justice bodies are being carried out. However, without a proper criminological study of the effectiveness of their work, it is impossible to determine the efficacy of such reforms. In addition, research is needed on methods related to assessing not only the work of criminal authority, but also the effectiveness of the criminal law itself, namely the transition from quantitative indicators of statistical reporting to its qualitative analysis, which can not be done without the achievements of criminology. In this context, it is important to conduct a criminological characterization of misappropriation, waste of property or seizure by abuse of office, as one of the most common types of corruption crimes.

Of course, the state takes various measures to counteract corruption. As I. Mezentseva notes: "In recent years, Ukraine has signed a number of international documents, namely: the UN Convention against Corruption, the Council of Europe Criminal Law Convention on Corruption and the Additional Protocol to the Criminal Anti-Corruption Convention, which obliged adoption of laws aimed at improving the current criminal anti-corruption legislation. Ukraine's desire to move closer to the standards of the international community in the field of counteracting and preventing corruption is embodied in the systematic work on reforming the system of criminal justice