МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

КРИМІНОЛОГІЧНА АСОЦІАЦІЯ УКРАЇНИ

30 РОКІВ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

ЗЛОЧИННІСТЬ І ПРОТИДІЯ ЇЙ В УМОВАХ ВІЙНИ ТА У ПОВОЄННІЙ ПЕРСПЕКТИВІ: МІЖДИСЦИПЛІНАРНА ПАНОРАМА

Збірник тез доповідей
Міжнародної науково-практичної конференції
(м. Вінниця, 19 квітня 2024 року)

DOI: https://doi.org/10.5281/zenodo.10997257

Вінниця 2024

УДК 343“364”(082)
368

Друкується згідно з рішенням оргкомітету
за дорученням Харківського національного університету
внутрішніх справ від 08.02.2024 № 12

Злочинність і протидія їй в умовах війни та у повоєнній перспективі: міждисциплінарна панорама : зб. тез доп. Міжнар. наук.-практ. конф. (м. Вінниця, 19 квіт. 2024 р.) / МВС України, Харків. нац. ун-т внутр. справ ; Кримінол. асоц. України. – Вінниця : ХНУВС, 2024. – 662 с.

368

У збірнику представлено тези наукових доповідей більше ніж 150 авторів. Праці вчених-правників, фахівців із кримінології, кримінального, кримінально-виконавчого права, кримінального процесу та криміналістики, судової експертології, оперативно-розшукової діяльності та інших галузей знань і спеціальностей, а також доробки здобувачів вищої освіти. У тезах доповідей висвітлено широке коло питань, пов’язаних з актуальними проблемами протидії злочинності в умовах війни та у повоєнній перспективі.

УДК 343“364”(082)
DOI: https://doi.org/10.5281/zenodo.10997257

Публікації наведено в авторській редакції з незначними коректорськими правками. Оргкомітет не завжди поділяє погляди авторів. За достовірність наукового матеріалу, професійного формулювання, фактичних даних, цитат, власних імен, географічних назв, а також за розголошення фактів, що не підлягають відкритому друку, відповідають автори публікацій та їх наукові керівники (за наявності).

Електронна копія збірника безоплатно розміщується у відкритому доступі на сайті Харківського національного університету внутрішніх справ (http://www.univd.edu.ua) у розділі «Наука», сторінка «Конференції, семінари та круглі столи», а також у репозитарії ХНУВС (http://dspace.univd.edu.ua/xmlui/).

© Харківський національний університет внутрішніх справ, 2024
© Кримінологічна асоціація України, 2024

УДК 347.9

Олексій Валерійович САЛМАНОВ,
кандидат юридичних наук, доцент,
доцент кафедри кримінального процесу
та організації досудового слідства факультету № 1
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0001-9421-5085

КІБЕРЗЛОЧИННІСТЬ І ПРОТИДІЯ ЇЙ В УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ

На сучасному етапі широке використання інтернет-технологій стало не просто невід'ємною частиною повсякденного життя, але й необхідністю в різних сферах діяльності. Практично кожна особа має можливість скористатися перевагами цифрового світу, незалежно від соціального статусу чи професійних занять. Введення електронного документообігу в державних установах і приватних підприємствах, автоматизація банківських операцій через сучасні електронні системи, а також використання електронних засобів зв'язку для забезпечення безперебійності роботи транспортних мереж - це лише кілька прикладів використання інтернет-комунікацій у різних сферах життя. Ці технології значно полегшують рутинні справи та сприяють підвищенню ефективності діяльності державних, комерційних та громадських організацій.

Процес науково-технічного прогресу та широке використання інтернет-технологій у всіх сферах суспільства супроводжується зростанням кількості кіберзлочинів. За даними Офісу Генерального прокурора, лише за останні 8 років кількість виявлених кіберзлочинів зросла майже у 9 разів [1].

Особливо актуальне це питання в Україні, де в умовах воєнного стану кіберзлочинці активно залучаються до зламу урядових серверів, розповсюдження дезінформації серед населення та використання фейкових профілів у соціальних мережах. Поширені форми кібершахрайства, коли злочинці видаються за різні види виплат, щоб отримати банківські реквізити громадян та заволодіти їх коштами, також стали загальним явищем.

Саме тому в Україні розпочато процес вдосконалення чинного кримінального та кримінально-процесуального законодавства, спрямований на притягнення кіберзлочинців до відповідальності. Це свідчить про те, наскільки важливим є вивчення та

аналіз законодавства, судово-слідчої практики і наукових джерел з даної тематики для забезпечення ефективного протидії кіберзлочинності в інформаційному просторі.

Багато вітчизняних вчених приділяли увагу проблемі кіберзлочинності, проте проблема запобігання кіберзлочинності в умовах воєнного стану залишається площиною, яка не отримала достатнього наукового аналізу та вивчення.

Хоча й було проведено деякі дослідження, аналізуючи взаємозв'язок між кіберзлочинністю та воєнним станом, а також шляхи ефективного запобігання цьому явищу в умовах конфлікту, проте більш глибоке дослідження і аналіз цієї проблеми залишаються важливим завданням для наукової спільноти. Додаткові дослідження і аналіз допоможуть розкрити особливості цього явища та розробити ефективні стратегії протидії кіберзлочинності в умовах воєнного конфлікту.

Українська законодавча база не містить окремого спеціального акту, який би регулював питання запобігання злочинності у сфері інформаційних технологій. Замість цього, українське законодавство включає кілька правових актів, які стосуються даної теми.

Один з основних правових документів щодо запобігання кіберзлочинності - це Закон України "Про основні засади забезпечення кібербезпеки України" від 5 жовтня 2017 року. Згідно з цим законом, кіберзлочин (комп'ютерний злочин) - це суспільно небезпечне винне діяння у кіберпросторі або з його використанням, за яке передбачена відповідальність згідно з Кримінальним кодексом України або визнано злочином міжнародними договорами України. Мета таких дій може включати розкрадання або руйнування інформації в інформаційних системах і мережах. [2].

Умови війни створюють додаткову загрозу кіберзлочинності, оскільки злочинці можуть використовувати ці дії для дестабілізації ситуації в країні, крадіжки конфіденційних даних, паралізації роботи державних інституцій та інші цілі. Ці питання деталізовані у Стратегії кібербезпеки України, яка була запроваджена Указом Президента України № 446/2021.

Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку визначені у Розділі IVI Кримінального кодексу України. Деякі норми щодо превенції містяться в Конституції України, Кримінальному процесуальному кодексі України, але вони залишаються більш декларативними і потребують подальшого опрацювання та вдосконалення. [3]

У зв'язку з міжнародним характером кіберзлочинності, важливим стає міжнародне співробітництво. Європейський Союз, крім вже згаданих документів, прийняв інші акти, спрямовані на боротьбу з кіберзлочинністю. Це включає Директиву про боротьбу із сексуальною експлуатацією дітей в Інтернеті та дитячою порнографією, Пропозицію про тимчасове регулювання обробки персональних та інших даних для боротьби із сексуальним насильством над дітьми та інші.

Для сприяння розслідуванням кіберзлочинності в ЄС був створений ключовий орган - Європейський центр з кіберзлочинності в Європолі, що об'єднує європейську експертизу в цій галузі. [4, с.19]

Незважаючи на ратифікацію Україною низки міжнародних договорів, що гарантують співробітництво у боротьбі з кіберзлочинністю, на практиці взаємодія з іншими країнами часто супроводжується бюрократичними процедурами, що уповільнюють процес запобігання кіберзлочинам.

Після повномасштабного вторгнення РФ на територію України кількість кримінальних правопорушень у сфері інформаційних технологій різко збільшилась. Країна-агресор активно використовує інтернет-технології для дезінформації стосовно вторгнення в Україну, пропаганди ворожих ідей та інших злочинних цілей. У зв'язку з цим Верховна Рада України провела оптимізацію кримінального та кримінально-процесуального законодавства, удосконаливши підстави та процедури притягнення до кримінальної відповідальності злочинців.

Зокрема, були внесені зміни до Кримінального процесуального кодексу України та Закону України "Про електронні комунікації" з питання підвищення ефективності досудового розслідування "за гарячими слідами" та протидії кібератакам (№ 2137-IX від 15 березня 2022 року) [5], та до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану (№ 2149-IX від 24 березня 2022 року). [6].

Відповідні зміни націлені на інтенсифікацію кримінальної відповідальності за порушення у сфері інформаційних технологій та розширення компетенції правоохоронних органів у виявленні таких злочинних дій. Фактично, після впровадження відповідних законодавчих змін спостерігається підвищення ефективності протидії кримінальній активності у сфері інформаційних технологій, що відбувається шляхом збільшення рівня відповідальності за зазначені кримінальні порушення. Однак залишається недостатньо

вивченим аспект щодо аналізу соціальних, економічних, політичних, демографічних, організаційних та інших факторів, які впливають на поширення кіберзлочинності. На сьогоднішній день для розробки системи запобігання злочинності в цій сфері використовуються в основному дані судово-слідчої практики. Потреба у посиленні кримінальної відповідальності за правопорушення у галузі інформаційних технологій виникала давно. Зміни до законодавства стосуються розширення повноважень правоохоронних органів у розслідуванні кіберзлочинів, визначених статтями 361, 361-1 Кримінального кодексу України. Посилення санкцій та додаткова криміналізація окремих дій можуть частково зменшити потенційний ризик вчинення нових кримінальних порушень.

Важливо зауважити, що сфера використання інтернет-технологій давно потребувала посиленого захисту. Вторгнення РФ стимулювало удосконалення чинного законодавства та забезпечення безпеки в сучасному інформаційному середовищі.

З початку воєнного стану стали відомі численні кібератаки на Україну. Один з сучасних видів кібершахрайства в Україні - це пенсійні афери, які включають у себе надання підроблених фінансових можливостей, обіцянки великої суми грошей та гарантовану допомогу від різних фондів. Злочинці, що оперують у цій галузі, активно використовують соціальні мережі, зокрема Facebook, для спекуляції на темі фінансових виплат українцям. Шахраї обіцяють виплати «за рахунок конфіскованих активів РФ» та посилаються на міфічні рішення різних органів влади України. Повідомляється, що в їх оголошеннях вони пропонують перейти за посиланням, яке веде на фішингову сторінку псевдо "Єдиного Компенсаційного Центру повернення невиплачених грошових коштів". На цьому вебсайті вони пропонують отримати виплату за умови надання особистих даних та здійснення додаткового платежу. У результаті, дані банківської картки стають під загрозу компрометування.

На теперішній час в Україні існує багато аналогічних злочинних схем. Боротьба з цим типом злочинності стає більш складною через широке використання ресурсів Інтернету, що ускладнює відстеження кібершахраїв. Крім того, кібершахрайство має трансконтинентальний рівень, що також ускладнює виявлення та запобігання цьому виду злочинності. Це лише один із аспектів кримінальних правопорушень у сфері інформаційних технологій.

На наш погляд, для побудови ефективної стратегії запобігання злочинності у сфері інформаційних технологій важливо розглядати не лише питання посилення відповідальності за кримі-

нальні правопорушення, але і розробку широкого спектру заходів, які б враховували соціально-економічні, організаційно-управлінські та психологічні аспекти.

Поділяємо думку науковців щодо необхідності розробки комплексних заходів протидії кіберзлочинності, що могли б бути впроваджені не тільки державними органами, а й приватними структурами та громадянами. До можливих заходів можна віднести:

1) Залучення професіоналів та спеціалізованих компаній для забезпечення кібербезпеки у державних установах та підприємствах. Це дозволить ефективніше захищати системи від кібератак і покращити реакцію на інциденти.

2) Посилення контролю та розповсюдження інформації про потенційні кібератаки серед громадян через офіційні канали зв'язку та інтернет-ресурси. Це може сприяти підвищенню рівня обізнаності та усвідомлення загроз. Так, наприклад, Міністерство цифрової трансформації за підтримки Google.org та Фонду Східна Європа розробили платформу «Дія. Освіта» на якій розмістили освітній контент за темами «Обережно! Кібершахраї» та «Персональна кібергігієна». [7]

3) Забезпечення ефективного механізму реагування на кібератаки шляхом встановлення тісного співробітництва між органами досудового розслідування, департаментом кіберполіції, спеціалізованими службами та іншими зацікавленими сторонами.

Ці заходи, призначені для протидії кіберзлочинності, можуть стати ефективними лише за умови їх комплексного застосування та системного підходу до проблеми.

Список бібліографічних посилань

1. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування: офіційний сайт Офісу Генерального прокурора. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2

2. Про основні засади забезпечення кібербезпеки України: закон України від 5 жовтня 2017 року 2163-VIII https://zakon.rada.gov.ua/laws/show/2163-19

3. Кримінальний кодекс України: Закон України від 05.04.2001 No 2341-III / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2341-14

4. Сащенко М.І. Проблемні аспекти запобігання кіберзлочинності в Україні. «Young Scientist». 2022. No 1 (101). С. 17–20.

5. 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

6. 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

7. Освітній портал Дія. Освіта URL: https://osvita.diia.gov.ua /courses/attention-cyber-fraudsters

УДК 343.97

Віталій Валерійович СОКУРЕНКО,
кандидат юридичних наук,
доцент кафедри кримінального права та кримінології
факультету підготовки фахівців для органів досудового розслідування
Одеського державного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0001-6879-7376

ВІЙНА У ФОКУСІ КРИМІНОЛОГО-АКСІОЛОГІЧНОГО АНАЛІЗУ

Будь-яка війна вимагає певного смислового виправдання з обох сторін, війна як екстремальний суспільний конфлікт потребує конструювання смислів «для чого?» або «за що воюємо?». Сучасна людина, головним чином, мислить з бінарних опозицій: «ворог – друг», «свій – чужий», «істина – брехня», «справедливе – несправедливе», «чесне – безчесне» [1, с. 32, 36].

Прогноз – це передбачення того, що може відбутися, статися, здійснитися в кінцевому результаті за певних умов, при здійсненні певної діяльності, розгортанні активності, або що може бути отримано, досягнуто в результаті спеціальних зусиль з боку суб'єкта прогнозу. Тобто прогноз – це образ майбутнього результату. А очікування – це фоновий психологічний і соціально-психологічний процес постійного перебування у свідомості суб'єкта образу бажаного (або небажаного) майбутнього, це процес, що супроводжує дію, реальний рух суб'єкта до кінцевої прогнозної точки, до мети, до реалізації бажання, потреби, до досягнення вигоди [1, с. 52].