КІБЕРЗЛОЧИННІСТЬ В УКРАЇНІ В УМОВАХ ВІЙНИ ЯК ОБ'ЄКТ КРИМІНОЛОГІЧНОГО АНАЛІЗУ

Петро Петрович ГАЛУШКО,

аспірант Харківського національного університету внутрішніх справ,
https://orcid.org/0009-0009-5631-9823

Російсько-українська війна загострила перманентні кризові соціальні стани, обумовлені широким спектром кримінально-криміногенних загроз, до яких додались неординарні виклики у сфері забезпечення національної безпеки. Зі всією повнотою ці виклики і загрози, поєднуючись, набуваючи гібридних форм, демонструючи специфічні форми синергії у сфері криміногенної детермінації і феноменології, спроєктувалися на площину кримінальних практик, що відтворюються у кіберпросторі.

На стратегічно-нормативному рівні визнано, що питома вага кіберзагроз зростає і ця тенденція в міру розвитку інформаційних технологій та їх конвергенції з технологіями штучного інтелекту в найближче десятиліття посилюватиметься. Зростання такого впливу на функціонування структур управління як національних, так і транснаціональних формує нову безпекову ситуацію. Між світовими центрами сили відбувається поділ сфер впливу у кіберпросторі, посилюється їх прагнення за рахунок такого поділу забезпечити реалізацію власних геополітичних інтересів [1]. Тож не підлягає жодним сумнівам те, що забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України. Реалізація зазначеного пріоритету буде здійснюватися шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі [1].

Відповідно до п. 8 ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII [2], кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність (ККУ) та/або яке визнано злочином міжнародними договорами України. До того ж це кримінальні правопорушення, передбачені розділом XVI КК України («Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку»), та зареєстровані кримінальні провадження із кваліфікуючою відміткою в картці про кримінальне правопорушення – «з використанням високих інформаційних технологій і телекомунікаційних мереж» [3].

Законодавчо визначено, що об'єктами кібербезпеки є:

1) конституційні права і свободи людини і громадянина;

2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;

3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;

4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;

5) об'єкти критичної інфраструктури [2].

Певна річ, цей поділ є досить умовним, але з операційної точки зору – функціональним, придатним для розгортання кримінологічного дослідження, спрямованого на первинне структурування феномену кіберзлочинності. Нескладна аналітична операція дозволяє представити сегментарну модель цього феномену, у якій виділяються такі блоки:

- кіберзлочинність, що посягає на конституційні права і свободи людини і громадянина (умовно – ординарна кіберзлочинність). Як правило, масив злочинів цього сегменту представлений практиками кібершахрайства. Серед поширених схем шахрайства у воєнний час можна виокремити: пропозиція з оренди неіснуючого чи вже зайнятого житла для осіб, які вимушені покинути власні домівки, фейкові перевезення та квитки для в'їзду в місто, недійсні талони на паливо, маніпуляції з продажу затребуваних під час війни товарів, надання недостовірної інформації про родичів, полонених військових, різного роду збори у соціальних мережах на допомогу військовим, постраждалим особам [3]. Поширеною шахрайською схемою стала пропозиція отримання грошової допомоги, яку видають за грошову допомогу від держави, Організації Об'єднаних Націй, благодійних фондів тощо для окремих категорій осіб. Вимога шахраїв – авторизаціія за схемою, яка передбачає введення своїх особистих даних, номеру телефону, інформації про банківські рахунки, де завершення процедури підтверджується прийняттям дзвінка або текстового повідомлення, після чого з картки отримувача списуються кошти [4, с. 522].

Дуже розповсюдженим є шахрайство-шопінг, коли користувачі купують потрібні їмречі на неперевірених сайтах, тому з метою уникнення подібного шахрайства були створенні спеціальні сервіси для перевірки справжності сайтів. Зокрема це «STOPHYPERLINK "http://cyberpolice.gov.ua/stopfraud/" HYPERLINK "http://cyberpolice.gov.ua/stopfraud/"FRAUD» Кіберполіції та «Black HYPERLINK "http://www.ema.com.ua/blacklist/" HYPERLINK "http://www.ema.com.ua/blacklist/"List» Асоціації «ЄМА». Сайти, які приймають онлайн-платежі мають бути захищеними, для цього в назві адреси вони мають містити https:// та значок « ». На сайті мають бути значки захисту онлайн-покупок від платіжних систем – Verified by Visa та MasterCard SecureCode [5]. Ще одним видом шахрайства з картками є «скімінг» це такий вид шахрайства, коли шахраї копіюють інформацію з платіжної картки за допомогою спеціальних пристроїв, які встановлюють на банкомат. Надалі це дозволяє злочинцям виготовити дублікат платіжної картки та викрасти гроші з рахунку власника картки. Знаряддям такого шахрайства виступає спеціальний пристрій, який встановлюють в картоприймач банкомату. Це може бути: тонка пластинка, яка вставляється всередину картоприймача або накладка, що кріпиться на картрідер банкомата. Але, слід зазначити, що копії даних з платіжної картки шахраю не достатньо, потрі-

бен ще і PIN-код. Тому, щоб вкрасти PINкод шахраї використовують: мікрокамеру, для того щоб на відео побачити, який PIN-код буде вводити жертва; накладну клавіатуру для зчитування PIN-коду. Її шахраї використовують рідше, оскільки мікрокамера набагато дешевша та непомітніша [5]. Як вберегтися від скімінгу? Порівнювати зовнішній вигляд банкомату з його екранною заставкою. Прикривати клавіатуру під час введення PIN-коду. У такій спосіб, щоб його неможливо було підгледіти за допомогою мікровідеокамери. Підключити послугу інформування про операції з використанням картки. Це дозволить вчасно заблокувати картку, у разі шахрайських операцій з вашим рахунком. Встановити індивідуальні ліміти на зняття готівки, які відповідають саме вашій платіжній поведінці. Шахраю не вдасться всю суму зняти одразу, у вас з'явиться час заблокувати свою картку. Надавати перевагу платіжним карткам з чіпом, у яких складніший алгоритм захисту на відміну від карток з магнітною смугою [5].

Крім того, в цьому ж сегменті відтворюються й злочинні порушення права на недоторканість приватного життя, що проявляється у незаконному збиранні, зберіганні, використанні, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації (ст. 182 КК України) з використанням ресурсів телекомунікаційних мереж;

- кіберзлочинність, об'єктом якого є суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;

- кіберзлочинність, що посягає на інтереси держави, на її конституційний лад, суверенітет, територіальну цілісність і недоторканність. Цей сегмент кіберзлочинності представлений кібертероизмом, кібердиверсіями, а також низкою інших кримінальних практик, спрямованих на підрив обороноздатності, економічного, військового, наукового, інтелектуального потенціалу держави, за виключенням злочинних посягань на об'єкти критичної інфраструктури;

Особливе занепокоєння в цьому контексті викликає діяльність так званих «ботоферм», анонімних каналів у месенджерах, створення та функціонування яких керується, фінансується російськими спецслужбами. Вони використовуються для широкої дезіфнормації населення, підриву довіри до органів державної влади, ескалації політичної напруженості, ускладення виконання задач з мобілізації, укомплектування штатів Збройних Сил України, приведення їх до вимог воєнного стану і конкретних задач у сфері відсічі збройній агресії;

- кібердиверсії на об'єкти критичної інфраструктури, що так само використовуються країною-агресором для послаблення обороноздатності України.

Таким чином, кіберзлочинність в сучасних умовах є складним кримінальним феноменом, у якому поєднуються як ординарні сегменти злочинної активності переважно корисливої спрямованості, так і політично умотивовані практики, які комбінуються державою-агресором з бойовими та іншими заходами для послаблення обороноздатності нашої держави. Відтак, протидія кіберзлочинності вимагає застосування новітніх стратегічних підходів, принципово нових способів взаємодії різних суб'єктів антикримінальної діяльності.

Список використаних джерел:

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.
2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 1263-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
3. Діброва Т. А., Пісенко Д. О., Сметаніна Н. В. Кіберзлочинність та кібершахрайство в умовах воєнного стану. *Юридичний науковий електронний журнал*. 2022. № 11. С. 546–549. URL: http://lsej.org.ua/11_2022/132.pdf.
4. Левківська Я. І. Вплив воєнного стану на трансформування та розвиток інтернет-шахрайства в Україні. URL: http://dspace.onua. edu.ua/handle/11300/19993 (дата звернення: 20.11.2022).
5. Офіційний сайт Національного банку України. Проєкт «#ШахрайГудбай». URL: https://promo.bank.gov.ua/stopfraud/#section-35.