2. Керування ризиком. Словник термінів (ISO Guide 73:2009, IDT) ДСТУ ISO Guide 73:2013. Видання офіційне. Київ, Мінекономрозвитку України. 2014. 13 с. С. 1.

3. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX. Верховна Рада України. Законодавство: вебсайт. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text.

4. Про об'єкти підвищеної небезпеки: Закон України від 18.01.2001 № 2245-III. Верховна Рада України. Законодавство: вебсайт. URL: https://zakon.rada.gov.ua/laws/show/2245-14#Text.

Левченко Юрій Олександрович,
завідувач кафедри кримінології
та кримінально-виконавчого права
Національної академії внутрішніх справ,
кандидат юридичних наук, професор

КІБЕРЗЛОЧИННІСТЬ В УКРАЇНІ НА СУЧАСНОМУ ЕТАПІ

Сьогодні кожна сучасна соціально активна людина в Україні використовує мобільні пристрої та користується інтернетом, державні органи переходять на електронний документообіг, стабільна діяльність банківського сектору, залізниці й авіатранспорту, великих підприємств залежить від стабільності кіберпростору, з яким вони працюють, та базується на комунікації за допомогою електронних засобів зв'язку.

Стрімкий розвиток інформаційних технологій в Україні, який ми спостерігаємо останнє десятиріччя, невблаганно супроводжується динамічним розвитком злочинів у цій сфері. Кіберзлочини є найдинамічнішою групою суспільно небезпечних діянь, адже з кожним роком кіберзлочини стають дедалі масовішими й небезпечнішими.

Фахівці у сфері інформаційних технологій визнають, що ситуація з кіберзлочинністю у світі погіршується. Організована злочинність дедалі частіше використовує Інтернет з метою приховання своєї діяльності. Як приклад, існування мережі Darknet, за допомогою якої злочинці фактично створили чорний ринок для збуту наркотиків, зброї, крадених товарів тощо. Завдяки технологіям, які забезпечують мережеву анонімність, ця частина Інтернету залишається абсолютно безконтрольною, а тому безпечною для діяльності різноманітних злочинних угруповань. За даними Національної поліції України, кількість організованих груп і злочинних організацій, що вчиняють кримінальні правопорушення з використанням високих інформаційних технологій, за останній рік збільшилась на 36 %.

Відповідно до офіційної статистики Офісу Генерального прокурора України, лише за останні 8 років кількість виявлених кіберзлочинів збільшилась майже в 7,5 разів (і це не враховуючи класичні правопорушення з використанням комп'ютерної техніки, а також рівня латентності такої злочинності).

В Україні нормативно-правове підґрунтя для боротьби з кіберзлочинністю становлять: Конституція України, Кримінальний кодекс України, Закони України «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про захист інформації в інформаційнотелекомунікаційних системах» та ін., Доктрина інформаційної безпеки України від 2017 р., Конвенція Ради Європи про кіберзлочинність, Додатковий протокол до неї та ін. міжнародні договори, згода на обов'язковість яких надана Верховною Радою України.

Відповідно до п. 5 ч.1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України», прийнятого 5 жовтня 2017 року (набув чинності 9 травня 2018 року), кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. Цей закон визначає основні напрями та цілі державної політики у сфері кібербезпеки, закріплює повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері та основні засади координації їхньої діяльності із забезпечення кібербезпеки. Проте слід зазначити, що в Законі відсутні правові інструменти для його практичного застосування під час здійснення кібератак [1].

Термін «кіберзлочин» є відносно новий, який утворений сполученням двох слів: «кібер» (розуміється як «кіберпростір», «віртуальний світ», «інформаційний простір») і «злочин». Під поняттям «кіберзлочину» слід розуміти соціальне явище, що являє собою навмисну мотивовану атаку з використанням мережі Інтернет на інформацію в комп'ютерній системі, програми або дані, що чиниться окремою особою або угрупуваннями, яке має суспільну небезпеку для суспільного ладу України, його політичної й економічної системи, власності, особі, політичним, трудовим, майновим та іншім правам і свободам громадян. Важливим аспектом правопорушень у кіберпросторі є їхній нелокальний характер, що створює серйозні проблеми для правоохоронних органів, адже національні злочини, які раніше мали місцеве значення, зараз потребують міжнародної співпраці. Тому більшість держав зацікавлені в зупиненні дій, пов'язаних з витоком персональних даних своїх громадян в мережу Інтернет, та зменшенні кібератак, які перешкоджають роботі органів державної влади, підприємств, установ, організацій, банків тощо[2].

Щодо класифікації кіберзлочинів, то в Конвенції Ради Європи про кіберзлочинність, яку Верховна Рада України ратифікувала й імплементувала до українського законодавства починаючи з 11.10.2005, виокремлено чотири основні типи кіберзлочинів: правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних

і систем – незаконний доступ, нелегальне перехоплення, втручання в дані, втручання в систему, зловживання пристроями; правопорушення, пов'язані з комп'ютерами, – підробка, пов'язана з комп'ютерами, шахрайство, пов'язане з комп'ютерами; правопорушення, пов'язані зі змістом, – правопорушення, пов'язані з дитячою порнографією; правопорушення, пов'язані з порушенням авторських і суміжних прав.

Найпоширенішими видами кіберзлочинів є: ***кардинг*** – шахрайські операції з кредитними картками (реквізитами кредитних карток), які не погоджені власником картки. Це може бути крадіжка чи незаконне отримання кредитної картки, викопіювання даних картки для подальшого її підроблення, викопіювання реквізитів картки для здійснення покупок через Інтернет без участі власника картки. У будь-якому разі основною метою злочинців є отримання доступу до чужих грошових коштів. Для досягнення цієї мети зловмисники вигадують різноманітні способи отримання потрібної інформації в неуважних і легковірних громадян. Одним із таких способів є фішинг. ***Фішинг*** – шахрайські дії, спрямовані на виманювання реквізитів картки у її власника. Зазвичай власник кредитної картки сам добровільно повідомляє шахраям потрібну інформацію. Фішинг буває кількох видів: **СМС-фішинг**, коли потенційна жертва шахраїв отримує повідомлення про те, що її кредитну картку заблокував банк, а для розблокування необхідно надати реквізити, або ж про те, що власник картки отримав виграш, але потрібно заплатити за його доставку. Варіацій СМС-повідомлень безліч, тому потрібно бути особливо уважними й обачними, якщо ви отримуєте повідомлення. **Інтернет-фішинг**, коли шахраї створюють фішингові (підроблені) сторінки, які імітують офіційні сторінки банків, платіжних сервісів, інтернет-магазинів тощо. На жаль, не всі уважно перевіряють назву сайта, уводячи дані кредитної картки, що на руку кібершахраям. ***Вішинг*** – це майже той самий фішинг, однак виманювання реквізитів картки зловмисники здійснюють за допомогою телефонних дзвінків (шахраї часто представляються працівниками банку й намагаються вивідати у власника картки ПІН-код чи примусити здійснити якісь дії зі своїм рахунком). ***Скімінг*** – копіювання даних платіжної картки за допомогою спеціального пристрою (скімера). Зазвичай відбувається під час здійснення карткових операцій із банкоматами. Для отримання даних злочинці використовують міні-камери або змінні клавіатури. ***Шимінг*** – модернізований різновид скімінгу. У цьому разі шахраї використовують майже непомітний прилад, який розміщують усередині картридера. Таким чином дані кредитки копіюються непомітно. ***Онлайн-шахрайство*** – фальшиві інтернет-аукціони, інтернет-магазини, сайти й телекомунікаційні засоби зв'язку. ***Піратство*** – протиправне розповсюдження об'єктів інтелектуальної власності в Інтернеті.

Мальваре – створення та поширення вірусів і шкідливого програмного забезпечення. ***Протиправний контент*** – контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ

жорстокості й насильства. ***Рефайлінг*** – незаконна підміна телефонного трафіку.

Крім того, за даними кіберполіції сьогодні збільшилась кількість звернень про викрадення криптовалюти. Є шахрайські схеми, коли власник електронного гаманця надає доступ шахраям до своїх акаунтів і вони переводять десятки тисяч доларів на інший гаманець. Кіберполіція кваліфікує цей вид злочину як шахрайство з використанням електронно-обчислювальної техніки. На думку фахівців криптовалюта має бути легалізована й підконтрольна, адже за її допомогою вчиняють багато злочинів, таких як продаж наркотиків, зброї тощо [3].

Так, інформаційна революція призвела до того, що злочинцем може виявитися звичайний студент із ноутбуком та доступом до мережі.

А в умовах війни такий злочинець стає бойовою одиницею, а його основний інструмент - кібератаки. Крім того, під час воєнного стану атаки можливі не лише з боку ворога, який використовує інфопростір для завдання шкоди обороноздатності України, а й з боку тих, хто вирішив скористатися ситуацією, коли правоохоронні органи перевантажені, та заволодіти коштами громадян. В наш час війна в інформаційному просторі може завдати не меншої шкоди, аніж війна на полі бою. В умовах війни кіберзлочини можуть здійснюватися з метою дестабілізації ситуації в країні, крадіжки необхідних (конфіденційних) даних, виведення з ладу державних інституцій, техніки, завдання іншої матеріальної шкоди.

Війна в Україні у 2022 році не стала стартом для кібератак зі сторони Російської Федерації, проте стала своєрідним каталізатором, адже кількість та інтенсивність кіберзлочинів значно зросла. Щодня росія вдається до кібератак різного масштабу та рівня та діє в основному трьома способами.

По-перше, кіберзлочинці сприяють веденню бою та розгортанню військового конфлікту на місцях, здійснюючи атаки на об’єкти критично важливої інфраструктури на рівні держави та регіонів, зокрема банки, електростанції, ЗМІ, сервери великих корпорацій й таке інше.

Окрім цього, росія використовує кібератаки як один з методів гібридної війни, що дозволяють, не розгортаючи відкритого конфлікту з Заходом, Європейським союзом чи НАТО, здійснювати опосередкований вплив на цільові країни (особливо в поєднанні з кампаніями з дезінформації й політичними кроками). Кібервійна має постійний характер та в більшості випадків відбувається й в мирний час. Ще один спосіб кіберманіпулювання – точкові сигнальні погрозливі кіберзлочини, які є своєрідним доповненням до класичної дипломатії.

Так, від початку війни стало відомо про велику кількість кібератак на Україну: 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.

Ще одним прикладом є отримання українськими користувачами нових небезпечних електронних листів, відкриття яких призводить до отримання хакерами повного контролю над вашим комп'ютером та загрожує крадіжкою та пошкодженням комп'ютерних даних.

Під прицілом знаходяться також об'єкти критичної інфраструктури. Український провайдер Укртелеком зазнав потужної атаки 28 березня 2022 року, під час якої хакери намагались · проаналізувати, як влаштована ІТ-інфраструктура, вивести з ладу обладнання та сервіси, а також отримати контроль над мережею та обладнанням компанії. Ворог намагався здійснити кібератаку на державні установи України з використанням шкідливої програми Cobalt Strike Beacon, яка уражає комп'ютер у випадку її відкриття.

Відповідальність за кіберзлочини передбачена розділом XVI Кримінального кодексу України (ККУ), саме 2 норми із цього розділу і зазнали змін відповідно до нового Закону 2149-IX. Підвищення ефективності боротьби з кіберзлочинністю під час війни та посилення відповідальності за відповідні злочини є давно назрілим кроком. Новий закон розширює межі діяльності правоохоронних органів щодо розслідування кіберзлочинів, передбачених статями 361, 361-1 ККУ. Посилення санкцій та додаткова криміналізація окремих діянь здатні частково стримати потенційних злочинців від вчинення нових злочинів.

Виправданим є й запровадження відповідальності за злочини, що скоєні у воєнний час. Настільки суворі санкції за їх вчинення продиктовані поточною ситуацією в країні, адже особа, яка завдає шкоди національним інтересам України чи українцям у кіберпросторі, тим самим допомагаючи агресору у цій війні, не може нести відповідальності меншої, ніж військові злочинці.

Сфера кіберпростору і раніше потребувала посиленого захисту та змін. Відкрите вторгнення росії стимулювало вдосконалення чинного законодавства та гарантій безпеки у сучасному інформаційному середовищі.

Отже під час війни в зоні ризику перебувають державні органи, великі підприємства, підприємства оборонної та критичної інфраструктури, а також підприємства, які забезпечують населення та оборону усім необхідним в умовах війни. Є ризики й для місцевих жителів, які перебувають в зоні бойових дій [4].

Якою б не була кібератака, в який час би вона не відбувалась та в яких масштабах, мета залишається непохитною – руйнування громади, організацій чи механізмів. Змінюється лише контекст: гібридна війна під маскою дипломатії чи відкриті військові дії. Але ж результат лише один – страждають невинні люди, маси втрачають довіру до органів управління, й відбувається своєрідний регрес через пошкодження, викрадення чи зміну інформаційних ресурсів [5].

Сьогодні закони повинні відповідати вимогам, що пред'являються сучасним рівнем розвитку технологій. Пріоритетним напрямком є також організація взаємодії і координація зусиль правоохоронних органів, спецслужб, судової системи, забезпечення їх необхідною матеріально-технічною базою. Жодна держава сьогодні не в змозі протистояти кіберзлочинності самостійно. Нагальною є необхідність активізації міжнародної співпраці в цій сфері. Експерти впевнені: саме хакери в недалекому майбутньому стануть загрозою номер один, змістивши тероризм. Незважаючи на віртуальність злочинів, збиток вони завдають цілком справжній.

Отже, найкращим способом протидії високотехнологічної злочинності можна вважати реалізацію випереджаючого правового регулювання. Також слід додати, що відсутність єдиної міжнародної нормативної правової бази, істотні відмінності в національних законодавствах країн, об'єднаних ідеєю спільної боротьби з комп'ютерною злочинністю, та відсутність єдиного підходу до визначення понятійного апарату розглянутої сукупності суспільно небезпечних діянь суттєво ускладнюють ефективну протидію використанню комп'ютерних технологій при здійсненні злочинів.

Важливе значення має посилення співпраці підрозділів, що здійснюють боротьбу з комп'ютерною злочинністю, та суб'єктами інформаційного обігу. Об'єднана протидія кіберзлочинам може здійснюватися тільки на основі ефективної та високопрофесійної роботи підрозділів по боротьбі з комп'ютерними злочинами. Діяльність цих підрозділів необхідно забезпечити відповідною правовою, матеріальною та кадровою підтримкою держави. Ефективна і високопрофесійна діяльність правоохоронних органів повинна поєднуватися з принципами конфіденційності, довірчої взаємодії і гарантіями збереження державної, банкової, комерційної таємниці та інших цінних відомостей. На стадії запобігання комп'ютерним злочинам важливо, по-перше, змінювати умови зовнішнього середовища таким чином, щоб утруднити чи виключити кримінальне використання комп'ютерної інформації та техніки; по-друге, забезпечувати цілеспрямований позитивний вплив на людей і запобігати тим самим їх кримінальну поведінку в даній сфері. На державному рівні значима розробка спеціальних систем захисту комп'ютерної інформації загальнодержавного, загальнонаціонального значення, а також створення правової основи їх функціонування. Важливу роль при цьому має відігравати спеціалізоване правове виховання суб'єктів інформаційного обігу, власників і користувачів комп'ютерної інформації та техніки.

Список використаних джерел

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовтня 2017 р. № 2163-VIII. Законотворчість : база даних. URL: https://zakon.rada.gov.ua/ laws/show/2163-19.

2. Кіберзлочинність в Україні: виклики сучасності. URL: http://www.lsej.org.ua/9_2021/51.pdf.

3. Кіберзлочинність в Україні. Ера цифрових технологій – ера нових злочинів. URL: https://uz.ligazakon.ua/ua/magazine_article/EA013606.
4. Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX. URL: https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ixБ.
5. Кібербезпека в умовах гібридної війни. URL: https://rubryka.com/article/cyber-security-and-hybrid-warfare/.

Лисенко Альона Олександрівна,
викладач кафедри кримінології
та кримінально-виконавчого права
Національної академії внутрішніх справ

ЗАПОБІГАННЯ ХУЛІГАНСТВУ, ВЧИНЕНОМУ ДІТЬМИ, В УКРАЇНІ

Злочинну поведінку детермінує значна кількість факторів, однак усі вони мають різний рівень важливості. Ефективність же боротьби із злочинністю, у тому числі з кримінальними правопорушеннями проти громадського порядку, залежить від своєчасного виявлення та врахування усієї сукупності факторів, що характеризують даний вид злочинів.

Запобігання вчиненню хуліганству дітьми є об'єктивною потребою суспільства, що будує правову державу. Головний напрям цієї протидії – запобігання злочинності дітей, усунення причин та умов, що її породжують і сприяють її різноманітним проявам. Тим самим створюються реальні передумови поступового ослаблення суспільної небезпечності злочинів та зменшення масштабів самої злочинності.

Питанням, пов'язаним із кримінально-правовим та кримінологічним запобіганням хуліганству, присвятили свої праці такі вчені як О.М. Джужа, А.О. Джужа, В.В. Василевич, Д.М. Тичина, Ю.А. Абросімова, О.Г. Колб, Н.В. Кулакова, О.О. Пустовий, П.А. Зеленяк, В.В. Артюхова, В.І. Борисов, О.А. Галемін, О.А. Івахненко, Л.О. Кузнецова, В.В. Налуцишин, Г.І. Піщенко, Є.В. Фесенко, В.В. Шаблистий, та ін.

Останніми роками спостерігається нестабільність рівня життя більшості сімей в Україні. Найбільш уразливими є багатодітні родини, та сім'ї, в яких нема годувальника, а також ті, в яких працездатні її члени не мають регулярного доходу. Найбільш незахищеними від соціальних потрясінь і вразливими до впливу криміногенних факторів є діти. Також багато хуліганських дій, що вчиняються дітьми пов'язані з тим, що вони відтворюють у громадському місці стереотипи поводження, до яких звикли в родині, як до норми.

Вважається, що хуліганство є одним із найпоширеніших правопорушень, спрямованих проти громадського порядку. Особа, яка вчинила хуліганство, посягає на суспільні відносини, що забезпечують