УДК 343.98:004.056

ГУЦАЛЮК М.В., *кандидат юридичних наук, доцент,* головний науковий співробітник Міжвідомчого центру з проблем боротьби з організованою злочинністю при РНБО України.
ORCID: https://orcid.org/0000-0003-4496-5173.

ШЛЯХИ ПОСИЛЕННЯ СПРОМОЖНОСТЕЙ ПРАВООХОРОННИХ ТА ІНШИХ ДЕРЖАВНИХ ОРГАНІВ У СФЕРІ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

Анотація. *У статті розглянуто проблеми боротьби з кіберзлочинністю та надаються рекомендації щодо посилення спроможностей правоохоронних та інших органів у цій сфері.*
Ключові слова: *Інтернет, кіберзлочинність, кібербезпека, електронна комерція.*

Summary*. The article considers issues of cybercrime fighting and provides recommendations with regard to strengthening the capacity of law enforcement and other government agencies in this sphere.*
Keywords*: Internet, cybercrime, cybersecurity, e-commerce*

Аннотация: *В статье рассматриваются проблемы борьбы с киберпреступностью и даются рекомендации по усилению правоохранительных и других органов в этой сфере.*
Ключевые слова*: Интернет, киберпреступность, кибербезопасность, электронная коммерция.*

Постановка проблеми. Наприкінці минулого століття проблема профілактики злочинності, пов'язаної із застосуванням комп'ютерів, та боротьби з нею набула міжнародних масштабів та вже досліджувалася на рівні ООН [1]. Подальше поширення доступу до Інтернету та кількості підключених до глобальної мережі різноманітних пристроїв продовжує надавати кіберзлочинцям дедалі більше можливих векторів атак для здійснення злочинів. Якщо у 2008 році по всьому світу було 1,5 млрд. користувачів Інтернету, то у 2019 році Міжнародний союз телекомунікацій (МСЕ) визначив це число у 4,1 млрд., що становить більше половини населення планети [2]. За інформацією Державної служби статистики України, станом на 1 січня 2020 року в Україні було зафіксовано 28 млн. 787 тисяч користувачів Інтернету, що перевищує половину населення держави [3].

Відповідно до звіту Cisco (Cisco Annual Internet Report) кількість пристроїв, підключених до мережі Інтернет, до 2023 року перевищить кількість населення у світі втричі та складе 3,6 мережевих пристроїв на душу населення [4]. Завдяки цьому слід очікувати подальшого збільшення кількості можливих кібератак.

Кіберзлочинці постійно застосовують нові технології та методи кібератак, з метою уникнення своєї ідентифікації, користуючись прогалинами в законодавствах країн щодо належної ідентифікації особи в Інтернет-просторі. Для цього, наприклад, використовують технологію VPN (Virtual Private Network) та TOR (The Onion Router). Дедалі більшого поширення в Україні набуває практика використання провайдерами телекомунікаційних послуг технології NAT (Network Address Translation), яка за відсутності належного обліку використання внутрішніх IP-адрес провайдера фактично унеможливлює ідентифікацію конкретного користувача, який вчинив протиправне діяння.

З огляду на вказані тенденції кіберзлочинність залишається постійною загрозою для приватних осіб, суб'єктів господарювання і держави, яка продовжує зростати в кількості і масштабах та різновидах. Особливістю поширення кіберзлочинності є її

транскордонний характер і її поширюваність як серед країн, що розвиваються, так і тих, хто має більш високий рівень розвитку. Широке використання технологій та зростаючі темпи підключення до Інтернету по всьому світу в поєднанні з постійним розвитком нових технологій, які забезпечують анонімність в Інтернеті, дають змогу кіберзлочинності бути низько ризиковою та високоприбутковою справою. Через це у два найближчі десятиліття кіберзлочинність залишатиметься однією з найбільших проблем для розвитку суспільства як в Україні, так і в більшості країн світу. Згідно з офіційним щорічним звітом про кіберзлочинність 2020 року компанії Cybersecurity Ventures, збитки від кіберзлочинності становитимуть понад 6 трильйонів доларів щорічно до 2021 року, що на 3 трильйони доларів перевищує збитки у 2015 році [5].

Результати аналізу наукових публікацій. Різні аспекти проблем боротьби з кіберзлочинністю були предметом дослідження таких вітчизняних науковців, як Ахтирська Н.М., Бутузов В.М., Гавловський В.Д., Голубєв В.О., Демедюк С.В., Савченко А.В., Хахановський В.Г., Шеломенцев В.П. та ін. [6 – 11]. Проте багато питань потребують подальшого дослідження та вирішення у практичній площині.

Метою статті є надання рекомендацій щодо посилення спроможностей правоохоронних та інших органів у боротьбі з кіберзлочинністю.

Виклад основного матеріалу. В останні роки в Україні значно активізувався розвиток цифрової економіки. Цьому посприяв, зокрема, Закон України "Про електронну комерцію", який визначає організаційно-правові засади діяльності у сфері електронної комерції в Україні, встановлює порядок вчинення електронних правочинів із застосуванням інформаційно-телекомунікаційних систем та окреслює права і обов'язки учасників відносин у сфері електронної комерції. У січні 2018 року уряд ухвалив "Концепцію розвитку цифрової економіки та суспільства України на 2018 – 2020 роки", сред ключових напрямків якої – розвиток цифрової інфраструктури. Усю територію України заплановано покрити широкосмуговим Інтернетом, що дасть поштовх цифровим трансформаціям у системі освіти, медицини, екології, безготівкової економіки, інфраструктури, транспорту тощо. Діджиталізація (цифрові технології) приходить на заміну старим засобам електронної комунікації – телефону, факсу, телеграфу [12].

Також в Україні починаючи з вересня 2019 року, почало діяти Міністерство цифрової трансформації, яке реалізує державну політику у сферах цифрового розвитку, цифрової економіки, цифрових інновацій, розвитку цифрових навичок та цифрових прав громадян. Відповідно до Указу Президента України від 4.09.19 р. № 647/2019 передбачається переведення окремих публічних послуг в електронну форму [13].

У лютому 2020 року в Україні запустили мобільний додаток "Дія", завдяки якому можна отримати десятки публічних послуг он-лайн, зокрема, стати підприємцем, змінити вид діяльності чи припинити її тощо [14].

9 червня 2020 року Президент України подав на розгляд Верховної Ради України проект Закону "Про народовладдя через всеукраїнський референдум", який передбачає реалізацію права голосу виборця шляхом електронного голосування.

Разом з тим, в українському сегменті кіберпростору продовжують вчинятися кіберзлочини. З кожним роком кількість потерпілих від протиправних дій кіберзлочинців стає дедалі більше. Як уже зазначалося, самі правопорушення стають більш масштабними.

Найбільшу небезпеку становлять кібератаки на об'єкти критичної інформаційної інфраструктури, які за останні 5 років постійно здійснюються різноманітними кіберугрупованнями. Деякі з них завдали значних матеріальних збитків – зокрема сумновідомий вірус Petya Ransomware, через який постраждало понад 60 країн світу, а збитки від нього сягають 8 млрд. доларів США [15].

На важливості питання забезпечення кібербезпеки у процесі цифрової трансформації держави та кіберзахисті державних електронних інформаційних ресурсів наголосив Секретар Ради національної безпеки і оборони України Олексій Данілов під час 14-го засідання Національного координаційного центру кібербезпеки, яке відбулося 22 травня 2020 року.

Під час засідання Координаційного центру Секретар РНБО України звернув увагу представників органів влади на незадовільний стан захищеності державних електронних інформаційних ресурсів, реєстрів, баз даних та інших інформаційних масивів та наголосив на необхідності удосконалення практичної взаємодії між суб'єктами забезпечення кібербезпеки.

Наприклад, у травні 2020 року в месенджері Telegram з'явився бот, який видавав персональні дані громадян та іншу інформацію, зокрема було надано 4,5 млрд. логінів і паролів. За фактом розповсюдження персональної інформації громадян розпочато розслідування кримінального провадження за ч. 2 ст. 361 Кримінального кодексу України (несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації) [16]. Під час проведення операції під умовною назвою "ДАТА", спрямованої на протидію несанкціонованим діям з інформацією та незаконному розповсюдженню чи збуту даних з обмеженим доступом, кіберполіція спільно зі слідчими підрозділами НП України, Міністерством цифрової трансформації України та Службою безпеки України, під процесуальним керівництвом прокуратури провели 36 обшуків у різних областях України. За результатами виявлено велику кількість файлів, що містять персональні дані громадян України, фрагменти баз даних державних, банківських та комерційних установ. Наразі встановлено 25 причетних до правопорушень осіб. Такі злочини підривають довіру суспільства до впроваджених Урядом цифрових ініціатив, відтак потребують значної уваги та інтенсивної роз'яснювальної роботи з громадськістю. Важливим напрямком є також відслідковування та впровадження прогресивних рішень захисту персональних даних громадян країни проти можливого втручання з боку третіх країн, і в цьому зв'язку подальше вдосконалення законодавства України і приведення його у відповідність до відповідних Директив Європейського Союзу (зокрема про електронну комерцію, про захист персональних даних тощо).

Поглиблення міжнародної співпраці є також на часі, оскільки завдяки розвитку ІТ-індустрії України та значному авторитету українських фахівців цієї галузі, на жаль дедалі частішими стають явища виявлення недобросовісних суб'єктів, які вчиняють злочини в цій сфері як на території України так і поза її кордонами. Так в липні 2020 року Секретна служба США і Держдепартамент оголосили про винагороду у 2 млн. доларів за інформацію, яка допоможе арештувати або засудити двох громадян України.

У США їх звинувачують у кібершахрайстві, зламі комп'ютерних систем і незаконних операціях з цінними паперами. На кібершахрайстві хакери незаконно заробили понад 4,5 млн. доларів, стверджує відомство. Секретна служба США наголошує, що це перший випадок, коли федеральна служба звертається за допомогою до громадськості у всьому світі.

В цьому ж місяці українські правоохоронці виявили та затримали відомого хакера під ніком "Sanix", який проживав в Івано-Франківську. У прес-службі СБУ повідомили, що саме цей хакер у минулому році звернув на себе увагу світових фахівців з

кібербезпеки після того, як виклав на одному з форумів оголошення про продаж бази із 773 млн. адресів поштових скриньок та 21 млн. унікальних паролів [17].

Слід також зауважити, що несанкціоновані дії з інформацією на інформаційних ресурсах здійснюють не тільки хакери чи спецслужби інших країн, але й адміністратори та інші особи, які мають право доступу до неї. Наприклад, у травні 2020 року Служба безпеки України викрила факт втручання в електронну систему Державного земельного кадастру, який здійснив посадовець Держслужби України з геодезії, картографії та кадастру. За версією слідства, чиновник на замовлення "клієнтів" безпідставно видалив відомості щодо прав власності на земельну ділянку загальною площею 5 гектарів на території Ірпінської міської ради [18].

Також набувають поширення кіберзлочини, які не пов'язані безпосередньо з несанкціонованим доступом до інформації, але відповідають визначенню, наданому в Законі України "Про основні засади забезпечення кібербезпеки України" від 5.10.17 р. № 2163-VIII, – кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України.

Серед таких кіберзлочинів найбільш поширеними є шахрайство (чч. 3 і 4 ст. 190 КК України).

Наприклад, у червні 2020 року співробітники кіберполіції в Дніпропетровській області із залученням полку поліції особливого призначення та працівників виправної установи припинили злочинну діяльність групи осіб, які під виглядом продажу товарів заволоділи грошима громадян. Кіберполіція встановила, що до такої діяльності причетні четверо мешканців Дніпропетровської області. Фігуранти створили власний веб-сайт, за допомогою якого під виглядом продажу побутових товарів відомих брендів ошукували громадян. Своїми протиправними діями вони завдали збитків на загальну суму два мільйони гривень. Від їхніх дій постраждало близько 200 громадян України. Зазначимо, що організатор групи раніше неодноразово засуджений та відбуває покарання за вчинення злочину, передбаченого ст. 190 (Шахрайство) Кримінального кодексу України [19].

Посилене використання Інтернету під час пандемії надає кіберзлочинцям більше можливостей для реалізації шахрайських схем для інфікування шкідливими програмами або продажу лікарських, зачасти фальсифікованих товарів. З початку спалаху COVID-19 кіберзлочинці активно експлуатують цю проблему, створюючи сайти, заражені зловмисним програмним забезпеченням, та спонукаючи людей купувати підроблені ліки, добавки та вакцини. За даними, зібраними та проаналізованими Atlas VPN, ***кількість фішингових веб-сайтів під час карантину COVID-19 зросла на 350 %*** [20].

За кордоном вказаним видам злочинів приділяється значна увага з огляду на їх велику кількість та зростаючу динаміку шахрайських діянь. Наприклад, компанія з кібербезпеки RiskIQ (https://www.riskiq.com) почала сканувати нові домени, пов'язані з коронавірусом, відстежуючи такі ключові слова, як ковід, вірус, вакцина чи пандемія, та виявила понад 300 тисяч підозрілих веб-сайтів.

Як відповідь на подібні виклики, у Великобританії реєстратори доменних імен веб-сайтів активізують свої зусилля для боротьби з аферистами, і це починається ще до того, як їх веб-сайти з'являться в реальному часі.

Реєстратори перевіряють відповідність назв сайтів їх змісту та вимогам щодо їх утворення та наявність прав у замовника реєстрації оперувати відповідною назвою сайту. При виявленні невідповідності законодавчо визначеним вимогам такі сайти не

реєструють. Даний метод застосовується для попередження різних видів шахрайств, наприклад, пов'язаних із банківською діяльністю або сплатою податків, щоб зменшити діяльність шахрайських веб-сайтів, на етапі їх реєстрації. Спеціальні алгоритми підбирають спроби реєстрації доменів імен, які містять ключові слова, та оцінюють їх. Реєстратори доменних імен вже призупинили 600 підозрілих веб-сайтів, пов'язаних з темою коронавірусу.

Промисловий масштаб, в якому шахраї встановлюють веб-домени, змусив урядовців і інших країн закликати реєстраторів доменних імен посилити боротьбу з шахрайськими сайтами. Так, Генпрокурор Нью-Йорка Летітія Джеймс нещодавно надіслала відкриті листи шести найбільшим реєстраторам домену в Інтернеті з проханням посилити свої контрзаходи [21]. Об'єднання зусиль всіх реєстраторів і опрацювання проблеми з боку представників профільної галузі є важливою запорукою отримання позитивного ефекту в боротьбі з окресленою проблемою та створення інструментів відповідного саморегулювання з боку бізнесу.

Вчиненню подібних правопорушень в Україні сприяє наявність прогалини у чинному вітчизняному законодавстві.

Так Законом України "Про електронну комерцію" визначено організаційно-правові засади діяльності у сфері електронної комерції в Україні, встановлено порядок вчинення електронних правочинів із застосуванням інформаційно-телекомунікаційних систем та визначено права й обов'язки учасників відносин у сфері електронної комерції. Зокрема частиною 1 статті 7 передбачено обов'язок продавця товарів забезпечити прямий, простий, стабільний доступ інших учасників відносин у сфері електронної комерції до такої інформації:

повне найменування юридичної особи або прізвище, ім'я, по батькові фізичної особи-підприємця;

місцезнаходження юридичної особи або місце реєстрації та місце фактичного проживання фізичної особи-підприємця;

адреса електронної пошти та/або адреса Інтернет-магазину;

ідентифікаційний код для юридичної особи або реєстраційний номер облікової картки платника податків для фізичної особи.

Наведена норма повною мірою відповідає положенням Директиви ЄС "Про захист прав споживачів та щодо електронної комерції" (Directive 2011/83/EU), проте, на відміну від законодавства ЄС, Закон України "Про електронну комерцію" ***не визначає*** відповідальність суб'єкта електронної комерції за невиконання обов'язків, встановлених Законом, а також не визначений контролюючий орган, який зобов'язаний моніторити виконання зазначених положень закону.

Це надає можливість недобросовісним учасникам відносин у сфері електронної комерції ***уникати сплати податків, продавати фальсифіковані товари, реалізовувати контрабандний товар*** – адже юридична особа не вказана і відсутні державні органи, які повинні контролювати зазначену сферу.

Наприклад, у липні 2020 року кіберполіція викрила осіб, які під виглядом продажу товарів та послуг "заробили" майже 1,5 млн. гривень. Члени групи створили 14 веб-сайтів, де продавали неіснуючі товари. У результаті від дій зловмисників постраждало понад дві сотні громадян. Правопорушникам загрожує до дванадцяти років ув'язнення з конфіскацією майна [22].

У результаті споживачі таких товарів можуть зазнавати загрози життю та здоров'ю, матеріальних збитків. Бюджет держави недоотримує відповідних надходжень, а шахраї

продовжують користуватися недоліками законодавства. Це є однією з причин, що надає можливість понад половині бізнесу перебувати в тіні.

На нашу думку, слід чітко визначити відповідальність за невиконання статті 7 Закону України "Про електронну комерцію" та державні органи, які уповноважені здійснювати контроль у зазначеній сфері. За аналогією з законодавством Європейського Союзу відповідними контролюючими органами можуть бути підрозділи податкової служби або кіберполіції та Державної служби України з питань безпечності харчових продуктів та захисту споживачів.

Так *Державна служба України з питань безпечності харчових продуктів та захисту споживачів* відповідно до Положення про службу перевіряє додержання суб'єктами господарювання, що провадять діяльність у сфері торгівлі і послуг, вимог законодавства про захист прав споживачів, а також правил торгівлі та надання послуг. До правил надання послуг в електронній комерції належить зокрема дотримання суб'єктами господарювання вимог щодо електронної комерції, зокрема в частині ідентифікації суб'єкта господарювання.

Також, безперечно, зазначену роботу можуть проводити співробітники *Департаменту кіберполіції НП України*, який спеціалізується на попередженні, виявленні, припиненні та розкритті кримінальних правопорушень, механізмів підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), телекомунікаційних та комп'ютерних Інтернет-мереж і систем.

У зв'язку з тим, що власники зазначених сайтів, як правило, ухиляються від сплати податків, доцільною видається перевірка таких підприємців співробітниками регіональних підрозділів податкової служби.

Вирішення зазначених вище проблемних питань потребує здійснення системних заходів із створення відповідної законодавчої бази. Зокрема необхідно внести зміни до Податкового кодексу України, Кодексу України про адміністративні правопорушення, Кодексу адміністративного судочинства України, Закону України "Про захист прав споживачів", Закону України "Про авторське право та суміжні права" тощо. Вирішення зазначеного питання потребує оперативного опрацювання фахівцями профільних відомств.

Певна робота у цьому напрямі вже проводиться. Зокрема, зареєстровані законопроекти № 3860 та № 3861 щодо присвоєння та використання офіційної електронної адреси для юридичних та фізичних осіб. На нашу думку, необхідно впровадити реєстрацію офіційних сайтів на основі системи ID-Web. Реєстрація та адміністрування таких сайтів повинно здійснюватися за допомогою електронних ID-документів, що забезпечило б повну ідентифікацію власників сайтів, які займаються підприємницькою діяльністю, та значно зменшило б кількість шахрайських сайтів [23].

Окремо хочемо торкнутись питання щодо розподілу відповідальності та удосконалення законодавчого врегулювання діяльності правоохоронних органів у сфері кіберпростору, зокрема, СБУ та НП України. Адже фахівці Служби безпеки України регулярно нейтралізують сотні кібератак на інформаційні ресурси державних органів влади, протидіють поширенню шкідливих програм у банківському секторі, витоку інформації з обмеженим доступом. При цьому особливу увагу слід приділити питанням розслідування кіберзлочинів на об'єктах критичної інфраструктури. Такі об'єкти знаходяться під постійною увагою хакерів та спецслужб іноземних держав. Безумовно, необхідно в найкоротші строки створити реєстр як об'єктів критичної інфраструктури, так і реєстр об'єктів критичної інформаційної інфраструктури як необхідного елементу забезпечення відповідного рівня кіберзахисту.

Наприклад, у липні 2020 року за повідомленням прес-служби концерну "Укроборонпром" було здійснено чергову кібератаку на інформаційно-телекомунікаційну систему концерну. На корпоративні електронні поштові скриньки працівників концерну розсилалися електронні повідомлення, інфіковані вірусом типу "троян". Атака відбувалася з електронної адреси, розміщеної на серверах одного американського телекомунікаційного провайдера.

Для забезпечення кібербезпеки національного сегменту Інтернет задіяні і інші суб'єкти національної системи кібербезпеки.

У липні 2020 року фахівці Національного координаційного центру кібербезпеки при РНБО України виявили в DarkNet перелік з майже 3 млн. сайтів, які використовують сервіс Cloudflare для захисту від DDoS і низки інших кібератак. Опублікований перелік містить реальні IP-адреси сайтів українського сегменту Інтернет, що створює загрози спрямованих на них атак. Серед 6500 записів з доменом "ua" є адреси 45 записів з доменом "gov.ua" та ресурси, що належать об'єктам критичної інфраструктури.

Слід зазначити, що під час розслідування кібератак необхідно тісно співпрацювати з провайдерами комунікаційних послуг. Вони першими можуть виявляти такі атаки та зберігати шкідливий мережевий трафік для подальшого його аналізу. Водночас існує серйозна проблема отримання інформації від приватного сектору, оскільки на законодавчому рівні не встановлені вимоги щодо обов'язкового зберігання провайдерами інформації, наявність "сірої" адресації NAT, що призводить до унеможливлення отримання необхідної інформації або взагалі до її відсутності. У більшості випадків інформація надається виключно на підставі рішення суду, що призводить до отримання неактуальної або застарілої інформації. Також, при відсутності в Україні судової практики винесення судами ухвал за пришвидшеною процедурою про вжиття запобіжних заходів, правовласник, або особа, чиї права були порушені неправомірними діями власника веб-сайту, є фактично позбавленим можливості ефективного правового захисту.

Позитивний ефект роботи мають норми статті 52-1 Закону України "Про авторські та суміжні права" щодо залучення провайдера комунікаційних послуг до врегулювання відносин з власником веб-сайту у зацікавленої сторони, в разі, якщо власник веб-сайту всупереч законодавству не розголошує свої дані на створеній ним сторінці. Зазначений механізм повною мірою відповідає практикам взаємодії між провайдерами телекомунікаційних послуг та зацікавленими суб'єктами господарювання або державними органами країн в питаннях захисту авторських прав, наявній в судовій системі ЄС. Доцільним є подальше законодавче удосконалення ролі провайдера комунікаційних послуг, підвищення його відповідальності перед зацікавленими сторонами в разі якщо веб-сайт, розміщений на ресурсі, що ним обслуговується, порушує права третіх осіб.

Для протидії кібератакам важливого значення набуває обізнаність користувачів інформаційних систем щодо правил кібергігієни. Адже більшість кібератак розпочинаються за допомогою простого електронного листа. Більше 90 відсотків успішних атак та порушення даних відбуваються шляхом використання фішингових електронних листів, створених для того, щоб спровокувати своїх одержувачів натиснути посилання, відкрити документ або кому-небудь пересилати певну інформацію. За словами Кеті Х'юз – директора з інформаційної безпеки Northwell Health (найбільший приватний роботодавець США – 68000 осіб), люди – найслабша ланка в ланцюжку безпеки [24]. Наприклад, проведене у червні 2020 року масштабне дослідження

кіпрського студента щодо використання паролів показало, що кожен 142-ий пароль із мільярда облікових записів був “123456” [25], який легко визначається зловмисниками.

Тому важливе значення для посилення кібербезпеки, а отже й запобігання кіберзлочинності має впровадження у навчальний процес як цивільних, так і навчальних закладів правоохоронних органів спеціалізованих предметів із захисту інформації та систематичне проведення тренінгів і навчань з кібербезпеки.

Цікавим у цьому аспекті є досвід Національної академії внутрішніх справ, де у 2019 – 2020 навчальному році запроваджено вивчення особливостей пошуку й аналізу криміналістичної інформації під час здійснення досудового розслідування у відкритій (“поверхневій”, Surface Web) і прихованій (“темній”, Dark Web) частинах мережі Інтернет, застосування програмних засобів Microsoft Office, Power BI та IBM i2 Analyst’s Notebook як сучасного інструментарію для обробки й аналізу: телефонного трафіку; даних із відповідних реєстрів, баз даних та інформаційно-довідкових систем; даних про банківські транзакції та рух матеріальних цінностей; даних, отриманих з електронних платіжних систем і систем он-лайн банкінгу, тощо.

Корисною також є започаткована Національним банком України у липні 2020 року Всеукраїнська інформаційна кампанія з протидії платіжному шахрайству, у рамках якої громадян навчатимуть основним правилам безпеки безготівкових та он-лайн-платежів. Адже минулого року в Україні зафіксували майже 72 тисячі випадків незаконних дій із платіжними картами. 58 % із них сталися в Інтернеті. Найпопулярніший метод шахрайства – соціальна інженерія, коли люди самі переказують гроші аферистам або розкривають їм дані. У 2020 році через карантинні заходи в шахраїв з’явилися й нові сценарії – під виглядом державних органів обіцяють грошову допомогу через карантин і у такий спосіб виманюють інформацію з платіжних карток.

Оскільки для поширення атак кіберзлочинці використовують засоби автоматизації і алгоритми машинного навчання, правоохоронцям необхідно використовувати ті ж інструменти для протидії сучасним і витонченим методам атак. Зокрема небезпечними є кібератаки, які вчиняються через пристрої Інтернету речей, які в переважній більшості випадків ніяк не захищені. Доступ до цих пристроїв дозволяє кіберзлочинцям стежити за приватним життям, планувати протиправну діяльність на фізичному об’єкті, отримувати доступ до мережевих систем для запуску DDoS атак або атак з метою вимагання викупу. Корисним у цьому сенсі є нещодавно підписаний Меморандум між Департаментом кіберполіції НП України та Національним технічним університетом України “Київський політехнічний інститут імені Ігоря Сікорського”, відповідно до якого фахівці технічного вузу будуть ділитися з правоохоронцями технічними особливостями роботи комп’ютерних систем.

За дослідженнями кримінологів кіберзлочини вчиняються широким спектром дійових осіб з різноманітними мотиваціями. Загрози кіберзлочинності можуть надходити від організованих злочинних угруповань, терористів, суб’єктів, що безпосередньо працюють або наймаються суб’єктами ворожих держав, одиноких хакерів та інших осіб, які можуть бути мотивовані фінансовими, ідеологічними, політичними чи іншими причинами.

Особливо слід зазначити, що, незважаючи на відмінності в профілях злочинців та їх мотивації, більшість діянь, пов’язаних із кіберзлочинністю, за оцінками експертів, мають транснаціональний характер. Транскордонний характер Інтернету дає змогу легко створювати абсолютно нові категорії кіберзлочинів. Один кіберінцидент може вразити значну кількість об’єктів у багатьох країнах, незалежно від місцезнаходження кіберзлочинців, а це означає, що до розслідування кіберзлочинів та притягнення до

відповідальності лише деяких злочинців необхідно залучати представників різноманітних правоохоронних органів, прокурорів та суддів у різних юрисдикціях, що значно ускладнює розслідування кіберзлочинів, включаючи вирішення питання щодо екстериторіальної юрисдикції та ефективності механізмів міжнародного співробітництва у транснаціональному розслідуванні. І хоча для комунікації та обміну оперативною інформацією з правоохоронними органами іноземних держав і міжнародними компаніями Департамент кіберполіції Національної поліції України активно використовує канали захищеного зв'язку NCP (National Contact Point) та Siena (Secure Information Exchange Network Application), проте більшість країн та компаній відмовляють у наданні інформації на відповідний запит, регламентуючи це необхідністю направлення на правоохоронні органи іноземних держав MLAT (доручення про міжнародну правову допомогу). А це, у свою чергу, призводить до незначної кількості засуджених за вчинення кіберзлочинів (не тільки в Україні).

Наприклад, в Англії та Уельсі за законом про комп'ютерне зловживання у 2017 році було винесено менше 50-ти вироків, незважаючи на повідомлення Бюро національної статистики Великобританії про те, що з квітня 2017 по березень 2018 року було вчинено понад 1,2 млн. правопорушень [26].

Згідно із судовою статистикою в Україні у 2019 році за вчинення злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку розглянуто 101 провадження (кількість засуджених осіб – 66; осіб, щодо яких кримінальне провадження закрито, – 27; примусові заходи виховного характеру застосовано до 1 особи).

Відсутність правоохоронного потенціалу та спроможності розслідувати кіберзлочини дозволяє кіберзлочинцям бути досить впевненими щодо низьких шансів, що вони коли-небудь будуть виявлені, заарештовані та будуть нести покарання.

У зв'язку з постійним збільшенням кількості кібератак, вчиненням інших кіберзлочинів постає питання посилення спроможностей як безпосередньо правоохоронних підрозділів, так й інших державних органів, які протидіють кіберзлочинності.

Підтримка потенціалу для зміцнення знань, умінь та навичок суб'єктів кримінального правосуддя для подолання загрози кіберзлочинності та посилення верховенства закону й поваги до прав людини та громадянських свобод – це підхід, який користується широкою міжнародною підтримкою, зокрема ООН.

У травні 2019 року Комісія ООН з питань запобігання злочинності та кримінального правосуддя рекомендувала Генеральній Асамблеї прийняти проект резолюції, яка закликає держави-члени забезпечувати сталу розбудову потенціалу в галузі кіберзлочинності по всьому світу. Хоча певні країни вкладають значні кошти в нарощування потенціалу для власних систем кримінального правосуддя, глобальне посилення спроможностей щодо кіберзлочинності часто передбачає певну форму взаємовідносин донор – реципієнт, тобто такі відносини, коли країна, яка має певні знання, навички, технології тощо щодо протидії кіберзлочинності, допомагає або підтримує в розвитку інші країни.

Такий підхід використовує і Рада Європи, яка оцінила переваги розбудови потенціалу як одного з підходів до боротьби з кіберзлочинністю та класифікувала типи програм для нарощування спроможностей, які впроваджуються у всьому світі. Заходи такого програмування розбудови потенціалу можуть включати підтримку розробки стратегій боротьби з кіберзлочинністю; створення нової та/або оновлення законодавчої бази із гарантіями верховенства права; створення систем звітності про кіберзлочинність; створення або зміцнення спеціалізованих підрозділів з питань кіберзлочинності поліції чи прокуратури; розширення криміналістичних можливостей; проведення

правоохоронних, прокурорських та судових тренінгів; створення механізмів державно-приватного співробітництва для забезпечення успішних розслідувань кіберзлочинності.

У рамках проекту "Розбудова спроможностей кіберполіції" представники Координації проектів ОБСЄ в Україні передали підрозділам кіберполіції Національної поліції України 194 одиниці спеціалізованої техніки [27].

Разом з тим потребує свого подальшого розвитку спеціалізація слідчих та прокурорів, які задіяні у розслідуванні кіберзлочинів. Зокрема у структурі Головного слідчого управління Національної поліції України у 2017 році був створений відділ, який спеціалізуються на розслідуванні кіберзлочинів. Водночас після збільшення кількості оперативних працівників кіберполіції збільшилася кількість виявлених кіберзлочинів та навантаження на слідчих, кількість яких не змінилася. Збільшення кількості слідчих, які спеціалізуються на розслідуванні кіберзлочинів, надасть можливість належним чином проводити досудове розслідування.

Також проблемним питанням у проведенні досудового розслідування є існуюча процедура звернення до місцевих судів із клопотаннями про надання тимчасових доступів, обшуків, арештів тощо. Відсутність повноцінного електронного документообігу і зокрема не визначеність його використання під час проведення досудових розслідувань, існуюча процедура звернення до місцевих судів з клопотаннями про надання тимчасових доступів, обшуків, арештів тощо яка передбачає здійснення цих дій лише з використанням документів в паперовій формі створює перешкоди ефективному здійсненню відповідних процесуальних дій, значно відстає від сучасних практик електронного документообігу країн Євросоюзу.

Зокрема, для підготовки додатків до клопотань витрачається багато часу, паперу, витратних матеріалів, оскільки відсутній механізм звернення до суду з такими клопотаннями, додатками, у яких є відскановані матеріали (в електронному варіанті). Крім того, процесуальні документи, наприклад, ухвали слідчого судді, передаються в правоохоронні підрозділи тривалий час (за наявності засобів комунікації та Інтернет-зв'язку). Відсутність електронного документообігу між органом досудового розслідування та судами значно збільшує строк досудового розслідування. Тому вкрай необхідно Міністерству цифрової трансформації долучитися до впровадження в Україні електронного судочинства, зокрема організувати оперативну передачу електронних доказів та процесуальних документів мережами передачі даних.

Серед ***основних напрямів підвищення рівня спроможності правоохоронних органів*** у сфері боротьби з кіберзлочинністю слід виокремити такі:

нарощування спроможності спеціалізованих підрозділів правоохоронних органів щодо аналізу електронних доказів з метою забезпечення прийнятності їх в суді;

розробка нормативно-правової бази у сфері кіберзлочинності та імплементація міжнародних конвенцій і договорів, включаючи необхідні зміни до кримінального та кримінально-процесуального законодавства, узгодження їх з чинними глобальними конвенціями;

розробка методик розслідування кіберзлочинів, забезпечення належного використання нових технологій та обмін інформацією з приватним сектором;

поширення позитивного досвіду у сфері протидії кіберзлочинності для працівників правоохоронних органів та належне укомплектування відповідних підрозділів, які протидіють кіберзлочинності, кваліфікованими спеціалістами;

забезпечення обміну інформацією між правоохоронними органами та іншими державними органами, які протидіють кіберзлочинності на всіх рівнях, включаючи органи прокуратури та спецслужби;

налагодження механізмів обміну інформацією та співпраці між правоохоронними органами, приватним сектором;

удосконалення процесу звітування правоохоронних органів, задіяних у боротьбі з кіберзлочинністю, перед громадськістю;

повна імплементація положень Конвенції про кіберзлочинність, зокрема статей, які стосуються збереження електронних даних.

Як уже зазначалося вище, ефективне розслідування кіберзлочинів потребує чіткого законодавчого розмежування підслідності кіберзлочинів у контексті повноважень Національної поліції України та Служби безпеки України.

Висновки.

В Україні, як і у всьому світі кіберзлочинність продовжує поширюватися, завдаючи значних економічних збитків. Водночас існують певні проблеми щодо виявлення кіберзлочинів та притягнення винних осіб до кримінальної відповідальності.

Очевидно, що одним із найважливіших шляхів протидії кіберзлочинності є стимулювання глобальної співпраці у розслідуванні кіберзлочинів як між правоохоронними органами різних країн, так і приватним сектором. Транснаціональний характер загроз кіберзлочинності потребує посилених та розширених зусиль, спрямованих на подолання перешкод, які гальмують таку співпрацю.

Іншою необхідною умовою успішної боротьби з кіберзлочинністю є вдосконалення механізмів обробки електронних доказів для проведення експертизи та передачі їх до суду.

Враховуючи зазначене, для посилення спроможностей правоохоронних та інших державних органів у сфері боротьби з кіберзлочинністю пропонується:

1. Забезпечити імплементацію положень статей 16 і 17 Конвенції про кіберзлочинність щодо термінового збереження комп'ютерних даних та часткового розкриття їх трафіку.

2. Сприяти посиленню ідентифікації суб'єктів кіберпростору та зокрема суб'єктів електронної комерції шляхом внесення змін до Закону України "Про електронну комерцію", Податкового кодексу України, Кодексу України про адміністративні правопорушення, Кодексу адміністративного судочинства України щодо відповідальності за ненадання інформації про продавця товарів на веб-сайтах, які здійснюють електронну комерцію.

3. Посилити кримінальну відповідальність за вчинення кіберзлочинів на об'єктах критичної інфраструктури та критичної інформаційної інфраструктури.

4. Внести зміни до Кримінального процесуального кодексу України щодо розмежування повноважень розслідування кіберзлочинів Національної поліції України та Служби безпеки України.

5. Внести до Кримінального процесуального кодексу України зміни у частині визначення поняття "електронні докази", а також нормативно визначити положення щодо особливостей їх отримання, зберігання та подання до суду, засвідчення факту їх існування органами нотаріату.

6. Посилити міжнародну співпрацю правоохоронних органів шляхом участі у спільних слідчих групах та обміну, у тому числі, оперативною інформацією каналами Європолу та Інтерполу.

7. Сприяти постійно діючому процесу навчання та перепідготовки слідчих Національної поліції України методикам розслідування кіберзлочинів, у тому числі на основі аналізу інформації з Інтернет.

8. У зв'язку з тим, що Стратегія кібербезпеки України, затверджена Указом Президента України від 15.03.16 р. № 96/2016, спрямована на реалізацію заходів кібербезпеки до 2020 року, а План заходів з її реалізації виконаний не повністю, необхідно розробити та затвердити нову Стратегію кібербезпеки на 2020 – 2025 роки.

Використана література

1. United Nations Manual on the Prevention and Control of Computer-related Crime, International Review of Criminal Policy, Series M, Nos. 43-44 (United Nations publication, No. E.94.IV.5). URL: http://216.55.97.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_UN_ Guide.pdf

2. Скільки людей у світі користуються Інтернетом – ООН. URL: https://www.the-village.com.ua/village/city/city-news/290933

3. Держстат порахував, скільки закарпатців користуються Інтернетом і телебаченням. URL: https://zakarpattya.net.ua/News/199742

4. Cisco Annual Internet Report (2018–2023) White Paper URL: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

5. Cybercrime Damages $6 Trillion By. 2021. URL: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016.

6. Ахтирська Н.М. Актуальні проблеми розслідування кіберзлочинів: навч. посіб. Київ: ВПЦ "Київський університет", 2018. 229 с

7. Організаційно-правові та тактичні основи протидії злочинності у сфері високих інформаційних технологій: навч. посіб. / В.М. Бутузов та ін. – (Рада нац. безпеки і оборони України, Міжвід. наук.-дослід. центр з проблем боротьби з організованою злочинністю, Служба безпеки України, Нац. акад. СБУ). Київ, 2011. 404 с.

8. Голубєв В.О. Розслідування комп'ютерних злочинів: монографія. Запоріжжя: Гуманітарний ун-т "ЗІДМУ", 2003. 296 с.

9. Klymenko, Olga A.; Gutsaliuk, Mykhailo V.; Savchenko, Andrii V. Combater o cibercrime como pré-requisito para o desenvolvimento da sociedade digita. JANUS.NET e-journal of International Relations, Vol. 11, N.º 1, Maio-Outubro 2020. Consultado [em linha] em data da última consulta, https://doi.org/10.26619/1647-7251.11.1.2

10. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій: наук.-практ. посіб. / Б.В. Романюк, В.Д. Гавловський, М.В. Гуцалюк, В.М. Бутузов. Київ: Вид. ПАЛИВОДА А.В., 2004. 144 с.

11. Демедюк С.В., Марков В.В. Кіберполіція України. *Наше право*. 2015. № 6. С. 87-93. URL: http:// nbuv.gov.ua/UJRN/Nashp_ 2015_6_15

12. Концепція розвитку цифрової економіки та суспільства України на 2018 – 2020 роки: Розпорядження Кабінету Міністрів України від 17.01.18 р. № 67-р. URL: https://www.kmu.gov.ua/npas/pro-shvalennya-koncepciyi-rozvitku-cifrovoyi-ekonomiki-ta-suspilstva-ukrayini-na-20182020-roki-ta-zatverdzhennya-planu-zahodiv-shodo-yiyi-realizaciyi

13. Про деякі заходи із забезпечення надання якісних публічних послуг: Указ Президента України № 647/2019. URL: https://www.president.gov.ua/documents/6472019-29441

14. В Україні запустили мобільний додаток "Дія". URL: https://www.unian.ua/science/10862255-v-ukrajini-zapustili-mobilniy-dodatok-diya.html

15. Збитки від атаки вірусу Petya.A у світі сягають 8 мільярдів доларів – експерт. URL: https://www.unian.ua/science/2003241

16. Витік персональних даних українців: Що сталося і хто за цим стоїть. URL: https://ua.112.ua/golovni-novyni/vytik-personalnykh-danykh-ukraintsiv-shcho-stalosia-i-khto-za-tsym-stoit-535795.html

17. СБУ затримали відомого хакера з Івано-Франківська. URL: https://frankivsk.znaj.ua/311983-haker-z-frankivska-postaviv-na-vuha-ves-svit-prodavshi-naybilshu-bazu-danih-v-istoriji-bond-nervovo-kurit

18. СБУ викрила протиправне втручання в електронну систему Державного земельного кадастру для зміни інформації. URL: https://ssu.gov.ua/ua/news/1/category/21/view/7641#.sq7YnPH7.dpbs

19. Кіберполіція викрила шахраїв, які ошукали близько 200 громадян. URL: https://stopcor.org/kiberpolicziya-vykryla-shahrayiv-yaki-oshukaly-blyzko-200-gromadyan

20. Google Registers a 350 % Increase in Phishing Websites Amid Quarantine. URL: https://atlasvpn.com/blog/google-registers-a-350-increase-in-phishing-websites-amid-quarantine

21. Domain name registry suspends 600 suspicious coronavirus websites. URL: https://www.zdnet.com/article/domain-name-registrar-suspends-600-suspicious-coronavirus-websites/

22. Кіберполіція викрила осіб, які під виглядом продажу товарів та послуг "заробили" майже 1,5 мільйони гривень. URL: https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-osib-yaki-pid-vyglyadom-prodazhu-tovariv-ta-poslug-zarobyly-majzhe--miljony-gryven-7838

23. Гуцалюк М.В. Впровадження ID-web як необхідна умова безпеки в Інтернет. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2008. № 18. С. 265-269.

24. 2019 Official Annual Cybercrime Report. URL: https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

25. One out of every 142 passwords is '123456'. URL: https://www.zdnet.com/article/one-out-of-every-142-passwords-is-123456/?ftag=CAD-03-10abf6j

26. Crime in England and Wales: year ending March 2018, United Kingdom Office for National Statistics (19 July 2018). URL: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2018

27. Кіберполіція отримала 194 одиниці спеціального обладнання для протидії кіберзагрозам. URL: http://mvs.gov.ua/ua/news/9208_Kiberpoliciya_otrimala_194_odinic_specialnogo_obladnannya_dlya_protidii_kiberzagrozam_FOTO_VIDEO.htm

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~