УДК 343.9.024:004.056

ГУЦАЛЮК М.В., *кандидат юридичних наук, доцент,* головний науковий співробітник Міжвідомчого центру з проблем боротьби з організованою злочинністю при РНБО України.

ЗАГРОЗЛИВІ ТЕНДЕНЦІЇ ОРГАНІЗОВАНОЇ КІБЕРЗЛОЧИННОСТІ

Анотація. *У статті досліджуються сучасні тенденції кіберзлочинності, у тому числі її організовані форми, надаються пропозиції щодо посилення протидії цьому явищу.*

Ключові слова: *кіберзлочинність, кібератака, Даркнет, електронні докази.*

Summary. *The article deals with current trends in cyber crime, including its organized forms, and proposes to strengthen the counteraction to this phenomenon.*

Keywords: *cyber crime, cyber attack, Darknet, electronic evidence.*

Аннотация: *В статье исследуются современные тенденции киберпреступности, в том числе ее организованные формы, представлены предложения по усилению противодействия этому явлению.*

Ключевые слова: *киберпреступность, кибератака, Даркнет, электронные доказательства.*

Постановка проблеми. Сучасний глобальний світ характеризується широким використанням переваг кіберпростору для отримання інформації, віддаленої роботи, взаємодії з державними органами, Інтернет-торгівлі тощо. Водночас інформаційні технології стали потужним інструментом для злочинців, який вони можуть використовувати для протиправної діяльності, у тому числі на транснаціональному рівні, для фінансового шахрайства, викрадення інформації, незаконного поширення наркотичних засобів тощо. Протиправна діяльність у кіберпросторі створює тіньову економіку, яка за доходами порівняна з економікою деяких держав.

Інтернет забезпечує злочинцям доступ до потенційних жертв у будь-якому куточку світу. Кіберзлочинці використовують властивість електронних даних миттєво передавати інформацію у кіберпросторі на значні відстані. Також Інтернет використовується для обміну знаннями та таємного спілкування, продажу викрадених даних, товарів та послуг, відмивання доходів, одержаних злочинним шляхом, а також обміну тактиками та інструментами кіберзлочинності.

Кіберзлочинність постійно та активно розвивається за складністю та організаційною спроможністю, а за багатьма аспектами вона сформована подібно до великого підприємства з ієрархічною структурою, в якій кожен має чітко визначену роль та відповідальність. Організатори таких структур контролюють проведення операцій, визначають стратегію та бізнес-модель, інспектують виконання плану. Основою злочинного бізнесу є технології, групи фахівців, які здатні розгорнути складні зловмисні програми, організувати приватні ботнети та створити фіктивні антивірусні програми, а також набори інструментів для несанкціонованого доступу до комп'ютерних систем. Для проведення масштабних кібероперацій спеціальні підрозділи розробляють програми набору персоналу, для пошуку виконавців з конкретними технологічними профілями під конкретну кібератаку.

У зв'язку із значним негативним впливом кіберзлочинності на цифрове суспільство це явище в останні роки досліджувалось як окремими науковцями, так і установами та організаціями через призму кримінології, криміналістики, психології, соціології, а також

інших наукових дисциплін. Подальше зростання кількості кіберзлочинів, збитків цифрової економіки від них та суттєве ускладнення кібератак спонукає проведення подальших досліджень щодо протидії кіберзлочинності та в особливості її організованим формам.

Результати аналізу наукових публікацій. У зв'язку із значним негативним впливом кіберзлочинності на цифрове суспільство це явище досліджувалось багатьма закордонними Maras Marie-Helen, Eoghan Casey, Thomas J. Holt, Adam M. Bossler, Kathryn C. Seigfried-Spellar та вітчизняними вченими Н. Ахтирська, П. Біленчук, В. Бутузов, В. Гавловський, О. Кравцова, А. Марущак, К. Тітуніна, В. Шеломенцев, В. Хахановський, О. Юрченко та інші.

В той же час сьогодні ще не достатньо досліджені особливості діяльності організованих злочинних угруповань (далі – ОЗУ) у кіберпросторі та методи і способи виявлення та розслідування їх діянь та боротьби з ними.

Метою статті є дослідження сучасного стану організованої кіберзлочинності та визначення основних тенденцій її розвитку.

Виклад основного матеріалу. Починаючи з 2000-х років у зв'язку з широким поширенням Інтернету по всьому світу проблема боротьби з кіберзлочинністю набула міжнародного характеру. Ще у 2001 р. Генеральна асамблея ООН резолюцією 55/63 від 22 січня 2001 року [1] на виконання Декларації тисячоліття Організації Об'єднаних Націй щодо забезпечення усіх благами нових інформаційно-телекомунікаційних технологій рекомендувала вжити низку наступних заходів:

– держави повинні забезпечити, щоб їх законодавство і практика не залишали можливості тим, хто зловживає інформаційними технологіями, ховатися де б то не було;

– співробітництво правоохоронних органів у розслідуванні випадків транскордонного злочинного використання інформаційних технологій і судове переслідування в зв'язку з цим має координуватися усіма відповідними державами;

– держави повинні обмінюватися інформацією про проблеми, з якими вони стикаються в боротьбі зі злочинним використанням інформаційних технологій;

– режими взаємної допомоги повинні забезпечувати своєчасне розслідування випадків злочинного використання інформаційних технологій і своєчасний збір доказів і обмін ними в подібних випадках;

У 2011 році в ООН була створена Міждержавна група експертів з вивчення кіберзлочинності, зусиллями якої у 2013 році було проведено "Всебічне дослідження проблеми кіберзлочинності". У цьому документі проаналізовані такі аспекти як законодавство у даній сфері, діяльність правоохоронних органів, міжнародне співробітництво тощо. В ньому, зокрема, зазначається, що 80 відсотків кіберзлочинів вчиняється в організованій формі [2].

Робота міждержавної групи експертів продовжується і сьогодні. Так у доповіді за наслідками наради даної групи 27-29 березня 2019 року у Відні були розглянуті питання удосконалення законодавства, у тому числі міжнародного, проблеми діяльності правоохоронних органів, використання електронних доказів. Було зазначено, що, зважаючи на транснаціональний характер кіберзлочинності і той факт, що значна більшість глобальних кіберзлочинів вчиняються організованими групами, державам-членам слід більш широко застосовувати Конвенцію Організації Об'єднаних Націй проти транснаціональної організованої злочинності для сприяння обміну інформацією та доказами в ході кримінальних розслідувань, що стосуються кіберзлочинності [3].

Термін “кіберзлочин” визначено Законом України “Про основні засади забезпечення кібербезпеки України”. Види кіберзлочинів визначені у Конвенції про кіберзлочинність 2001 року, яка була ратифікована Законом України від 07.09.05 р. № 2824-IV. Кіберзлочини можна поділити на власне кіберзлочини, метою вчинення яких є порушення конфіденційності, доступності або цілісності інформації в комп’ютерній системі (несанкціонований доступ до комп’ютерних систем, атаки на відмову в обслуговуванні, незаконне перехоплення комп’ютерних даних тощо), та кіберзалежні злочини, які вчиняються з використанням інформаційно-комунікаційних технологій, наприклад шахрайство. На сьогодні в чинному українському законодавстві поки що не визначено чіткого переліку статей Кримінального кодексу України, які слід відносити до кіберзлочинів.

На практиці злочинці можуть вчиняти декілька видів кіберзлочинів послідовно або навіть одночасно. Наприклад, у 2017 році кіберзлочинці вчинили несанкціонований доступ до системи відомого литовського пластичного хірурга та отримали конфіденційну інформацію про пацієнтів із різних куточків світу, про процедури, які вони проводили, 25000 фотографій оголених пацієнтів та медичні дані. Після цього кіберзлочинці погрожували кожному пацієнтові оприлюднити цю інформацію у разі, якщо не буде сплачено викуп. Вартість викупу змінювалася залежно від кількості та якості викраденої інформації про пацієнта [4].

Зазначимо, що більшість досліджень вказують на зростання як кількості кіберзлочинів, так і збитків від них. Наприклад, лише у Лондоні за період із квітня по вересень 2018 року було зареєстровано 13357 кіберзлочинів, від яких потерпілі втратили 34,6 мільйона фунтів стерлінгів. Кількість інцидентів продовжує зростати. За словами начальника поліції міста Лондона Карен Бакстер, “кіберзлочинність – це зростаюча тенденція, загальні збитки від якої щорічно збільшуються на 24 відсотки”. Уряд Великобританії серйозно сприймає цей ризик, визначаючи кіберзлочинність як загрозу національній безпеці першого рівня та вкладаючи майже 2 мільярди фунтів у Національну стратегію кібербезпеки, розроблену для її протидії [5].

В Україні за останні п’ять років кількість інформаційних злочинів зросла щонайменше у 2,5 рази. Про це повідомляє прес-служба Opendatabot. Збільшення кількості всіх кіберзлочинів відбулося у 2017 році, що значною мірою пов’язано з вірусом Petya. Відтоді кількість інформаційних злочинів не зменшується [6].

Збитки від кіберзлочинів можуть коливатися від кількох доларів до кількох мільярдів доларів. Наприклад, вірус Petya спричинив збитків по всьому світі на 8 млрд доларів. Тільки вітчизняна Укрпошта зазнала збитків у 100 млн гривень [7]. Кількість викраденої або модифікованої інформації також може значно відрізнятися в різних випадках. Наприклад, У січні 2019 року на хмарному сервісі MEGA була виявлена база даних користувачів із майже 773-ма мільйонами адрес електронної пошти і 22-ма мільйонами унікальних паролів. Це був найбільший витік вкрадених даних з усіх відомих обсягом 87 гігабайт [8].

Особливе занепокоєння викликає активний розвиток упродовж останніх років такого явища, як “кіберзлочин-послуга” – он-лайн-ринку для обміну викраденими даними, хакерськими інструментами й уразливостями інформаційних систем, а також іншими кримінальними послугами, такими як оренда бот-мереж і спам-серверів. Також на цьому “ринку” надають послуги, які полегшують вчинення злочинів та кіберзлочинів, такі як дані та документи, що посвідчують особу (наприклад, фінансові та медичні дані, паспорти тощо); зловмисне програмне забезпечення (тобто, виготовлене на замовлення або вже відоме зловмисне програмне забезпечення – наприклад, Zeus (“Зевс”),

банківський троян, розроблений для прихованого захоплення банківських даних користувачів; кібератак відмови в обслуговуванні (DDoS) та ботнет-послуг; інструменти фішингу; хакерські підручники; а також інформацію про вразливості різноманітних інформаційних ресурсів та інструкції, як ними скористатися).

Вартість таких послуг досить помірна. Наприклад, у Звіті Underground Hacker Marketplace зазначено, що дані кредитної картки можна придбати за 30 доларів США, набори інструментів для віддаленого доступу до комп'ютера всього за 5 доларів США та розподілені атаки типу "відмова в обслуговуванні" на певних сайтах всього за 5 доларів США на годину [9].

А у дослідженні "Cybercrime and the Underground Market [Updated 2019]" приведено наступні приклади продажу шкідливого програмного забезпечення [10]:

"Продам вихідний код ZeuS 2.0.8.9. Приватний продаж вихідного коду. Ціна: 400–500 доларів США; можливі торги (можлива заміна)".

"Налаштування ZeuS: 100 доларів США, підтримка ботнету: 200 доларів США на місяць, консультація: 30 доларів США".

Модель продажу "зловмисне програмне забезпечення як послуга" є дуже небезпечною, оскільки надає можливість для звичайних злочинців без особливих знань здійснити серйозні кібератаки на банківські системи. У деяких випадках, щоб захистити свою анонімність, виробники зловмисного програмного забезпечення розгортають продаж своїх виробів у Darknet.

Наприклад, розробник "Butterfly Bot" рекламував це шкідливе програмне забезпечення в Інтернеті як таке, що здатне взяти під контроль комп'ютери Windows та Linux. Він також продавав плагіни (plug-in – додаток, що динамічно підключається до основної програми), які модифікували функції зловмисного програмного забезпечення. Різноманітні кримінальні мережі поширили цей Butterfly Bot, унаслідок чого цією шкідливою програмою були заражені ***12,7 мільйона*** комп'ютерів у всьому світі. Улітку 2019 року розробник "Butterfly Bot" був заарештований німецькою поліцією [11].

У січні 2019 року міжнародна спільна слідча група, до складу якої входили співробітники Генеральної прокуратури України, Національної поліції України, а також правоохоронців з Бельгії, за сприяння Європолу та ФБР США провели обшуки у дев'яти локаціях в Україні.

Четверо українців віком від 27 до 37 років створили та підтримували діяльність відомого у Darknet ресурсу "xDedic", що давав змогу користувачам продавати й купувати доступ до зламаних серверів, викрадення банківських коштів, конфіденційної інформації, блокування інформації вірусами-вимагачами тощо

Щорічний дохід кожного із організаторів групи налічував більш як 1.2 млн доларів. Отримані кошти фігуранти зберігали в електронних гаманцях криптовалютних електронних систем та періодично виводили їх у готівку через неофіційні обмінні пункти. Одночасно із обшуками були заблоковані доменні імена, необхідні для функціонування xDedic [12].

Слід зазначити, що широкий спектр постачальників послуг в Інтернеті активно експлуатується терористичними групами. Вони використовують найновіші технології для он-лайн спілкування. Тому при вдалому плануванні та підтримці прихильників терористів кібератаки, організовані терористами, можуть поширюватися швидше, ніж провайдери та правоохоронні органи зможуть на них відреагувати.

Багато ОЗУ використовують Інтернет-технології для зв'язку правопорушників щодо скоєння традиційних злочинів, після чого злочинна організація припиняє діяльність, щоб знову утворити нову. Крім того, ОЗУ можуть використовувати мережеві

технології для створення більш “стійких” організаційних форм, для захисту злочинців, що працюють під їх “дахом”, від інших злочинців у цій сфері, а також правоохоронних органів. Між цими двома крайнощами спектру існують також “гібридні” форми. Часто члени таких злочинних організацій знають один про одного лише через нікнейми (вигадані імена), що значно ускладнює розслідування діяльності таких груп.

Наприклад, злочинці використовують інформаційно-комунікаційні технології (далі – ІКТ) для удосконалення різних форм традиційної оф-лайн-організованої злочинності, таких як контрабанда мігрантів та торгівля людьми, наркотиками, вогнепальною зброєю та цигарками.

Наприклад, співробітниками БКОЗ СБ України спільно з поліцією Ізраїлю припинена діяльність найбільшої за останні десятиліття міжнародної мережі Інтернет-торгівлі наркотиками.

Правоохоронці встановили, що у 2017 році громадянин Ізраїля в одному із соціальних месенджерів створив Інтернет-канал для збуту оптових партій наркотичних засобів та психотропних речовин. За кілька років нелегальний бізнес розширився, і такі “торговельні майданчики” почали функціонувати в інших соціальних мережах. За даними ізраїльської поліції, географія злочинної діяльності наркоторгівців розповсюджувалася на країни Південної та Північної Америки, Європейського Союзу, Близького Сходу, Азії та Африки. У синдикат входило понад тринадцять тисяч осіб, у тому числі контрабандисти, дилери, адміністратори груп у соцмережах.

У березні 2019 року на підставі клопотання про міжнародну допомогу українські правоохоронці затримали главу наркокартеля в Києві, куди він прибув для налагодження “бізнес-зв’язків” із представниками місцевих кримінальних кіл. Одночасно в Ізраїлі було затримано 42 особи [13].

При вивченні організованої кіберзлочинності слід враховувати цільову групу потерпілих. Деякі злочинні групи навмисно атакують окремих користувачів, щоб вчинити шахрайство чи шантаж. Інші групи зорієнтовані на середній бізнес чи урядові організації і вчиняють шахрайство більш масштабного обсягу. Нарешті, як правило, спеціальні державні суб’єкти свідомо націлюють свою діяльність на інфраструктуру інших держав, щоб створити недовіру до них чи вчинити масштабні кіберзлочини. Кількість учасників таких угруповань може коливатися від кількох злочинців до кількох тисяч, які вчиняють скоординовані дії.

Наприклад, Shadowcrew – “міжнародна організація”, нараховувала близько 4000 членів та сприяла широкому спектру злочинних дій, включаючи, серед іншого, електронні крадіжки особистої ідентифікаційної інформації, шахрайство з кредитними картками, а також виробництво та продаж фальшивих ідентифікаційних документів [14].

Незаконні товари та послуги в мережі Інтернет та в закритій її частині Darknet в основному купуються за допомогою криптовалюти. На ринку є чимало криптовалют (наприклад, Bitcoin, Litecoin, Dogecoin, Ethereum та Monero). Водночас більшість ринків Darknet в основному використовують Ethereum і Monero через те, що відслідкувати переказ таких платежів украй складно.

Зазначимо також, що обіг криптовалют в Україні законодавчо не визначений, що також ускладнює розслідування кіберзлочинів та вилучення коштів, здобутих злочинним шляхом. Сьогодні на розгляді Верховної Ради України знаходиться проєкт закону “Про внесення змін до Податкового кодексу України та деяких інших законів України щодо оподаткування операцій з криптоактивами” (реєстр. № 2461 від 15.11.19 р.), в якому будуть надані базові визначення криптовалют. Разом із тим, цей законопроект

стосується лише сфери оподаткування та не охоплює питань, пов'язаних із кримінальними провадженнями.

Варто зазначити, що відповідно до дослідження X-Force Threat Intelligence Index кожне окреме ОЗУ спеціалізується на конкретному шкідливому програмному забезпеченні і зосереджується на різних частинах земної кулі. Проте з 2018 року виявилася нова тенденція – різні ОЗУ почали співпрацювати між собою для організації широкомасштабних операцій у банківській сфері. Така тенденція співпраці між троянськими операторами пояснюється бажанням отримати більший прибуток, незважаючи на вдосконалення контролю безпеки в банківській сфері [15].

У листопаді 2019 року на Черкащині Служба безпеки України припинила діяльність міжнародного хакерського угруповання, учасники якого викрадали кошти з рахунків користувачів електронних платіжних систем Європи та США.

Оперативники спецслужби встановили, що організаторами оборудки є громадянин РФ, який проживає у Києві, та троє мешканців Черкащини. Кіберзлочинці через спеціальні закриті хакерські форуми купували дані платіжних рахунків іноземців. За привласнені кошти вони закуповували товари у популярних закордонних Інтернет-магазинах. Потім продукцію реалізовували в Україні через онлайн-сервіси. Діяли хакери з 2010 року, їх річний обіг становив 500-700 тисяч доларів США.

Наразі вирішується питання щодо здійснення зловмисникам повідомлення про підозру у вчиненні кримінального правопорушення, передбаченого ч. 2 ст. 361 та ч. 2 ст. 209 Кримінального кодексу України [16].

Європол створив Європейський центр кіберзлочинності (далі – ЕС3) у 2013 році, щоб посилити реагування правоохоронних органів на кіберзлочинність у ЄС і таким чином допомогти захистити європейських громадян, підприємств та уряди від злочинності в Інтернеті. З моменту свого створення ЕС3 зробив вагомий внесок у боротьбу з кіберзлочинністю: він був залучений до десятків гучних операцій та сотень оперативних розгортань на місці, що призвели до сотні арештів, і проаналізував сотні тисяч файлів, переважна більшість з яких виявилася шкідливою.

Вагомий внесок у боротьбу з організованою кіберзлочинністю вносить Європол, який для посилення реагування правоохоронних органів на кіберзлочинність у ЄС у 2013 році створив Європейський центр кіберзлочинності (ЕС3), який брав участь у десятках гучних спеціальних операцій та проаналізував сотні тисяч файлів, що призвело до сотень арештів кіберзлочинів.

Починаючи з 2011 року Європол щорічно готує та оприлюднює звіт про оцінку загроз організованої кіберзлочинності – IOCTA (Internet Facilitated Organised Crime Tread Assessment) [17]. Завдяки матеріалам IOCTA визначаються реальні та потенційні загрози у кіберпросторі для країн-членів ЄС, можливі сценарії реагування на них. Європейський Союз та його інформаційно-комунікаційні мережі й інфраструктура залишаються найбільш уразливими об'єктами для кіберзлочинців.

У 2019 році експерти Європолу дійшли таких висновків.

Віруси-вимагачі (ransomware).

На даний час віруси-вимагачі (ransomware) залишаються найбільшою загрозою. Хоча загальний обсяг кібератак знизився, проте зловмисники зосереджуються на меншій кількості цілей, проте з більшим економічним збитком.

Найбільш значимі кібератаки у 2019 році були здійснені проти органів місцевого самоврядування, зокрема в Сполучених Штатах. Ця тенденція розпочалася раніше, коли у 2018 році кібератака паралізувала місто Атланта протягом декількох тижнів. Після цього вже більше півтисячі міст і різноманітні державні служби США стали жертвою

віруса-вимагача викупу, у зв'язку з чим губернатор Луїзіани навіть оголосила надзвичайну ситуацію у штаті.

Також на початку листопада 2019 року спрямовані атаки вірусу-вимагача вивели з ладу дві іспанські компанії в один день: велику фірму Everis, що належить NTT Data Group і працює у сфері IT-послуг та консалтингу, а також радіокомпанію Sociedad Española de Radiodifusión [18]. Багато компаній, у тому числі іспанський оператор аеропорту Aena, відмовилися від ряду послуг в якості запобіжного заходу.

24 жовтня 2019 року в ході цілеспрямованої кібератаки хакери зламали комп'ютерну мережу міста Йоганнесбург (ПАР). Вони за допомогою вірусу-вимагача заблокували дані міської адміністрації і обіцяли повернути їх тільки після виплати викупу. Група кіберзлочинців, відома під назвою Shadow Kill Hackers, вимагала виплати чотири біткойни ($ 30 000) [19].

11 листопада 2019 року мексиканська державна нафтогазова корпорація Pemex повідомила про атаку вірусу-здирника на свої комп'ютери, в результаті якої вона змушена була припинити адміністративну роботу. Хакери вимагали викупу у 5 млн доларів США [20].

Зниження кількості кібератак можна пояснити низкою причин, серед яких:

– підвищення обізнаності щодо основ кібербезпеки серед користувачів;

– правозастосовні ініціативи для зменшення наслідків загроз (наприклад, NoMoreRansom);

– збільшення використання мобільних пристроїв серед користувачів (більша частина програм-вимагачів зорієнтована на Windows) тощо.

DDOS-атаки.

Значною загрозою для інформаційних систем включно з критичною інфраструктурою залишаються DDos-атаки. Іноді вплив таких атак на он-лайн-банківські сервіси завдає більше збитків, аніж прямі атаки з метою пошкодження даних в комп'ютерних системах.

У Даркнеті ще залишаються поширеними нелегальні ринки збуту послуг з організації DDos-атак.

Під час проведення у квітні 2018 року спільної операції правоохоронних органів із десяти країн "Power Off" за підтримки Європолу було виявлено базу даних із 150000 зареєстрованих користувачів таких послуг та джерело 4 мільйонів кібератак.

У 2019 році правоохоронці долучилися до значно ширшого кола різноманітних розслідувань нападів на об'єкти критичної інфраструктури, включаючи енергетику, транспорт, водопостачання, галузь охорони здоров'я тощо.

У березні 2019 року норвезька компанія NorskHydroAS – постачальник відновлюваної енергії та один з найбільших виробників алюмінію у світі був скомпрометований програмою-вимагачем LockerGoga через цілеспрямовану кібератаку. Кібератака суттєво вплинула на бізнес, у результаті чого сталися перебої виробничих потужностей в Європі та США. Компанія зазнала збитків до 350 мільйонів норвезьких крон (≈ 35 млн. Євро) [21].

За допомогою іншого вірусу-вимагача Locker GOGA були здійснені атаки на понад 1200 промислових об'єктів по всьому світу. Правоохоронні органи Франції у грудні 2019 року звернулися до українських силовиків із проханням допомогти в пошуку хакерів. Як встановили французькі правоохоронці, деякі поштові скриньки і IP-адреси низки електронних скриньок (через які відбувалося зараження) належать Україні.

Співробітники Департаменту кіберполіції Національної поліції України встановили чотирьох можливих учасників злочинного угруповання. Слідство триває [22].

У відповідь на великі транскордонні кібератаки необхідно використовувати механізми міжнародного співробітництва, включаючи можливості підтримки Інтерполу, Європолу, Євроюсту та юридичних інструментів, розроблених для транскордонної співпраці (такі як Міжнародні спільні слідчі групи (Joint Investigation Team – JITs) та Спільні робочі групи з питань кіберзлочинності (Joint Cybercrime Action Taskforce - J-CAT) з метою обміну ресурсами та координації дій.

Успішна робота таких груп неможлива без обробки електронних даних, які можуть знаходитись на серверах у різних частинах світу. Більшість таких комп'ютерів знаходяться у приватному секторі. Тому успішна боротьба зі злочинцями можлива лише при тісній співпраці правоохоронних органів та приватного сектору IT-індустрії. З іншого боку така співпраця дозволить приватному сектору проводити необхідну профілактику для кіберзахисту себе та своїх клієнтів.

З лютого 2018 року Інтерпол бере участь у дослідницькому проєкті, який має на меті сприяти обміну електронними доказами в межах Європейського Союзу та активізувати міжнародну співпрацю щодо протидії злочинності. Його мета – створити інструмент для обміну електронними (цифровими) доказами через e-CODEX у рамках процедур взаємної правової допомоги [23].

Статті 16 та 17 Конвенції про кіберзлочинність від 2001 року передбачають прийняття країнами-підписантами Конвенції нормативних актів та процедур щодо термінового збереження комп'ютерних даних та часткового розкриття даних про рух інформації. На жаль, на сьогодні дані положення ще не імплементовані у Кримінальний процесуальний кодекс України. Також варто надати чіткі визначення електронних доказів та процедур щодо їх збирання.

У Комітеті Верховної Ради України з питань правоохоронної діяльності 10 грудня 2019 року створена робоча група щодо вдосконалення чинного законодавства з питань боротьби з кіберзлочинністю та використання електронних доказів, метою діяльності якої стала необхідність імплементації Будапештської Конвенції про кіберзлочинність у вітчизняне законодавство, пошук оптимальних шляхів удосконалення законодавчого забезпечення правоохоронної діяльності у цьому сегменті. Автором була внесена пропозиція щодо доповнення частини 2 статті 84 КПК України категорією "електронних доказів", а саме "Процесуальними джерелами доказів є показання, речові докази, електронні докази, документи, висновки експертів".

Відповідно до статистичної звітності Національної поліції України за 2019 рік Департаментом кіберполіції НП України виявлено 4 організовані групи, якими вчинено 84 кіберзлочини. За 2018 рік було виявлено 10 організованих груп, якими вчинено 119 кіберзлочинів. Очевидно, протиправною діяльністю сьогодні займаються ще не виявлені групи, що пояснюється високою латентністю кіберзлочинів. Наприклад за словами начальника підрозділу Центру розгляду скарг на кіберзлочини ФБР, загальна кількість кіберзлочинів, що повідомляються, становить лише 10 – 12 % від фактичної кількості [24].

Існує також кілька технічних причин, які ускладнюють боротьбу з кіберзлочинністю, у тому числі її організованими формами.

Перша причина – складність виявлення IP-адрес злочинців. Проблема полягає в тому, що є багато способів приховати IP-адресу або навіть підробити дані так, наче підключення здійснюється з іншої IP-адреси. Більш того, злочинці можуть використовувати різні інструменти, щоб уникнути виявлення їх правоохоронними органами, та приховати свої сайти у Darknet.

Інша технічна проблема пов'язана з уразливістю програмного забезпечення. Це дозволяє зловмисникам, наприклад, здійснювати несанкціонований доступ до

інформаційних систем. Іноді зловмисники знаходять уразливість раніше компанії, що виробляє програмне забезпечення (так звана уразливість “нульового дня”). Крім того, останнім часом хакери починають активно використовувати складні алгоритми “віруса-мутанта”, який складно виявити внаслідок постійної зміни сигнатури віруса.

Уразливості призводять до втрати даних і є відносно поширеними навіть для великих організацій, оскільки завдання створення, налаштування і захисту цифрових систем належним чином є складною проблемою.

Дії, які вживаються для протидії кіберорганізованій злочинності, зосереджуються на правоохоронних заходах, технічних рішеннях та освітніх кампаніях. Правоохоронні органи повинні здійснювати моніторинг веб-сайтів (як видимих, так і у Darknet), які сприяють кіберорганізованій злочинності, виявлення цих сайтів та притягнення до відповідальності осіб, які організують злочинну діяльність. Як приклад успішних можна навести спільні операції правоохоронних органів США та Нідерландів щодо сайтів у Darknet AlphaBay та Hansa, на яких здійснювалися продажі різноманітних протизаконних товарів, таких як наркотики, банківські картки, зброя тощо. Розслідування під керівництвом США було спрямоване на AlphaBay. Коли доступ до AlphaBay був закритий, користувачі (продавці та покупці) платформ перейшли на інший сайт – Hansa, що знаходився під контролем нідерландської поліції, яка проводила таємну операцію з виявлення та припинення незаконної діяльності. Ця міграція дозволила голландським правоохоронцям ідентифікувати та притягнути злочинців до відповідальності. Розслідування AlphaBay та Hansa демонструють важливість міжнародного співробітництва.

Також для боротьби з кіберорганізованою злочинністю впроваджуються різноманітні технологічні рішення. Програмне забезпечення використовується для виявлення повідомлень у рекламі, які вказують на торгівлю людьми. Сьогодні широко застосовується технологія розпізнавання облич для ідентифікації жертв торгівлі людьми та сексуальної експлуатації дітей. Програмне забезпечення для розпізнавання зображень також може використовуватися для ідентифікації об’єктів дикої природи та незаконних товарів, таких як наркотики чи вогнепальна зброя. Це програмне забезпечення може прискорити ідентифікацію незаконних товарів в Інтернеті та вказати незаконний вміст для огляду модераторами веб-платформ.

Український стартап Traces AI розробив систему розпізнавання людей навіть не на основі облич, а завдяки аналізу 2000 інших параметрів, включаючи колір шкіри, тип і деталі одягу, зачіску, форму тіла та таке інше. Впровадження такої системи повинно бути досить ефективним, адже жертви торгівлі людьми зазвичай ховають своє обличчя [25].

Оскільки чисельність кіберзлочинів продовжує постійно зростати, необхідно посилювати спроможність кіберполіції. Водночас збільшення числа підрозділів кіберполіції потребує значного збільшення кількості необхідного кваліфікованого персоналу. Його підготовка здійснюється через масштабні навчальні програми. Наприклад, у 2018 році поліція Великобританії співпрацювала з Мережевою академією Cisco щодо навчання у сфері кібербезпеки для 120000 офіцерів. Також регулярно проводяться тренування поліцейських щодо спеціальних навичок з кібербезпеки, які охопили понад 80 відсотків особового складу по всій країні. Також були проведені спеціальні курси для слідчих, які присвячені поглибленому вивченню фізичних та логічних мереж, що охоплюють бездротові мережі, операційні системи Linux, логи та методи збору даних.

Проводяться і інші курси, які охоплюють принципи управління інформаційною безпекою, методи використання Інтернет-ресурсів для отримання інформації про підозрюваного тощо. Кримінальним слідчим необхідний розширений доступ до навчання методикам розслідування в Інтернеті, використанню та вилученню криптовалют, таких як біткойн, та вилученню доказів, отриманих у чатах та інтернет-комунікаціях [1].

Висновки.

Організована кіберзлочинність постійно трансформується, у зв'язку з чим з'являються нові загрози та виклики, що потребує вжиття різноманітних заходів, у тому числі організаційного, правового та технічного характеру з метою адекватного превентивного захисту як користувачів кіберпростору, так і об'єктів критичної інфраструктури, банківської системи тощо.

Для посилення боротьби з кіберзлочинністю, у тому числі з її організованими формами пропонується:

1. Враховуючи, що організована кіберзлочинність носить транскордонний характер, необхідно посилити міжнародну співпрацю правоохоронних органів шляхом участі у спільних слідчих групах, та обміну інформацією, у тому числі оперативною, каналами Європолу та Інтерполу.

2. Провести імплементацію положень статей 16 та 17 Конвенції про кіберзлочинність щодо термінового збереження комп'ютерних даних та часткового розкриття даних про рух інформації.

3. Внести поняття "електронні докази" в Кримінальний процесуальний кодекс України, а також положення щодо особливостей їх отримання, зберігання та подання до суду.

4. Для поглибленого вивчення тенденцій організованої кіберзлочинності в Україні доцільно провести дослідження на основі методології звіту Європолу про оцінку загроз організованої кіберзлочинності – IOCTA.

5. Постійно проводити навчання та перепідготовку слідчих Національної поліції України методикам розслідування кіберзлочинів, у тому числі на основі аналізу інформації з Інтернет.

Використана література

1. Борьба с преступным использованием информационных технологий: Резолюция ООН от 22 января 2001 р. № 55/63. URL: https://www.undocs.org/ru/A/RES/55/63 (дата звернення 14.01.2020).

2. Всестороннее исследование проблемы киберпреступности URL: https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Russian.pdf. С. 31 (дата звернення 14.01.2020).

3. Доклад о работе совещания Группы экспертов для проведения всестороннего исследования проблемы киберпреступности, проведенного в Вене 27–29 марта 2019 года. С. 4. URL: https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-March-2019/Report/UNODC_CCPCJ_EG.4_2019_2_R.pdf (дата звернення 14.01.2020).

4. Hackers publish private photos from cosmetic surgery clinic. *The Guardian,* 31 May 2017. URL: https://www.theguardian.com/technology/2017/may/31/hackers-publish-private-photos-cosmetic-surgery-clinic-bitcoin-ransom-payments

5. Why police need the skills to counter cybercrime. URL: https://www.raconteur.net/technology/police-skills-cybercrime (дата звернення 14.01.2020).

6. Кількість кіберзлочинів в Україні зросла вдвічі за останні п'ять років – Opendatabot. URL: https://www.mind.ua/news/20203511-kilkist-kiberzlochiniv-v-ukrayini-zrosla-vdvichi-za-ostanni-p-yat-rokiv-opendatabot (дата звернення 14.01.2020).

7. “Укрпошта” зазнала 100-мільйонних збитків через вірус Petya. URL: https://www.epravda.com.ua/news/2018/04/24/636312 (дата звернення 14.01.2020).

8. The 773 Million Record “Collection #1” Data Breach. URL: https://www.troyhunt.com/the-773-million-record-collection-1-data-reach (дата звернення 14.01.2020).

9. Underground Hacker Marketplace Report. URL: https://www.secureworks.com/resources/rp-2016-underground-hacker-marketplace-report (дата звернення 14.01.2020).

10. Cybercrime and the Underground Market [Updated 2019]. URL: https://www.resources.infosecinstitute.com/cybercrime-and-the-underground-market/#gref (дата звернення 14.01.2020).

11. Mariposa Botnet Author, Darkcode Crime Forum Admin Arrested in Germany. URL: https://www.krebsonsecurity.com/tag/butterfly-bot (дата звернення 14.01.2020).

12. Найвідомішим у Darknet ресурсом заправляли українці – Кіберполіція. URL: https://www.pravda.com.ua/news/2019/01/28/7205116 (дата звернення 14.01.2020).

13. У Києві затримали керівника одного з наймасштабніших наркосиндикатів у світі. URL: https://www.unian.ua/incidents/10476900-u-kiyevi-zatrimali-kerivnika-odnogo-z-naymasshtabnishih-narkosindikativ-u-sviti-foto.html (дата звернення 14.01.2020).

14. История разгрома ShadowCrew. URL: https://www.kv.by/archive/index2005302201.htm (дата звернення 14.01.2020).

15. X-Force Threat Intelligence Index 2019. URL: https://www.securindex.com/downloads/8b9f94c46a70c60b229b04609c07acff.pdf (дата звернення 14.01.2020).

16. СБУ викрила хакерське угруповання на знятті коштів клієнтів електронних платіжних систем Європи та США. URL: https://www.ssu.gov.ua/ua/news/1/category/2/view/6782#.xr1LH33i.dpbs (дата звернення 14.01.2020).

17. Internet Organised Crime Threat Assessment (IOCTA). URL: https://www.europol.europa.eu/iocta-report (дата звернення 14.01.2020).

18. Ransomware attacks in Spain leave radio station in “hysteria”. URL: https://www.nakedsecurity.sophos.com/2019/11/06/spanish-ransomware-hits-two-companies (дата звернення 14.01.2020).

19. Shadow Kill Hackers cripple City of Jozi; demand Bitcoin ransom. URL: https://www.biznews.com/briefs/2019/10/25/hackers-cripple-city-jozi-bitcoin-ransom (дата звернення 14.01.2020).

20. A Hacker Wants About $5 Million in Ransom From Pemex By End of November. URL: https://www.bloomberg.com/news/articles/2019-11-13/a-hacker-wants-about-5-million-from-pemex-by-end-of-november (дата звернення 14.01.2020).

21. In its ransomware response, Norsk Hydro is an example for us all. URL: https://www.grahamcluley.com/in-its-ransomware-response-norsk-hydro-is-an-example-for-us-all (дата звернення 14.01.2020).

22. Франция ищет в Украине хакеров, запустивших опасный вирус. URL: https://www.internetua.com/franciya-isxet-v-ukraine-hakerov-zapustivshih-opasnyi-virus18 (дата звернення 14.01.2020).

23. EVIDENCE2e-CODEX. URL: https://www.interpol.int/es/Quienes-somos/Marco-juridico/Information-communications-and-technology-ICT-law-projects/EVIDENCE2e-CODEX (дата звернення 14.01.2020).

24. 11 Eye Opening Cyber Security Statistics for 2019. URL: https://www.cpomagazine.com/tech/11-eye-opening-cyber-security-statistics-for-2019 (дата звернення 14.01.2020).

25. “Ми знайдемо людину навіть якщо є лише фото зі спини”: як стартап Traces AI розпізнає людей на відео без обличчя. URL: https://www.epravda.com.ua/publications/2019/11/26/653992 (дата звернення 14.01.2020).

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