УДК 343.9.024 : 004.056

**ГУЦАЛЮК М.В.,** *доктор філософії (Ph.D.) з юридичних наук, доцент, с.н.с.*,
провідний науковий співробітник Міжвідомчого науково-дослідного
центру з проблем боротьби з організованою злочинністю
при РНБО України

# СУЧАСНІ ТЕНДЕНЦІЇ ОРГАНІЗОВАНОЇ КІБЕРЗЛОЧИННОСТІ

***Анотація**. В статті досліджуються сучасні тенденції кіберзлочинності, зокрема організовані її форми. Пропонуються заходи щодо посилення протидії кіберзлочинності.*
***Ключові слова:** кіберзлочинність, "Даркнет", міжнародне співробітництво.*

***Summary**. The article investigates the current trends of cybercrime, in particular, its organized forms. Measures to enhance the fight against cybercrime are proposed.*
***Keywords:** cybercrime, "DarkNet", international cooperation.*

***Аннотация**. В статье исследуются современные тенденции киберпреступности, в частности, ее организованные формы.*
***Ключевые слова:** киберпреступность, "Даркнет", международное сотрудничество.*

**Постановка проблеми.** Серед основних ознак сучасного інформаційного суспільства слід зазначити бурхливий розвиток інформаційних технологій та поширення мережі Інтернет, які впроваджуються у всі сфери життєдіяльності. Якщо перший в історії веб-сайт було створено в 1991 році, то на сьогодні у світі існує вже понад 1,3 мільярда веб-сайтів. Постійно зростає кількість Інтернет-користувачів: у 1995 році було лише 16 млн, у 2005 – 1 млрд, а у 2018 році – понад 4 млрд [1]. В Україні, за результатами дослідження агентства "PlusOne", кількість користувачів соціальної мережі Facebook за останні 5 років зросла на 9,8 млн (+ 306,2 %) і нині становить 13 млн. [2].

Використання кіберпростору сприяє обміну інформацією по всьому світу та забезпечує свободу вираження поглядів. Соціальні мережі принципово змінили методи взаємодії людей, а штучний інтелект та хмарні обчислення нині дозволяють обробляти значні обсяги даних та впроваджувати різноманітні новації, які сприяють становленню якісно нового рівня розвитку людини, держави та суспільства.

Водночас з'явилася і новітня форма злочинної діяльності – кіберзлочинність, яка сьогодні опанувала середовище комп'ютерних мереж і мобільних пристроїв. Анонімність глобальних інформаційних мереж та швидкість передачі інформації дає змогу використовувати ці переваги не тільки для розвитку інформаційного суспільства, але й для вчинення протиправних діянь. Цьому сприяє і те, що інформаційно-комунікаційні технології впроваджуються і розвиваються набагато швидше, ніж законодавці та правоохоронні органи можуть на це реагувати. Тому злочинність у кіберпросторі – одна з найгостріших проблем, яка постала сьогодні перед міжнародним співтовариством.

Генеральний секретар Організації Об'єднаних Націй Антоніу Гутерріш у травні 2018 року у день відкриття 27-ї сесії Комісії ООН з попередження злочинності та кримінального правосуддя зазначив, що нові технології, включаючи великі дані і аналітику, штучний інтелект та автоматизацію надають значні переваги для людства, але, разом з тим, створюють нові форми злочинності. Збитки світової економіки від кіберзлочинності оцінюються у $ 1,5 трлн. на рік. А за негативним сценарієм у 2019 році вони сягатимуть $ 2 трлн. [3].

**Результати аналізу наукових публікацій**. Різні аспекти проблем боротьби з кіберзлочинністю були предметом дослідження таких вітчизняних науковців, як: О. Амелін, Н. Ахтирська, П. Біленчук, В. Бутузов, В. Голубєв, В. Гавловський, С. Демедюк, М. Літвінов, В. Пилипчук, М. Погорецький, В. Шеломенцев, В. Хахановський та інші. Водночас, у зв'язку з появою новітніх інформаційних технологій та способів вчинення кіберзлочинів, ці питання потребують подальшого дослідження та ретельного вивчення як науково-теоретичної проблеми.

**Метою статті** є визначення сучасних тенденцій кіберзлочинності, у тому числі організованих її форм.

**Виклад основного матеріалу.** Тривалий час у чинному законодавстві України було відсутнє нормативно-правове закріплення ключових термінів, зокрема таких, як "кіберзлочин" і "кіберзлочинність", що спричиняло численні дискусії як серед науковців, так і практиків – співробітників правоохоронних органів.

Законом України "Про основні засади забезпечення кібербезпеки України", який набув чинності 9 травня 2018 року, визначено, що кіберзлочин (комп'ютерний злочин) – це 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, а кіберзлочинність – сукупність кіберзлочинів [4]. Водночас повного переліку злочинів, передбачених Кримінальним кодексом України, які слід вважати кіберзлочинами, на сьогодні поки що не існує.

Кіберзлочини, на відміну від традиційних, мають низку характерних особливостей, серед яких слід зазначити такі:

- місце вчинення кіберзлочину, на відміну від традиційних, може знаходитись в різних юрисдикціях – правопорушник активізує кібератаку, наприклад, з Інтернет-кафе однієї країни, бот-мережа знаходиться в іншій, а атакована інформаційна система – у третій;
- переважна кількість доказів кіберзлочинів існують в електронній формі (так звані "електронні" або "цифрові" докази). Вони, на відміну від традиційних, можуть швидко знищуватися чи модифікуватися. Для їх отримання, зберігання та аналізу необхідне спеціалізоване обладнання;
- внаслідок специфічної природи кіберпростору постраждалий не завжди обізнаний про вчинення кіберзлочину тощо.

До кіберзлочинів слід віднести не тільки злочини, об'єктом яких є комп'ютерні дані інформаційних систем, але й інші злочини, які вчиняються з використанням кіберпростору. До таких, наприклад, слід віднести торгівлю наркотиками через Інтернет, поширення дитячої порнографії, протиправні дії з платіжними картками тощо.

Кіберзлочинність, як уже зазначалося, завдає значних збитків. Так, масштабна хакерська атака у червні 2017 року, що здійснювалася за допомогою вірусної програми "Petya.A", порушила роботу багатьох важливих українських державних і приватних підприємств, зокрема: аеропорту Бориспіль, Укртелекому, ЧАЕС, Укрзалізниці, Кабінету Міністрів України тощо. Експерти Міжнародного валютного фонду підрахували, що економічні втрати від атаки вірусу "NotPetya" склали $ 850 млн. [5].

Сьогодні практично всі фахівці визнають, що ситуація з кіберзлочинністю у світі має сталу тенденцію до погіршення. При цьому посилюється зв'язок між кіберзлочинністю та організованою злочинністю. Інтернет використовують уже не тільки як допоміжний засіб, а й як місце та основний засіб вчинення традиційних злочинів – шахрайства, крадіжок, вимагання.

Однією з причин посилення організованості злочинної діяльності в мережі Інтернет можна вважати те, що така деструктивна діяльність стає більш вигідною, ніж інші способи незаконного збагачення. Експерти вказують на тривожну тенденцію: за останні роки кіберзлочинність стала більш організованою і набула ознак бізнесу, у якому важливими складовими є прибуток та опанування нових ринків.

Завдяки відсутності кордонів протиправна діяльність поширюється на нові регіони в усьому світі. Координація злочинної діяльності здійснюється на будь-яких відстанях з високою швидкістю. Відбувається зрощення національних злочинних угруповань з транснаціональними злочинними організаціями.

Посиленню організованості кіберзлочинності в сучасних умовах сприяють дві взаємопов'язані складові: по-перше, організована злочинність намагається використовувати кіберпростір у своїх цілях, по-друге, складний характер кіберзлочинів змушує осіб, які спеціалізуються на вчиненні злочинів у мережевому інформаційному просторі, координувати свої дії, об'єднуватися і створювати організовані кримінальні співтовариства.

У поле зору оперативних підрозділів дедалі частіше потрапляють організовані злочинні групи зі складною структурою, що мають транскордонні зв'язки. Зростає не тільки організованість кримінальних груп, але і їх законспірованість, збільшується кількість осіб, що займаються протиправною діяльністю в Інтернеті на професійній основі, посилюється спеціалізація таких осіб.

Організовані злочинні угруповання у своїй діяльності часто використовують мережу "Даркнет" (англ. DarkNet) [6], веб-сайти якої не індексуються і на які неможливо потрапити через пошукові системи, такі, як Google чи Yahoo. У "Даркнеті" широко використовуються криптографічні технології мережевої анонімності і он-лайн-розрахунків, які дозволили злочинцям створити чорний ринок, де продають і купують наркотики, крадені і контрафактні товари, дитячу порнографію, зброю тощо.

На даний час ця частина Інтернету ніяк не врегульована законодавчо, діяльність у ній майже неможливо проконтролювати, а тому організовані злочинні угруповання, використовуючи цю мережу, удосконалюють протиправну діяльність. У "Даркнеті" існує велика кількість хакерських спільнот, які спеціалізуються у своїй діяльності за конкретними напрямами, наприклад, неправомірний доступ до комп'ютерних систем, продаж шкідливого програмного забезпечення (далі – ШПЗ), організація кібератак, викрадення та продаж персональних даних тощо.

Такі приховані ринки самі по собі організовують злочинні співтовариства. Вони мають великих і дрібних функціонерів. Основна відмінність від традиційних організацій полягає в тому, що члени віртуальної організації, ймовірно, ніколи не зустрічалися один з одним і не знають один одного в реальності. Вони відомі під "ніком" (вигаданим ім'ям) та аутентифіковані онлайн-історіями і посиланнями на них інших користувачів сайту.

Як приклад функціонування транснаціональної злочинної групи, можна навести протиправну діяльність з торгівлі персональними даними в мережі "Даркнет", організованої громадянином України. У 2018 році працівники Департаменту кіберполіції Національної поліції України встановили чотирьох українців, які причетні до створення, організації та адміністрування однієї із найвідоміших у мережі "Даркнет" он-лайн-платформи з продажу персональних даних користувачів мережі. До документування цієї злочинної групи були залучені правоохоронці Домініканської Республіки, Індонезії, Іспанії, Франції та України.

Хакери упродовж останніх п'яти років безперешкодно отримували доступ до облікових записів "PayPal", "Amazon", "eBay", "WellsFargo", "Suntrust", "Bank of

America". Постраждалими від їхніх дій стали як громадяни України, так і мешканці Канади, Великобританії, Іспанії, Франції.

Для отримання такого доступу вони використовували спеціально створене шкідливе програмне забезпечення. Серед інформації, яка поширювалася, були логіни, паролі, персональні дані користувачів, номери їх телефонів, реквізити банківських карток та інші необхідні для авторизації дані. Наприклад, у результаті злому однієї із соціальних мереж, зловмисники отримали дані майже з півмільярда облікових записів.

Отримавши перелік таких записів, хакери використовували спеціалізовані скрипти для визначення облікових записів, які дають доступ до банківських акаунтів та веб-сайтів електронної комерції. Приблизний загальний річний обіг он-лайн-платформи становив майже 22 млн. доларів США.

Працівники кіберполіції провели санкціоновані обшуки на території трьох регіонів України в Одеській та Волинській областях, а також у місті Києві. За їх результатами вилучено комп'ютерну техніку, мобільні телефони та чорнові записи. Вилучену техніку направлено на експертизу.

Кримінальне провадження розпочато за ч. 2 ст. 361 ("Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку") КК України [7].

Для посилення боротьби з кіберзлочинністю Європол у 2013 році створив Європейський центр кіберзлочинності (англ. European Cybercrime Centre, далі – ЕСС). З моменту свого створення ЕСС вніс значний внесок у боротьбу з кіберзлочинністю, брав участь у десятках великих операцій і здійснював сотні операцій з оперативної підтримки, що призвело до багатьох арештів злочинців.

Починаючи з 2014 року, ЕСС щорічно готує та оприлюднює Звіт про оцінку загроз організованої кіберзлочинності (англ. Internet Facilitated Organised Crime Thread Assessment, далі – ІОСТА) [8]. У звіті досліджуються тенденції та нові загрози, які впливають на уряди, бізнес та громадян ЄС. Аналітичні матеріали для ІОСТА готуються на основі досліджень експертів Європолу, правоохоронних органів, партнерів з приватного сектору та наукового середовища.

У звіті приділяється увага сферам злочинності, що належать до компетенції ЕСС. До них відносяться: кіберзлочини (кібератаки, зловмисне програмне забезпечення, бот-мережі та ін.), сексуальна експлуатація дітей в Інтернеті, шахрайство з платіжними картками (викрадення даних карток – "кардінг", "скіммінг"). До інших напрямів, які аналізуються ІОСТА, належать так звані наскрізні чинники злочинів, які охоплюють багато сфер злочинності, але самі по собі не завжди є кримінально караними діяннями. Зокрема, це зловживання криптовалютами, відмивання брудних коштів, отриманих злочинним шляхом, компрометація корпоративної електронної пошти тощо.

Метою доповідей ІОСТА є інформування осіб, відповідальних за прийняття рішень на стратегічному, політичному та тактичному рівнях у сфері боротьби з кіберзлочинністю для спрямування оперативної діяльності правоохоронних органів ЄС, а також інформування громадськості про реальні та потенційні загрози у кіберпросторі, можливі сценарії реагування на них, здобутки правоохоронних органів ЄС у сфері боротьби з кіберзлочинністю.

Доповідь ІОСТА готується групою стратегічних аналітиків Європолу, яка у своїй роботі спирається переважно на матеріали держав-членів ЄС, Цільової групи Європейського союзу з кіберзлочинності (далі – EUCTF), аналітичних проектів Європолу "Cyborg", "Terminal" і "Twins", а також групи кіберрозвідки (англ. Cyber Intelligence Team) та групи SOCTA у вигляді структурованих досліджень, опитувань та

модерованих семінарів. Також у доповіді використовуються результати досліджень з відкритих джерел та внески від приватного сектору, включаючи консультативні групи ECC, Євроюст, ENISA, CERT-EU, EBF та спільноту CSIRT. Ці внески відіграють ключову роль у підготовці доповіді. Водночас на сьогодні в Україні такого дослідження проведено ще не було.

Аналіз матеріалів IOCTA за 2016 – 2018 роки дозволяє визначити наступні тенденції організованої кіберзлочинності:

1) Розповсюдження програм-вимагачів (“Ransomware”) становить одну з основних загрозу у кіберпросторі. Вони поширили свій вплив на різноманітні галузі як у державному, так і в приватному секторах. При цьому успіх та попит на програми-вимагачі призвів до різкого зростання (на 750 % за 2 роки) кількості їх сімейств.

Активне розповсюдження таких програм пояснюється тим, що порівняно з іншими шкідливими програмами, які викрадають інформацію, програми-вимагачі легше монетизувати (отримати викуп), а також за допомогою криптовалют (наприклад Bitcoin) здійснити подальше відмивання таких злочинних грошей. Крім того, за допомогою програми-вимагача можна атакувати значно різноманітніший спектр цілей, тобто майже будь-кого, хто зберігає конфіденційні дані.

Незважаючи на те, що об’єктами кібератак є, у переважній більшості, звичайні люди, їхніми цілями стають також малі та середні підприємства, яким часто бракує ресурсів для повного захисту своїх даних та мереж.

Деякі напади були спрямовані на критичні національні інфраструктури (лікарні, правоохоронні органи, державні установи та служби) та створили безпосередню загрозу життю громадян. Серія кібератак “WannaCry” у травні 2017 року стала яскравим прикладом втручання у роботу лікарень у Великобританії, порушення функціонування залізничної мережі в Німеччині, телекомунікаційних компаній в Іспанії та Португалії, нафтохімічних компаній в Китаї та Бразилії.

Поєднання факторів, що стояли за атаками середини 2017 року “WannaCry” та “NotPetya”, призвели до того, що національні правоохоронні органи усвідомили свою неспроможність самостійно протидіяти таким кібератакам та необхідність більшої та посиленої співпраці між правоохоронними органами різних країн, компаніями приватного сектору, науковими колами та іншими відповідними зацікавленими сторонами.

В 2016 році для боротьби з програмами-вимагачами правоохоронними органами ЄС (ECC, поліція Нідерландів) у співпраці з приватним сектором був створений і впроваджений у роботу портал “No More Ransom” [9]. Метою цієї ініціативи є широке інформування громадськості про небезпеки, пов’язані з програмами-вимагачами, і надання допомоги жертвам даного ШПЗ у відновленні своїх даних без сплати викупу зловмисникам. Даний портал діє і сьогодні для підвищення обізнаності та забезпечення безкоштовними засобами дешифрування постраждалих від кібератак.

2) Поширення DDoS-атак.

Продовжуються DDoS-атаки на державні та приватні організації, у т.ч. на критичну інфраструктуру. Зокрема, у 2018 році одна третина держав-членів ЄС повідомила про випадки нападу на критичну інфраструктуру.

Спостерігається зростання інтенсивності та складності DDoS-атак, поширюються пропозиції “DDoS-атака як послуга” (англ. DDoS-as-a-service).

Як правило в організації потужних кібератак задіяна значна кількість виконавців. Так у грудні 2016 року Європол та правоохоронні органи з Австралії, Бельгії, Франції, Угорщини, Литви, Нідерландів, Норвегії, Португалії, Румунії, Іспанії, Швеції, Сполученого Королівства Великобританії та Сполучені Штати Америки здійснили

скоординовані дії, орієнтовані на користувачів сервісу DDoS-атаки, що призвело до 34 арештів та допиту 101 підозрюваних осіб.

Сьогодні, на відміну від попередніх років, вимоги, що висуваються під час таких атак, мають не лише корисливий, а й політичний та ідеологічний характер, що не виключає безпосередню участь у такій діяльності спонсорованих державою організованих злочинних угруповань.

Для протидії таким атакам правоохоронні органи повинні зосередитися на суб'єктах, які розробляють та надають засоби для кібератак, зокрема банківські трояни та інші шкідливі програми, а також на постачальниках засобів для DDoS-атаки, служб бот-мережі тощо.

Небезпечним в експертному середовищі вважається також динамічний розвиток "Інтернету речей" (англ. Internet of Things, IoT, далі – IP). З'явилися DDoS-атаки, що походять від бот-мереж компрометованих пристроїв IP. До 2020 року прогнозується зростання кількості таких кібератак на 25 %. В Україні також прогнозується поширення IP. Для оперативного обговорення проблем щодо розвитку IP в Інтернет-асоціації України створена відкрита група фахівців [10].

Традиційно метою злочинних організацій є кошти банківських установ.

У березні 2018 року в місті Аліканте в Іспанії заарештували лідера злочинного угруповання 34-річного українця К. Дане угруповання розпочало свою діяльність у 2013 році, здійснюючи кібератаки на банки, системи електронних платежів та фінансові установи, використовуючи свої власні розробки, відомі як "Carbanak" і "Cobalt".

За даними слідства, постраждалими від злочинної діяльності злочинних угруповань стали понад 100 банків з 40 країн. Однак основні крадіжки були здійснені ним в банках Росії. За попередніми даними, сума викраденого перевищує 1 мільярд євро, хоча мова може йти і про значно більшу суму (до 10 мільярдів). Пізніше у США арештували ще трьох громадян України – членів злочинного угруповання "Carbanak" або ж "Fin7" [11].

3) Незважаючи на те, численна аудиторія споживачів користується мережею Tor та іншими подібними анонімізуючими мережами для розповсюдження незаконних товарів, розширилася сфера використання мережі "DarkNet" у напрямку реалізації наркотичних та психотропних речовин, зброї, засобів ураження, скомпрометованих платіжних даних, дитячої порнографії, підроблених документів тощо.

У квітні 2017 року Європол та Інтерпол надавали підтримку іспанській національній поліції у проведенні операції "Tantalio" з комплексного розслідування поширення дитячої порнографії через мережу "DarkNet". Спільні слідчі дії проводилися у 5 країнах Європи під керуванням Європолу та в 13 країнах Центральної та Південної Америки за координації Інтерполу. В результаті операції було заарештовано 39 підозрюваних у Європі та Південній Америці.

У червні 2017 року Європол організував проведення кампанії "Скажи НІ" (англ. Say NO) [12], спрямованої на допомогу потенційним жертвам сексуальної експлуатації дітей, надання он-лайн-консультацій з метою отримання навичок із розпізнавання спроб примушення до такої експлуатації та шляхів звернення за допомогою до компетентних національних органів у разі вчинення таких злочинів.

Станом на червень 2017 року в мережі "Tor" було понад 2,2 мільйона безпосередньо підключених користувачів і майже 60 тис. унікальних доменів ".onion". Проблему становить лише кількісне визначення співвідношення незаконної активності в цих мережах до законного їх використання звичайними користувачами для більш безпечного перегляду веб-сторінок. Майже 57 % активних засекречених сайтів пов'язані з певною формою незаконної діяльності [12].

Загалом можна констатувати, що наразі найбільш динамічно збільшується кількість кіберзлочинів, спрямованих на мобільні платформи, в яких протягом останніх років удвічі зросла кількість виявлень зловмисного програмного забезпечення.

Ще однією загрозою у світі є масштабне впровадження у більшості країн криптовалют, які стають повноцінним платіжним засобом та інвестиційним активом. Зацікавленість до використання криптовалют сприяє інвестиційній привабливості платіжних інфраструктур. Проте "Bitcoin" та інші цифрові валюти адаптовані для використання організованими злочинними угрупованнями, оскільки вони досить поширені в міжнародному обігу та забезпечують необхідний рівень анонімності. Маючи спеціальні технічні навички та вміння, міжнародні терористичні угруповання можуть використовувати віртуальні валюти для фінансування терористичних заходів. Загроза відмивання грошей, пов'язаних з віртуальними валютами, демонструє, що кримінальний світ може використовувати віртуальні валюти для доступу до "чистої готівки" і одночасно приховувати сліди транзакцій.

Водночас криптовалюти є також ціллю кіберзлочинців. За повідомленням "Reuters", з криптобірж у ході кібератак за перші 9 місяців 2018 року вивели 927 мільйонів доларів, що на 250 % більше, ніж за весь 2017 рік. У компанії відзначають, що дослідження базується на офіційних даних, реальні ж цифри можуть бути набагато вищі [13].

Щодо труднощів, пов'язаних з проведенням слідчих дій, які стосуються розслідувань кіберзлочинів, слід зазначити зростаючу ступінь витонченості злочинної діяльності та необхідність для слідчих органів бути обізнаними в сучасних технологіях так само, як кіберзлочинці. Адже кібератаки стають дедалі складнішими, їх дедалі важче виявити, і в той же час ці методи швидко знаходять вихід до широкого загалу користувачів.

Зростання кількості кіберзлочинів обумовлюється удосконаленням технічних і програмних засобів, доступних для зловмисників, і посилюється існуванням нелегального ринку з продажу засобів для здійснення кіберзлочинів.

Зростаюча ступінь витонченості злочинної діяльності викликає ще більші труднощі, пов'язані з виявленням електронних доказів, застосуванням зловмисниками методів заплутування, необхідністю аналізу великих обсягів даних і отриманням даних від постачальників послуг.

Функції зберігання інформації в цифровій формі і використання глобальної мережі дедалі частіше інтегруються в звичайні предмети побуту і особистого вжитку, такі як ручки, камери, годинник з флеш-пам'яттю і ювелірні прикраси з USB-накопичувачами. Крім того, бездротові пристрої зберігання можуть бути заховані в поглибленнях стін, в надстелевому просторі і під підлогою. Той факт, що комп'ютерні дані фізично легко заховати, створює труднощі для розслідування.

Останнім часом рівень кіберзлочинності швидко зростає і в Україні. Експерти зазначають, що Україна – дуже важливий центр хакерства, поряд із Бразилією, Китаєм та меншою мірою – Індією.

Відповідно до статистичних даних, наданих Національною поліцією України, кількість організованих груп і злочинних організацій, що вчиняють кримінальні правопорушення з використанням високих інформаційних технологій за останній рік збільшилося на 36 %.

Вже у 2019 році працівники Поліського управління Департаменту викрили групу осіб у створенні вірусів та їх використанні для незаконного збагачення. Зловмисники створили бот-мережу, яка сканувала та перебирала паролі до комп'ютерів для отримання повного контролю над ними. Отримавши доступ, в тому числі і до он-лайн-

банкінгу, хакери перераховували усі кошти з рахунків власника інфікованого комп'ютера на підконтрольні рахунки. Зловмисники змогли отримати таким способом понад 5 млн. гривень [14]. Кримінальне провадження розпочато за декількома статтями кримінального кодексу України: ст. 361 ("Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку") та ст. 185 ("Крадіжка") КК України.

В Україні також продовжується розповсюдження шкідливого програмного забезпечення. Наприклад, у м. Глухів громадянин А. здійснював продаж шкідливого програмного забезпечення для викрадення паролів через різноманітні форуми та через програми Skype і Telegram. Слобожанським управлінням кіберполіції НП України було встановлено також, що даний громадянин організував свій відеоблог на YouTube, на якому розповідається про використання шкідливого програмного забезпечення.

Для отримання коштів від покупців правопорушник використовував заборонені в Україні платіжні системи. Кримінальне провадження розпочато за статтею 361-1 КК України [15].

Правоохоронні органи України виявляють непоодинокі випадки несанкціонованого доступу до державних баз даних.

Так у лютому 2019 року працівники Департаменту внутрішньої безпеки та Головного слідчого управління Національної поліції України, під процесуальним керівництвом Генеральної прокуратури України, викрили колишнього начальника одного з департаментів Національної поліції України в організації схеми незаконного збагачення шляхом продажу службової інформації. Полковник поліції разом зі спільниками тривалий час за грошову винагороду надавав конфіденційні відомості та безпосередній доступ до них колекторським конторам, мережі банківських установ і приватним підприємствам. За легалізовані кошти чиновник придбав 9 квартир у столиці.

Готується оголошення підозри 6 учасникам організованого злочинного угруповання за ч. 3 ст. 28 (скоєння злочину групою осіб, групою осіб за попередньою змовою, організованою групою або злочинною організацією), ч. 2 ст. 361 (несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж або мереж електрозв'язку) і ч. 2 ст. 361-2 (несанкціонований збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації) Кримінального кодексу України [16].

Також продовжуються розробка та розповсюдження усіляких шахрайських схем, які вчиняються з використанням мережі Інтернет.

Усі схеми діяльності шахраїв схожі між собою. Як приклад, вже у 2019 році кіберполіція припинила діяльність офісу, який позиціонував себе як "бінарний опціон". Зловмисники, під виглядом участі в он-лайн торгах валютними парами ("бінарні опціони") пропонували бажаючим отримання додаткового пасивного прибутку. Для цього необхідно було створити свій робочий он-лайн кабінет на сайті "dax100.org" та зробити внесок – 100 євро.

Коли ж клієнт намагався вивести гроші, шахраї під різними приводами відмовляли в цьому та пропонували продовжити торги. Якщо клієнт відмовлявся й надалі вкладати кошти в торги, адміністрація майданчика цілеспрямовано проводила ряд операцій, що призводили до повної втрати клієнтом грошей.

За оперативною інформацією, у 2018 році тисячі громадян як України, так і за кордоном, стали жертвами подібних схем. За приблизними оцінками, в Україні один шахрайський офіс протягом місяця приносив близько мільйона гривень. Найбільші з

них – “HQbroker” та “Trade12”. Протягом року в Україні кіберполіція припинила діяльність 18 злочинних груп. За усіма цими фактами розпочато кримінальні провадження та триває досудове розслідування [17].

Водночас за даними судової статистики, у 2017 році за статтями, передбаченими Розділом XVI КК України (ст. 361 – 361-3), засуджено лише 42 особи: з яких 5 осіб позбавлено волі на строк до 3 років та 2 особи – на строк від 3 до 5 років, тобто часто покарання за вчинення кіберзлочинів обмежується тільки невеликим штрафом – тому, що ці злочини кваліфікуються як середньої тяжкості.

А дані судової статистики за 2018 рік вказують на те, що з 70 засуджених осіб позбавлено волі лише 3, серед яких так само як і в попередньому році ***тільки 2 особи позбавлено волі на строк до 5 років***.

При цьому варто зазначити, що цей вид злочинів (учинених повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду) в Україні максимально карається позбавленням волі на строк від трьох до шести років.

В той же час за повідомленням ЗМІ українські хакери засуджуються в різних державах за протиправну діяльність в кіберпросторі на строки від 30 – 40 років і більше позбавлення волі. Наприклад, членів організованого злочинного угруповання “Western Express”, яка спеціалізувалася на викраденні платіжних карток, і до якої входив громадянин України Ш., у 2013 році було засуджено Верховним судом штату Нью-Йорк до 40 років позбавлення волі [18 ].

Сьогодні, на думку фахівців, жоден комплексний кримінологічний аналіз не здатний дати повного уявлення про глобальні масштаби кіберзлочинності, у тому числі організованих її форм, що суттєво відрізняється від традиційної.

Розглянувши комплекс проблем у сфері забезпечення кібербезпеки та констатуючи її кризовий стан, що загрожує національній безпеці, Рада національної безпеки і оборони України своїм Рішенням від 29 грудня 2016 року “Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації”, введеним в дію Указом Президента України від 13 лютого 2017 року №32/2017, зобов’язала Кабінет Міністрів України у тримісячний строк внести в установленому порядку на розгляд Верховної Ради України законопроекти щодо імплементації положень Конвенції про кіберзлочинність, ратифікованої Законом України від 7 вересни 2005 року № 2824-IV, передбачивши, низку організаційних заходів, серед яких на сьогодні залишається невиконаним запровадження дієвого механізму використання в кримінальному процесі доказів в електронній формі, зібраних у процесі здійснення оперативно-розшукової діяльності. У зв’язку з цим особливого значення набуває повна імплементація Конвенції про кіберзлочинність [19].

У зв’язку з подальшим поширенням використання у злочинній діяльності інформаційних технологій правоохоронним органам також слід розробляти нові підходи у боротьбі з новими видами злочинної діяльності та створювати відповідні організаційні структури. Наприклад, ФБР створило відділ боротьби з високотехнологічною організованою злочинністю (англ. Hi-Tech Organized Crime Unit, далі – HTOCU), основним завданням якого є аналіз та дослідження проблем і загроз від діяльності організованих злочинних угруповань, які використовують передові технології у незаконної діяльності.

Це дасть змогу не тільки розробити стратегічні рекомендації, але й посилити координацію правоохоронних органів, зосередившись на глобальних загрозах, що виникають від організованих злочинних угруповань. HTOCU співпрацює з “Cyber Division” ФБР для підготовки слідчих до розслідування діяльності організованих злочинних угруповань “під прикриттям” в Інтернеті та у співпраці з Міжнародним

центром розвідки та операцій з організованою злочинністю (англ. The International Organized Crime Intelligence and Operations Center – IOC-2) розробляє он-лайн-платформу для дослідження протиправної діяльності у "Даркнеті" тощо [20].

**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 її організованим формам пропонується:

- враховуючи тяжкі наслідки, які можуть бути завдані вчиненням кіберзлочинів, ініціювати питання щодо посилення санкцій за вчинення злочинів, передбачених статтями 361, 361-1, 361-2, 362, 363, 363-1 КК України, доповнивши ці статті відповідними частинами, що дасть змогу перевести їх у розряд тяжких злочинів, посилить кримінальну відповідальність за їх вчинення, а також розширить перелік негласних слідчих (розшукових) заходів, що можуть бути проведені для їх припинення або документування;
- законодавчо унормувати поняття "криптовалюта" для можливості притягнення до відповідальності осіб за вчинення злочинних дій з їх використанням;
- посилити державно-приватне партнерство у протидії кіберзлочинності, у тому числі при підготовці нормативно-правових документів у цій сфері;
- внести зміни до Глави 4 Докази і доказування Кримінального процесуального кодексу України в частині порядку отримання, зберігання, оцінки та передачі електронних доказів під час судового та досудового розслідувань;
- підготувати аналітичний звіт ІОСТА в Україні, який мав би велике значення для виконання Угоди між Європолом та Україною щодо стратегічного співробітництва та сприяв ефективному впровадженню положень Стратегії кібербезпеки України.

## Використана література

1. Internet World Stats. URL: https://www.internetworldstats.com/emarketing.htm (дата звернення: 07.12.2018).

2. Украинская аудитория Facebook выросла на 3 млн человек за 2018 год, общее количество пользователей соцсети в нашей стране составляет 13 млн. URL: https://itc.ua/news/ukrainskaya-auditoriya-facebook-vyirosla-na-3-mln-chelovek-za-2018-god-obshhee-kolichestvo-facebook-polzovateley-teper-sostavlyaet-13-mln-infografika/#disqus_thread (дата звернення: 19.02.2019).

3. Киберпреступники наживаются на самых бедных. URL: https://www.unodc.org/unodc/ru/frontpage/2018/May/much-work-to-do-and-no-time-to-waste-in-cybercrime-fight--says-un-chief. html (дата звернення: 19.02.2019).

4. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163-VIII. URL: http://zakon2.rada.gov.ua/laws/show/2163-19 (дата звернення: 07.09.2018).

5. Збитки від глобальних кібератак у світі сягнули $ 53 мільярдів – МВФ. URL: https://www.ukrinform.ua/rubric-world/2322816-zbitki-vid-globalnih-kiberatak-u-sviti-sagnuli-53-milardiv-mvf.html (дата звернення: 07.09.2018).

6. Гуцалюк М.В. Протидія використанню учасниками злочинних угруповань мережі "Даркнет". *Інформація і право*. № 3(26)/2018. С. 102-108.

7. Кіберполіція припинила діяльність одного з найвідоміших майданчиків у DarkNet із продажу персональних даних. URL: https://cyberpolice.gov.ua/news/kiberpolicziya-prypynyla-diyalnist-odnogo-z-najvidomishyx-majdanchykiv-u-darknet-iz-prodazhu-personalnyx-danyx-4672 (дата звернення: 27.12.2018).

8. Internet Organised Crime Threat Assessment (IOCTA). URL: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment (дата звернення: 27.12.2018).

9. No More Ransom. URL: https://www.nomoreransom.org/ru/index.html (дата звернення: 19.02.2019).

10. В Украине взялись за популяризацию Интернета вещей. URL: http://internetua.com/v-ukraine-vzyalis-za-populyarizaciua-interneta-vesxei (дата звернення: 19.02.2019).

11. У США арештували українських хакерів. URL: https://www.pravda.com.ua/news/2018/08/1/7188031 (дата звернення: 27.12.2018).

12. Internet Organised Crime Threat Assessment (IOCTA) 2017. URL: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017

13. Хакери вкрали з криптобірж майже 1 мільярд доларів з початку року. URL: https://www.epravda.com.ua/news/2018/10/11/641522 (дата звернення: 27.12.2018).

11. Рынок киберкриминала: спрос втрое превышает предложение. URL: http://channel4it.com/publications/Rynok-kiberkriminala-spros-vtroe-prevyshaet-predlozhenie-31263.html# (дата звернення: 27.12.2018).

12. Here's how easy it is to buy anything – legal or illegal – on the 'dark web'. URL: https://www.businessinsider.com/find-anything-on-dark-web-tor-internet-2016-11.

Hacking communities in the Deep Web. URL: https://resources.infosecinstitute.com/hacking-communities-in-the-deep-web/#gref (дата звернення: 07.09.2018).

13. Cryptocurrency Attacks Are Rising. URL: https://www.bloomberg.com/news/articles/2018-05-29/cryptocurrency-attacks-are-rising-as-rouge-miners-exploit-flaw (дата звернення: 07.09.2018).

14. Кіберполіція викрила групу хакерів, які ошукали українців більш як на 5 мільйонів гривень. URL: https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-grupu-xakeriv-yaki-oshukaly-ukr ayinczіv-bilsh-yak-na--miljoniv-gryven-968 (дата звернення: 19.02.2019).

15. Украинскому видеоблогеру грозит два года тюрьмы за продажу вирусов. URL: http://internetua.com/ukrainskomu-videoblogeru-grozit-dva-goda-tuarmy-za-prodaju-virusov (дата звернення: 19.02.2019).

16. Екс-начальник Нацполіції купив дев'ять квартир на відмиті від продажів баз даних МВС гроші. URL: https://ukranews.com/ua/news/615126-eks-nachalnyk-natspolitsiyi-kupyv-dev-yat-kvartyr-na-vidmyti-vid-prodazhiv-baz-danyh-mvs-groshi (дата звернення: 19.02.2019).

17. Кіберполіція фіксує збільшення випадків шахрайств, вчинених під виглядом інвестування на фінансових ринках. URL: https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-fiksuje-zbilshennya-vipadkiv-shaxrajstv-vchinenix-pid-viglyadom-investuvannya-na-finansovix-rinkax (дата звернення: 19.02.2019).

18. США: приговоры по делу хакеров из России и Украины. URL: https://www.bbc.com/russian/international/2013/08/130812_usa_hackers_carders_sentences (дата звернення: 19.02.2019).

19. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 07.09.05 р. № 2824-IV. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 27.12.2018).

20. Organized Crime Has Gone High Tech. URL: http://www.policechiefmagazine.org/organized-crime-has-gone-high-tech (дата звернення: 27.12.2018).

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