УДК 342.951

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

ОСОБЛИВОСТІ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ПІД ЧАС ВОЄННОГО СТАНУ

DOI…

Анотація. *У статті розкриті особливості протидії кіберзлочинності під час воєнного стану. Дано короткий аналіз розвитку спроможностей України щодо протидії кіберзлочинності. Наголошено на необхідності імплементувати положення Конвенції про кіберзлочинність включно з Другим додатковим протоколом щодо використання електронних доказів, а також прискорити формування кібервійськ в Україні .*

Ключові слова: *кіберзлочинність, кібербезпека, кібероборона, електронні докази, кібервійна, міжнародне співробітництво.*

Summary. *The article reveals the specifics of combating cybercrime during martial law. A brief analysis of the development of Ukraine's capabilities to combat cybercrime is given. The need to implement the provisions of the Convention on Cybercrime, including the Second Additional Protocol on the use of electronic evidence, and accelerate the formation of cyber troops in Ukraine, is emphasized.*

Keywords: *cybercrime, cyber security, cyber defense, electronic evidence, cyberwar, international cooperation.*

Постановка проблеми. Інформаційні системи та мережі відіграють ключову роль у розвитку сучасного суспільства. Адже без обробки постійно зростаючих обсягів інформації сучасними технічними засобами неможливо уявити будь-яку сферу управління, виробництва, освіти тощо. Крім того, особливо після пандемії Covid-19, зростання кількості користувачів різноманітних соціальних мереж та месенджерів стало одним з найважливіших та найбільш поширених засобів соціальної комунікації громадян, що здатні впливати на формування суспільної свідомості суспільства.

Разом з тим, незважаючи на суттєві переваги використання інформаційних технологій, зростання кількості підключень до Інтернету та довіру користувачів до різноманітних Інтернет-сервісів постійно підвищуються ризики крадіжки інформації, кібершахрайства та інших кіберзлочинів.

Крім того, з поширенням по всьому світу глобальної мережі Інтернет та появи електронної комерції, Інтернет-реклами, появою різноманітних месенджерів для обміну зашифрованою інформацією на постійно зростаючий кіберпростір звернула увагу і організована злочинність – адже це дозволяє їй поступово переходити від традиційної злочинної діяльності до більш прибуткових і менш ризикованих операцій у кіберпросторі.

Наприклад, широкого розповсюдження набув безконтактний метод передачі наркотиків, коли продавець та покупець безпосередньо не зустрічаються, а всі операції, починаючи від реклами “товару”, обговорення на форумах, обмін повідомленнями та оплата за продукт відбуваються з використанням інформаційних технологій. Торгівля великими партіями заборонених товарів партіями здійснюється через Даркнет.

Крім того, в останнє десятиліття широко розповсюдилися маркетплейси, які завдяки найнятим фахівцям з реклами надають “послуги” щодо продажу персональних даних, шкідливого програмного забезпечення, організації кібератак тощо.

Оплата заборонених у вільному продажі товарів, як правило, проводиться з використанням криптовалюти, відслідковування якої має певні складнощі [1].

Організаторами та виконавцями незаконної торгівлі як товарами, так і шкідливим програмним забезпеченням можуть бути як окремі індивідууми, так і потужні корпорації на кшталт реальних підприємств зі складною ієрархічною структурою. Такі “кібер-організації” можуть налічувати від десяти до кількох тисяч учасників. Незалежно від кількості членів і філій, віртуальними злочинними мережами зазвичай керує невелика кількість досвідчених онлайн-злочинців, які самі не скоюють злочини, а діють як підприємці, залучаючи до злочинної діяльності нових членів. Один з форумів – “RaidForums” – мав спільноту з понад ***мільйона користувачів***. Під час проведення міжнародної операції TOURNIQUET, яка відбулася в квітні 2022 року, в організаторів були виявлені бази даних, які належать низці американських корпорацій у різних галузях, дані кредитних карток, паролі доступу в Інтернет та інша інформація [2].

Після початку військових дій, розв’язаних державою-агресором, всі сили безпекового блоку України, у тому числі кібербезпеки, були спрямовані на відсіч ворогу. Такою ситуацією скористалися кіберзлочинці, у першу чергу кібершахраї, активізувавши свою злочинну діяльність. Разом з тим, кібероперації ворога, які є невід’ємною складовою сучасної гібридної війни, потребують постійної адекватної відповіді. Однак кібероборона, яка почала активно формуватися, потребує відповідного правового регулювання. Протидія правопорушенням у кіберпросторі та активна кібероборона під час воєнного стану вимагає нових підходів та методів, удосконалення чинного законодавства у зазначеній сфері та дослідження проблемних питань діяльності правоохоронних органів щодо розслідування кіберзлочинів та протидії кібероперaціям держави-агресора.

Результати аналізу наукових публікацій. Питання протидії кіберзлочинності (раніше комп’ютерної злочинності) досліджували з кінця 1990-х років та початку 2000-х такі науковці, як Н. Ахтирська [3], П. Біленчук [4], В. Бутузов, В. Гавловський, Б. Романюк [5], К. Тітуніна [6], В. Хахановський [7], В. Шеломенцев [8] та інші.

В цей же час розпочалося формування організаційних структур, спрямованих на протидію кіберзлочинності. Зокрема Указом Президента “Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 р. “Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України” від 06.12.01 р. № 193/2001 було передбачено створення Міжвідомчого центру з питань боротьби з комп’ютерною злочинністю, проте це завдання не було виконане.

На початку 2000-х було визначені різноманітні структурні підрозділи в системі МВС для боротьби зі злочинами у сфері високих технологій. У жовтні 2015 року створений повноцінний спеціалізований підрозділ для протидії кіберзлочинності – Департамент кіберполіції Національної поліції України, який і сьогодні постійно вдосконалюється. Після появи значної бази для дослідження кіберзлочинів та налагодження тісної співпраці з міжнародними партнерами почали з’являтися нові наукові роботи та захищатися численні дисертаційні дослідження, присвячені питанням протидії кіберзлочинності, зокрема О. Волкова [9], М. Кравцової [10], М. Яцишиної [11] та інших. Разом з цим багато аспектів протидії кіберзлочинності та протидії кіберагресії залишаються недостатньо дослідженими, відсутні науково обґрунтовані рекомендації

щодо виявлення та розслідування конкретних видів кіберзлочинів, ефективного обміну інформацією з міжнародними партнерами.

Виклад основного матеріалу. Основним міжнародним документом у сфері боротьби з кіберзлочинністю є Конвенція про кіберзлочинність, прийнята у 2001 році. Конвенція підписана Україною та ратифікована у 2005 році.

Цим документом передбачені наступні правопорушення:

Заголовок 1 - Правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем

Стаття 2 - Незаконний доступ

Стаття 3 - Нелегальне перехоплення

Стаття 4 - Втручання у дані

Стаття 5 - Втручання у систему

Стаття 6 - Зловживання пристроями

Заголовок 2 - Правопорушення, пов’язані з комп’ютерами

Стаття 7 - Підробка, пов’язана з комп’ютерами

Стаття 8 - Шахрайство, пов’язане з комп’ютерами

Заголовок 3 - Правопорушення, пов’язані зі змістом

Стаття 9 - Правопорушення, пов’язані з дитячою порнографією

Заголовок 4 - Правопорушення, пов’язані з порушенням авторських та суміжних прав

Заголовок 5 - Додаткова відповідальність і санкції

Стаття 11 - Спроба і допомога або співучасть

Стаття 12 - Корпоративна відповідальність [12].

Конвенцією також визначені процедурні питання, що стосуються збереження комп’ютерних даних, розкриття даних про рух інформації, обшуку комп’ютерних даних, перехоплення змісту інформації тощо. Окремим розділом визначені питання міжнародного співробітництва під час розслідування кримінальних правопорушень, пов’язаних з комп’ютерними системами і даними та з метою збирання доказів у електронній формі.

У травні 2022 року у Римі було прийнято Другий додатковий протокол до Конвенції [13], який дозволяє поглиблене співробітництво різних держав та розкриття електронних доказів. Даним протоколом, який теж підписала Україна, розширено використання положень Конвенції, зокрема:

- сфера: кримінальні розслідування та провадження, пов’язані з комп’ютерними системами, а також збір електронних доказів щодо будь-яких кримінальних злочинів;
- пряма співпраця з постачальниками послуг та реєстраторів інших Сторін;
- прискорена співпраця у надзвичайних ситуаціях;
- спільні слідчі групи та спільні розслідування;
- захист даних та інші гарантії.

Усі ці питання вкрай важливі при розслідуванні кіберзлочинів. На жаль, не всі положення Конвенції, особливо ті, що стосуються електронних доказів, імплементовані у чинне законодавство України. Навіть саме поняття “електронні докази” на сьогодні відсутнє в Кримінальному процесуальному кодексі України. Це суттєво ускладнює використання електронних доказів у кримінальних провадженнях не тільки для кібер-, але і для усіх інших кримінальних правопорушень.

У червні 2023 року депутати Європарламенту проголосували за ухвалення нових правил обміну електронними доказами між правоохоронними органами для того, щоб зробити транскордонні розслідування більш ефективними. Адже електронні докази, актуальні для 85 % кримінальних розслідувань, але в 65 % випадків вони походять з іншої країни.

Законодавчий пакет, ухвалений Європейським Парламентом запровадить узгоджену структуру ЄС для обробки електронних доказів, прискорить процес збору доказів і збереже гарантії основних прав. Нові правила дозволять національним органам влади вимагати докази безпосередньо від постачальників послуг в інших державах-членах або вимагати збереження даних протягом 60 днів, щоб відповідні дані не були знищені або втрачені. Закон також вводить обов'язковий 10-денний термін для відповіді на такі запити (вісім годин у екстрених випадках). У рамках того самого пакету євродепутати прийняли директиву, яка зобов'язує постачальників послуг, які пропонують послуги в ЄС, називати призначені установи або законних представників, до яких органи держав-членів можуть надсилати запити щодо електронних доказів [14].

Крім законодавчого забезпечення щодо протидії кіберзлочинності, в різних країнах були утворені окремі підрозділи правоохоронних органів, які спеціалізуються на кіберзлочинах. До найбільш досвідчених та технічно забезпечених слід віднести підрозділи ФБР та Секретної служби США, NHTCU Великобританії, Франції та інших країн.

Для посилення реагування правоохоронних органів на кіберзлочинність та захисту європейських громадян і, таким чином, підприємств і урядів від онлайн-злочинців в ЄС у 2013 році в структурі Європолу був створений Європейський центр боротьби з кіберзлочинністю (ЕС3) [15].

З моменту заснування в ЕС3 зробив значний внесок у боротьбу з кіберзлочинністю та брав участь у багатьох резонансних операціях і сотнях розгортань операційної підтримки.

Новий етап використання інформаційних технологій стався після випуску вірусу Stuxnet у 2012 році, який зруйнував центрифуги на іранському заводі зі збагачення урану. За повідомленнями різноманітних видань вірус був розроблений США та Ізраїлем. У відповідь Іран оголосив, що ця країна готова захищатися у випадку кібервійни і що може завдати більше шкоди, ніж фізичне зіткнення [16].

Ця подія поставила низку запитань щодо міжнародної спільноти, зокрема щодо того, яка кібероперація може бути належною відповідно до конкретних обставин, який вид кібератаки є еквівалентом збройної атаки тощо. Відповіді на дані питання повністю не вирішені і сьогодні та є досить актуальними для України під час військової агресії рф.

Одим з висновків щодо ролі військових формувань у кіберпросторі зроблено на 15-й щорічній Міжнародній конференції з кіберконфліктів (CyCon) у Таллінні. Зокрема представники НАТО зазначили, що почнуть визнавати кіберпростір як "середовище постійного конфлікту". Адже війна росії в Україні підтвердила багато теорій про те, яку роль відіграє кібернетика в конфлікті, зокрема рф широко використовувала кіберпотенціал перед вторгненням в Україну, під час військових дій, і, ймовірно, вона продовжить його використовувати після кінетичної фази цього конфлікту [17].

Сьогодні в Європейському Союзі також активно впроваджується Закон про цифрові послуги (Digital Services Act - DSA) та Закон про цифрові ринки (Digital Market Act - DMA), які спрямовані на створення безпечнішого цифрового простору, де захищені основні права користувачів, і створення рівних умов для бізнесу. Дані нормативні акти визначають чіткі обов'язки та відповідальність для постачальників посередницьких послуг, зокрема для онлайн-платформ, таких як соціальні медіа та ринки щодо видалення незаконного контенту та запобігання поширенню дезінформації. Адже сьогодні, на жаль, у 90 % рекламних повідомлень Інтернету міститься недостовірна інформація, що є основою для різноманітних шахрайських схем [18].

В Україні кримінальну відповідальність за комп'ютерні злочини було передбачено ще у 1994 році – ст. 198-1 КК України 1960 року "Порушення роботи автоматизованих систем". І хоча кількість справ за цією статтею не перевищувала 10 в рік,

загальносвітові тенденції поширення таких злочинів та втрати фінансових установ привернули увагу і вітчизняних практиків та науковців.

Відчутного прориву щодо питань кібербезпеки і боротьби з кіберзлочинністю в Україні вдалося досягти після створення Національного координаційного центру кібербезпеки у 2016 році.

Також слід відзначити прийняття Закону України "Про основні засади забезпечення кібербезпеки України", який набрав чинності 9 травня 2018 року. Законом визначено основні цілі, напрями та принци державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері.

З прийняттям цього закону вперше на законодавчому рівні закріплено визначення основних термінів сфери кібербезпеки, зокрема таких, як: "кібербезпека", "інцидент кібербезпеки", "кіберзагроза", "кіберзахист", "кіберпростір", "кіберзлочинність", "кібероборона" та інші.

Законом визначені також об'єкти кібербезпеки та кіберзахисту, суб'єкти забезпечення кібербезпеки, регламентована національна система кібербезпеки. Саме від ефективного функціонування цієї системи залежить високий рівень захищеності життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, забезпечується сталий розвиток інформаційного суспільства [19].

І нарешті стратегічні напрями забезпечення кібербезпеки були викладені у Стратегії кібербезпеки України, яка затверджена Указом Президента України від 26.08.21 р. № 447/2021.

В Стратегії зокрема зазначено, що "Кіберпростір разом з іншими фізичними просторами визнано одним з можливих театрів воєнних дій. Набирає сили тенденція зі створення кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, що включає виведення з ладу критично важливих об'єктів інфраструктури противника шляхом руйнування інформаційних систем, які управляють такими об'єктами" [20].

Після відкритої агресії рф у 2022 році з'явилися нові виклики, пов'язані з кібервійною. Зазначимо, що активну фазу гібридної війни в інформаційному просторі України рф розпочала ще з часу анексії Криму. Після 2014 року на об'єкти критичної інфраструктури України почали здійснюватися кібератаки, які проводилися різноманітними кіберугрупованнями, що підтримуються урядовими структурами держави-агресора.

Зокрема, слід згадати кібератаки на такі об'єкти, як ЦВК, Закарпаттяобленерго, Бориспільський аеропорт, Укрзалізниця, банківські установи тощо.

Проте справжні військові кібероперації відбувалися напередодні та під час військових дій рф. У доповіді Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України "Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки" зазначено, що "протягом 2022 року Державним центром кіберзахисту було зареєстровано в 2,8 разів більше кіберінцидентів, ніж в 2021 році" [21].

Незважаючи на зусилля ворога, українська інформаційна інфраструктура залишилась діючою, у тому числі банківська система, державні реєстри, системи зв'язку тощо. Значною мірою цього вдалося досягти завдяки своєчасним заходам щодо посилення кібербезпеки та допомозі, наданій нашими союзниками – США, ЄС, Великобританії та іншими цивілізованими країнами.

На жаль, під час воєнного стану не полишили свою діяльність кіберзлочинці, які використовують складну економічну ситуацію громадян у власних цілях. У вітчизняному кіберпросторі одним з найпоширеніших видів правопорушень залишається кібершахрайство. У шахрайських схемах використовуються злам акаунтів у соцмережах, фейкові повідомлення від банку, фішинг та смс-повідомлення про соцвиплати та різноманітні виграші тощо.

Від початку 2023 року в Україні було відкрито більше проваджень за фактом шахрайства, аніж за весь 2021 рік. Про це повідомляє платформа відкритих даних "Опендатабот" .

За січень-квітень 2023 року було зареєстровано вдвічі більше кримінальних проваджень за статтею про шахрайство, ніж за відповідний період 2021 року, та у понад чотири рази більше, ніж за відповідний період торік: 12235 справ та 6385 справ відповідно.

В середньому, на місяць у 2023 відкривається 6683 проваджень за фактами шахрайства. Для порівняння, у відповідний період 2021 фіксувалось 3059 справ про шахрайство на місяць.

Зазначається, що цього року до суду доходить лише кожна дев'ята справа про шахрайство. Так, за січень-квітень 2023 року на судовий розгляд потрапили лише 11 % від загальної кількості зареєстрованих проваджень. Для порівняння, у відповідний період 2022 суд розглядав 14 % справ за статтею 190 КК України, а у той самий період у 2021 році – 19 % [22].

Наприклад у квітні 2023 року правоохоронці викрили шахрайську діяльність 32-річного жителя Дніпра, який ошукав родини військовослужбовців, що перебувають у полоні, загинули чи зникли безвісти.

Підозрюваний перевипускав sim-картки й у такий спосіб отримував доступ до фінансових номерів телефонів військовослужбовців, які перебувають у полоні, загинули чи зникли безвісти. Далі зловмисник заходив до акаунтів онлайн-банкінгу і пересилав гроші на підконтрольні рахунки. Встановлено, що зловмисник "вивів" гроші із рахунків 19 військовослужбовців. Загальна сума збитків склала понад 3 мільйони гривень. Кіберполіцейські у співпраці з працівниками ПриватБанку забезпечили відшкодування збитків на рахунки потерпілих у повному обсязі. Гроші вдалося повернути завдяки оперативному блокуванню рахунків шахрая [23].

Члени організованої злочинної групи для отримання даних банківських карток громадян використовували фішингові посилання продавцям товарів, яких підшукували на майданчиках оголошень і надалі привласнювали гроші з їхніх рахунків.

Людей запевняли, що надсилають посилання для оформлення послуги доставки, просили вказати дані карток нібито для отримання грошей за проданий товар. Дані, введені на шахрайських ресурсах, автоматично ставали відомі фігурантам, завдяки чому гроші потерпілих виводилися на підконтрольні рахунки.

Шістьом фігурантам правоохоронні оголосили підозри, їм може загрожувати до 12-ти років ув'язнення. Встановлюється кількість постраждалих від протиправної діяльності фігурантів. За попередньою інформацією, сума збитків може становити понад два мільйони гривень – ці дані будуть встановлені під час досудового розслідування [24].

Щоденно кіберзлочинці використовують десятки нових схем та методів власного збагачення за рахунок інших громадян та підприємств по всьому світу з використанням мережі Інтернет. Відповідно до п. 8 статті 1 Закону України "Про основні засади забезпечення кібербезпеки України" 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.

При цьому у Кримінальному кодексі України не згадуються поняття кіберпростору, натомість передбачена кримінальна відповідальність у сфері використання комп'ютерів. Тобто конкретного переліку кіберзлочинів на сьогодні не існує. Не використовуються у правовому полі і специфічні терміни щодо поширених кіберзлочинів, таких як фішинг, кардинг, програма-вимагач (ransomware) тощо. Це ускладнює аналіз відповідних тенденцій у кіберпросторі, які досить динамічно змінюються.

Також слід зазначити, що одним з найпоширеніших методів зараження комп'ютерів як окремих користувачів, так і підприємств та організацій є розсилка електронних листів начебто від імені адміністраторів поштових сервісів, суду, банківських установ чи урядових інституцій. Наприклад, за повідомленням CERT-UA, влітку 2023 року були поширені листи за темою "Помічена підозріла активність @ukr.net" та додатком у вигляді PDF-файлу "Попередження про безпеку.pdf" надісланий, начебто, від імені технічної підтримки UKR.NET. Згаданий PDF-документ містить посилання на шахрайський веб-ресурс, що імітує веб-сторінку поштового сервісу.

У випадку автентифікації на підробному веб-сайті, логін та пароль користувача будуть надіслані зловмисникам, що створить передумови для отримання несанкціонованого доступу до електронної поштової скриньки користувача третіми особами. Описана активність відстежується за ідентифікатором UAC-0036, що також відома під назвами COLDRIVER, CALLISTO та здійснюється в інтересах спецслужб російської федерації [25].

На жаль подібні методи використовують і "звичайні" кіберзлочинці, а тому відрізнити підготовку до кіберзлочину від кібератаки спецпідрозділів рф вкрай важко. І на відміну від кіберзлочину, виконавця якого з високою вірогідністю можна ідентифікувати та притягнути до кримінальної відповідальності, хакерські угруповання рф, задіяні у кібервійні, знаходяться під прикриттям держорганів агресора і проводити певні слідчі дії у цьому випадку досить складно.

Правоохоронні органи різних країн також удосконалюють методи боротьби з кіберзлочинністю. Наприклад, Національне агентство по боротьбі зі злочинністю Великобританії проникло на онлайн-ринок злочинців, створивши низку сайтів, які нібито пропонують послуги DDoS-атак за наймом.

Служби DDoS-найму або "завантажувачі" дозволяють користувачам створювати облікові записи та замовляти DDoS-атаки за лічені хвилини. Такі атаки потенційно можуть завдати значної шкоди бізнесу та критичній національній інфраструктурі та часто перешкоджають людям отримати доступ до основних державних послуг.

На сайті, яким зараз керують офіцери, що залучені до постійної програми протидії DDoS-атаки як злочинної послуги, з'явилося оголошення, що попереджає користувачів про те, що їхні дані зібрано та з ними зв'яжуться правоохоронні органи. Усі веб-сайти, створені правоохоронцями, які наразі відвідували близько кількох тисяч людей, були розроблені так, ніби вони пропонують інструменти та послуги, які дозволяють кіберзлочинцям здійснювати ці атаки.

Однак після реєстрації користувачів, замість того, щоб отримати доступ до інструментів кіберзлочинності, їхні дані збираються слідчими. З користувачами, які перебувають у Великобританії, зв'яжеться Національне агентство боротьби зі злочинністю або поліція та попередить їх про участь у кіберзлочинах. Інформація про тих, хто перебуває за кордоном, передається до міжнародних правоохоронних органів.

Видалення сайтів і арешти є ключовими компонентами відповіді правоохоронних органів на цю загрозу [26].

Що стосується боротьби у кіберпросторі з проявами військової агресії, то тут необхідні інші підходи як організаційного, так і правового забезпечення. Наприклад, у США Кіберкомандування армії США об'єднує та проводить операції в кіберпросторі, електромагнітну війну та інформаційні операції, забезпечуючи домінування рішень і свободу дій для дружніх сил у кіберсфері [27]. Кібервійська США мають складну структуру, де кожен підрозділ виконує специфічні операції, починаючи від наступальних операцій і кіберрозвідки, закінчуючи кіберзахистом та психологічними операціями у кіберпросторі.

Тому в умовах воєнного стану в Україні, крім існуючих на сьогодні правоохоронних органів, які протидіють кіберзлочинності, слід сформувати спеціальні підрозділи для захисту від кібервоєнних операцій супротивника та адекватних відповідей щодо його інформаційної інфраструктури.

Кібервійська, або служба кібероборони, повинна перебувати у складі Збройних сил України та серед інших містити структурні підрозділи, які здійснюють кіберрозвідку, проводять спеціальні кібероперації, у тому числі і психологічні на ресурсах супротивника.

Діяльність таких підрозділів повинна бути унормована на законодавчому рівні. Це складне завдання – адже в світі ще немає однозначних відповідей щодо проведення військових дій у кіберпросторі, зокрема щодо їх початку, масштабів, відмежування від традиційних кіберзлочинів тощо. Проте поточна ситуація вимагає вирішення даного питання вже сьогодні.

Рішенням РНБО від 30.12.21 р., введеного в дію Указом Президента України від 01.02.22 р. № 37/2022, затверджено План реалізації Стратегії кібербезпеки України, яким передбачено створення у першому півріччі 2023 року в системі Міністерства оборони України кібервійськ, забезпечивши їх належними фінансовими, кадровими та технічними ресурсами для стримування збройної агресії у кіберпросторі та надання відсічі агресору.

Висновки.

Кількість правопорушень, що вчиняються з використанням інформаційних систем та мереж як в усьому світі, так і в Україні, продовжує зростати. Ускладнюються методи та способи їх вчинення, у тому числі з використанням штучного інтелекту, що потребує відповідної протидії як правоохоронних органів, так і користувачів інформаційних систем. Задля проведення більш системного аналізу та відстеження тенденцій кіберзлочинності доцільно затвердити перелік кримінальних правопорушень, які належать до кіберзлочинів. При цьому кожен вид кіберзлочинів потребує власної методики розслідування та методів профілактики.

Основними напрямами протидії кіберзлочинності слід вважати вдосконалення методів збору, аналізу та зберігання електронних доказів, покращення міжнародного співробітництва та посилення технологічного і кадрового потенціалу спеціальних підрозділів.

Що стосується питань забезпечення кібероборони України, то найактуальнішим на сьогодні залишається формування вітчизняних кібервійськ у відповідності до Рішення РНБО України.

При створенні кібервійськ необхідно використати практичний досвід аналогічних формувань НАТО та США та в подальшому діяти в чіткій координації з ними.

Використана література

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

2. One of the world's biggest hacker forums taken down. URL: https://www.europol.europa.eu/media-press/newsroom/news/one-of-world%E2%80%99s-biggest-hacker-forums-taken-down

3. Ахтырская Н. Формы противодействия расследованию преступлений, совершаемых в сфере компьютерных технологий. Компьютерная преступность и кибертерроризм: сборник научных работ. Вашингтон, Запорожье, 2004. С. 258-267.

4. Комп'ютерна злочинність: навч. посібник / Б.П. Діленчук, В.В. Бут, В.Д. Гавловський, М.В. Гуцалюк, Б.В. Романюк. Київ: Атіка, 2002. 240 с.

5. 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.

6. Тітуніна К.В. Характеристика комп'ютерних злочинів, учинених із використанням мережі Інтернет: аналіз матеріалів анкетування. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. Київ: МНДЦ, 2009. № 21. С. 307-314.

7. Електронні (цифрові) докази у кримінальних провадженнях: методичні рекомендації / М.В. Гуцалюк, В.Д. Гавловський, В.Г. Хахановський та ін. / за заг. ред. О.В. Корнейка. Вид. 2-ге, доп. Київ: Вид-во Нац. акад. внутр. справ, 2020. 104 с.

8. Шеломенцев В.П. Поняття та сутність кібернетичної атаки. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2011. № 25 – 26. С. 337-344.

9. Волков О. Початковий етап розслідування створення використання, розповсюдження або збуту шкідливих програмних чи технічних засобів: автореф. дис. ...канд. юрид. наук. Дніпро, 2023. С. 26. URL: https://dduvs.in.ua/wp-content/uploads/2023/05/5_3.pdf

10. Яцишин М. Міжнародно-правове співробітництво у сфері боротьби з кіберзлочинністю. URL: http://scc.univ.kiev.ua/upload/iblock/bd0/aref_Yatsyshyn%20M.Y.pdf

11. Кравцова М. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ: автореф. дис. ...канд. юрид. наук. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/8da73c50-5c7d-4ae4-85b4-30fa7107489f/content

12. Конвенція про кіберзлочинність. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

13. Ахтирська Н., Гуцалюк М. Правові засоби боротьби з кіберзагрозами під час воєнного стану в світлі використання механізмів Другого додаткового протоколу до Конвенції про кіберзлочинність: матеріали Міжнародної науково-практичної конференції *Актуальні питання розвитку юридичної науки та практики*, м. Київ, 12 трав. 2022 р. / за заг. ред. д.ю.н., акад. НАПрН України О.П. Орлюк, к.ю.н., доц. Г.З. Остапенко, к.ю.н. А.В. Айдинян. Київ, 2022. С. 283-286.

14. Electronic evidence: new rules to speed up cross-border criminal investigations. URL: https://www.europarl.europa.eu/news/en/press-room/20230609IPR96203/electronic-evidence-new-rules-to-speed-up-cross-border-criminal-investigations

15. European Cybercrime Centre. URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

16. Declarations of Cyberwar. What the revelations about the U.S. Israeli origin of Stuxnet mean for warfare. URL: https://spectrum.ieee.org/declarations-of-cyberwar#toggle-gdpr

17. NATO: Military cyber defenders need to be present on networks during peacetime. URL: https://therecord.media/nato-peacetime-cyberdefense-david-van-weel-cycon

18. The Digital Services Act package. URL: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

19. Науково-практичний коментар Закону України "Про основні засади забезпечення кібербезпеки України" (станом на 1 січня 2019 року) / М.В. Гуцалюк та ін. / за ред. М.В. Гребенюка. Київ: Національна академія прокуратури України, 2019. 220 с.

20. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року “Про Стратегію кібербезпеки України”: Указ Президента України від 26.08.21 р. № 447/2021. URL: https:// www. president.gov.ua/documents/4472021-40013

21. У 2022 році кількість зареєстрованих кіберінцидентів виросла майже втричі: звіт. URL: https://cip.gov.ua/ua/news/u-2022-roci-kilkist-zareyestrovanikh-kiberincidentiv-virosla-maizhe-vtrichi-zvit

22. Пандемія шахрайства: в Україні зафіксовано рекордна активність шахраїв. URL: https://opendatabot.ua/analytics/fraud-pandemic

23. Шахрай “вивів” гроші із рахунків 19 військовослужбовців. URL: https://ua.Korrespondent.net/ukraine/4597499-shakhrai-vyviv-hroshi-iz-rakhunkiv-19-viiskovosluzhbovtsiv

24. Привласнили понад 2 мільйони гривень за допомогою фішингу: кіберполіція викрила організовану злочинну групу. URL: https://cyberpolice.gov.ua/news/pryvlasnyly-ponad--miljony-gryven-za-dopomogoyu-fishyngu-kiberpolicziya-vykryla-organizovanu-zlochynnu-grupu-7102

25. Цільові кібератаки UAC-0036 (COLDRIVER) у відношенні користувачів сервісу UKR.NET (CERT-UA#6858). URL: https://cert.gov.ua/article/4928679?fbclid=IwAR0qT-uzXZ8rgFKzyZY10QNRmHpYgjeGYM58KkV_3SO69gzHr0YL5_Mruek

26. NCA проникає на ринок кіберзлочинності за допомогою прихованих сайтів DdoS. URL: https://www.nationalcrimeagency.gov.uk/news/nca-infiltrates-cyber-crime-market-with-disguised-ddos-sites

27. US Army Cyber Command. URL: https://www.arcyber.army.mil

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