АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРЗЛОЧИННОСТІ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

ДУМЧИКОВ Михайло Олександрович - кандидат юридичних наук, старший викладач кафедри кримінально-правових дисциплін та судочинства Навчально-наукового інституту права Сумського державного університету
ORCID: https://orcid.org/0000-0002-4244-2419,
e-mail: m.dumchykov@yur.sumdu.edu.ua
АНДРІЄНКО Р.І. - студент 2-го курсу магістратури Навчально-наукового інституту права Сумського державного університету
ORCID ID: https://orcid.org/0000-0003-2950-3528
e-mail: boriska2018@ukr.net
УДК 343.2/.7(043.5)
DOI 10.32782/LAW.UA.2023.4.26

Глобалізація та стрімкий розвиток комп'ютерних та інформаційно-телекомунікаційних технологій призвели до виникнення нового виду правопорушень у кіберпросторі. Авторами пропонується аналіз актуального стану злочинності у кіберпросторі на теренах України протягом останніх 10 років. Наведено огляд сучасних заходів протидії кіберзлочинності в Україні та за кордоном. Визначено деякі рекомендації щодо забезпечення корпоративної кібербезпеки та перспективні напрямки досліджень.

Наголошується, що актуальною проблемою останнього десятиліття є колосальне зростання кіберзлочинності у всій світовій спільності. В Україні також спостерігається негативна тенденція цього негативного явища. Найважливіше значення має вдосконалення заходів протидії кіберзлочинності. У статті позначено тенденції кіберзлочинності в останні роки, а також заходи, що вживаються державою протидії аналізованому негативному соціальному явищу. Підкреслюється, що Україна виступає за консолідацію та об'єднання зусиль світового співтовариства у протидії виду злочинності, що розглядається.

Водночас очевидною є необхідність подальшого вдосконалення заходів протидії кіберзлочинності. Таким чином, кіберзлочинність є глобальним викликом суспільству. У зв'язку з цим, очевидна необхідність удосконалення та впровадження нових заходів протидії злочинності у кіберпросторі. В даний час найважливіше значення має: удосконалення діяльності правоохоронних органів; ефективна організація міжнародного та міжгалузевого співпраці правоохоронних, державних органів, банківського сектора та приватних компаній у протидії кіберзлочинності; удосконалення віктимологічної профілактики.

Ключові слова: кіберзлочинність, кіберзлочин, кіберпростір, злочинність у кіберпросторі, кримінальні правопорушення у кіберпросторі.

Постановка проблеми

Науково-технологічний прогрес у світі призвів до з'яви значної кількості нових технологій, які впроваджують численні інновації у громадське життя людей. Визначенням ключової точки розвитку стало виникнення перших комп'ютерів та комп'ютерних мереж, що відкрило широкі можливості для людства. З урахуванням усіх аспектів прогресу та інших впливових факторів, можна констатувати закономірну появу нового виду кримінальності в кіберпросторі.

Кіберзлочинність стала надзвичайно актуальною проблемою сучасного суспільства, про що свідчать міжнародні новини, статис-

тика кримінальності, проблематика кримінального права та аспекти кримінального процесу. Це пов'язано з тим, що як явище, кіберзлочинність є вкрай специфічною категорією, що постійно розвивається паралельно із технічним прогресом.

Стан дослідження проблеми

У сучасній науці цьому питанню також приділили увагу такі науковці як Карчевська Ю. С., Болгар Т. М., Дзюндзюк В. Б., Кураков Л. П., Голубєв В. А., Рассолов І. М., Щербаков Е. С., Трофимчук В. С., Дубов Д. В., Користін О. Є., Кравцова М. О., Літвінов М. Ю., Котляревський О. І., Кузнєцов В. В., Лукашевич В. Г., Машуков В. М. та інші.

Мета і завдання дослідження

Метою статті є дослідження феномену кіберзлочинності, визначення всіх особливостей та видів кримінальних правопорушень у кіберпросторі на конкретних прикладах, надання загальної характеристики суміжним явищам, визначення суспільної небезпечності кіберзлочинності, а також вивчення шляхів протидії цій кримінальній категорії.

Виклад основного матеріалу

Протягом всієї відомої історії людства, існувала велика кількість різних злочинів, сутність яких не змінилися і до сьогодні, чого не можна сказати про кіберзлочинність, так як явище це відносно новітнє, і своїй появі повністю завдячує технологічному прогресу.

Періодом виникнення кіберзлочинності прийнято вважати 1970-ті роки, саме в цей час почали з'являтися перші кіберзлочинці, яких іменували «хакери». Злочинний феномен був дуже масовим та швидко поширився по всьому світу, через що достовірно не відомо хто був його першовідкривачем, однак у більшості джерел, першим кіберзлочинцем називають Джона Дрейпера, він же перший хто займався фрикінгом, тобто був телефонним хакером. В ті роки Інтернет, який сьогодні є основною частиною кіберпростору, ще не був явищем масовим, отже перші хакери діяли в телефонній мережі. Про масштабність феномену свідчить і той факт, що фрикінгом в свій час займалися приміром Стів Джобс та Стів Возняк, які в майбутньому стали засновниками компанії «Apple Computers». Отже, 70-ті роки XX століття є відправною точкою в історії кіберзлочинності. З цього часу активно починають розвиватися інформаційні технології, Інтернет, протягом десяти років, стає доступним для простих користувачів, можливостей в кіберпросторі стало більше, що не могло не зацікавити кіберзочинців. Так приміром у 1983 році зафіксовано перший факт арешту, за злочин вчинений в Інтернеті. Кілька підлітків з США, штату Мілуокі вчинили перший зареєстрований Інтернет-злом. Ці підлітки за дев'ять днів зламали 60 комп'ютерів, в тому числі комп'ютери Лос-Аламоської державної лабораторії. Важливою деталлю цього злочину є те, що ці молоді люди визнали себе угрупуванням та діяли під іменем «Група 414», що свідчило про популяризацію кіберзлочинності. Для членів цієї групи все закінчилось умовним строком, після того як заарештований підліток дав проти них свідчення. У 1984 році Фредом Коеном були опубліковані відомості про шкідливі комп'ютерні програми, які здатні до самостійного поширення та розмноження. Так в обіг увійшло словосполучення «комп'ютерний вірус» [1].

З масовістю кримінальні правопорушення у кіберпросторі дуже сильно почав зростати і їх рівень небезпечності. Чудовим прикладом є випадок, що стався у 1998 році, коли підліток, віком усього 12 років, зміг отримати доступ в комп'ютерну систему контролю водоспуску на дамбі Теодора Рузвельта в штаті Арізона. Таким чином він міг без будь-яких перешкод відкрити злив та затопити ціле місто Темп, в якому ,на той момент, населення було приблизно 1 мільйон людей. Сам факт такого злому, згодом, посприяв появі термінів «Інтернет-тероризм», «комп'ютерний тероризм», «кібертероризм» [1].

Протягом наступних років поширеності набувають масові кібератаки. Велика кількість таких атак мають транснаціональний характер, а причини найчастіше політичні.

Причиною масовості став той факт, що державні структури багатьох країн, завдяки розвитку інформаційних технологій, також діяли в кіберпросторі, так наприкінці XX століття в Інтернеті створювались різні

державні сайти, до мережі мали доступ державні сервери з великою кількістю інформації, крім того з'явилося багато ресурсів з новинами, а також сайти національних університетів, міжнародні сервіси онлайн-торгівлі тощо. Така велика кількість та різноманітність ресурсів в мережі давала змогу не лише поширювати якісь політичні ідеї, а і безпосередньо діяти в інтересах таких ідей, активно захищаючи їх. Таким чином виник «хактивізм» - активізм в кіберпросторі [2].

Таким чином до початку XXI століття сформувалися всі основні тенденції, напрямки та форми діяльності кіберзлочинців. З часу прийняття першого комп'ютерного закону, нормативна база всіх країн світу з цього питання значно розширилась. Проблема сьогодні регулюється великою кількістю як державних, так і міжнародних правових актів.

Кримінальні правопорушення у кіберпрострі, які вчиняються сьогодні відрізняються від тих, що були в минулому столітті, лише своїми масштабами та наслідками, особливістю варто виділити той факт, що технологічні інновації лише допомагають знаходити нові способи вчинення вже відомих злочинів.

Слід відмітити також, що методи боротьби зі злочинами в кіберпросторі постійно розвиваються та приносять позитивні результати, і з часом цей простір поступово стає більш врегульованим та безпечним. Хоча кіберзлочинність, як кримінальна категорія, також продовжує активно розвиватися і множитись, і процес цей неймовірно швидкий, адже відбувається в міжнародних масштабах, тому загальна статистика, з цього питання, на момент 2019 року лишається невтішною.

Основною проблемою злочинності в кіберпросторі є сам факт існування цього явища, в сукупності з усіма його особливостями та специфікою, які забезпечують постійний розвиток цієї кримінальної категорії. Як результат, кіберзлочинність на сьогодні є одним з найбільших джерел суспільної небезпеки.

Юридичний склад кримінальних правопорушень у кіберпросторі досить специфічний, через що кожен вид таких злочинів має велику кількість підвидів, мета, способи вчинення і наслідки яких дуже різняться.

Відповідно до цього можна виділити головну особливість кримінальних правопорушень у кіберпросторі – їх різноманітність. Ця їх властивість пояснюється тим, що вчинення одних і тих самих дій, в залежності від умислу і мети, може призвести до різних наслідків. Крім того, технічний прогрес та особливості таких злочинів дозволяють знаходити нові шляхи до їх вчинення, наприклад використавши спеціальні навички, знання, або застосувати спеціальне обладнання тощо [3].

Говорячи про спеціальні навички та знання, варто виділити ще одну особливість – професіоналізм кіберзлочинців. Значна кількість злочинців у кіберпросторі є справжніми хакерами-професіоналами. Такі люди навчилися заробляти на своїх здібностях і вміннях, просувати свої політичні ідеї та реалізовувати особисті потреби, шляхом вчинення кримінальних правопорушень у кіберпросторі. Дехто може красти гроші в мережі чи за допомогою спеціальних засобів, хтось продає свої послуги або заробляє іншим чином. Якщо злочинцем керують політичні ідеї та інтереси, він зробить усе щоб їх відстоювати та просувати, причому робитиме він це професіонально, не без наслідків для інших. Декому просто цікаво проявити свої здібності, здобути визнання у кіберпросторі. Об'єднують всіх цих людей різні знання та вміння, свого роду професіоналізм, які допомагають їм віднаходити нові способи та можливості вчинення різних кримінальних правопорушень у кіберпросторі. Важливе значення на це також справила ідеологія та культура хакерів, які популяризують саморозвиток та стимулюють до активних дій і самореалізації [1].

Однак, ідеологія також посприяла формуванню іншої особливості, пов'язаної також з доступністю кіберпростору для кожного. Наразі комп'ютерами та різними мережами користується більше половини населення Землі. Серед такої великої кількості людей, різних за віком, соціальним статусом тощо, знаходяться ті хто без особливого умислу вчиняють кримінальні правопорушення у кіберпросторі. Можливо хтось просто надихнувся ідеологією хакерів, або наприклад в силу вікових особливостей, не усвідомлюю-

чи свого діяння, вчиняє кримінальні правопорушення у кіберпросторі. Крім того були прецеденти коли такі злочини вчинялися з необережності або недбалості [4]. Звідки випливає наступна особливість, яка полягає в швидкому поширенні явища кіберзлочинності.

Не зважаючи на те професійний хакер чи простий аматор вчиняє кримінальне правопорушення у кіберпросторі, так чи інакше в мережі вони, хоч і в різній мірі, але наділені певною анонімністю, що є технічною особливістю кіберпростору. Серед інших таких особливостей обов'язково слід виділити транснаціональність, через що людина, яка має доступ до мережі може вчинити кіберзлочин в будь-якій частині планети, знаходячись в іншому місці.

Важливою властивістю кіберзлочинності є те, що зазвичай кримінальні правопорушення у кіберпросторі характеризуються сукупністю або повторністю, в залежності умислу. Відповідно до цього існують цілі схеми, в яких одні кримінальні правопорушення у кіберпросторі забезпечують виконання інших, або їх сукупність дозволяє досягти мети.

Сукупність всіх цих особливостей формує ще одну. Вона полягає в тому, що природа кримінальних правопорушень у кіберпросторі робить дуже складними пов'язані з ними процеси. Особливо складними є попередження, розслідування та припинення таких злочинів [5]. Серед іншого, труднощі також виникають на етапі правової оцінки діянь у кіберпросторі, класифікація ускладнена тим, що одне і те саме діяння може мати кілька різних наслідків, об'єктивна сторона може бути зовсім іншою, а крім того суб'єктивну сторону дуже встановити [15]. Відповідно до цього, боротьба із кіберзлочинністю це дуже складний процес, як з точки зору права, так і на практиці, тому цей процес потребує високого професіоналізму на всіх етапах та часто залучення значних матеріальних витрат. Також це пов'язано з тим, що сфера кримінальні правопорушення у кіберпросторі постійно розвивається.

Серед інших проблем слід виділити те, що кіберпростір також використовується для вчинення інших злочинів. Наприклад дуже поширені випадки порушення конституційних прав і свобод людей. Найчастіше порушуються саме особисті права на недоторканість приватного життя, таємницю листування, авторські та інші суміжні права. Нерідко вчиняються злочини проти честі і гідності особи, та проти суспільної моральності та порядку. Крім того, Інтернет використовується для продажу нелегальних товарів, таких як наркотики, зброя, інформація тощо. Дуже небезпечними слід виділити злочини проти безпеки держави, приміром кіберпростір використовують для шпигунства, а особливо небезпечним є кібертероризм [1].

На особливу увагу заслуговує випадок використання мережі для здійснення злочину проти життя і здоров'я. Перший такий випадок зафіксований в США. 1998 року, в лютому, поранений свідок злочину був поміщений в закритий госпіталь на території військової бази. Злочинці, використавши Інтернет, змінили роботу кардіостимулятора й апарату вентиляції легень , що призвело до смерті [1].

Проблема суспільної небезпечності кримінальні правопорушення у кіберпросторі полягає в тому, що їх особливості та різноманітність призводять до завдання різної матеріальної і нематеріальної шкоди. Транснаціональність кримінальні правопорушення у кіберпросторі може призвести до політичних наслідків, що в свою чергу є особливо небезпечним. Суспільні відносини, які були порушені кримінальним правопорушенням у кіберпросторі, дуже важко, а інколи неможливо відновити. Крім того, боротьба з кіберзлочинністю теж вимагає значних затрат, що не завжди виправдовується. Відповідно до цього, рівень суспільної небезпечності кримінальні правопорушення у кіберпросторі є дуже високим та на даний момент зростає.

Розглядаючи кримінальні правопорушення у кіберпросторі в контексті тіньової економіки дуже важко переоцінити їх значення в цій системі. Економічний аспект злочинів в мережі стосується не лише фінансових збитків, завданих ними, а і мотивів та причин таких злочинів. Значна частина кримінальні правопорушення у кіберпросторі мають посередньо та безпосередньо економічний характер. Деякі з них направлені на отримання неправомірного прибутку

шляхом викрадення грошей або інформації з метою її продажу. Інші кримінальні правопорушення у кіберпросторі, які вчиняються з комерційних мотивів стосуються надання неправомірних послуг, пов'язаних з кіберпростором, наприклад псування серверів конкурентів, чи налагодження нелегальних фінансових структур в мережі [5].

Кіберпростір можна вважати однією з основних ланок у всій системі тіньової економіки, це пов'язано з рядом його особливостей, які дають можливість негласно здійснювати різні економічні операції, такі що необмежені і не контролюються державою. Інтернет сьогодні використовують для здійснення легальних і нелегальних фінансових трансферів, які направлені на підтримку злочинних діянь. Гроші, отримані злочинним шляхом, сьогодні зберігають і використовують в кіберпросторі. Світова мережа стала каналом фінансування тероризму [5].

Кіберпростір дає змогу не лише отримувати прибуток, а і відмивати фінанси, отримуючи на виході «чистий» прибуток з мережі. Способів відмивання грошей за допомогою Інтернету дуже багато, з цією метою створюють різні проекти, онлайн-фонди, Інтернет-компанії та інші мережеві фінансові структури, через які проводять незаконні кошти, тим самим перетворюючи їх на легальний прибуток [6, с. 175].

Також, значущим джерелом тіньової економіки є чорний ринок, який існує в мережі. В Інтернеті сьогодні існують ціль маркетплейси (онлайн-маркети) незаконних товарів. На таких ресурсах продається як інформація, так і реальні речі, наприклад зброя або наркотики. Крім того, сьогодні в інтернеті можна замовити послуги злочинця, навіть найняти вбивцю. Найбільшим осередком таких маркетплейсів є даркнет, в цій частині мережі існують спеціалізовані ресурси з забороненим контентом і товарами. Варто відмітити, що і на легальних ресурсах іноді можна знайти заборонені товари, це пов'язано з глобальністю Інтернету, а отже навіть легальні платформи можуть бути джерелом тіньової економіки [7].

Особливим та значущим суміжним феноменом між кіберпростором і тіньовою економікою є криптовалюта. Це один з різновидів електронних грошей, в основі якого лежить технологія криптографії – шифрування даних. Особливістю цих грошей є анонімність процесів їх використання, а також децентралізація і захищеність їх використання, адже ця валюта не регулюється жодною країною чи банком світу, а будь які дії з її використанням шифруються. Сьогодні існує велика кількість різної криптовалюти, що значно облегшило будь-які нелегальні економічні дії в мережі, наприклад найвідоміша. Цьому також сприяє той факт, що в більшій частині світу криптовалюта є легальною, при цьому майже не регулюється законами, відповідно до чого, набагато простіше стали процеси відмивання і транзакцій грошей з використанням Інтернету. Електронні гаманці криптовалюти також відкрили нові можливості для зберігання грошей в інтернеті, транзакції здійснені за допомогою таких електронних грошей фактично неможливо відстежувати, а так як криптовалюта є по суті комп'ютерними файлами, її можна накопичувати на різних носіях інформації, навіть на переносних, відповідно до чого з'являється можливість зберігати та використовувати її за межами кіберпростору [8, с. 133].

Отже, економічне значення кіберзлочинності, а також кіберпростору є дуже високим. Сукупність технічних, економічних та правових особливостей роблять Інтернет майже ідеальним місцем, та фактично центром тіньової економіки сього світу.

Про сучасний стан кіберзлочинності свідчить невтішна статистика, «гучні» новини та підрахунки фінансових збитків. Приміром 28 жовтня 2019 року, в Грузії відбулася одна з найбільших кібератак в історії країни. Трохи більше ніж за добу, хакери зламали приблизно 15 тисяч сайтів та встановили дефейси з політичним вмістом. Таким чином політичні мотиви призвели до завдання значної економічної шкоди [9, с. 26]. Не дивлячись на світову практику боротьби з кіберзлочинністю, сьогодні такі масові випадки є нерідкістю.

Дуже важливим аспектом в регулюванні кіберпростору є саме юридичний. В більшості країн світу, це питання стандартно регулюється законами про кримінальну відповідальність, процесуальними та суміжними законами, а також іншими актами. Особливе

значення мають міжнародні акти, так як проблема кіберзлочинності є транснаціональною.

В Україні кіберпростір регулюється великою кількістю різних актів. До основних варто віднести Закони України «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про телекомунікації», «Конвенція про кіберзлочинність», а також Кримінальний і Кримінальний Процесуальний Кодекси України [10]. Зазначені закони по більшій мірі дають визначення усього кіберпростору та окремих його ланок, а також регулюють окремі питання його функціонування, однак закон про основні засади забезпечення кібербезпеки, крім того, також встановлює принципи та особливості боротьби з кіберзлочинністю. «Конвенція про кіберзлочинність» дуже детально регулює питання протидії кіберзлочинності, особливо на міжнародному рівні [11]. Кримінальний кодекс встановлює вичерпний перелік таких злочинів [12]. Щодо Кримінально Процесуального Кодексу, в ньому питання кримінальні правопорушення у кіберпросторі врегульовано досить загально, на рівні з іншими злочинами, не враховуючи особливостей цього явища [13].

В Україні сьогодні існує Стратегія кібербезпеки України, затверджена відповідним Указом Президента. Особливістю слід відзначити, що в її змісті, кіберпростір прирівняли до окремої сфери ведення бойових дій, на рівні з землею, повітрям чи морем [14].

На перший погляд питання кримінальні правопорушення у кіберпросторі достатньо врегульоване, однак саме питання протидії має декілька серйозних прогалин, по більшій мірі це стосується саме недосконалості кримінального процесу. Сьогодні ця правова сфера активно розвивається, реформи направлені на посилення правового забезпечення кібербезпеки та протидії кримінальним правопорушенням у кіберпросторі.

Світова практика свідчить про те, що найбільших успіхів, в правовому забезпеченні кібербезпеки, досягла Америка. Яскравий приклад – Закон «The Computer Fraud and Abuse Act», прийнятий ще в 1986 році, він зазнав великої кількості змін і діє навіть в наш час. Про його якість свідчить той факт, що протягом довгого часу його критикували за те що він надто детально регулює різні аспекти, через що в 2011 році навіть були прийняті поправки, які трохи узагальнили та уточнили деякі моменти [15]. Цей закон не є еталоном, однак досить якісний і заслуговує бути прикладом для законодавства інших країн.

Реформи, які тривають сьогодні повністю виправдані і є необхідними, однак в ідеалі, правова сфера повинна враховувати не лише економічні та соціальні аспекти кіберзлочинності, а і технічні, особливо в питаннях процесуального законодавства.

Узагальнюючи матеріали дослідження, можна впевнено сказати, що проблема кіберзлочинності є однією з найважливіших сьогодні, та такою що потребує негайного втручання в її вирішення. Історичний аспект, а також сучасний стан цього питання свідчать про те, що явище кіберзлочинності активно розвивається. Як кримінальна категорія, злочини в кіберпросторі є джерелом високого рівня суспільної небезпеки, що напряму пов'язано з їх особливостями, різноманітністю та проблемами боротьби з ними. Про глобальність проблеми свідчить і той факт, що сьогодні весь світ об'єднує зусилля для протидії кримінальним правопорушенням у кіберпросторі.

Найважливіші питання в боротьбі з кіберзлочинністю – регулювання кіберпростору державою, та повне, з її боку, забезпечення боротьби з кримінальним правопорушенням у кіберпросторі. Методи регулювання та протидії кіберзлочинності повинні включати не лише правову, матеріальну, технічну, наукову, а й інші види підтримки. В ідеалі, кіберпростір повинен стати окремою правовою категорією в системі державного управління, та всесторонньо бути врегульованим, адже з кожним днем він все більше впроваджується в повсякденну діяльність суспільства і держави, що в свою чергу сприяє розвитку кіберзлочинності.

Сьогодні в Україні, як і в світі в цілому, рівень кібербезпеки явно недостатній. Звісно міжнародна співпраця сприяє вирішенню цієї проблеми, однак найважливіші дії повинні бути здійснені в середині країни, щоб згодом передати світу наш успішний досвід боротьби з кіберзлочинністю і регулювання

кіберпростору. Для цього держава і суспільство повинно об'єднати свої зусилля та зробити все можливе для подолання проблеми кіберзлочинності.

Лишається велика кількість питань, які необхідно вирішити науковцям і працівникам сфери права, однак очевидним є те, що вирішувати їх потрібно негайно.

Література

1. Дзюндзюк В. Б. Поява і розвиток кіберзлочинності. URL: http://www.kbuapa.kharkov.ua/e-book/db/2013-1/doc/1/01.pdf.
2. The MIT Press Journals : Terror and Play, or What Was Hacktivism? (Peter Krapp). URL : https://clck.ru/K5gJj.
3. Анастасія Г.В. Безпечне місто : Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби. URL: http://safe-city.com.ua/kiberzlochynnist-u-vsih-yiyi-proyavah-vydy-naslidky-ta-sposoby-borotby/.
4. Кравцова М. О. Сучасний стан і напрями протидії кіберзлочинності в Україні. URL: https://clck.ru/K5g7G.
5. Пушкаренко П. І. Кіберзлочинність як новітній феномен тіньової економіки. URL: https://clck.ru/K5g9r.
6. Іванченко О. М. Кримінологічна характеристика кіберзлочинності, запобігання кіберзлочинності на національному рівні. Актуальні проблеми вітчизняної юриспруденції. 2016. № 3. С. 172–177.
7. Мельник С.В. До проблеми формування понятійно-термінологічного апарату кібербезпеки URL : http://www.nbuv.gov.ua/portal/natural/Znpviknu/2011_30/Zbirnik_30_28.pdf.
8. Проценко А. Т. Правовий статус віртуальних валют: світовий досвід та українські реалії. Право і суспільство. 2016. № 2. с. 130–134.
9. Карчева Г.Т. Віртуальні інноваційні валюти як валюти майбутнього. Фінансовий простір. 2015. № 2. С. 24–30.
10. Правове регулювання «інтернет – засобів масової інформації». Офіційний вебресурс Міністерства юстиції України. URL: https://minjust.gov.ua/m/str_24640.
11. Конвенція про кіберзлочинність від 23.11.2001 р. URL: http://zakon.rada.gov.ua/laws/show/994_575.

SUMMARY

Globalization and the rapid development of computer and information and telecommunication technologies have led to the emergence of a new type of crime in cyberspace. The authors offer an analysis of the current state of crime in cyberspace in Ukraine over the past 10 years. An overview of modern cybercrime countermeasures in Ukraine and abroad is presented. Some recommendations for ensuring corporate cyber security and promising areas of research are defined.

It is emphasized that the urgent problem of the last decade is the colossal growth of cybercrime in the entire global community. A negative trend of this negative phenomenon is also observed in Ukraine. Improving countermeasures against cybercrime is of the utmost importance. The article indicates trends in cybercrime in recent years, as well as measures taken by the state to counter the analyzed negative social phenomenon. It is emphasized that Ukraine advocates the consolidation and unification of the efforts of the world community in combating the type of crime under consideration.

At the same time, the need for further improvement of countermeasures against cybercrime is obvious. Thus, cybercrime is a global challenge to society. In this regard, there is an obvious need to improve and implement new measures to combat crime in cyberspace. Currently, the most important are: improving the activities of law enforcement agencies; effective organization of international and cross-industry cooperation of law enforcement, state bodies, the banking sector and private companies in countering cybercrime; improvement of victimological prevention.

Keywords: cybercrime, cybercrime, cyberspace, crime in cyberspace, criminal offenses in cyberspace.

12. Кримінальний кодекс України від 05.04.2001 р. URL : http://zakon.rada.gov.ua/laws/show/2341-14.
13. Кримінальний Процесуальний Кодекс України від 13.04.2012 р. URL : https://zakon.rada.gov.ua/laws/main/4651-17.
14. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15.03.2016 р. URL: https://zakon.rada.gov.ua/laws/show/96/2016.
15. Search Compliance : Computer Fraud and Abuse Act (CFAA) URL: https://clck.ru/K5gC9.