Cybercrime as a new phenomenon and a source of high levels of public danger

Кіберзлочинність як новітній феномен та джерело високого рівня суспільної небезпеки

Vladimir Pakhomov, Mikhail Dumchikov

Keywords:

cybersecurity, cybercrime, criminal offenses, cybercrime, computer crimes.

Ключові слова:

кібербезпека, кіберзлочинність, кримінальні правопорушення, кіберзлочин, комп'ютерні злочини.

Актуальність теми дослідження. Світовий науково-технологічний прогрес призвів до появи великої кількості нових технологій. Такі технології впровадили велику кількість інновацій в суспільне життя людей. Кіберзлочинність сьогодні є дуже актуальною проблемою суспільства. Про її актуальність свідчать новини по всьому світу, кримінальна статистика, проблемні питання науці кримінального права, а також проблеми в кримінальному процесі. Все це пов'язано з тим, що як явище, кіберзлочинність є дуже специфічною категорією, яка постійно розвивається паралельно з технічним прогресом.

Метою дослідження є дослідження феномену кіберзлочинності, визначення всіх особливостей та видів кіберзлочинів на конкретних прикладах, надання загальної характеристики суміжним явищам, визначення суспільної небезпечності кіберзлочинності, а також вивчення шляхів протидії цій кримінальній категорії. Крім того, на меті привернути більше уваги до цієї проблеми.

Об'єктом дослідження є суспільні відносини, що виникають у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

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.

Станом на 2020 рік, майже з будь-якої точки світу, будь-хто має доступ до мережі «даркнет» – це окрема мережа в Інтернеті, яка згідно з різними даними стала місцем опосередкування кіберзлочинців. Саме в цій частині інтернету відбувається велика кількість правопорушень, тут же існують торгові платформи з нелегальними товарами та послугами, з протиправними намірами створюють закриті канали зв'язку, а велика кількість користувачів даркнету, завдяки використанню спеціальних засобів, є анонімами. Найбільша проблема полягає саме в доступності такої мережі, що часто сприяє поширенню кіберзлочинності[1]2.

Поняття кіберзлочину та суміжні поняття визначені в Законі 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[2].

Кіберпростір - середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних.

Всі види кіберзлочинів зазначені у Кримінальному Кодексі України (далі – ККУ), розділі XVI – Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку[3].

Стаття 361 – Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Ця стаття передбачає втручання,

---

1 DGL.RU : На темной стороне интернета: Что такое Dark Web и Deep Web? [Електронний ресурс] – Режим доступу до ресурсу: https://clck.ru/K5gLD.

2 Про основні засади забезпечення кібербезпеки України : Закон Уркїни від 05.10.2017 р. [Електронний ресурс] – Режим доступу до ресурсу: https://clck.ru/K5gGV.

3 Кримінальний кодекс України від 05.04.2001 [Електронний ресурс] – Режим доступу до ресурсу: http://zakon.rada.gov.ua/laws/show/2341-14.

яке призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу її обробки або порушення її маршрутизації.

Відповідно до статті 361, найпоширенішими злочинами є злом, або несанкціоновані модифікації приладів чи програм[1]. Злом може бути направлений безпосередньо на комп'ютери, інші електронно-обчислювальні машини та їх системи, або на комп'ютерні мережі, наприклад Інтернет, та інші мережі електрозв'язку[2].

Методів злому дуже багато, однак можна виділити основні, принцип роботи яких лежить в основі інших. Найпоширенішим методом є Brute-force (Брутфорс). Його сутність полягає в простому переборі даних для авторизації – логінів, паролів тощо[12]. Цей метод дозволяє отримати доступ до різних мереж, електронних ресурсів, захищених приладів та зашифрованої інформації. Наразі, у відкритому доступі) існує велика кількість баз даних з інформацією для бруту. Найефективнішим та найнебезпечнішим методом вважається 0day (zero day) – атака (вразливість) нульового дня. Цей метод оснований на пошуку прогалин в системних кодах (основах роботи систем, приладів тощо).

Такі прогалини дозволяють втручатись і змінювати принцип роботи мереж, систем і приладів, при цьому доступ отриманий цим шляхом майже завжди повнйи. Небезпечність полягає в тому, що така вразливість виявляється вже після її застосування, а отже її дуже важко попередити. 0day, як і брут, метод універсальний[3]. SQL injection (Сік'юель інєкція) – метод який застосовується для злому Інтернет-ресурсів – сайтів, серверів тощо. Метод оснований на принципах роботи мережі, тобто на онлайн-адресу сервера чи сайту надсилається запит, який містить SQL код, після потрапляння коду в систему, з'являється можливість отримати доступ до управління ресурсом, що в свою чергу дозволяє проводити різні роботи з інформацією[4]. Fishing (Фішинг) – це метод який базується на обмані. Фішинг є основним методом Інтернет-шахрайства. З його допомогою, різним користувачам мережі розсилаються, наприклад, електронні листи чи повідомлення, в яких від імені працівника банку або якоїсь компанії, зловмисники просять надати особисті дані – номери телефону, паролі, логіни, номери кредитних карток тощо, після чого ці данні використовують для несанкціонованого втручання в роботу систем, мереж і приладів. Крім того, фішинг використовується для розсилки та розміщення на різних Інтернет-ресурсах шкідливих посилань, при використанні яких, жертви потрапляють на сторонні ресурси, які викрадають їхні данні, або завантажують на їх комп'ютери чи в систему шкідливе програмне забезпечення, чи навіть отримують до них повний доступ.

Поширення комп'ютерних вірусів – це ще один спосіб злому, який базується на розповсюдженні шкідливих програм, які в свою чергу здійснюють певні роботи з інформацією, в тому числі її викрадення та пересилання, що забезпечує доступ до різних приладів, систем і мереж[5].

Поширення вірусів відбувається частково легальними шляхами, спочатку заражається якийсь файл, який Інтернет-користувачі самостійно завантажують на свої комп'ютери чи в системи, де з активацією файлу, активується і сам вірус. Віруси, як метод злому, також є універсальними, але крім того, вони використовуються ще для ряду різних кіберзлочинів.

Після того як зловмисники отримали доступ, вони вчиняють різні незаконні дії з інформацією. Виток інформації передбачає викрадення чи розповсюдження захищеної інформації. Це може бути службова, особиста, комерційна та навіть таємна інформація. ЇЇ виток тягне за собою суспільно-небезпечні наслідки, а в деяких випадках сприяє вчиненню інших злочинів. Втрата інформації наступає у випадку, якщо зловмисники, отримавши до неї доступ, видаляють її чи пошкоджують. Видалення, як і ушкодження інформації може бути повним або частковим. В будь-якому випадку це може завдати економічних або інших збитків власнику інформації та тим хто має до неї доступ, та користується нею. Дії, які призводять до втрати інформації, в основному, за мету мають лише нанесення шкоди. Підробка інформації передбачає роботу з нею яка призводить до зміни чи заміни інформації. Найкращий приклад – Deface (дефейс)[6]. Це вид кібератаки на Інтернет-ресурси (сайти), коли вміст головної або іншої сторінки частково або повністю заміняється. Таких прикладів велика кількість в мережі[4]. Що стосується інших випадків підробки інформації – це випадки, коли створюються копії вже існуючих Інтернет-ресурсів, серверів які використовують для здійснення різних злочинів. Крім того, фальшиву інформацію створюють спеціально, для шахрайських цілей. Блокування інформації – це нелегальне встановлення обмежень доступу до інформації. Чудовий приклад – віруси-локери[7].

---

[1] Kaspersky daily : Карточные фокусы: криминальный бизнес на банкоматах [Електронний ресурс] – Режим доступу до ресурсу: https://clck.ru/K5gaR.

[2] Learnthatlook.com : КОМП'ЮТЕРНИЙ ЗЛОМ - це ... Що таке КОМП'ЮТЕРНИЙ ЗЛОМ? 2019 [Електронний ресурс] – Режим доступу до ресурсу: https://learnthatlook.com/computer-hacking.

[3] Яндекс Дзен : Что такое уязвимость нулевого дня [Електронний ресурс] – Режим доступу до ресурсу: https://clck.ru/K5haQ.

[4] Яндекс Дзен : Хакеры. Методы взлома. [Електронний ресурс] – Режим доступу до ресурсу: https://clck.ru/K5hVu.

[5] Zillya : Основні види вірусних програм [Електронний ресурс] – Режим доступу до ресурсу: https://clck.ru/K5gh2.

[6] Habr : Делаем deface сайта с помощью XSS [Електронний ресурс] – Режим доступу до ресурсу: https://habr.com/ru/post/328276/.

[7] Habr : CTB-Locker. Мы решили платить [Електронний ресурс] – Режим доступу до ресурсу: https://habr.com/ru/post/256573/.

Це шкідливі програми, які після активації на пристрої або в системі блокують доступ до інформації, а за знаття блокування вимагають кошти. Головна проблема полягає в тому, що такі віруси найчастіше повністю знищують або пошкоджують інформацію, навіть якщо умови повернення доступу виконані. Також, зміна процесу обробки інформації може призвести і до зміни порядку роботи електроніки, або навіть цілої системи чи мережі, що в свою чергу, може їх пошкодити[8]. Порушення маршрутизації інформації – це зміна порядку або припинення її розповсюдження. Порушенням маршрутизації це також дії, спрямовані на псування каналів зв'язку, перешкоджання поширення сигналу, пошкодження кабелів тощо. Інше – це несанкціоновані модифікації приладів, наприклад банкоматів, з метою крадіжки інформації, в процесі використання банківських карток[9]. В будь-якому випадку такі дії завдають збитків і мають негативні наслідки, хоч і не завжди явні.

Стаття 361-1 – Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут[10]. Злочини, передбачені цією статтею стосуються нелегальних дій пов'язаних зі шкідливими програмами або технічними засобами. Щодо шкідливих програм – це комп'ютерні віруси. Віруси – це програми, які здатні самостійно множитись та поширюватись в системах, а крім того виконують різні функції. Віруси бувають дуже різними за функціоналом та шкідливістю. Серед основних видів можна виділити декілька. Віруси хробаки – програми, які багаторазово копіюють себе тим самим засмічують комп'ютер, що погіршує його функціональність.

Троянські віруси – це ті , які знаходяться в середині інших програм, часто нешкідливих. Активація програм запускає сам вірус. Він може мати будь-які функції інших вірусів, однак не може розмножуватись самостійно. Особливо небезпечними, особливо зараз є два типи вірусів – локери і майнери. Локери – це віруси, які блокують доступ до комп'ютерної інформації або системи, після надсилають вимогу сплатити кошти за розблокування. Насправді більшість таких вірусів знищують інформацію і навіть виконання вимог від цього не рятує. Останній найвідоміший випадок масового поширення такого вірусу – це вірус Petya, який завдав значних збитків Українським і Російським компаніям, а також державним установам. Майнери – віруси які активно почали поширюватись після популяризації криптовалюти. Ці програми, після проникнення в систему запускають процеси, які спрямовані на видобування електронної валюти, що в свою чергу дуже сильно навантажує системи і погіршує роботу техніки. Також довготривале функціонування такого вірусу може повністю вивести з ладу систему.

Протизаконні технічні засоби також бувають дуже різноманітними, в залежності від своїх функцій. До таких засобів належить приміром обладнання для кардингу – так звані скримери. Це спеціальні прилади, які кріпляться до банківських терміналів, банкоматів, з метою викрадення данних. Коли таким банкоматом користуються, скример зчитує данні з картки, після чого передає їх зловмиснику. Інший приклад – Wi-fi Jummer (Вай-фай джемер), це прилад, який псує сигнал Wi-fi.

Пристрій USB killer (USB кілер) – це модифікований USB накопичувач (флешка), який при підключенні його до комп'ютера, завдає шкоду. Така шкода може полягати у програмному втручанні в систему, що призводить до зараження вірусом, блокування, вимкнення комп'ютера тощо. Також комп'ютеру може завдаватись фізична шкода, оскільки USB кілер може бути налаштованим на уражати комп'ютера електричним струмом, що в свою чергу призводить до критичної поломки.

Існує багато інших таких засобів, головна їх суть в тому, що їх виготовляють для вчинення інших злочинів, не лише у кіберпросторі.

Використання таких програм та засобів є злочином, якщо вони завдали реальної шкоди стороннім особам. Їх розповсюдження, є протиправним, так як навіть це може завдавати шкоду, наприклад якщо поширюються комп'ютерні віруси. Поширення є особливо небезпечним, зважаючи на цільове призначення таких програм і засобів. Їх збут також незаконний, адже це один зі способів їх поширення, який крім того пов'язаний з нелегальним товарообігом та крім того, є джерелом тіньової економіки.

Стаття 361-2 – Несанкціоновані 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. Такі несанкціоновані дії з інформацією, передбачають, що вони вчинені особою, яка не мала на це право, а також що доступ до інформації отримано нелегальним шляхом. Ця стаття більш чітко регулює питання витоку інформації. Збут інформації, тобто її продаж, має кілька особливостей. Наприклад, інформація буває різною, службовою, таємною, особистою тощо, у відповідності до чого, її збут може призвести до порушення диспозицій інших статей ККУ. Збут інформації це також особливий вид її поширення, який передбачає комерційний умисел.

Розповсюдження інформації стосується дій, які призвели до її витоку, у результаті чого, до неї отримали доступ особи, які такого права не мали. Також, особливість кіберпростору передбачає, що в його межах,

---

[8] Habr : Взлом сайта и его последствия [Електронний ресурс] – Режим доступу до ресурсу: https://habr.com/ru/post/262579/.

[9] Kaspersky daily : Карточные фокусы: криминальный бизнес на банкоматах [Електронний ресурс] – Режим доступу до ресурсу: https://clck.ru/K5gaR.

[10] Кримінальний кодекс України від 05.04.2001 [Електронний ресурс] – Режим доступу до ресурсу: http://zakon.rada.gov.ua/laws/show/2341-14.

сторонні особи можуть отримати таку інформацію не маючи на те умислу, адже існує велика кількість способів її розповсюдження в мережі. Як збут, так і розповсюдження може стосуватись забороненої інформації: рецептів заборонених речовин, інструкцій з виготовлення вибухівки, порнографії тощо. У цьому випадку також можуть порушуватись інші статі ККУ.

Стаття 362 – Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї. Ця стаття є дуже неоднозначною, адже передбачає велику кількість можливих дій та наслідків, а особливо велике значення має форма вини. Якщо такі дії вчинені умисно, то наслідки будуть подібні до тих, що передбачені статтею 361 ККУ, тобто це виток, втрата, підробка, блокування інформації, спотворення процесу обробки інформації або порушення встановленого порядку її маршрутизації. Такі дії також можуть бути близькі за змістом до інших кіберзлочинів, а крім того можуть бути направлені на їх вчинення, наприклад використання комп'ютера для втручання в роботу іншого комп'ютера тощо. Більш складне питання, якщо такі дії вчинені з необережності. Тобто, відповідно до нинішньої диспозиції статті, приміром, якщо працівник якоїсь компанії, яка має локальну мережу, через необережність, допустив потрапляння вірусу-локера на комп'ютер з Інтернету, у результаті чого були уражені всі комп'ютери компанії, що завдало значних збитків, то відповідальність повинен нести саме працівник, а не зловмисники, які поширили цей вірус. Тут же виникають питання до компанії, стосовно їх методів захисту від шкідливих програм тощо, а вирішення справи залежить від ряду інших об'єктивних обставин, не зважаючи на спеціальний суб'єкт цього злочину.

Стаття 363 – Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється. Ця стаття передбачає дії, пов'язані з нелегальним використанням комп'ютерної електроніки, систем та мереж. В основному це стосується саме дій, які направлені на вчинення інших кіберзлочинів, або злочинів з використанням кіберпростору. До таких дій належить наприклад умисне розповсюдження шкідливих програм, втручання в роботу (злом) інших приладів, систем чи мереж, нелегальне поширення інформації тощо. Особливе місце займає питання порушення порядку чи правил захисту інформації, яке приміром може виражатися у «піратстві», тобто порушенні авторських і суміжних прав на інформацію в кіберпросторі. Піратство стосується не тільки порушення умов експлуатації інформації, захищеної ліцензією, а і несанкціонованого втручанні в її обробку – злом програм, копіювання, зараження їх вірусом.

Стаття 363-1 – Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку. Як і у статті 363, всі дії пов'язані з порушенням правил експлуатації, однак стаття 363-1 окремо виділяє конкретні дії, які направлені на перешкоджання функціонування інших комп'ютерних приладів, їх систем і мереж. Найпоширенішим такими злочинами є DDoS (дудос) атака – дії спрямовані на перенавантаження окремої лаки кіберпростору (комп'ютера, сайту, або сервера), шляхом перевищення мережевих запитів, тобто перевантаження системи інформацією, що в свою чергу може вповільнити її роботу або повністю вивести з ладу. Для реалізації такої атаки використовують велику кількість техніки, однак часто ця техніка не належить хакеру.

Дуже поширений метод вчинення DDoS атак за допомогою бот-нета, а це в свою чергу окрема мережа, елементами якої виступають комп'ютери уражені вірусом віддаленого доступу, зламані сервери та сайти, потужність яких направляють на ураження цілі[1].

«Конвенція про кіберзлочинність»[13], що набрала чинність від 01.07.2006 року також передбачає ці злочини, але поділяє їх на три категорії: злочину проти конфіденційності, цілісності і працездатності комп'ютерних даних і систем; комп'ютерні злочини; злочини, пов'язані з контентом[2,3]. Така різноманітність кіберзлочинів, їх видів та особливостей, роблять це явище джерелом високого рівня суспільної небезпеки, яке крім того постійно розвивається, а боротьба з яким ускладнена різними об'єктивними обставинами і проблемами правового та державного забезпечення цього питання, особливо в контексті протидії йому.

Узагальнюючи матеріали роботи, 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 кіберзлочинам[4].

---

1 DDOS-GUARD : DDoS-атака — что это такое? [Електронний ресурс] – Режим доступу до ресурсу: https://clck.ru/K5gSF.

2 ProstoCoin : Вирус майнер – как обнаружить и удалить [полное руководство] [Електронний ресурс] – Режим доступу до ресурсу: https://prostocoin.com/blog/virus-miner.

3 VPAUTINUCOM : Что такое вай-фай Джаммер и как сделать его своими руками [Електронний ресурс] – Режим доступу до ресурсу: https://clck.ru/K5gjJ.

4 Zillya : Основні види вірусних програм [Електронний ресурс] – Режим доступу до ресурсу: https://clck.ru/K5gh2.

Анотація.

Найважливіші питання в боротьбі з кіберзлочинністю – регулювання кіберпростору державою, та повне, з її боку, забезпечення боротьби з кіберзлочинами. 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.

Summary.

The most important issues in the fight against cybercrime are the regulation of cyberspace by the state, and full, on its part, ensuring the fight against cybercrime. Methods of regulating and combating cybercrime should include not only legal, material, technical, scientific, but also other types of support. Ideally, cyberspace should become a separate legal category in the system of public administration, and be comprehensively regulated, because every day it is increasingly introduced into the daily activities of society and the state, which in turn contributes to the development of cybercrime. Today in Ukraine, as in the world as a whole, the level of cybersecurity is clearly insufficient. Of course, international cooperation helps to solve this problem, but the most important actions must be taken within the country to later share with the world our successful experience in combating cybercrime and regulating cyberspace. To do this, the state and society must join forces and do everything possible to overcome the problem of cybercrime. There are still many issues that need to be addressed by legal scholars and practitioners, but it is clear that they need to be addressed immediately.

Reference:

1. DDOS-GUARD : DDoS-атака — что это такое? [Електронний ресурс] – Режим доступу до ресурсу: https://clck.ru/K5gSF.
2. 2. DGL.RU : На темной стороне интернета: Что такое Dark Web и Deep Web? [Електронний ресурс] – Режим доступу до ресурсу: https://clck.ru/K5gLD.
3. Habr : CTB-Locker. Мы решили платить [Електронний ресурс] – Режим доступу до ресурсу: https://habr.com/ru/post/256573/.
4. Habr : Взлом сайта и его последствия [Електронний ресурс] – Режим доступу до ресурсу: https://habr.com/ru/post/262579/.
5. Habr : Делаем deface сайта с помощью XSS [Електронний ресурс] – Режим доступу до ресурсу: https://habr.com/ru/post/328276/.
6. Information Security Squad : USB Киллер: что это такое и как защитить ваши устройства [Електронний ресурс] – Режим доступу до ресурсу: https://clck.ru/J5NSC.
7. Kaspersky daily : Карточные фокусы: криминальный бизнес на банкоматах [Електронний ресурс] – Режим доступу до ресурсу: https://clck.ru/K5gaR.
8. Learnthatlook.com : КОМП'ЮТЕРНИЙ ЗЛОМ - це ... Що таке КОМП'ЮТЕРНИЙ ЗЛОМ? 2019 [Електронний ресурс] – Режим доступу до ресурсу: https://learnthatlook.com/computer-hacking.
9. ProstoCoin : Вирус майнер – как обнаружить и удалить [полное руководство] [Електронний ресурс] – Режим доступу до ресурсу: https://prostocoin.com/blog/virus-miner.
10. VPAUTINUCOM : Что такое вай-фай Джаммер и как сделать его своими руками [Електронний ресурс] – Режим доступу до ресурсу: https://clck.ru/K5gjJ.
11. Zillya : Основні види вірусних програм [Електронний ресурс] – Режим доступу до ресурсу: https://clck.ru/K5gh2.
12. Безпечне місто : КІБЕРЗЛОЧИННІСТЬ У ВСІХ ЇЇ ПРОЯВАХ: ВИДИ, НАСЛІДКИ ТА СПОСОБИ БОРОТЬБИ (Анастасія Голуб) [Електронний ресурс] – Режим доступу до ресурсу: http://safe-city.com.ua/kiberzlochynnist-u-vsih-yiyi-proyavah-vydy-naslidky-ta-sposoby-borotby/.
13. Конвенція про кіберзлочинність від 23.11.2001 року [Електронний ресурс] – Режим доступу до ресурсу: http://zakon.rada.gov.ua/laws/show/994_575.
14. Кримінальний кодекс України від 05.04.2001 [Електронний ресурс] – Режим доступу до ресурсу: http://zakon.rada.gov.ua/laws/show/2341-14.

15. Про основні засади забезпечення кібербезпеки України : Закон Уркїни від 05.10.2017 р. [Електронний ресурс] – Режим доступу до ресурсу: https://clck.ru/K5gGV.
16. Яндекс Дзен : Хакеры. Методы взлома. [Електронний ресурс] – Режим доступу до ресурсу: https://clck.ru/K5hVu.
17. Яндекс Дзен : Что такое уязвимость нулевого дня [Електронний ресурс] – Режим доступу до ресурсу: https://clck.ru/K5haQ.

Vladimir Pakhomov,
Doctor of Law Sciences, Professor, Head of the Department of Criminal Law and Judiciary
Educational-Scientific Institute of Law of Sumy State University

Mikhail Dumchikov,
Candidate of Law, Assistant of the Department of Criminal Law and Judiciary
Educational-Scientific Institute of Law of Sumy State University