**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**ХЕРСОНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ**
**ІСТОРИКО-ЮРИДИЧНИЙ ФАКУЛЬТЕТ**
**КАФЕДРА ГАЛУЗЕВОГО ПРАВА**

# КІБЕРЗЛОЧИНИ ПРОТИ ВЛАСНОСТІ: КРИМІНАЛЬНО-ПРАВОВА ТА КРИМІНОЛОГІЧНА ХАРАКТЕРИСТИКА

Кваліфікаційна робота (проєкт)
на здобуття ступеня вищої освіти «бакалавр»

Виконала: студентка IV курсу 13-421 групи
Спеціальності: 081 Право
Освітньо-професійної програми «Право»

**Чокас Юлія Сергіївна**

Керівник: **к.ю.н., доц. Гавловська А.О.**

Рецензент: **д.ю.н., проф. Правоторова О.М.**

Херсон – 2020

# ЗМІСТ

# ВСТУП

**Актуальність теми.** На сучасному етапі у зв‘язку з поширенням застосування комп’ютерних технологій питання кібербезпеки є актуальним у всіх напрямках діяльності правоохоронних органів. Законом України «Про основні засади забезпечення кібербезпеки України» визначені правові та організаційні основи інтересів людини та громадянина, суспільства та держави, державної політики у сфері кібербезпеки, національних інтересів України у кіберпросторі, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Результативність у подоланні кіберзлочинності залежить й від співпраці громадян з правоохоронними органами. Це дозволить запобігати злочинам та розкривати їх на більш ранніх етапах. Але все ж першочерговим завданням для єффективності боротьби з кіберзлочинністю є розробка цілістної концепції кримінально-правових та кримінологічних основ.

Аналіз статистичної звітності правоохоронних органів України засвідчує швидкий ріст кримінальних правопорушень в кіберпросторі з кожним роком. Такого виду злочини стали переважати у порівнянні з традиційними злочинами проти власності, вчинення яких стає важчим в умовах вдосконалення правоохоронних систем. В наслідок поширення даного виду злочинів є необхідність вивчення та подальшого вдосконалення правової системи в сфері кібербзпеки.

У сучасний період значний внесок у становлення й розвиток окремих теоретичних поглядів щодо кримінально-правової охорони власності загалом та дослідження кіберзлочинів зокрема, зробили такі зарубіжні та українські вчені, як: Д.С. Азаров, О.А. Баранов, В.С. Батиргареєва, Ю.М. Батурін, П.Д. Біленчук, І.Г. Богатирьов, Т.М. Богданова, В.І. Борисов, Л.П. Брич, О.Ю. Бусол, Б.М. Головкін,

О.О. Горішний, В.К. Грищук, І.І. Гуня, В.О. Глушков, Н.О. Гуторова, Л.М. Демидова, М.Ю Дворецький, Ю.А. Дорохіна, О.О. Дудоров, К.М. Євдокімов, В.П. Ємельянов, А.Ю. Караманов, М.В. Карчевський, Д.І. Ковальов, Т.М. Лопатіна, К.Б. Марисюк, М.І. Мельник, М.А. Погорецький, О.Е. Радутний, Н.В. Савінова, І.І. Сухих, В.Я. Тацій, В.В. Тиенко та інших.

Таким чином, подальші дослідження питань кібербезпеки являються актуальними та зможуть сприяти розвитку забезпечення захисту права власності у кіберпросторі.

**Мета і завдання дослідження.** Метою кваліфікаційної роботи є формування комплексної кримінально-правової та кримінологічної характеристики кіберзлочинів проти власності.

Визначена мета зумовила необхідність з’ясування низки таких головних **завдань**:

- розкрити теоретичні засади кіберзлочинності;
- висвітлити правову основу кібербезпеки України;
- надати кримінально-правову характеристику кіберзлочинів;
- надати кримінологічну характеристику кіберзлочинів;
- здійснити аналіз заходів щодо запобігання кіберзлочинам проти власності, які проводяться в Україні;
- здійснити аналіз міжнародного досвіду у сфері запобігання кіберзлочинам проти власності;

**Об'єктом дослідження** є суспільні відносини пов’язані з кібербезпекою України.

**Предметом дослідження** є кіберзлочини проти власності: кримінально-правова та кримінологічна характеристика.

**Методи дослідження.** Методологічною основою дослідження є сукупність загальнонаукових і спеціально-юридичних методів дослідження, зокрема:

- *діалектичний метод* (дозволяє розкрити сутність загальної характеристики кіберпростору та кіберзлочинів проти власності та забезпечити проведення аналізу правової основи кібербезпеки України);

- *порівняльно-правовий метод (*дозволяє визначити кількісні та якісні показники кіберзлочинності);

- *догматичний метод* (забезпечує дослідження змісту правових норм та з'ясування закономірностей дії права за допомогою правил юридичної логіки);

- *системно-структурний метод (*дозволяє розкрити сутність, класифікувати та проаналізувати види кіберзлочинів проти власності).

**Практичне значення одержаних результатів** полягає у тому, що вони можуть бути використані та слугувати, як у вивченні теми кіберзлочинів проти власності та кібербезпеки вцілому, і в допомозі в написанні робіт пов’язаних з даною темою.

**Апробація результатів дослідження.** Основні положення кваліфікаційної роботи оприлюднено на П’ятій Всеукраїнській студентській науково-практичній конференції «Реформування правової системи України під впливом євроінтеграційних процесів» (м. Херсон, 20 березня 2020 р.).

**Публікації.** Основні теоретичні положення роботи знайшли відображення в наступних публікаціях:

Чокас Ю. С. Кіберзлочини як сучасний прояв транснаціональної злочинності. Матеріали П’ятої Всеукраїнської студентської науково-практичної конференції «Реформування правової системи України під впливом Євроінтеграційних процесів». Херсон, 20 березня 2020 року.

**Структура роботи** складається зі вступу, трьох розділів, що включають шість підрозділів з даної теми, висновків та списку використаних джерел.

# РОЗДІЛ 1

# ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ КІБЕРЗЛОЧИНІВ ПРОТИ ВЛАСНОСТІ

## 1.1.Теоретичні засади кіберзлочинів проти власності

На сучасному етапі інформаційна сфера – це одна з найбільш динамічно розвинутих сфер суспільних відносин, яка потребує правового регулювання. «Інтернет» став невід'ємною частиною життя сучасного суспільства, в ньому зявилася власна інфраструктура: мережева мова, магазини, публічні форуми, освітні курси тощо. В «Інтернеті» знайшло свій прояв таке нове явище, як кіберпростір.

Поняття «кіберпростір» було впроваджено канадським письменником – фантастом Вьямом Гібсоном у 1982 році.

«Кіберпростір – це форма співіснування сукупності матеріальних та нематеріальних об'єктів і процесів, спрямованих на породження, сприйняття, запам'ятовування, переробку та обмін інформацією. Деякою мірою, кіберпростір – це віртуальний світ, який базується на реальному матеріальному фундаменті та з реальними наслідками свого існування та розвитку» [1, с. 118].

Масове поширення комп'ютерів та поява інформаційних мереж спровокувало появу кіберзлочинності. Історію даного типу злочинності в умовно можна поділити на два етапи.

Перший етап (1960 – 1991 рр.). У 1960-х роках почалося використання комп'ютерів у світі, а саме в США, але комп'ютери використовувалися лише деякими державними органами через їх цінову недоступність. Комп'ютерні злочини 1960-х років були зовсім не поширеними і полягали в неправомірному доступі до комп'ютерної інформації та персональних даних, їх модифікації або видаленні, а через неточність та неповноту законодавчого регулювання та відсутність способів отримання доказової бази більшість справ «розвалювалися» [2].

«Комп'ютерний бум» і, як наслідок, поява нових видів кіберзлочинності, стався в кінці 1970-х – початку 1980-х років в США з появою перших персональних комп'ютерів IBM 5100 і Apple I, а також з появою пращура мережі «Інтернет» - «Арпанет».

У 1975 році Агенство передових досліджень Міністерства оборони США спільно с Стендфордським і Каліфорнійським університетами запустили в робочому режимі першу інформаційно – телекомунікаційну мережу «Арпанет». У той же час масово з'явилися випадки злочинів, вчинених з використанням комп'ютерів і мережі «Арпанет» [3].

У 1977 році був схвалений перший законопроект «Про захист федеральних комп'ютерних систем», на основі якого в 1986 році було прийнято Закон №1030 «Про шахрайство і зловживання використанням комп'ютера» [4, с. 72].

Перші локальні комп'ютерні мережі в СРСР з'явилися також на кінці 1970-х – початку 1980-х рр. Вони являли собою високотехнологічні та інноваційні комп'ютерні системи. Перший злочин з використанням комп'ютера в СРСР було зареєстровано в 1979 році у Вільнюсі, таким злочином було розкрадання 78 584 рублів. Цей злочин було занесено до міжнародного реєстру правопорушень і він став відправною точкою у розвитку комп'ютерних злочинів в СРСР [4].

На початку початку 1980-х років в США з'явилася інформаційно – телекомунікаційна мережа «Мілнет», яка використовувалася лише Міністерством оборони США. Через деякий час «Арпнет» і частина «Мілнет» були інтегровані, а для іх загального позначення було придумано спеціальну назву «Інтернет». В результаті почався сплеск кіберзлочинності.

Другий період (1991р. – до сьогодні). У 1991 році «Інтернет» став світовою інформаційною мережею, відповідно хакери різних країн отримали можливість безперешкодно вчиняти злочини по всьому світу, а комп'ютерна злочинність набула транснаціональних ознак.

У 1995 році з’явився перший Інтернет – магазин «Amazon», в той же рік з’явилася перша соціальна мережа «Classmates» та перший віртуальний банк «Security First Network Bank». На наш погляд, кіберпростір в тому вигляді, що ми сьогодні спостерігаємо, з’явився саме в цей період часу. Через рік Верховний Суд США вперше дав легальне визначення кіберпростору.

Зокрема, згідно з рішенням Верховного Суду США, під кіберпростором розуміється «унікальне середовище, що не розташовано в географічному просторі, але доступно кожному в будь-якій точці світу, за допомогою доступу в мережу Інтернет» [5, с. 24], який Верховний Суд США визначає як «глобальне об’єднання комп’ютерних мереж і інформаційних ресурсів, що не має чітко визначеного власника і служить для інтерактивної комунікації фізичних і юридичних осіб» [5, с. 24-25].

Відправною точкою для визначення поняття «кіберзлочин» є Конвенція про кіберзлочинність від 23 листопада 2001 року. Сьогодні вона ратифікована 18 державами та підписана 25 країнами, у тому числі й Україною 7 вересня 2005 року [6, с. 71]. Згодом, нашою державою було ратифіковано додатковий протокол до Конвенції, що «...стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп’ютерні системи» [7, с. 328].

Як зазначається: «На сучасному етапі одним із найпоширеніших злочинів проти власності є шахрайство, який має динаміку до зростання як за кількісним, так і за якісним показниками. Зростання обсягу цього виду злочинних посягань на власність пов’язано, насамперед, зі стрімким розвитком телекомунікацій і глобальних комп’ютерних мереж, які полегшують умови вчинення злочинів проти власності та утворюють нові склади шахрайства, такі як кібершахрайство» [8, с. 208].

Поняття кіберзлочинів проти власності доцільно визначити як сукупність заборонених кримінальним законодавством діянь проти

власності, спосіб вчинення яких передбачає обов’язкове використання кіберпростору як знаряддя або засобу.

Щодо класифікації кіберзлочинів, слід вказати, що деякі дослідники пропонують поділити кіберзлочини на: «агресивні та неагресивні. Так, до першої групи належать кібертероризм, погроза фінансової розправи, кіберпереслідування, кібersталкінг.

Друга група охоплює кіберкрадіжку, кібервандалізм, кібершахрайство, кібершпигунство, розповсюдження спаму та вірусних програм» [9, с. 333].

У спеціальній літературі зазначається, що *найбільш поширеними видами кіберзлочинів* у сучасному світі є:

«1) Картинг – використання в операціях реквізитів платіжних карт, отриманих зі зламаних серверів інтернет-магазинів, платіжних і розрахункових систем, а також їз персональних комп’ютерів;

2) Фішинг – клієнтам платіжних систем надсилаються повідомлення електронною поштою нібито від адміністрації або служби безпеки цієї системи із проханням вказати свої рахунки та паролі;

3) Вішинг – у повідомленнях міститься прохання зателефонувати на певний міський номер, а під час розмови запитуються конфіденційні дані власника картки;

4) Онлайн-шахрайство – несправжні інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв’язку;

5) Піратство – незаконне розповсюдження інтелектуальної власності в Інтернеті;

6) Кард-шарінг – надання незаконного доступу до перегляду супутникового та кабельного телебачення;

7) Соціальна інженерія – технологія управління людьми в інтернет-просторі;

8) Мальваре – створення та розповсюдження вірусів і шкідливого програмного забезпечення;

9) Протиправний контент – контент, що пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості та насильства;

10) Рефайлінг – незаконна підміна телефонного трафіка» [10, с. 62].

Доцільно зазначити, що злочини проти власності почали зростати над швидкими темпами і поряд із традиційними з'явились нові кваліфіковані види злочинів – «кібершахрайство», «кіберрозкрадання» тощо.

Специфіка кібершахрайства в першу чергу пов'язана з тим, що наявна віддаленість об'єкту посягання, складнощі з виявленням, доведенням вини, а так само висока прибутковість. У зв'язку з наведеним цей вид злочинної діяльності став одним з найбільш привабливих для представників злочинного світу.

Зазначається, що: «Кібершахрайство в сфері платіжних інструментів – актуальна проблема для України. Щодня у середньому жертвами кіберзлочинців стають більше 120 українців. Наразі найбільше незаконних операцій фіксується в інтернеті. У минулому році їх кількість сягнула 45 тисячі, сума збитків – майже 98 мільйонів гривень. За допомогою банкоматів шахраї зняли з рахунків українців 15,4 мільйона гривень – це 9,7 тисячі незаконних операцій. У торгівельних мережах зафіксовано 4,8 тисячі випадків шахрайства із платіжними інструментами на суму 13,6 мільйона гривень» [11, с. 10].

За словами С. Шацького, директора департаменту платіжних систем та інноваційного розвитку Національного банку України: «35% звернень громадян до банків – саме з приводу шахрайства з платіжними картками, найбільше скарг фіксується у містах-мільйонниках. Лідером за кількістю збитків від незаконних дій є місто Київ – 40% шахрайських випадків зафіксовано у столиці» [11, с. 10].

Науковці визначили найбільш поширені види кібершахраств:

«1. Шахрайство в мережі Інтернет, зокрема: створення фінансових пірамід в мережі Інтернет; шахрайство при продажу товарів через Інтернет або на Інтернет-аукціонах; діяльність по створенню програмних засобів з метою розкрадання фінансової, комерційної або персональної інформації;

2. Шахрайство в системах дистанційного банківського обслуговування (ДБО), зокрема: створення комп'ютерних вірусів і троянських програм для прихованого перехоплення управління комп'ютером клієнта з встановленим програмним забезпеченням ДБО; відкриття рахунків, проведення несанкціонованих операцій і отримання готівкою коштів в результаті несанкціонованих операцій у системах ДБО;

3. Підробка платіжних карток і банкомат не шахрайство, зокрема:

- Використання втрачених, викрадених або підроблених платіжних карток; викрадення реквізитів платіжних карт, у тому числі із застосуванням технічних засобів їх клонування;

- Скіммінг – виготовлення, збут і установка на банкомати пристроїв читання, копіювання інформації з магнітної смуги платіжної картки та отримання ПІН-коду до неї;

- Використання так званого «білого пластику» для клонування платіжної картки та зняття готівки в банкоматах;

- Transaction Reversal Fraud – втручання в роботу банкомату при здійсненні операції видачі готівки, яка залишає незмінні баланс карткового рахунку при фактичному отриманні готівки зловмисником;

- Cash Trapping – заклеювання диспенсера для присвоєння зловмисником готівки, яка була списана з карткового рахунку законного держателя картки» [12, с. 33].

Доцільно підкреслити, що серед найбільш швидко еволюціонуючих злочинів, що вчиняються з використанням комп'ютерних систем є шахрайства з електронними платіжними

системами. Зокрема асоціація ЕМА підбила підсумки і склала класифікацію шахрайських веб-ресурсів [13].

Найчастіше, за висновками експертів, українці страждають від фітингу-шахрайства, вчиненого в інтернеті за допомогою сайтів, створених злочинцями для того, щоб виманювати у користувачів дані інших банківських карт і згодом красти з них гроші.

Широкого поширення набули й інші різновиди кібершахрайства, що зачіпають споживчі й майнові права довірливих інтернет-користувачів:

1. Шахрайство з використанням методів соціальної інженерії – шахрайство із застосуванням психологічного впливу на банківського клієнта і мотивуванням вчинити дії, які він зв інших обставин не здійснив би.

2. Шахрайство з відміною транзакції – захоплення злочинцем готівки в момент її видачі банкоматом за допомогою спеціального пристосування типу «вилка» з одночасною генерацією операції анулювання результату транзакції, в результаті чого залишок на картковому рахунку не змінюється.

3. Шахрайство з під лімітними сумами – різновид шахрайства, при якому шахраєм здійснюється операції на суми нижче авторизованого ліміту, встановленого для торгівця банком-еквайром.

Під вимаганнями на сучасному етапі розуміють вид злочинної діяльності, пов’язаної з незаконним придбанням чи втратою майнових благ. Це значення виражає зміст та безпосередньо склад протиправного діяння при вимаганні, так як вбачає його в цілісності, як єдності процесу вимагацької діяльності та його результату.

Обєктивна сторона вимагання складається із двох обов’язкових складових – вимоги і погрози. Окремі вчені вказують, що вимога у цьому складі злочину має ряд характерних ознак: «конкретність, час виконання» [14, с. 212].

Найчастіше пред’явлення злочинної вимоги здійснюється:

«а) шляхом безпосереднього особистого контакту з потерпілим і прямою вимогою передачі майна під загрозою розправи у разі невиконання вимоги злочинця;

б) шляхом анонімної вимоги передачі майна;

в) шляхом нав’язування невигідних і збиткових для потерпілого угод;

г) шляхом втягування потерпілого в злочин, імітація дорожньо-транспортної пригоди, з подальшим відшкодуванням нібито заподіяної шкоди тощо» [15, с. 79].

Проте кібервимагання принципово відрізняється відсутністю фізичного контакту між винним і потерпілим, що не знижує суспільної небезпеки такого діяння, а передбачає більш серйозний підхід до планування і реалізації злочинного наміру. Остання обставина певним чином підвищує ступінь суспільної небезпеки «безконтактного» вимагання.

З 2016 р. Україна приєдналася до глобальної ініціативи No More Ransom в боротьбі з кібервимаганнями.

Найбільш поширеними загрозами при вимаганні у кіберпросторі є:

1. Загроза поширення відомостей, які можуть зганьбити жертву (потерпілого) або його близьких, або інших відомостей, які певним чином можуть істотно зашкодити правам чи законним інтересам потерпілого або його близьких;

2. Загроза видалення, блокування або модифікації комп’ютерної інформації, загроза іншого втручання у функціонування засобів зберігання, обробки або передачі комп’ютерної інформації або інформаційно-телекомунікаційних мереж.

Врахувавши зарубіжний досвід та проаналізувавши норми різних держав, учені запропонували наступну класифікацію кіберзлочинів:

«1. Злочини проти конституційних прав і свобод людини та громадянина, такі як порушення недоторканості приватного житла, порушення таємниці листування, телефонних переговорів, поштових, телеграфних та інших повідомлень, порушення авторських і суміжних прав;

2. Злочини проти життя та здоровя;

3. Злочини проти честі та гідності особи;

4. Злочини проти власності;

5. Злочини у сфері комп'ютерної інформації, такі як неправомірний доступ до інформації, створення, використання та розповсюдження шкідливих програм;

6.Злочини проти суспільної моральності;

7. Злочини проти безпеки держави» [16, с. 9-10].

### 1.2. Правова основа кібербезпеки України

Протягом останніх років Україна, як і більшість інших країн світу, здійснює важливі заходи щодо розбудови інформаційного суспільства, забезпечення кібербезпеки. Нормативно – правову базу в цих сферах діяльності становлять: «Конвенція Ради Європи про кіберзлочинність» [53], ратифікована Законом України від 07.09.2005 року № 2824-IV [6], а також відповідні Закони України: «Про Державну службу спеціального зв'язку та захисту інформації України» [54], «Про інформацію» [55], «Про державну таємницю» [56], «Про національну безпеку України» [57], Укази Президента України, присвячені цій проблемі, окремі постанови Кабінету Міністрів України, рішення РНБО України та відповідні положення Кримінального кодексу України.

Окрім того, ще у 2010 році відповідним Указом Президента України «Про виклики та загрози національній безпеці України» [58] було ухвалено: «рішення про початок створення Єдиної загальнодержавної системи протидії кіберзлочинності» [58]. Окремо,

Законом України «Про внесення змін до деяких законів України про структуру і порядок обліку кадрів Служби безпеки України» [59] від 9 грудня 2011 року № 4157-VI у структурі СБ України «створено Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки» [59]. З огляду на динаміку поширення комп'ютерних інцидентів теренами України в липні 2010 року у структурі МВС України на базі Департаменту боротьби зі злочинами, пов'язаними з торгівлею людьми, було утворено нову службу – Департамент боротьби з кіберзлочинністю та торгівлею людьми.

Ще одним кроком у напрямку забезпечення кібербезпеки був Указ Президента України від 15 березня 2016 року №96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України"» [18], яким було введено в дію відповідне рішення Ради національної безпеки і оборони України.

Метою Стратегії кібербезпеки України є: «створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави» [18].

Загалом: «дана Стратегія базується на положеннях «Конвенції про кіберзлочинність» [53], ратифікованої Законом України від 7 вересня 2005 року № 2824-IV, законодавства України щодо засад внутрішньої та зовнішньої політики, національної безпеки України, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом та була спрямована на реалізацію до 2020 року Стратегії національної безпеки України, затвердженої Указом Президента України від 26 травня 2015 року № 287 «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України"» [17].

Наступним етапом в сфері забезпечення кібербезпеки стало рішення Ради національної безпеки та оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх

нейтралізації» [60], введено в дію Указом Президента України від 13 лютого 2017 року. Такий стан справ фактично означає, що Україна поступово накопляє важливий досвід у захисті власної ІТ – інфраструктури від кіберзагроз сучасності та протидії проявам кібертероризму.

Розмаїття термінологічних тлумачень було запропоновано 5 жовтня 2017 року Законом України «Про основні засади забезпечення кібербезпеки України» [19], а 7 листопада Закон підписано Президентом України.

Україна активно залучилася до світового процесу формування доступного для всіх інформаційного суспільства, у зв'язку з чим на державному рівні було схвалено низку нормативно-правових актів.

У жовтні 2017 року прийнято Закон України «Про основні засади забезпечення кібербезпеки України» [19]. Загалом, даний Закон визначає: «правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки» [19].

На сьогоднішній день за статистичними даними відомо, що терористи активно використовують інформаційно-комунікаційні технології та Інтернет не тільки для вчинення своїх злочинних намірів, а й для підшукування однодумців , використовуючи переконливі доводи та активно маніпулюючи.

«Стратегія кібербезпеки України» визначає Національну систему кібербезпеки, яка: «є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових,

оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного засобу національних інформаційних ресурсів, кіберзахисту об’єктів критичної інформаційної інфраструктури» [20, с. 30].

Суспільні відносини у сфері забезпечення кібербезпеки є неоднорідними, комплексними та мають характерні особливості. Саме кіберпростір та національна телекомунікаційна мережа с об’єктами суспільних відносин у сфері забезпечення кібербезпеки, а їх основний зміст полягає у застосуванні користувачами цифрових інформаційних технологій.

# РОЗДІЛ 2
# ОСОБЛИВОСТІ КВАЛІФІКАЦІЇ КІБЕРЗЛОЧИНІВ ПРОТИ ВЛАСНОСТІ

## 2.1. Кримінально-правова характеристика кіберзлочинів проти власності

Загалом, питання протидії злочинам проти власності почали досліджуватися ще у дореволюційні часи, зокрема, такими вченими як: Л. Бєлогріц-Котляревський, А. Круглевський, С. Познишев, Д. Тальберг, І. Фойницький та інші.

Серед сучасних науковців, які досліджували певні питання боротьби зі злочинами проти власності, важливе місце посідають такі відомі правники: М. Гельфер, І. Даньшин, А. Закалюк, А. Зелінський, В.П. Ємельянов, Б. Курінов, Ю. Ляпунов, Г. Матусовський, П. Михайленко, М. Панов, А. Піонтковський, В. Тихий, С. Фролов, В. Шакун та інші.

Комп'ютеризацію як суспільне явище можна вважати не лише прогресивним кроком людства, але й негативним стимулом, що призвів до появи нового виду злочинів проти власності - злочинів цієї групи, які вчиняються в кіберпросторі. Кіберзлочинність можна вважати об'єднуючим поняттям, що характеризує пов'язані кримінальні дії: кіберзалежні та кіберутворюючі злочини проти власності.

Зазначається, що: «Кіберзалежні злочини проти власності - це злочини, які вчиняються з використанням комп'терів, комп'ютерних мереж чи інших комунікаційних форм. Такі, наприклад, як поширення вірусів та інших шкідливих програм, хакерство, зламування серверів для захоплення мережевої інфраструктури або веб-сторінок. Кіберзалежні злочини проти власності спрямовані на пошкодження комп'ютерів та джерел мережі, мають наслідки у вигляді, наприклад, шахрайства.

Кіберутворюючі злочини проти власності - це традиційні види злочинів, які стали кіберзлочинами через використання комп'ютерів,

комп'ютерних мереж та інших видів комунікації. На відміну від кіберзалежних злочинів проти власності, вони можуть вчинятися і без застосування комп'ютерного елементу» [21, с. 29].

Кіберзлочини можуть становити загрозу різним суспільним відносинам, а не тільки відносинам у сфері комп'ютерної інформації. Це пов'язано з тим, що в кіберпросторі існує можливість здійснення двох видів кіберзлочинів: одно- і двухоб'єктних. У першому випадку винний заподіює шкоду одній групі суспільних відносин - відносинам власності, у другому - відразу двом - відносинам власності і відносинам у сфері комп'ютерної інформації.

Родовим об'єктом усіх злочинів проти власності, вчинених в кіберпросторі, слід визнати відносини власності, що забезпечуть матеріальний добробут особи, суспільства і держави, оскільки на них направлено суспільно небезпечне діяння і саме їм в першу чергу завдається шкода. Залежно від способу вчинення злочину додатковим об'єктом може виступати сукупність суспільних відносин щодо правомірного безпечного використання комп'ютерної інформації, а також громадська безпека і громадський порядок тощо.

На підставі проведеного нами дослідження доцільно виділити наступні злочини проти власності, які вчиняються в кіберпросторі за родовим об'єктом посягання: шахрайство, вимагання, привласнення і розтрата, заподіяння майнової шкоди шляхом обману та зловживання довірою, умисне знищення або пошкодження чужого майна.

Предмет таких кіберзлочинів може відрізнятися від предмета аналогічних злочинів, вчинених в матеріальному світі, і мати свої особливості. Оскільки кіберпростір є сферо діяльності в інформаційному просторі, тобто певною віртуальною реальністю, то такі суспільно небезпечні діяння, як, наприклад, крадіжка, не можуть бути спрямовані на вилучення конкретних матеріальних предметів, оскільки вони просто не можуть існувати в кіберпросторі. Однак дані злочини можуть бути

спрямовані на інші предмети, що мають таку ж економічну значимість, існування яких можливе в цифровому середовищі.

У той же час кіберпростір дає доступ до таких матеріальних предметів, як комп'ютер, планшет або смартфон, які при певних навичках можна навмисне пошкодити або зовсім знищити. У зв'язку з наведеним, на наш погляд, докладніше варто зупинитися на таких предметах економічних кіберзлочинів, як електронні гроші і криптовалюта.

Пункт 1.3 Постанови Правління Національного банку України «Про внесення змін до деяких нормативно-правових актів Національного банку України з питань регулювання випуску та обігу електронних грошей» [61] від 4 листопада 2010 р. № 481, певним чином звужує поняття та визначає «електронні гроші як одиниці вартості, які зберігаються на електронному пристрої, приймаються як засіб платежу іншими, ніж емітент, особами і є грошовим зобов'язанням емітента» [61].

Ці визначення дали змогу виокремити ознаки відповідної категорії неправомірного випуску й використання електронних грошей, що вчиняються в системах інтернет-розрахунків для встановлення точності надання кримінально-правової кваліфікації:

«а) за своєю правовою природою електронні гроші становлять собою грошове зобов'язання певної особи, що здійснює їх випуск, тобто є зобов'язанням боржника сплатити кредитору певну грошову суму відповідно до цивільного правочину та на певних підставах, передбачених законодавством України;

б) їх матеріальним виразом є одиниця вартості, яка зберігається на електронному пристрої у формі певного технічного символу;

в) електронні гроші приймаються як засоби платежу» [22, с. 13-16].

Ці ознаки дають можливість зробити висновок, що електронні гроші мають самостійну економічну цінність. Підтвердженням тому є п. 2.3 названої вище Постанови Правління Національного банку України «Про внесення змін до деяких нормативно-правових актів Національного банку України з питань регулювання випуску та обігу електронних грошей» [61], в якому зазначається, що: «електронні гроші вважаються випущеними з часу їх завантаження емітентом чи оператором на електронний пристрій, що перебуває в розпорядженні користувача» [61]. Сьогодні криптовалюту можна обміняти не тільки на звичні гроші (гривні, долари або євро), але і на різні товари або послуги. Так, Університет Нікосії в якості оплати навчання приймає BTC [23, с. 89]; компанія «Virgin Galactic» здійснює авіаперевезення за криптовалюту; «Ламборджині» продає свої автомобілі [24], як і американська компанія «Philipp Preuss» - нерухомість [25, с. 39-40]. Однак переважна більшість послуг, за які береться криптовалюта, надається лише в кіберпросторі - це, як правило, хостинг, оплата онлайн-ігор та інших послуг.

На підставі наведеного, можна зробити висновок, що криптовалюта однозначно є засобом платежу. Однак це не робить її справжніми грошима. Основною причиною, за якою не можна визнати криптовалюту грошима, це те, що вона емітується децентралізовано, і не існує суб'єкта, який забезпечує її платоспроможність.

Пристрої доступу в кіберпростір можуть виступати в якості допоміжних засобів, оскільки без доступу в кіберпростір вони втрачають свою значимість для злочинця і унеможливлюють доведення кіберзлочину до кінця. Це положення відноситься також й для вірусів і іншого шкідливого програмного забезпечення.

Що стосується об’єктивної сторони кіберзлочинів проти власності, то їх особливість проявляється не в обов’язкових ознаках, а в факультативних, таких як спосіб, місце і засіб вчинення злочину.

Названі ознаки називаються факультативними, так як законом вони можуть передбачатися як ознаки об’єктивної сторони складу злочину, а можуть і взагалі не передбачатися в кримінально-правових нормах.

Спосіб вчинення злочину – це сукупність прийомів і методів, які використовуються під час вчинення злочину. Дистанційне вчинення злочину не зменшує його суспільної небезпеки. Такий спосіб дозволяє не залишати фізичних слідів, що ускладнює процес доказування та виявлення злочинця.

Кіберпростір може розглядатися в якості місця вчинення злочину, це дозволяє зрозуміти простоту і легкість вчинення кіберзлочинів проти власності. Пристрої доступу в кіберпростір можуть виступати в якості допоміжних засобів, оскільки без доступу в кіберпростір вони втрачають свою значимість для злочинця і унеможливлюють доведення кіберзлочину до кінця

Як елемент складу злочину суб'єкт кіберзлочинів проти власності характеризується: «певними ознаками, які традиційно поділяються на обов'язкові та додаткові. До обов'язкових ознак суб'єкта злочину належать: фізична особа; загальний вік, з якого може наставати кримінальна відповідальність; осудність особи. Відсутність будь-якої із цих обов'язкових ознак вказує на відсутність суб'єкта злочину» [26, с. 142]. До додаткових зазвичай відносять ознаки, що дають змогу охарактеризувати суб'єкта кіберзлочинів проти власності як спеціального.

Однією з обов'язкових ознак суб'єкта кіберзлочинів проти власності є вік особи. У ч. 1 ст. 22 КК України закріплено: «кримінальній відповідальності підлягають особи, яким до вчинення злочину виповнилося шістнадцять років» [45]. Проте у ч. 2 ст 22 КК України закріплено наступне: «щодо віку осіб, що вчинили крадіжку, вимагання, умисне знищення або пошкодження майна, вік притягнення

до відповідальності знижено - у разі вчинення цих злочинів проти власності він становить 14 років» [45].

Однією з причин сучасного стану кіберзлочинності серед неповнолітніх слід вважати стрімкий розвиток інформаційно-телекомунікаційних технологій, який фактично формує інформаційно-комунікативне середовище, для якого притаманні: «віртуальність - як існування речей, подій, процесів тощо; глобальність - як існування єдиних, універсальних для всієї системи відносин, усіх локальних співтовариств (формальних і неформальних) та інститутів взаємодії; фрагментарність - властивість, що характеризується уривчастістю та неповнотою» [27, с. 9].

Дослідження даної практики показало, що віртуалізація є однією з основних причин збільшення кількості кіберзлочинів проти власності, яка породжує кібердевіантність та кіберзлочинність. Зазначене відображується на динаміці й структурі кіберзлочинності: «відбувається скорочення насильницьких злочинів проти власності, стає молодшим сам злочинець. У зв'язку з цим науковцями обговорюються питання щодо необхідності як зниження, так і розширення меж віку кримінальної відповідальності. Так, деякі вчені, з огляду на те, що злочини проти власності вчиняють особи до 14 років, пропонують переглянути положення кримінального законодавства України щодо віку кримінальної відповідальності» [28, с. 27].

Деякі науковці навіть «пропонують знизити вікову межу кримінальної відповідальності до тринадцяти років осіб, які вчинили злочини проти власності за обтяжуючих обставин» [29, с. 35].

Наступною характерною ознакою суб'єкта злочинів проти власності слід вважати здатність особи сприймати і розуміти суспільну значущість своєї поведінки у певній обстановці та керувати своїми діями, мається на увазі її осудність. Відповідно до ст. 19 КК України: «Осудною визнається особа, яка під час вчинення злочину могла

усвідомлювати свої дії та керувати ними. Зокрема, осудність - юридична передумова вини та кримінальної відповідальності, обов'язкова ознака суб'єкта злочинів проти власності» [45].

Крім обов'язкових ознак суб'єкта злочинів проти власності, передбачаються його додаткові ознаки, наявність яких дає змогу охарактеризувати суб'єкта цієї групи злочинів як спеціального [30, с. 146].

Так, аналіз юридичної літератури показує, що найбільш поширеним у науці кримінального права є їх поділ на наступні групи:

«1) ті, що характеризують соціальну роль і правове становище особи;

2) ті, що характеризують фізичні властивості особи;

3) ті, що характеризують взаємовідносини винного з потерпілим та іншими особами» [31, с. 286].

Наступною «обов'язковою складовою аналізу складу злочинів проти власності є суб'єктивна сторона, яку в теорії кримінального права традиційно визначають як внутрішній бік загальнонебезпечного посягання» [32, с. 115].

Аналіз спеціальної літератури показав, що більшість вчених під «суб'єктивною стороною злочину розуміють психічне ставлення особи до вчиненого нею суспільно небезпечного діяння та його наслідків, що характеризуються конкретною формою вини, мотивом та метою злочину» [33, с. 136].

Проблема суб'єктивної сторони кіберзлочинів проти власності, до якої згідно із загальноприйнятою точкою зору належать вина, мотив та мета, займає особливе місце і належить до такої, що не знайшла одного теоретичного визначення в науці кримінального права. Так, зазначається, що: «суб'єктивне сприйняття особою дії або бездіяльності, що порушує особисті майнові права на об'єкти власності, а також її ставлення до злочинних наслідків, передбачених чинним законом про

кримінальну відповідальність, значною мірою обумовлено тими складними психологічними процесами, що відбуваються у свідомості особи та її ставленні як до власне факту порушення, так і до інших об'єктивних ознак» [26, с. 78].

Вина особи в проблематиці суб'єктивної сторони кіберзлочинів проти власності, як єдина обов'язкова ознака цього елементу має важливе теоретичне та практичне значення. Проблеми вини під впливом часу та розвитку науки змінюються та набувають нових форм. Водночас основні підходи щодо розуміння вини в межах відповідних концепцій залишаються незмінними.

Аналіз спеціальної літератури засвідчив, що в кримінальному праві існують кілька підходів до досліджуваної проблематики. Так, за часів егалітарного періоду склалася концепція психологічного розуміння вини, яка фактично відтворювала положення кримінального права XIX століття з цього питання [34, с. 8-9].

Саме така концепція вини діставала підтримку серед більшості науковців кінця XIX - початку XX століття, які зазначали, що особа підлягає відповідальності лише за умов, коли вчинене посягання знаходиться у відповідному співвідношенні зі свідомістю такої особи, із його «психічною роботою», що передує такій діяльності, та виявляє його бажання чи волю [35, с.452]. «Вина - це зміст волі, який заслуговує на осуд суб'єкта» [36, с. 394].

Таким чином, основний зміст вини становив психічне ставлення злочинця:

а) до моменту відповідності діяння складу злочину та;

б) до моменту протиправності діяння.

При цьому представники цієї теорії наголошують, що вина - це психічне ставлення суб'єкта до вчиненого діяння. Саме таке розуміння вини було закріплено у ст. 48 Кримінального уложення 1903 р., де передбачалося, що суд при визначенні ступеня покарання повинен

розрізняти вчинення діяння з усвідомленням заподіяної шкоди або з неосвіченості та несвідомості.

Проведений аналіз дає підстави дійти висновку, що з суб'єктивної сторони, всі досліджувані склади злочинів вчиняються умисно, при цьому, як правило, з прямим умислом, що говорить про характер суспільної небезпеки.

## 2.2. Кримінологічна характеристика кіберзлочинів проти власності

Необхідність у наданні кримінологічної характеристики насамперед викликана подальшим з'ясуванням кількісних та якісних показників злочинності, що є необхідною умовою успішного контролю вказаного явища та запорукою ефективної діяльності у запобіганні злочинності. Тому важливе значення приділяється кримінологічній характеристиці, тобто елементам, що у своїй сукупності і взаємозв'язку становлять її структуру. О. Г. Кальман визначав, що така характеристика вирізняється наявністю кількісно-якісних статистично значущих показників про злочини та особу злочинця, що виражають ступінь їх суспільної небезпеки [37, с. 78].

Поняття «кримінологічна характеристика», що використовується в кримінологічних дослідженнях, визначено як: «сукупність даних про певний вид злочинів або конкретне суспільно небезпечне діяння, що використовується для їх запобігання» [46, с. 125].

Якісними показниками злочинності є такі, що визначають структуру злочинності, географію та динаміку.

Загалом: «Злочинність слід розглядати в динаміці, адже її рівень, структура та характер, розглянуті в статичному стані, не дадуть змоги з'ясувати її рух, наступність між різними станами цього явища в певні проміжки часу, перешкоджаючи розробленню відповідних прогнозів» [39, с. 298]. Проте, офіційна статистика, на жаль, не сприяє грунтовному

дослідженню кіберзлочинності у зв'язку з відсутністю показників у кримінальній статистиці України. Більшість злочинів, що вчиняться з використанням комп'ютерних технологій, знаходяться у звітності різних підрозділів правоохоронних органів серед економічної та інших видів злочинності.

Серед якісних кримінологічних показників важливе місце посідає структура злочинності. Як зазначають В. В. Василевич та А. П. Мозоль: «структура злочинності - це внутрішня будова злочинності, яку визначають:

а) за об'єктами посягання;

б) за об'єктивною стороною злочину;

в) за ознаками суб'єктивної сторони;

г) за особою злочинця;

ґ) за мірою покарання» [40, с. 159].

У провідних, економічно розвинутих країнах відсоток кіберзлочинності вимірюється кількісно тисячами, а економічні збитки становлять мільярди доларів США.

За всіма вказаними підходами до структури злочинності, на наш погляд, можна віднести такі обов'язкові елементи:

1) внутрішню побудову загального масиву злочинності на відповідній території за певний період часу;

2) класифікаційні групи злочинів, поділені за об'єктивним та суб'єктивними ознаками злочинів чи розділами Особливої частини КК України;

3) частку злочинів певного виду за родовим об'єктом відповідно до загальної кількості офіційно зареєстрованих злочинів, що в сукупності виражає питому вагу.

Слід зазначити, що: «Стан злочинності - це кількість вчинених злочинів, а також осіб, які їх вчинили, на тій чи іншій території за конкретний проміжок часу. Показники стану злочинності

відображаються лише в абсолютних цифрах. Проте, говорячи про злочинність у цілому та надаючи їй загальну оцінку, інколи допускається застосування такого поняття як - загальний стан злочинності. Цей термін використовується з метою одночасної оцінки всіх п'яти показників злочинності» [41, с. 202].

«Динаміка злочинності - це зміна показників стану, рівня, структури злочинності за певні проміжки часу. Зазвичай динаміка злочинності відображає зміну її кількісних показників за місяць, квартал, півріччя, рік, п'ять, десять років» [41,236].

Основним показником динаміки є темп зростання чи зниження кількості зареєстрованих злочинів. Цей показник вказує на скільки разів або на скільки відсотків кількість злочинів чи злочинців більша або менша за аналогічний показник, узятий для порівняння. За базу порівняння може бути взятий показник першого року періоду, за який аналізується злочинність, або показник кожного попереднього року.

Якщо розглядати динаміку кіберзлочинів проти власності, її зміст не може обмежуватися виключно показниками офіційної статистики 3 урахуваннмя високого рівня латентності. Тому можливим видається аналіз даного показники з урахуванням оцінки відомостей із засобів масової інформації, аналізу емпіричної бази, опитування, інтерв'ювання компетентних осіб у сфері кібербезпеки [42, с. 52].

На основі аналізу матеріалів слідчої та судової практики визначено, що найбільш поширеним видом злочинів проти власності є шахрайство, що має динаміку до зростання за кількісними, та якісними показниками. Так, якщо у 2018 р. частка цього виду злочинів проти власності від усіх посягань на власність становила 5,8%, то у 2019 р. вона була вже 19,6%. Таке зростання обсягу цього виду злочинних посягань на власність пов'язано зі стрімким розвитком телекомунікацій та глобальних комп'ютерних мереж, які полегшують умови вчинення

злочинів проти власності та утворюють нові склади шахрайства, як кібершахрайство.

Викладене позначається на динаміці та структурі кіберзлочинності: «відбувається скорочення насильницьких злочинів проти власності, стає молодшим сам злочинець. У зв'язку з цим науковцями обговорюються питання щодо необхідності як зниження, так і розширення меж віку кримінальної відповідальності».

Визначено високий рівень та неможливість їх відшкодування жертвам кіберзлочинності. Так, у 2013 р. потерпілими від кіберзлочинів стали 341 млн., а у 2019 р. - вже 894 млн. осіб. Близько 70% інтернет-користувачів хоча б раз стикалися з шахрайством в Мережі, та ці показники щороку збільшуються, на підставі чого зроблено висновок про високий рівень зростання злочинів зазначеної категорії.

Означена криміногенна ситуація щодо зростання кібрезлочинів проти власності дає можливість зробити певні висновки з метою подальшої розробки заходів запобігання:

- динаміка кіберзлочинів має сталу тенденцію до зростання з швидкими темпами приросту;

- збільшення матеріальних та моральних збитків від кібератак;

- якісна характеристика кбірезлочинності дає можливість визначити, що більша частина умисних злочинів у сфері комп'ютерних технологій мають корисливий мотив.

Виходячи з означенного, найбільш розповсюджені та характерні для даного виду злочинів причини та умови, які сприяють їх вчиненню є наступні:

1) Соціальні протиріччя між потребами в програмному забезпеченні із нормативною регламентацією можливості використання комп'ютерної продукції та неможливістю задовольняти ці потреби на законному рівні;

2) В пошуках за прибутками на ринку продаж комп'ютерних новинок присутня велика кількість піратської продукції, тому система саморегулювання ринку в зазначеній ситуації не гарантує захисту законних власників програмного забезпечення, а тому держава зобов'язана втручатися в регулювання таких правовідносин;

3) Корислива мотивація комп'ютерних злочинців, мета яких полягає у отриманні будь-яких матеріальних чи нематеріальних благ. У зв'язку з цим, з'явилася нова категорія професійних комп'ютерів, які мають необхідне комп'ютерне устаткування з метою отримання незаконної вигоди здійснюють несанкціоноване втручання до компютерної мережі, у тому числі через мережу Інтернет, та займаються викраденням компютерної інформації, що становить комерційний інтерес;

4) В кримінальному, цивільному та адміністративному законодавстві остаточно не врегульовано питання щодо оцінки завданих збитків від вчинення кіберзлочинів, а також не визначені критерії, відповідно до яких суд повинен призначати розмір завдавданих збитків [43, с. 122-123].

На основі аналізу статистичних даних причиновий комплекс щодо зростання рівня кіберзлочинів в Україні розташовано наступним чином:

1) 61,5 % - це можливість здійснювати незаконний доступ до конфіденційної інформації або використання даних з корисливою метою;

2) 12,7 % - віртуалізація, що є однією з причин збільшення кількісних та якісних показників кіберзлочинів проти власності, яка породжує кібердевіантність та кіберзлочинність;

3) 8,4 % - анонімність;

4) 9,1 % - зростання кіберзлочинності серед неповнолітніх, спровоковане стрімким розвитком інформаційно-телекомунікаційних технологій;

5) 8,3 % - формування інформаційно-комунікативного віртуальності, глобальності, фрагментарності.

Запропоновано до таких причин відносити:

- соціальні фактори, обумовлені наявністю протиріч між необхідністю легального якісного програмного забезпечення в межах кібернетичної безпеки та відсутністю законодавчої регламентації програмного забезпечення; економічні фактори, обумовлені наявністю корисливої зацікавленості у вчиненні кіберзлочинів проти власності, вартісне програмне ліцензійне забезпечення;

- організаційно-правові фактори - неналежне правове забезпечення та відсутність комплексної державної програми протидії кібрезлочинам та недоліки і неналежна компетенція в діяльності правоохоронних та судових органів;

- кримінологічний фактор - високий рівень латентності кіберзлочинів проти власності, відсутність єдиної судової практики точності кваліфікації злочинів означеної категорії, організований та професійний характер кіберзлочинів в межах аналізу суб'єкта злочину.

# РОЗДІЛ 3
# СТРАТЕГІЯ ПРОТИДІЇ КІБЕРЗЛОЧИНАМ ПРОТИ ВЛАСНОСТІ: ВІТЧИЗНЯНИЙ ТА МІЖНАРОДНИЙ ДОСВІД

## 3.1. Заходи запобігання кіберзлочинам проти власності в Україні

Вивчивши історію виникнення кіберзлочинності в Україні та інших країнах, визначивши основні види кіберзлочинів проти власності, виявивши їх основні причини та умови, можна сформувати систему заходів протидії кіберзлочинів проти власності в Україні, зокрема спрямованих на:

1) виявлення, усунення або послаблення і нейтралізацію причин кіберзлочинності проти власності;

2) виявлення і усунення ситуацій, безпосередньо мотивуючих або провокують на вчинення злочинів проти власності в кіберпросторі;

3) виявлення осіб підвищеного кримінального ризику і зниження цього ризику;

4) викриття осіб, поведінка яких може вказувати на реальну можливість вчинення кіберзлочинів проти власності, і розробка шляхів стримуючого і коригуючого впливу на них.

Під запобіганням злочинів слід розуміти: «систему заходів економічного, соціально-культурного, виховного та правового характеру, що здійснювалися державними органами та громадськими організаціями з метою боротьби зі злочинністю та усунення її причин. Складовою частиною цих заходів було законодавство та практична діяльність правоохоронних органів, безпосередньо суду, який застосовував специфічні заходи боротьби зі злочинністю - кримінальне покарання» [44, с. 366].

Попередження в кримінальному праві - один із примусових заходів виховного впливу, що може бути призначений неповнолітньому,

який вперше вчинив злочин невеликої або середньої тяжкості [45, с. 343].

В.М. Кудрявцев та В.Є. Емінов розглядають попередження як багаторівневу систему заходів та суб'єктів, які здійснюють відповідні заходи, що спрямована на:

«а) виявлення, усунення чи послаблення або нейтралізацію причин злочинності, окремих її видів, а також умов, що їм сприяють;

б) виявлення та усунення ситуацій на окремих територіях чи у певному середовищі, безпосередньо тих, що мотивуть чи провокуть вчинення злочинів;

в) виявлення у структурі населення груп підвищеного кримінального ризику та зниження цього ризику;

г) виявлення осіб, поведінка яких вказує на реальну можливість вчинення злочину, і надання стримувального та корекційного впливу, а у випадку необхідності - вплив на їх найближче оточення» [46].

Основними напрямами є: «запобігання, спрямоване на виявлення та усунення умов технічного й соціального оточення індивіда, які можуть провокувати злочини; на виявлення заздалегідь потенційних правопорушників з метою втручання в життя окремих індивідів або цілих груп у зв'язку з визначеними на даний час криміногенними обставинами; запобігання, що стосується лише злочинців, з метою недопущення рецидиву злочинів» [47, с. 211-214].

Як вже зазначалося, Указом Президента України від 15.03.2016 р. № 96/2016 було: «затверджено рішення Ради національної безпеки і оборони України від 27 січня 2016 року Про Стратегію кібербезпеки України» [18]. Таким чином, в національному законодавстві України було передбачено створення «активного кіберзахисту» та забезпечення належних умов для безпечного використання кіберпростору, інтересах держави і суспільства. Головним суб'єктом забезпечення кібербезпеки в

Україні відповідно до даної стратегії є Національний координаційний центр кібербезпеки.

Основні шляхи щодо кримінологічних засад протидії кіберзлочинам закріплені у Стратегії кібербезпеки України, «яка була розроблена на виконання Стратегії національної безпеки України від 2015 року, затверджена рішенням Ради національної безпеки і оборони України та введена в дію Указом Президента України» [18] від 27.01.2016 р.. Провідним розробником Стратегії кібербезпеки України виступила Державна служба спеціального зв'язку та захисту інформації. В роботі над документом приймали участь представники Громадської Ради при Держспецзв'язку, представники приватного бізнесу, експерти НАТО, ОБСЄ, RAND corporation. Також документ був узгоджений з усіма іншими державними службами, які мають відношення до кібербезпеки, був доопрацьований в Уряді та в Раді національної безпеки і оборони України.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» [19] основними суб'єктами національної системи кібербезпеки є: «Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України» [19].

Даний нормативно-правовий акт також визначає: «державно-приватну взаємодію у сфері кібербезпеки та встановлює відповідальність за порушення законодавства у цій сфері та контроль за законністю заходів із забезпечення кібербезпеки України» [19].

Також зазначається, що: «Організаційне забезпечення системи кібербезпеки також можна розглядати як цілеспрямовану діяльність суб'єкта забезпечення кібербезпеки, пов'язану зі створенням і впорядкуванням організаційних структур, найбільш доцільних для забезпечення безпеки у кіберпросторі; впорядкуванням процесу

управління у сфері забезпечення безпеки у кіберпросторі, забезпеченням найліпших умов для прийняття та реалізації відповідних управлінських рішень» [48, с. 8].

У свою чергу, В.І. Шакун пропонує низку таких напрямів:

«1. Здійснення глибокого перегляду ряду загальноприйнятих у теорії та практиці вихідних понять та підходів до проблеми злочинності і методів боротьби з нею.

2. Розробка пропозицій щодо заборони перепрофілювання та використання не за призначенням підліткових, молодіжних фізкультурноспортивних клубів та інших позашкільних навчально-виховних закладів, спортивних споруд незалежно від форм власності та підпорядкування.

3. Продовження роботи зі збереження та формування мережі державногромадських інститутів надання соціальної підтримки підліткам, організації їх змістовного дозвілля і відпочинку, зокрема: центрів соціальних служб для молоді, бюро, центрів з надання послуг учням і студентам у працевлатуванні у вільний від навчання та канікулярний час, системи підліткових, молодіжних фізкультурно-спортивних клубів, що функціонують за місцем проживання неповнолітніх» [49].

Слід зазначити, що значна частина кіберзлочинів, стає можливою завдяки необізнаності населення те недотриманню основних правил безпеки. Такими чинниками зокрема є:

1) обмежена кількість даних та інформації про кіберзлочини проти власності;

2) недостатній, а іноді і взагалі відсутній, рівень обізнаності щодо ризиків, які спричинені впровадженням нових платіжних платформ та сервісів, а також щодо пов'язаних з ними легалізацією та відмиванням коштів;

3) встановлення та використання неліцензійного програмного забезпечення;

4) ненадійне зберігання електронного цифрового підпису та кодів доступу клієнтами банківських установ;

5) недотримання елементарних правила безпеки при користуванні Інтернет-банкінгом та спеціальними платіжними засобами в мережі Інтернет; невиконання політики кодової та інформаційної безпеки.

У зв'язку з цим, найефективнішу користь в попередженні кіберзлочинності проти власності, мають саме інформаційно-просвітницькі заходи щодо нових ризиків та загроз в комп'ютерних системах.

### 3.2. Міжнародний досвід у сфері запобігання кіберзлочинам проти власності

Кіберзлочини є злочинами транснаціональними, так вони, найчастіше відбуваються поза державними кордонами. У зв'язку з цим у багатьох країнах світу сформувалися власні уявлення щодо боротьби з кіберзагрозами. Зрозумілим є те, що для втілення найбільш ефективних заходів боротьби з кіберзлочинами проти власності в нашій державі, необхідно звернутися до досвіду міжнародних організацій і зарубіжних країн. Через транскордонний характер таких кіберзлочинів необхідність у міжнародному врегулюванні відповідної проблеми виникла ще в 70-80-х роках минулого століття.

На 93-му пленарному засіданні 56-ї сесії Генеральної Асамблеї ООН, була прийнята Резолюція №56 / 261 від 31 січня 2002 року, що закликає до посилення боротьби з комп'ютерною злочинністю. У Резолюції було запропоновано: «розвивати національні законодавства країн-членів ООН про кримінальну відповідальність за кіберзлочини і розробити комплекс заходів щодо боротьби зі злочинами, пов'язаними з використанням високих технологій та комп'ютерів».

У свою чергу, у Будапештській Конвенції «Про кіберзлочинність» від 23.11.2001 р. містяться положення щодо протидії кіберзлочинності У 2005 р. Україна ратифікувала цю Конвенцію та імплементувала положення міжнародного акта у вітчизняне законодавство.

Питанням співробітництва компетентних органів різних держав у боротьбі з комп'ютерними злочинами присвячена глава з Конвенції «Міжнародне співробітництво» щодо екстрадиції, спільної діяльності державучасниць у сфері боротьби з комп'ютерними злочинами та досягнення узгодженості для збору доказів у електронній формі. Пропонуємо розглянути основні форми взаємодії.

Отже, Конвенція про кіберзлочинність на сьогоднішній день є одним з фундаментальних міжнародно-правових актів у сфері права телекомунікацій. Її можна поставити в один ряд з Окінавською хартією глобального інформаційного суспільства. Однак якщо в хартії йдеться скоріше про закріплення загальної концепції розвитку інформаційно-комунікаційних технологій, то в Конвенції пропонується реальний механізм правового регулювання.

Також слід зазначити, що «Конвенція Ради Європи про кіберзлочинність» [53] від 21.11.2001 р. поділяє всі кіберзлочини на 5 груп:

«1) злочини проти конфіденційності, цілісності й доступності комп'ютерних даних;

2) злочини, пов'язані з використанням комп'тера як засобу вчинення злочинів, тобто як засіб маніпуляції інформацією (комп'ютерне шахрайство та підроблення);

3) злочини, повязані з контентом, тобто змістом даних, розміщених в комп'ютерних мережах;

4) злочини, пов'язані з порушенням авторського права і суміжних прав;

5) акти расизму і ксенофобії» [53].

Особливу роль в питанні протидії міжнародним кіберзлочинам виконувала «Велика Вісімка» (G-8). Так, 26 червня 1996 року у Франції, у місті Ліон (Франція) відбулися чергові збори «G-8», підсумком якого став Регламент № 16, згідно якого держави-члени «G-8» повинні змінити законодавчі норми, задля гарантування криміналізації та караності діянь, які вчиняються з використанням сучасних технологій.

На зустрічі: «Держави-члени «G-8» домовилися про вдосконалення зв'язку між співробітниками правоохоронних органів різних країн з метою обміну досвідом та сприяння в подальшій діяльності. На виконання даного Регламенту була створена «Ліонська група». Через деякий час, за прикладом Німеччини і Франції, в інших країнах-членах «G-8» були створені спеціальні правоохоронні органи, які в цілодобовому режимі здійснюють комплекс заходів щодо розвитку міжнародного співробітництва в боротьбі з кіберзлочинністю» [50, с. 12].

В той час в Німеччині у складі Поліцейського управління Мюнхена з 1994 року існувала спеціальна Група по боротьбі зі злочинами у сфері високих технологій, а в Франції - Служба з протидії зловживанням в сфері високих технологій. У Великобританії у 2001 році було створено Національний підрозділ по боротьбі зі злочинами у сфері високих технологій, а 1 квітня 2006 було створено Національне агентство боротьби з організованою злочинністю.

У зв'язку з реформою 2013 року «функції по боротьбі з комп'ютерною злочинністю були передані Національному підрозділу протидії кіберзлочинам» [51, с. 24].

В 2013 році влада Японії повідомила про створення відділення поліції з боротьби з кіберзлочинами. Європейський союз також відреагував на проблему кіберзлочинності, створивши цілу мережу правоохоронних органів для боротьби з нею: «Європейський центр кіберзлочинів», який складається з 10 самостійних груп та команд, які

здійснюють аналіз статистичних даних, підготовку спеціальних способів виявлення і затримання кіберзлочинців тошо.

Слід зазначити, що: «У 2010 році в Бразилії пройшов дванадцятий Конгрес ООН, на якому обговорювалися питання боротьби з комп'ютерними злочинами і розробки державної кібербезпеки. На Конгресі було розглянуто рекомендації щодо необхідності вивчення питання кіберзлочинності і прийняття рішення по розробці Глобальної Конвенції щодо боротьби з нею» [52, с. 311, 312.].

Серед найпоширеніших напрямків державної політики щодо боротьбі з кіберзлочинами в різних країнах стали:

«1) захист стратегічних і урядових інформаційних систем від кібератак і актів кібертероризму (Німеччина, Великобританія, Канада, Литва, Люксембург, Нідерланди, США, Естонія);

2) правове регулювання, а також вдосконалення кримінального та інформаційного законодавства (Німеччина, Канада, Люксембург, США, Естонія, Японії);

3) захист інформації та персональних даних (Словаччина, Франція, Чеська Республіка, Литва);

4) державне і міжнародне співробітництво (Люксембург, США, Японія). Серед інших напрямків можна виділити навчання співробітників правоохоронних органів і інформування громадян про кіберзагрози (Люксембург, Естонія) та просування міжнародних стандартів економічної безпеки (США, Люксембург)» [47, с. 83].

Ґрунтуючись на вищенаведеному, можна зробити наступні висновки:

1) найпоширенішим напрямом державної політики різних країн є захист стратегічних та урядових систем, таких як інформаційна система на об'єктах атомної енергетики, об'єктах бюджетної та фінансової сфери, державних банках, в нафтопромисловому і військово-промисловому комплексі;

2) заходом протидії більшості країн є правове регулювання: вдосконалення законодавства, криміналізація нових діянь, посилення відповідальності за існуючі кіберзлочини;

3) основними складами кіберзлочинів проти власності в кримінальному законодавстві різних країн є: кібершахрайство та кібервимагання;

4) криміналізація нових складів кіберзлочинів не є оптимальним рішенням для кримінального законодавства України. Найбільш ефективним рішенням, було б вдосконалення чинного кримінального законодавства за рахунок розширення поняття «шахрайства», «вимагання», а також врахування використання засобів комп'ютерної техніки в якості обставини, що обтяжують покарання.

# ВИСНОВКИ

Провівши аналіз кримінально-правової та кримінологічної характеристики кіберзлочинів проти власності, дослідивши методи протидії кіберзлочинності у вітчизняному та міжнародному досвіді ми можемо зробити наступні висновки.

1. Аналіз розвитку кіберзлочинності дозволив встановити, що масове поширення комп'ютерів і поява інформаційних мереж спровокувало виникненню нового виду злочинності - кіберзлочинності, історію становлення якої в Україні і світі можна умовно розділити на два етапи: до і після появи глобальної інформаційної мережі «Інтернет», яка і породила кіберпростір у звичному нам вигляді. Перший етап - 1960-1991 рр., другий - 1991 р. - до сьогодні.

2. Проаналізовані теоретичні концепції кваліфікації сприяли формуванню висновку щодо найпоширеніших видів кіберзлочинів:

1) Картинг;

2) Фішинг;

3) Вішинг;

4) Онлайн-шахрайство;

5) Піратство;

6) Кадр-шарінг;

7) Соціальна інженерія;

8) Мальваре;

9) Протиправний контент;

10) Рефайлінг.

3. Кіберзлочини проти власності визначено як самостійний вид комп'ютерних злочинів, що має об'єктом суспільні відносини, а кіберзлочини проти власності є лише частиною злочинів, що вчиняються у кіберпросторі, ознаками яких є анонімність, транскордонність, дистанційність, а також використання комп'ютера, вірусів або інших шкідливих програм, інформаційно-

телекомунікаційних мереж і кіберпростору. Єднальними ознаками всіх кіберзлочинів визначено сферу їх вчинення - кіберпростір, інформаційно-телекомунікаційні мережі та засоби комп'ютерної техніки.

4. Правову основу кібербезпеки України становлять Конституція України, закони України «Про захист інформації в інформаційно-телекомунікаційних системах», «Про інформацію», «Про національну безпеку України», та інші закони, Конвенція Ради Європи про кіберзлочинність, міжнародні договори, Стратегія кібербезпеки України, нормативно-правові акти. Найважливішими з-поміж них є Конвенція Ради Європи про кіберзлочинність та Стратегія кібербезпеки України.

5. Проаналізувавши кримінально-правову характеристику кіберзлочинів проти власності дійшли таких висновків:

1) родовим об'єктом є відносини власності, що забезпечують матеріальний добробут особи, суспільства і держави. Залежно від способу вчинення таких кіберзлочинів додатковим об'єктом можуть виступати відносини у сфері комп'ютерної інформації;

2) криптовалюта, як цифровий інформаційний продукт, тобто сукупність унікальних комп'ютерних даних, об'єднаних у віртуальний носій, що містить всі ознаки товару, визначена вартістю і належать за правом власності іншій особі, може виступати предметом кіберзлочинів проти власності;

3) ознаками об'єктивної сторони кіберзлочинів проти власності є діяння у вигляді дії, дистанційний спосіб їх вчинення; віддаленість один від одного місця вчинення суспільно небезпечного діяння і місця настання наслідків; використання кіберпростору як основного засобу вчинення такого злочину;

4) в залежності від конкретних складів, суб'єкт таких злочинів може бути як загальним, так і спеціальним;

6. З'ясовано, що кількісні та якісні показники кіберзлочинів проти власності характеризуються сталою тенденцією до зростання і у частці злочинів проти власності близько 90 % становить шахрайство та кібершахрайство, що зумовлено стрімким розвитком телекомунікацій і глобальних комп'ютерних мереж.

7. Досліджено причини та умови кіберзлочинів проти власності: віртуалізація; анонімність користувачів кіберпростору; зростання кіберзлочинності серед неповнолітніх, спровоковане стрімким розвитком інформаційно-телекомунікаційних технологій; формування інформаційно-комунікативного середовища з ознаками віртуальності, глобальності, фрагментарності.

8. Визначено, що заходами запобігання кіберзлочинам проти власності є: вдосконалення чинного законодавства за рахунок розширення поняття «шахрайства», «вимагання», врахування використання засобів комп'ютерної техніки як обставин, що обтяжують покарання та визначення як кваліфікуючої ознаки завдання істотної шкоди при вчиненні злочину із використанням комп'терної техніки.

Аналіз стратегій кібербезпеки різних країн дозволив сформулювати висновок, що найбільш загальним напрямом державної політики є захист стратегічних та урядових інформаційних систем, таких як інформаційна система на об'єктах атомної енергетики, об'єктах бюджетної та фінансової сфери, державних банках, в нафтопромисловому та військово-промисловому комплексі та інших об'єктах критичної інфраструктури.

На державному рівні, з метою запобігання кіберзлочинам проти власності, найважливішими заходами є:

1) активізувати державну інформаційну політику щодо забезпечення входження України до єдиного світового інформаційного простору;

2) розробити програму кібербезпеки в інформаційному просторі України з метою посилення заходів запобігання кіберзлочинам проти власності;

3) удосконалення правового регулювання, визначення та організація реалізації державної політики у сфері інформаційних відносин;

4) формування нових органів, відділів, що координують діяльність щодо запобігання кіберзлочинам.

9. Ґрунтуючись на проведеному аналізі міжнародного досвіду у сфері протидії кіберзлочинам проти власності, доведено, що:

1) загальним напрямом державної політики різних країн є захист стратегічних та урядових інформаційних систем, таких як інформаційна система на об'єктах атомної енергетики, об'єктах бюджетної та фінансової сфери, державних банках, у нафтопромисловому і військово-промисловому комплексах;

2) основним заходом запобігання в більшості країн є правове регулювання, вдосконалення кримінального, адміністративного та інформаційного законодавства, криміналізація нових діянь, посилення відповідальності за вже наявні кіберзлочини;

3) найпоширенішими складами кіберзлочинів проти власності в кримінальному законодавстві різних країн є: комп'ютерне шахрайство або комп'ютерне розкрадання; викрадення відомостей, що становлять комерційну таємницю шляхом неправомірного доступу до комп'ютерної інформації; вимагання з використанням засобів комп'терної техніки; несанкціоноване проникнення в комп'ютерні мережі.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Півняк Г.Г., Бусигін Б.С., Дівізінюк М.М. та ін. Тлумачний словник з інформатики. Дніпропетровськ, Нац. Гірнич. Ун-т, 2010. 600 с.

2. Компьютерная преступность. URL: http://ulfek.ru/osnovy-bezopasnosti-informationnykh-tekhnologij/3469-kompyuternaya-prestupnost.html (дата звернення: 31.01.2020).

3. История компьютерного андеграунда. Хакеры 80-х. URL: http://bugtraq.ru/library/underground/underground4.html (дата звернення: 31.01.2020).

4. Мобильная связь и компьютерные сети в СССР. URL: http://www.rusproject.org/node/72 (дата звернення: 31.01.2020).

5. Безкоровайный М.М., Татузов А.Л. Кибербезопасность – подходы к определению понятия. *Вопросы кибербезопасности*. 2014. № 1 (2). С. 22-27.

6. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 07.09.2005 р. № 2824-IV / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2824-15 (дата звернення: 31.01.2020).

7. Про ратифікацію Додаткового протоколу до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи: Закон України від 21.07.2006 № 23-V / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/23-16 (дата звернення: 31.01.2020).

8. Логінова Н.І., Дробожур Р.Р. Правовий захист інформації: навч. посіб. Одеса: Фенікс, 2015. 264 с.

9. Голіна В.В., Головкін Б.М. Кримінологія: Загальна та Особлива частини: навч. посіб. Харків: Право, 2014. 513 с.

10. Голуб А. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби. URL: http://www.gurt.org.ua/articles/34602 (дата звернення: 03.02.2020).

11. Протидія кібершахрайству – убезпечити кошти можливо. URL: https://diamantbank.ua/content/upload/files/Press-release_Cybercrime_Combating_Conference_EMA_(ukr).pdf (дата звернення: 03.02.2020).

12. Пфо О.М. Основні поняття і класифікація кіберзлочинності. URL: http://dspace.kntu.kr.ua/jspui/bitstream/123456789/5119/1/AUConferenceCyberSecurity_November2016_p33.pdf (дата звернення: 03.02.2020).

13. А. Дубровик-Рохова. Що потрібно знати про «фішинг», «вішинг» і «кеш-треппінг»? URL: https://day.kyiv.ua/uk/article/ekonomika/shcho-potribno-znaty-pro-fishyng-vishyng-i-kesh-trepping (дата звернення: 03.02.2020).

14. Антонюк Н.О. Кримінальна відповідальність за заподіяння майнової шкоди шляхом обману або зловживання довірою: дис. ... канд. юрид. наук: 12.00.08. Львівський національний ун-т ім. Івана Франка. Львів, 2006. 219 с.

15. Хилюта В.В. Хищение: понятие, признаки, проблеми квалификации: монография. Гродневский государственный университет имени Янки Купалы. Гродно: ГрГУ им. Я. Купалы, 2011. 335 с.

16. Дзундзюк В.Б., Дзундзюк Б.В. Поява і розвиток кіберзлочинності. URL: http://nbuv.gov.ua/j-pdf/DeBu_2013_1_3.pdf (дата звернення: 10.02.2020).

17. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України; Стратегія від 26.05.2015 № 287/2015 / База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/287/2015 (дата звернення: 10.02.2020).

18. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України; Стратегія від 15.03.2016 № 96/2016 / База даних

«Законодавство України». URL: https://zakon5.rada.gov.ua/laws/show/96/2016 (дата звернення: 10.02.2020).

19. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 10.02.2020).

20. Дубов Д., Ожеван М. Кібербезпека: світові тенденції та виклики для України. Київ: НІСД, 2016. 30 с.

21. Dr. Mike McGuire and Samantha Dowling Cybercrime: A review of the evidence Summary of key findings and implications // Home Office Research Report 75. University of Surrey, October, 2013. P. 29., c, 5.

22. Берзін П., Куцевич М. Неправомірний випуск й використання електронних грошей, що вчиняються в системах інтернет-розрахунків (проблеми кримінально-правової кваліфікації). *Вісник Київського національного університету імені Тараса Шевченка. Юридичні науки*. № 4 (98). 2013. С. 13-16.

23. Офіційний сайт «ІТАР-тасс». URL: http://itar-tass.com/ekonomika/783989 (дата звернення: 14.02.2020).

24. Форум «Ламборджині». URL: http://lamborghininewportbeach.blogspot.com/%202013/12%20/%20the-bitcoin-saga-continues.html (дата звернення: 14.02.2020).

25. Безкоровайный М.М., Татузов А.Л. Кибербезопасность – подходы к определению понятия. Вопросы кибербезопасности. 2014. № 1 (2). С. 39-41.

26. Безкоровайный М.М., Татузов А.Л. Кибербезопасность – подходы к определению понятия. Вопросы кибербезопасности. 2014. № 1 (2). С. 142.

27. Зотов В.В. Новые информационные технологи: фактор трансформации общественно-экономической формации или начало информационного общества. *Вестник Моск. академии рынка труда и информационных технологий.* 2006. С. 8–11.

28. Юзікова Н. Періодизація віку, з якого настає кримінальна відповідальність неповнолітніх: вітчизняна практика та європейський досвід. URL: http://do.gendocs.ru/docs/index-24101.html?page=27 (дата звернення: 20.02.2020).

29. Павлов В.Г. Субъект преступления и уголовная ответственность Санкт-Петербург: Лань; Фонд «Университет», 2000. 192 с.

30. Берзін П.С., Гацелюк В.О. Суб'єкт злочину. *Вісник Асоціації кримінального права України*. 2013. № 1(1). С. 142–159.

31. Борзенков Г.Н. Специальный субъект преступления. Курс уголовного права / под. ред. Н.Ф. Кузнецовой, И.М. Тяжковой. Москва: РГБ, 2004. С. 286.

32. Кримінальне право України. Загальна частина: Підручник для вузів / ред. П.С. Матишевський, П.П. Андрушко, С.Д. Шапченко. Київ: Юрінком Інтер, 1997. 512 с.

33. Светлов А.Я. Субъективная сторона преступления. Уголовное право Украинской ССР на современном этапе: Часть общая. Киев: Наукова думка, 1995. С. 160–168.

34. Утевский Б.С. Вина в советском уголовном праве. Москва: Госюриздат, 1950. С. 8–9.

35. Таганцев Н.С. Русское уголовное право. Часть общая. Т. 1. С. 452.

36. Сергеевский Н.Д. Избранные труды / отв. ред. А.И. Чучаев. Москва: Буквовед, 2008. С. 394.

37. Кальман О.Г. Стан та головні напрямки попередження економічної злочинності в Україні: теоретичні та прикладні проблеми: монографія. Харків, Гімназія, 2003. 352 с.

38. Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності: прийнята резолюцією 55/25 Генеральної Асамблеї від 15.11.2000 р. // База даних

«Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/995_789 (дата звернення: 20.02.2020).

39. Лунеев В.В. Курс мировой криминологии: учеб. для магистров: в 2 т. Москва: Юрайт, 2012. Т. 1. Общая часть. С. 298.

40. Кримінологія: навч.-метод. посіб. / За заг. ред. проф. О.М. Джужи. Київ, 2008. С. 159.

41. Аванесов Г.А. Криминология. Учебник. 2-е изд., перераб. и доп. Москва: Изд-во Акад. МВД СССР, 1984. 500 с.

42. Кримінологія: Загальна та Особлива частина. Підручник для студентів юрид. спец. вищ. навч. закладів. / І.М. Даньшин, В.В. Голіна, О.Г. Кальман, О.В. Лисодєд; За ред. І.М. Даньшина. Харків: Право, 2003. 352 с.

43. Ковалев Д.И. Причины компьютерной преступности. *Вестник Академии*. № 4. 2011. С. 122-123.

44. Юридический энциклопедический словарь / Гл. ред. А.Я. Сухарев; Редкол.: М.М. Богусловский и др. 2-е изд., доп. Москва, 1987. С. 366.

45. Кримінальний кодекс України від 05.04.2001 р. № 2341-III / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 20.02.2020).

46. Криминология: учеб. / С.Б. Алимов, В.К. Звирбуль, В.С. Овчинский и др. под ред. акад. В.Н. Кудрявцева, проф. В.Е. Эминова. Москва: Юрист, 1995. 512 с.

47. Голіна В.В. Запобігання злочинності: проблеми оптимізації соціальної активності. *Вісник Академії правових наук України*. 2006. № 3 (46). С. 211–214.

48. Діордіца І.В. Поняття та зміст національної системи кібербезпеки. URL: http://goal-int.org/ponyattyata-zmist-nacionalnoi-sistemi-kiberbezpeki/ (дата звернення: 20.02.2020).

49. Шакун В.І. Урбанізіція і злочинність: Монографія. Київ, 1996. С. 114 – 116.

50. Сухаренко А.Н. Современные криминальные вызовы и угрозы информационной безопасности. URL: http://sartraccc.ru/Press/special/contr_terror_1_12.pdf (дата звернення: 20.02.2020).

51. Інформаційний ресурс «Информационная безопасность». URL: http://www.itsec.ru/newstext.php?news_id=91024 (дата звернення: 20.02.2020).

52. Киселев Д.И. Причины компьютерной преступности. *Вестник Академии*. № 4. 2011. С. 122–123.

53. Конвенція Ради Європи про кіберзлочинність: прийнята від 23.11.2001 р. // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 23.02.2020).

54. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006 р. № 3475-IV / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3475-15 (дата звернення: 23.02.2020).

55. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 23.02.2020).

56. Про державну таємницю: Закон України від 21.01.1994 р. № 3855-XII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3855-12 (дата звернення: 23.02.2020).

57. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 23.02.2020).

58. Про рішення Ради національної безпеки і оборони України від 17 листопада 2010 року «Про виклики та загрози національній безпеці України у 2011 році»: Указ Президента України від 10.12.2010 №

1119/2010 (втратив чинність) // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/1119/2010 (дата звернення: 23.02.2020).

59. Про внесення змін до деяких законів України щодо структури та порядку обліку кадрів Служби безпеки України: Закон України від 09.12.2011 р. № 4157-VI / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/4157-17 (дата звернення: 23.02.2020).

60. Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації: Рішення РНБО від 29.12.2016 р. // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/n0015525-16 (дата звернення: 23.02.2020).

61. Про внесення змін до деяких нормативно-правових актів Національного банку України з питань регулювання випуску та обігу електронних грошей: Постанова Національного банку України від 04.11.2010 р. № 481 // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/z1336-10 (дата звернення: 23.02.2020).