**МІНІСТЕРСТВО ФІНАНСІВ УКРАЇНИ**

**УНІВЕРСИТЕТ ДЕРЖАВНОЇ ФІСКАЛЬНОЇ СЛУЖБИ УКРАЇНИ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ПРАВА**

**НАУКОВА РОБОТА**

на тему:

**«Запобігання кібершахрайству в Україні»**

Студента (ки) 2 курсу, групи \_\_ПБК-19-6\_ напряму підготовки\_\_\_Навчально-науковий інститут права\_\_\_\_\_\_

спеціальності \_\_081\_Право КП\_\_\_\_\_

\_\_\_\_\_\_\_\_Лучук А.М.\_\_\_\_\_\_\_\_\_\_\_\_\_

(прізвище та ініціали)

Науковий керівник: \_\_доцент кафедри кримінального права та кримінології, кандидат юридичних наук, доцент Лугіна Н. А.\_\_\_\_

 (посада, вчене звання, науковий ступінь, прізвище та ініціали)

**Ірпінь – 2021**

**ЗМІСТ**

**ВСТУП………………………………………………………………………………..2**

**РОЗДІЛ 1. ІСТОРИКО-ТЕОРЕТИЧНІ АСПЕКТИ ПОХОДЖЕННЯ ТА РОЗВИТКУ КІБЕРЗЛОЧИННОСТІ……………………………………………..5**

* 1. Історія виникнення кіберзлочинності, її характеристика……………...............5
	2. Становлення поняття «кіберзлочинність» та його особливості……………..11

**РОЗДІЛ 2. ВИДИ ПРОТИПРАВНИХ ДІЯНЬ У СФЕРІ НОВІТНІХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ....................................................................16**

2.1 Кібершахрайство, як особливо небезпечний вид кримінальних правопорушень в інформаційному просторі……………………………………...16

2.2 Giveaway як прояв кібершахрайства у соціальних мережах…………….22

**РОЗДІЛ 3. ОПТИМІЗАЦІЯ ПРАВОВОГО РЕГУЛЮВАННЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ..........................................................................................27**

3.1 Перспективи та тенденції розвитку правового регулювання боротьби з кіберзлочинністю в Україні.......................................................................................27

3.2 Специфіка правового регулювання боротьби з кіберзлочинністю у зарубіжних країнах.........................................................................................................................32

**ВИСНОВОК..............................................................................................................36**

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ..............................................................38**

**ДОДАТКИ…………………………………………………………………………..41**

**ВСТУП**

 **Актуальність дослідження.** Сьогодні важко сперечатися щодо питання важливості мережі Інтернет у нашому житті. Інтернет відкриває перспективи для саморозвитку, отримання нових знань, пошуку роботи тощо. Цей ресурс ми використовуємо щодня, навіть свій вільний час можемо проводити на його просторах. Але, пропри це, Інтернет має й іншу сторону, ту, в якій щодня, щогодини вчиняються кримінальні правопорушення, адже платформа забезпечує користувачів повною анонімністю та не обмежує їх у своїх діях.

 До прикладу, у 2018 році в Україні працівники Департаменту кіберполіції Національної поліції України були залучені до більше ніж одинадцяти тисяч кримінальних проваджень, пов’язаних з кримінальними правопорушеннями у сфері новітніх інформаційних технологій. Протягом року було встановлено, що найбільша кількість протиправних діячів знаходиться в Києві, а також на території Одеської, Миколаївської та Львівської областей. [1]

Розвиток та становлення проблеми «кібершахрайства» є новим, тому малодосліджуваним, проте серед вчених, що займалися її вивченням варто виділити В. Голубєва, А. Долгової, К. Касперськи, М. Кастельса, Т. Кесаревої,

Л. Куракова, Р. Лемоса, А. Лукацького, І. Рассолова, С. Смірнова. Хоча усі науковці достатньо ґрунтовно розкривають проблему у своїх дослідженнях, необхідно все ж таки узагальнити накопиченні знання, зануритися у саму історію виникнення та розвитку кібершахрайства для можливості аналізу дій злочинців відносно розвитку технологій.

 Проаналізувавши наукові дослідження та досвід різних країн у боротьбі з даним явищем, можна стверджувати, що дана проблема є чи не найнебезпечніною у ХХІ столітті і є нагальна потреба вдосконалення законодавства та проведення роз’яснювальних дій у суспільстві, задля подальшого запобігання створенню нових груп кібершахраїв та розповсюдженню даного явища.

Тому наукова робота спрямована на глибоке дослідження теми «Запобігання кіберщахрайству в Україні», а також способів та методів діяльності кібершахраїв.

 **Метою наукової роботи** є комплексний аналіз запобігання кібершахрайству в Україні, розроблення на його основі науково обґрунтованих пропозицій і рекомендацій та подальшого вдосконалення норм законодавства, що регулюють дану сферу суспільних відносин.

 Відповідно до поставленої мети було сформовано **завдання:**

* дослідити та охарактеризувати історію виникнення кіберзлочинності;
* охарактеризувати етапи становлення поняття «кібезлочинність», охарактеризувати його;
* визначити поняття «кібершахрайство» та здійснити його змістовну характеристику;
* дослідити Giveaway як прояв кібершахрайства у соціальних мережах;
* виявити основні методи боротьби з кібершахрайством в Україні, встановити тенденції їх розвитку;
* визначити основні напрямки інших держав, у подоланні «кібершахрайства» та з’ясувати можливість їх імплементації у законодавство України.

**Об'єктом наукової роботи** є суспільні відносини, що виникають у наслідок дій, пов’язаних із запобіганням кібершахрайству в Україні.

**Предметом наукової роботи** є запобігання кібершахрайству в Україні.

Методологічну основу наукової роботи становить система загальнонаукових та спеціально наукових методів і підходів, що забезпечили об’єктивний аналіз предмета дослідження. З урахуванням специфіки теми, мети і завдань наукової роботи використовувалися такі методи: історичний метод допоміг дослідити причину виникнення та поширення кіберзлочинності в різних країнах та в Україні (підрозділ 1.1). Діалектичний метод дав змогу теоретично осмислити поняття «кіберзлочинність», основні способи та методи її функціонування (підрозділ 1.2). Формально-логічний метод допоміг встановити сутність «кібершахрайства», способи та наслідки його впливу на діяльність осіб та організацій (підрозділ 2.1, 2.2). Структурно-аналітичний метод використовувався при встановленні особливого виду «кібершахрайства» та характеристиці його існуванняі (підрозділ 2.2). Прогностичний метод дав змогу визначити основні способи та заходи протидії «кібершахрайству», а також основні напрямки розвитку державної політики в даній сфері (підрозділ 3.1, 3.2).

**Наукова новизна** даної наукової роботи полягає у ґрунтовному та комплексному дослідженні проблематики запобігання кібершахрайству в Україні, у з’ясуванні основних наслідків його існування, а також визначенні головних перспектив щодо запобігання виникненню та поширенню кібершахрайства в Україні, дано авторське визначення поняттю «кібершахрайство». Також робота має практичне значення, адже запропоновано внести зміни до Кримінального кодексу України, а саме обґрунтовується доцільність доповнення КК України ст. 363-4 «Кібершахрайство». Також запропоновано на рівні Кабінету Міністрів України розробити Програму запобігання поширенню кібершахрайству в Україні (Додаток А).

**Загальна характеристика роботи.** Робота складається зі вступу, трьох розділів, логічно об’єднаних у шість підрозділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи становить 44 сторінок, із них основного тексту – 36 сторінки. Список використаних джерел налічує 22 найменувань і займає 3 сторінки. 1 додаток розміщено на 4 сторінках

**РОЗДІЛ 1**

**ІСТОРИКО-ТЕОРЕТИЧНІ АСПЕКТИ ПОХОДЖЕННЯ ТА РОЗВИТКУ КІБЕРЗЛОЧИННОСТІ**

* 1. Історія виникнення кіберзлочинності, її характеристика

 З появою та розвитком всесвітньої мережі Інтернет, неабиякого розвитку набув новий вид злочинності – кіберзлочинність. На сьогодні йому приділяється особлива увага, адже величезний потенціал всесвітнього павутиння може використовуватися у корисливих, нечесних цілях. Кожного дня кіберзлочинці демонструють неймовірну майстерність у виконанні своїх суспільно небезпечних дій, відповідно, це ще більше звертає нашу увагу на актуальність цієї проблеми та закликає до якнайшвидшого пошуку найкращого шляху для її вирішення, який має включати в себе створення відповідних комп’ютерних систем і технологій, з високим рівнем безпеки в мережі та, звичайно, законодавчої бази, яка буде регулювати сповна це питання та встановлювати належні міри покарання за скоєння кримінальних правопорушень даного виду.

 Якщо розглядати традиційні види кримінальних правопорушень, такі як вбивство або крадіжка, то кіберзлочинність в порівнянні з ними, явище відносно нове, адже виникло воно саме з появою мережі Інтернет. Слід звернути увагу й на те, що сама по собі мережа Інтернет дає чималі можливості для вчинення кримінальних правопорушень. Основними її рисами є глобальність, анонімність користувачів, охоплення різної за віком та географічним положенням аудиторії, саме вони дозволяють кіберзлочинцям використовувати усі ресурси мережі вправно та уникати покарання за вчинення кримінальних правопорушень.

 Становлення та розвиток кіберзлочинності не можна відокремлювати від інформаційної революції, тому початком її відліку доцільно вважати шістдесяті роки минулого століття. Саме у 1962 р. професор Джон Лікрайдер, опублікував свою концепцію розповсюдженої комп'ютерної мережі «Galactic Network» [2, с.304] Головним припущенням даної концепції було те, що в майбутньому з’явиться глобальна мережа, приєднатися до якої зможе будь-який охочий, а також у тому, що дана мережа у своїй діяльності може об’єднувати усі комп’ютерні системи світу. Окрім загальної думки вчений детально охарактеризував принципи глобальної мережі, які стали основоположними для мережі Інтернет [3].

 Оскільки така ідея та її втілення були новим та надзвичайно цікавим процесом, який міг спростити життя мільйонів людей по всьому світі, то результат не змусив себе чекати. Поява першої мережі комп’ютерів ARPANet (Advanced Research Projects Agency Network), створеної за замовленням Міністерства оборони США. Головна мета даної розробки полягала у тому, щоб створити розподілену систему, яка б не мала чіткого центру, і складалася б з взаємозамінних частин. Спочатку ARPANet мала у складі чотири комп’ютери, розташованих у великих дослідницьких центрах.

 Головним завдання мережі була передача інформації та електронне листування, тому жодні серйозні елементи, що обмежували б доступ, в її структурі не існували, оскільки тоді ніхто навіть і не припускав появи злочинців у мережі. Цей недолік надалі успадкує і мережа Інтернет, що в подальшому призведе до явища «анархізм». Непродуманість аспектів безпеки і юридичного контролю при розробці технічних принципів мережі, у майбутньому буде наслідком широкого розповсюдження кіберзлочинності. Далі хотілося б навести кілька фактів, які охарактеризують розвиток кіберзлочинності.

 У 1970-х роках з’являються перші комп’ютерні злочинці, яких почали називати «хакерами». Хто ж точно був першим хакером сказати важко, проте у переважній більшості літературних джерел про хакерів та для хакерів, як першого професійного кіберзлочинця згадують Джона Дрейпера, який також проводив першу спеціалізацію хакерів, - фрікери (phreaker), скорочене від телефонний хакер (phone haker). У рядах фрікерів того часу були усім відомі Стів Возняк та Стів Джобс, які в майбутньому стали засновниками «Apple Computers». Саме вони налагодили виробництво пристроїв для злому мереж у домашніх умовах. І цей час доцільно вважати початком розвитку кіберзлочинності [4, с. 296].

 У 1983 р. в США, а саме у штаті Мілоукі було проведено перший арешт Інтернет-злочинця, про який відразу повідомили громадськості. Безпосереднім приводом для цього був перший зареєстрований Інтернет-злом, який був скоєний групою підлітків із шести осіб, які називали себе «група 414» (414 – міжміський телефонний код штату Мілоукі). Ними було зламано 60 комп’ютерів протягом дев’яти днів, серед зламаних були комп’ютери Лос-Аламоської державної лабораторії. Один з членів групи, після проведеного арешту, дав показання і інші її учасники отримали умовний термін відбування покарання [5].

 Загалом у 80-х роках прослідковується значне збільшення кількості комп’ютерних атак. Якщо в 1988 р. було тільки шість звернень із даного приводу до центру Інтернет-безпеки CERT, який почав діяти у 1988 р., то в 1989 р. число звернень налічувало 132, а в 1990 – вже 252 [6, с. 118 ]Явище кіберзлочинності перестає бути рідкістю, створюються великі групи хакерів, і мережа Інтернет починає ставати простором для незаконної діяльності злочинів. Ці події стають початком другого етапу розвитку кіберзлочинності, для якого характерною є поява нових спеціалізацій Інтернет-злочинців.

 У 1984 р. Фред Коен опублікував повідомлення про відкриття перших шкідливих комп’ютерних програм, які здатні до саморозмноження, і визначив їх терміном «комп’ютерний вірус». Також він створив програму, яка ілюструвала спосіб зараження одного комп’ютера іншим [7, с. 320 - 324].

 У 1986 р. в США прийнято перший комп’ютерний закон «The Computer Fraud and Abuse Act» [8] який забороняв незареєстрований доступ до будь-якої комп’ютерної системи. Особливістю даного закону був захист трьох видів несекретної інформації, а саме: інформації, що належить фінансовим установам (інформація щодо кредитних карток або ж особистих рахунків); інформації, що належить урядовим установам; інформації, що належить міжнародним або міжштатним організаціям.

 Окрім вищезазначених даних закон також містив статті, зміст яких забороняв пошкодження даних, прикладом цього є розповсюдження вірусів.

Цікаво, що у цьому ж році було заарештовано члена групи «Legion of Doom» Лойда Бланкеншипа, відомого під псевдонімом «The Mentor», який написав знаменитий «Маніфест хакера», - «The Haker Manifesto». Висловлені у даному маніфесті ідеї, навіть до сьогодні вважаються фундаментом хакерської ідеології та культури, а також зазнали чималої популярності в мережі Інтернет. Звичайно, не випадково зростання кількості кіберзлочинів співпало зі зростанням актуальності в комп’ютерному світі ідей хакерів, що є свідченням взаємозв’язку даних явищ.

 У 1994 р. світ дізнався про так звану «справу Володимира Льовіна», яку міжнародною кримінальною поліцією було віднесено до категорії «транснаціональний мережевий комп’ютерний злочин». Міжнародна організована злочинна група, що складалася з 12 людей, використовуючи мережу Інтернет та мережу передачі даних «Спрінт/Теленет», подолала захист від незареєстрованого доступу, намагалася здійснити 40 грошових переказів, загальна сума яких становить 10 млн. 700 тис. 952 долари США з особистих рахунків клієнтів банку, які знаходяться в 9 країнах світу, на інші рахунки, зареєстровані у США, Фінляндії, Ізраїлі, Швейцарії, Німеччині, Росії, Нідерландах [8, с. 18]. Це було перше велике міжнародне фінансове кримінальне правопорушення з використанням мережі Інтернет, про яке сповістили громадськість, і яке дало зрозуміти, що кіберзлочини можуть завдавати серйозного фінансового збитку.

 У 1998 р. 12-річний хакер зламав комп’ютерну систему, яка координувала водоспуск дамби Теодора Рузвельта в Арізоні. Небезпека його злодіянь полягала у тому, що у разі відкриття зливних воріт дамби вода могла б затопити міста Темп і Месе, загальна чисельність населення яких нараховувала близько 1 млн. жителів. Оцінка даного діяння стала підґрунтям для появи таких термінів як «Інтернет-тероризм», «комп’ютерний тероризм», «кібертероризм». До того ж, це вказало на те, що найбільш уразливою до кібератак є сама мережа Інтернет, адже усі її ключові елементи доступні з будь-якої точки світу.

 Поява явища «кібертероризм» і гучні справи про злодіяння міжнародних угрупувань, є свідченням того, що в цей час кіберзлочинність набуває такої ознаки як транснаціональність. Це і стало початком третього етапу у розвитку кіберзлочинності. Небезпечним фактором стало і те, що з розвитком мережі серйозні наслідки могли наступати не тільки у разі умисних кібератак, а й через некомпетентність або ж необережність спеціалістів. Так, у 1997 р. помилка співробітника «Network solutions» стала наслідком того, що сайти, назви яких мали в закінченні «.net» та «.com» стали недоступними. Що свідчить про те, що збій в роботі усієї глобальної мережі стався через неуважність однієї людини.

 Також у даний період кібератаки стають способом досягнення політичної мети. Доречно зазначити, що прикладом цього є Інтернет-страйки, при яких усі задіяні особи одночасно заходять на відповідний сайт, приєднуються до відповідного сервісу, відправляють електронні листи, пишуть у форумах із метою обмежити або припинити доступ на сайт іншим користувачам. У наслідок чого відбувається перенавантаження сайту або сервісу, у зв’язку з кількістю надходження запитів, що призводить до збоїв або до повної зупинки роботи ресурсу.

 Вперше акцію подібного типу здійснила група, що має назву **«Strano Network»**, яка протестувала проти політики французького уряду щодо питань ядерних програм та й в соціальній сфері. 21.12.1995 дана організована група протягом години здійснювала кібертерористичні дії проти сайтів урядових агентств. При цьому учасники атаки діяли з різних куточків світу за єдиною вказівкою: їм потрібно було за допомогою мережі Інтернет одночасно зайти на урядові сайти, після чого деякі з них дійсно були виведені з робочого стану [9, с. 132-137]

 Що далі, тим масштабнішою стає транснаціональність проблеми кіберзлочинності. Таким чином, конфлікт в Косово вважається першою Інтернет-війною, в якій групи користувачів комп’ютерної мережі використовували Інтернет для критики бойових дій в Югославії та НАТО, свідомо порушуючи при цьому роботу урядових комп’ютерів, в наслідок чого отримуючи доступ до сайтів, надалі з метою змінити вміст, «дефейс» (deface). Разом з тим у мережі Інтернет поширювалися історії про безпеку і жахи Інтернет-війни, як приклад наводилися різні факти та ідеї громадських діячів, та навіть політиків, саме вони здійснювали пропагандистські дії на надзвичайну кількість користувачів по всьому світі. Усі ці дії дають нам уявлення про те, яким був третій етап розвитку кіберзлочинності.

 Слід згадати, що в даний час практично будь-який політичний або збройний конфлікт йде поряд з організованою протидією у мережі Інтернет. Зокрема, у 2005 р. пройшов ряд кібератак, приводом для яких був шкільний підручник історії, який був виданий в Японії, та у своєму змісті перекручував зміст подій в Китаї в 1930-1940-х рр. ХХ ст. Якщо детально, то в ньому замовчувалися військові кримінальні правопорушення японських військ під час вторгнення [10] До списку сайтів, які опинилися під атаками, ввійшли сайти Міністерств, відомств, а також сайти найбільших японських корпорацій та сайти, що були присвячені Другій світовій війні. До того ж, у даній ситуації китайські хакери показали високий рівень майстерності та організованості, що свідчить про надзвичайну синхронність їх атак. Знаючи про те, що у Китаї діє надзвичайний контроль над мережею Інтернет, можна припустити, що дана атака була санкціонована державою. Використання кібератак для досягнення політичних цілей можна вважати початком четвертого етапу в розвитку кіберзлочинності.

 Отож, на сьогодні можна виділити 4 етапи розвитку кіберзлочинності.

**Перший етап** – поява такого явища як кіберзлочинність та субкультури хакерів.

**Другий етап** – вихід кіберзлочинності на міжнародну арену, поява національних груп хакерів та спеціалізацій кіберзлочинності.

**Третій етап** – набуття кіберзлочинністю транснаціонального характеру, поява явища кібертероризму та міжнародних угрупувань хакерів у всіх сферах кіберзлочинності.

**Четвертий етап** – використання мережі Інтернет для досягнення політичної мети, поява таких явищ як Інтернет-страйк та Інтернет-війна, а також використання кібератак проти урядів окремих держав.

1.2 Становлення поняття «кіберзлочинність» та його особливості

 Явище кіберзлочинності доволі нове, тому для повного усвідомлення його значення слід визначити його так: **кіберзлочинність** – це протиправні дії у так званому «віртуальному просторі». Віртуальний простір, або як його ще прийнято називати кіберпростір можна характеризувати як створений за допомогою комп’ютера інформаційний простір, в якому можна знайти інформацію щодо осіб, предметів, фактів, подій, явищ та процесів, зображуваних у математичному, символьному або будь-якому іншому вигляді, які знаходяться в процесі руху по різних комп’ютерних мережах (глобальних та локальних), або відомості, які зберігаються в пам’яті якого-небудь фізичного чи віртуального носія, спеціальним призначенням якого є їх обробка, зберігання або передача [10]

 Зрозумівши суть кіберзлочинності, доречно виділити притаманні їй ознаки: інтелектуальний характер явища, - полягає у тому, що для того аби здійснити кіберзлочин потрібно володіти певними знаннями, а також інтелектуальність серед кіберзлочинців пропагується їх субкультурою, стимулюючи їх до розумового саморозвитку; кримінальні правопорушення такого типу не потребують від тих, хто їх скоює високого соціального статусу, для їх вчинення досить мати комп’ютер та доступ в Інтернет; анонімність та відсутність персоніфікації кіберзлочинців – ми вже згадували про те, що в мережі є так звана «анархія» через відсутність чіткого контролю за користувачами, це й дозволяє їм здійснювати свої операції анонімно або взагалі видати себе за іншу людину, змінювати свої персональні дані або соціальний стан; віддаленість кіберзлочинів, - злочинець та жертва можуть знаходитися у різних містах, країнах чи навіть частинах світу, оскільки немає відмінності між вчиненні такого кримінального правопорушення на сусідній вулиці або іншій країні, адже воно вчиняється виключно за допомогою мережі Інтернет; висока латентність кіберзлочинності, головною причиною якої є те, що збитки від кіберзлочину зазвичай здаються жертві незначними, порівняно, наприклад, з процедурою розслідування будь-якого іншого виду кримінального правопорушення, яка може забрати чимало часу, але не дає гарантій та не, що усі винні будуть притягнуті до відповідної відповідальності; транснаціональність кіберзлочинності, яка полягає у тому, що більшість комп’ютерних кримінальних правопорушень вчиняються складом організованих груп, які найчастіше знаходяться у межах різних країн; швидке зростання кіберзлочинності, яке безпосередньо пов’язане з надзвичайним розповсюдженням мережі Інтернет у різних сферах життя, а також зі здешевленням Інтернет-послуг.

Очевидно, що кіберзлочинність не стоїть на місці, постійно з’являються нові види кримінальних правопорушень, які здійснюються за допомогою кіберпростору. На сьогодні найбільш характерними видами кіберзлочинів, які становлять загрозу національній безпеці, виділяють наступні:

1. Кримінальні правопорушення проти конституційних прав і свобод людини та громадянина, як приклад, порушення недоторканності особистого життя, порушення таємниці листування, телефонних розмов, електронного та поштового листування, порушення прав на авторство та суміжні права.
2. Кримінальні правопорушення проти життя та здоров’я. Вперше зафіксували факт вбивства за допомогою Інтернет, це був інцидент, який відбувся у лютому 1998 р. в США. Зловмисники змінили режим роботи кардіостимулятора і апарату вентиляції легенів, внаслідок чого поранений свідок кримінального правопорушення помер. До того ж, масштаби мережі досягли небезпечних, адже було виявлено сайти, які пропагують наркоманію, публікують процес виготовлення заборонених речовин.
3. Кримінальні правопорушення проти честі та гідності особи. Надзвичайна кількість користувачів мережі, використовуючи основну з ознак Інтернету – анонімність, дозволяє безвідповідально порочити репутацію людини.
4. Кримінальні правопорушення проти власності. Найпоширенішим видом кримінального правопорушення в мережі є Інтернет-шахрайство, до того ж кожного для з’являються нові види, способи та форми його вчинення.
5. Кримінальні правопорушення у сфері комп’ютерної інформації, перш за все це довільний доступ до інформації, а також створення та поширення шкідливих програм.
6. Кримінальні правопорушення проти національної безпеки. Разом зі зростанням використання мережі в структурах держави з’являється можливість нелегально отримати доступ до приватної або корпоративної інформації, а також тієї, яка є державною таємницею.

Перше місце серед останнього виду кримінальних правопорушень займає кібертероризм, що з кожним днем набирає більших масштабів, при цьому маючи надзвичайні збіги із «звичайним» тероризмом.

Відсутність контролю та поширення Інтернету серед усіх верств населення, недостатність захисту з боку держави, а також доступ до інформації щодо вчинення кіберзлочинів. Згадані проблеми мають стати чи не пріоритетними напрямками роботи відповідних державних органів тих країн, де кіберзлочинність набирає найбільших обертів. Обов’язковим також є контроль і інших держав, навіть якщо рівень вчинення таких кримінальних правопорушень є меншим, адже кіберзлочинність вже давно набула транснаціонального характеру.

 Залученими до підписання Конвенції Ради Європи з кіберзлочинності, яке відбулося в 2001 році, були багато країн Європи, а також США, Канада, Японія, Південна Африка. На сьогодні вона ратифікована та діє в межах 39 країн світу, зокрема в Україні з 01.07.2006 р. Цей документ має позитивну регулятивну силу, на основі нього можна приймати закони, що не будуть суперечити аналогічним законами, прийнятим у тих країнах, які теж ратифікували його. Саме це дасть змогу створити міжнародну нормативно-правову базу, яка в свою чергу спростить роботу органів безпеки.

Надзвичайно швидкий процес зростання випадків кіберзлочинності зумовлений тим, що люди стають хакерами через відсутність бажаного матеріального достатку, або через бажання реалізувати свій розумовий потенціал за допомогою способу, який не буде сприймати суспільство. Якщо першу проблему вирішити легко, адже великі, тай малі компанії потребують справжніх фахівців своєї справи, то друга проблема потребує вирішення попереджувальними заходами. Також, варто звернути увагу на те, що усі верстви суспільства потребують хоча б елементарних навичок у сфері комп’ютерних мереж, адже саме через некомпетентність можна легко натрапити на кіберзлочинців.

**РОЗДІЛ 2**

**ВИДИ ПРОТИПРАВНИХ ДІЯНЬ У СФЕРІ НОВІТНІХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

2.1 Кібершахрайство як особливо небезпечний вид кримінальних правопорушень в інформаційному просторі

Опираючись на доктрину сучасного міжнародного кримінального права усі кримінальні правопорушення пов’язані з використанням комп’ютерних технологій відносять до кримінальних правопорушень міжнародного характеру. Звичайно, віднесення їх до такої категорії є цілком логічним, адже як ми вже зазначали у попередньому розділі для кіберзлочинності притаманний характер транснаціональності. Тому, у даному Розділі ставимо за мету дослідити ту небезпеку, яку несуть такі кримінальні правопорушення для різних сфер суспільного життя та охарактеризувати їх як особливий вид таких злодіянь – кібершахрайство.

Загалом, кібершахрайство доречно розглядати як вторгнення до процесу обробки інформації та/або її заміну, знищення, виправлення, протиправне використання, яке може нанести її власнику матеріальну шкожду.

Розглядаючи новизну такого поняття як «кібершахрайство», слід зосередити увагу і на його видах, отож існують:

* кібершахрайство, що пов’язане з викраданням коштів з банкоматів. Електронні автомати по видачі готівкових грошей розповсюджені у багатьох країнах світу. Впроваджуються вони сьогодні і в Україні. Зазвичай використовують персональні картки під час зняття готівки з автоматичного касового апарату (банкомату – АТМ - Automated Teller Machine). Деякі фінансові установи видають спеціальні картки для користування банкоматами. Для деяких типів цих машин використовуються кодовані пластикові банківські картки, такі як Visa та MasterCart.

В обох випадках картка використовується для доступу до банкомату разом із Персональним Ідентифікаційним Номером (ПІН-код). Персональний ідентифікатор відомий лише власнику картки. Незважаючи на засоби технічного захисту, зловмисники продовжують проникати до банкоматів, постійно підробляючи обидва (фізичні) джерела (злом, знищення тощо) та маніпулюючи електронною інформацією, записаною на магнітному носії пластикової картки. У більшості випадків злочинці отримують картки та особисті коди в результаті крадіжки у їх власника або шахрайства з боку відповідної фінансової установи (банку тощо).

Бувають випадки, коли шахрай просить в особи, в якості інспектора банку надати персональний ідентифікаційний номер, нібито з метою перевірки входу на карту. Потім рахунок стає доступним для крадіжки за допомогою готівкових записів. Відповідальність власника картки за збитки у разі неправильного використання його картки та особистого коду зазвичай не перевищує 50 доларів США.

Фінансові компанії постійно підкреслюють, що існує відповідальність за збереження персонального ідентифікаційного номера клієнта. З поширенням банкоматів в Україні є ймовірність, що кримінальні правопорушення з використанням їх, можуть поширитися й у нас. Розвиток сучасних інформаційних технологій дозволяє робити різні маніпуляції з картками.

* кібершахрайство, що пов’язане з заміною комп’ютерних даних або програм впроважденням «Логічної бомби».

 «Логічна бомба» у комп’ютерних технологіях не має чіткого офіційного, законодавчого визначення. Це логічний інструмент на рівні комп’ютерної програми, який застосовується злочинцями і стає активним при виконанні певних завдань системи (наприклад, коли комп’ютерна програма починає працювати для виплати заробітної плати). Перебуваючи в стані активності, «Логічна бомба» запустила невелику комп’ютерну програму, яка згубно впливає на комп’ютерну систему, мережу. Цей ефект може змінюватися: комп’ютер може вимкнутись, екран порожній або апарат може втратити дані. Різновидом «логічної бомби» є «часова бомба», яка приводиться в дію у певний день і час. (КК України: ст. 185-187, 191, 193 у сукупності зі ст. 361-361-2, 362, 363).

* кібершахрайство, що пов’язане з ігровими автоматами;

Сучасні ігрові автомати контролюються автоматизованою (комп’ютерною) програмою, яка записана на мікрочіпі. Ці чіпи розробляються компаніями з виробництва комп’ютерних програм і можуть бути об’єктом крадіжки, заміни даних або несанкціонованого копіювання. Технічний аналіз чіпа - це завдання для інженера-програміста. (КК України: ст.185, 190, у сукупності зі ст. 361-361-2, 362, 363).

* кібершахрайство, що пов’язане з платіжними засобами. До нього відносяться найбільш розповсюджені комп’ютерні кримінальні правопорушення, що пов'язані з викраданням коштів, саме вони складають майже 45% усіх кримінальних правопорушень, які пов’язані з використанням електронно-обчислювальних машин (ЕОМ) [17];
* кібершахрайство, що пов’язане з підмінами даних, зазвичай здійснюється при їх введені та виведені. Даний спосіб вчинення кримінального правопорушення такого типу є найпростішим, через що використовується найчастіше.

Зловживання комп’ютерною базою даних та шахрайство або зловживання майном через довіру є поширеною формою кіберзлочинів. У таких випадках потрібен повний технічний опис системи, включаючи програмне забезпечення. Неправильний висновок зустрічається рідше і зазвичай передбачає підготовку документів або інших роздрукованих матеріалів. Існує три типи комп’ютерного програмного забезпечення:

1) Комп’ютерні програмні продукти для комерційного продажу (комп’ютерні програми та автоматизовані бази даних).

2) Безкоштовне експериментальне програмне забезпечення, яке було перероблено з певною метою.

3) Спеціальні, спеціалізовані комп’ютерні програмні продукти, написані для спеціальних цілей, а не для продажу та розповсюдження (військові та інші державні чи комерційні цілі тощо). (КК України: ст. 190, у сукупності зі ст. 361-361-2, 362, 363).

- кібершахрайство, що пов’язане з телефонними комунікаціями; неавторизований доступ до комунікаційних послуг з порушенням стандартних протоколів та процедур. Шахрайство з телефонними розмовами може бути окреслене як неправильне використання телекомунікаційних послуг. Іноді ці кримінальні правопорушення вчинюються з метою уникнути сплати рахунків за послуги, іноді - щоб уникнути підслуховування. Прикладом телефонного шахрайства є застосування спеціального пристрою, який може маніпулювати обміном телефонними переговорами. Пристрій генерує звуки, на які автоматизована телефонна станція відповідає з’єднанням без включенням лічильника рахунку часу розмови.

 Іншим прикладом є неправомірне використання стільникових телефонів (у тому числі автомобільних). При цьому немає необхідності у фізичному контакті. Розмова може відбутися шляхом підключення за допомогою сканування номера-коду законного користувача. Можливе також перепрограмування коду стільникового телефону, після чого злочинець буде використовувати телефон, а рахунки надійдуть до іншої особи чи організації. (КК України: ст.185, 190 у сукупності зі ст. 361-361-2, 362, 363).

 Оскільки ми говоримо про те, що кібершахрайство можна розглядати як кримінальне правопорушення, то варто охарактеризувати його з цього аспекту. Отже саме шахрайство полягає у навмисному заподіянні майнової шкоди, шляхом протиправного заволодіння чужим майном та/або правом на нього. Натомість кібершахрайство передбачає такі самі дії, лише з використанням комп’ютерних технологій. У зв’язку з цим пропонуємо виключити із ч. 3 ст. 190 КК України фразу «шляхом незаконних операцій з використанням електронно-обчислювальної техніки» та доповнити Кодекс статтею 363-4 наступного змісту:

***«1. Заволодіння чужим майном або придбання права на майно, або заподіяння іншої майнової шкоди шляхом навмисного спотворення або приховування інформації, що заносяться до комп’ютерної системи (******кібер***[***шахрайство***](https://zakon.rada.gov.ua/laws/show/2341-14?find=1&text=%D1%88%D0%B0%D1%85%D1%80%D0%B0%D0%B9%D1%81%D1%82%D0%B2%D0%BE#w1_3)***) -***

***карається штрафом від двох тисяч до трьох тисяч неоподатковуваних мінімумів доходів громадян або громадськими роботами на строк від двохсот до двохсот сорока годин, або виправними роботами на строк до двох років, або обмеженням волі на строк до трьох років.***

***2.******[Кібершахрайство](https://zakon.rada.gov.ua/laws/show/2341-14?find=1&text=%D1%88%D0%B0%D1%85%D1%80%D0%B0%D0%B9%D1%81%D1%82%D0%B2%D0%BE" \l "w1_5), вчинене у великих розмірах, -***

***карається позбавленням волі на строк від трьох до восьми років.***

***3.******[Кібершахрайство](https://zakon.rada.gov.ua/laws/show/2341-14?find=1&text=%D1%88%D0%B0%D1%85%D1%80%D0%B0%D0%B9%D1%81%D1%82%D0%B2%D0%BE" \l "w1_6), вчинене в особливо великих розмірах, -***

***карається позбавленням волі на строк від п’яти до дванадцяти років з конфіскацією майна».***

 Варто зауважити, що на сьогодні такі кримінальні правопорушення є чи не найпоширенішими в світі, адже не потребують особливих матеріальних трат, а вимагають лише певних навичок та відповідних ресурсів (доступу до мережі Інтернет).

 Зазвичай «у руки» кібершахраїв потрапляють великі корпорації, банки, а також урядові установи, проте з надзвичайним розвитком новітніх інформаційних технологій все більше страждають і звичайні люди, які мають особисті сторінки у різних соціальних мережах на платформі Інтернет. Широкої популярності у світі набули такі соціальні мережі як Фейсбук (Facebook), Інстаграм (Instagram), Ютюб (YouTube), Вайбер (Viber). Усі вони користуються популярністю і в Україні, адже це значно спростовує життя людини. Ми кожного дня маємо можливість спілкуватися з людьми на відстані, отримувати величезну кількість інформації, навчатися та працювати не виходячи з дому, знайомитися з людьми тощо. Тай взагалі, важливість та особливе місце соціальних мереж у нашому житті заперечувати важко.

 Завдяки популяризації таких платформ з’являються нові професії, люди знаходять своє покликання, чим полегшують своє життя, а разом з тим і життя мільйонів людей у своєму світі, проте така популярність має і зворотній бік.

 Кібершахраї зламують облікові записи людей, чим отримують доступ до особистої інформації, рахунків і , відповідно, використовують її/їх у своїх цілях.

 Це ще раз звертає нашу увагу на необхідності бути грамотним у сфері новітніх технологій, мати базові навички, які не дадуть нам можливості потрапити у ситуації, які будуть нести нам збитки.

 Отож, враховуючи все викладене вище, пропонуємо ***авторське визначення терміну «кібершахрайство» під яким слід розуміти дії, направлені на заволодіння чужим майном або придбання права на майно, або заподіяння іншої майнової шкоди шляхом навмисного спотворення або приховування інформації, що заносяться до комп’ютерної системи чи інший вплив на процес обробки інформації, що має на меті отримання матеріальної вигоди для себе або інших осіб.***

2.2 Giveaway як прояв кібершахрайства у соціальних мережах

 На сьогодні розвиток протиправних діянь у кіберпросторі набирає нових обертів. Разом із всебічним розвитком бізнесу в мережі Інтернет, зростає і шахрайство у даній сфері, це зумовлено необмеженістю прав та відсутністю вузько спрямованого законодавства, яке б могло б регулювати дані відносини.

 Сфера заробітку в мережі є неосяжною, кожного дня створюються нові сайти, Інтернет-магазини, сторінки у тих чи інших соціальних мережах.

 Соціальна мережа - це веб-служба, віртуальна спільнота з інтересами, нахилами, діяльністю, друзями. Термін «соціальні мережі» був науково використаний у 1954 р. Соціологом Джеймсом Барнсом «Заняття та зустрічі на парафії Норвезького острова» [11].

 Раніше багато вчених, які вивчали суспільство, наголошували на важливості розуміння суспільства як складного втручання. Найбільшою тенденцією у Всесвітній павутині є створення Інтернет-спільнот та соціальних мереж. Термін «віртуальна спільнота» був введений Г. Рейнольдсом і визначається таким чином: підтримка сфери особистих стосунків у віртуальному просторі [12]. Сучасна теорія соціальних мереж була започаткована Рей Соломоном у 1959 р. та Анатолійським звітом. Теорія соціальних мереж передбачає, що на соціальну поведінку та спілкування впливають моделі людських стосунків, відповідно до одного з її пунктів, чим розвиненіші соціальні мережі, тим сильніші соціальні стосунки між людьми. Вони активніше спілкуються між собою, використовуючи всі доступні засоби масової інформації. Як і інші нововведення в комунікаційних технологіях, Інтернет продовжує підключати людей до соціальних мереж. Як і люди, так організації географічно розкидані, але пов’язані спільними інтересами. Теорія мережі «Shell» стверджує, що соціальне спілкування в Інтернеті доповнює і розширює традиційний соціальний підхід, тому чим активніші люди поводяться в суспільстві, тим більше вони взаємодіють між собою. Чим ближче вони наближаються до контактів, тим більше вони використовують електронну пошту та інші засоби масової інформації для спілкування [13].

 Опора на «соціальні мережі», що з’явилися за кордоном кілька років тому, поширилася на пострадянські країни, включаючи Україну. Інтернет дав можливість людям, які раніше були віддалені, знаходити можливість зв’язуватися між собою. Активно шукаючи друзів та родичів, ніхто не звертає уваги на те, як розгортається віртуальне життя, остаточно витісняючи реальність. Вплив соціальних мереж на суспільство може бути як частково позитивним, так і негативним: залежність від віртуального світу є найпоширенішою проблемою. На перший погляд, спілкування в соціальних мережах здається цілком безпечним. Але ця ідея може ввести в оману. При частому спілкуванні в Інтернеті у людей з рівнем несвідомості розвивається фобія спілкування з реальними людьми.

 Людям, які проводять весь вільний час у чаті через соціальні мережі, важко завести нових друзів у реальному житті, перестати спілкуватися зі своїми однолітками, і як результат, зовнішній світ починає сприймати їх як не пристосованих до соціуму людей.

 Ще однією причиною обмеження часу в соціальних мережах є те, що більшість людей вважають, що під час знаходження у віртуальному світі соціальних мереж, людям здається, що вони насправді знаходяться в реальному житті. Люди, які публікують правдиву інформацію про себе, можуть стати жертвами цього обману. У цьому випадку псевдо-особа шляхом ілюзії знаходить собі місце і рано чи пізно може загрожувати людині, з якою вона активно спілкується [14, с. 144-149].

 82% світових користувачів Інтернету користуються соціальними мережами. Це 1,2 мільярда людей. У жовтні 2011 року використання соціальних мереж стало найпопулярнішою професією серед інтернет-аудиторії. Кожна п'ята хвилина в Інтернеті є в будь-якій соціальній мережі. У березні 2007 року на соціальні мережі припадало лише 6% часу користувачів. На сьогодні відсоток користувачів соціальних мереж у світі коливається від 53% у Китаї до 98% у США. У 41 з 43 опитаних країн цей рівень перевищує 85%. За останній рік у кожній із цих областей спостерігалося зростання щонайменше на 35% у соціальних мережах [15, с. 338-342].

 Однією з провідних соціальних мереж в світі, і в Україні зокрема, є Instagram - соціальна мережа, заснована на обміні фотографіями, дозволяє користувачам публікувати світлини, накладати на них фільтри, а також розповсюджувати їх через свій профіль та різні інші соціальні мережі [11].

 Дана платформа багата на популярних сьогодні Інстаграм-блогерів, які активно показують своє життя на аудиторію, що стежить за ними. Через свою популярність та відкритість, прихильність публіки та зацікавленість у своїй особі, люди даного спрямування мають особливе звання – Інфлюенсер - людина, думка якої має значення для певної аудиторії [12].

 Щоденно аудиторія може спостерігати публікації на особистій сторінці, що несуть різний характер, сьогодні наайпопулярнішими є два види публікацій:

бартерна співпраця та розіграші, які в соціальній мережі мають назву Giveaway - розіграш або вікторина, в якій мають бути дотримані певні умови. Такі конкурси покликані залучити нових клієнтів, нову аудиторію та провести рекламу бренду..

 Giveaway - ефективний захід для привернення уваги. В порівнянні з рекламними кампаніями та PR-заходами, giveaway — дешевий та дієвий спосіб заявити про себе.

 У свою чергу бартерна співпраця діє на простих умовах, вони полягають у тому, що певна організація або бренд, безкоштовно надає свої послуги або товар інфлюенсеру, який у свою чергу розміщує публікацію з ним на своїй сторінці, чим заохочує свою аудиторію звернути увагу на річ або послугу, яку пропонує замовник.

 Якщо бартерна співпраця є найчастіше за простих та вигідних обом сторонах умов, то giveaway можуть нести корисливий характер. Він полягає у тому, що популярні сьогодні кругові розіграші, у яких кілька Інстраграм-блогерів об’єднуються задля обміну своєї аудиторією, можуть проводити їх нечесно. Призи, які розігруються можуть не потрапляти до переможців. Таким чином нову аудиторію інфлюенсери отримують, а головних умов, які ставляться до розіграшу не виконують.

 Дані злодіяння популярні і у інших соціальних мережах, але найболючішою проблемою вони є саме у Instagram, адже, як вже зазначалося раніше, сьогодні ця соціальна мережа є найбільш розповсюдженою у всьому світі.

 До грудня 2010 року у Instagram був один мільйон зареєстрованих користувачів. В липні 2012 року Instagram оголосив про 100 мільйонів завантажених фотографій, в серпні це число досягло 150 млн. Станом на вересень 2017 року сервіс нараховує 800 млн. користувачів, з них 500 млн. відвідують свої акаунти щодня. У червні 2018 року аудиторія Instagram досягла 1 млрд. користувачів [13].

 Шалена популярність, новизна та феномен даної платформи, щоденно дає можливість монетизувати свою діяльність численній кількості користувачів. Але разом з тим, дана галузь прибутку часто є незаконною. Рішення цієї проблеми є доволі простим, кожен успішний та впізнаваний Інстаграм-блогер вже давно став ФОПом, тобто діє як підприємець та сплачує податки.

 Не менш важливим є і те, що контроль даної галузі потребує змін в законодавстві, тому що бувають випадки ухилення користувачів від сплати податків, зборів (обов’язкових платежів) та від несення відповідальності за ті чи інші протиправні діяння, зокрема не тільки нечесні giveaway, а й розповсюдження контенту, який є недопустимим за правилами даної соціальної мережі, порушення авторських прав тощо.

 Звісно, на просторі даної платформи є багато цікавої та корисної інформацїі, сьогодні тут навчаються та заробляють мільйони людей. Хтось знаходить себе та своє покликання, однодумців.

 Простір даної соціальної мережі немає кордонів, тут кожен знаходить щось для себе, проте така необмеженість несе за собою у певних випадках негативні наслідки, які уже були згадані раніше.

 Додержання усіх вимог користування та чітке регулювання з боку держави додадуть даній соціальній мережі не тільки нових можливостей, а й зроблять користування безпечним та надійним.

**РОЗДІЛ 3**

**ОПТИМІЗАЦІЯ ПРАВОВОГО РЕГУЛЮВАННЯ БОРОТЬБИ З КІБЕРШАХРАЙСТВОМ**

3.1 Перспективи та тенденції розвитку правового регулювання боротьби з кіберзлочинністю в Україні

 На сучасному етапі розвитку суспільства все більше відчувається значущість інноваційних процесів, що відбуваються в нашому суспільстві у зв’язку з глобальною інформатизацією. Але разом із позитивними досягненнями, інформатизація супроводжується й іншими явищами негативного характеру, до яких відносять кібершахрайство. Це, очевидно, вимагає негайного створення системи протидії даному різновиду злочинності на державному рівні. Для сучасного суспільства актуальність цієї проблеми є беззаперечною. Оцінки експертів вказують на те, що щорічно збитки від діяльності кібершахраїв складають близько від 300 до 800 млрд. євро [18, с. 45-46 ] Державні підходи та механізми повинні сприяти поліпшенню національної безпеки та міжнародному правопорядку, а також скороченню кримінальних правопорушень у кіберпросторі.

 В Україні процес боротьби з кібершахрайством ускладнений тим, що самого терміну «кібершахрайство» в законодавстві не визначено, навіть не звертаючи уваги на те, що поняття є не новим як для правоохоронних органів України, так і для зарубіжних держав. На сьогодні інформаційні технології застосовуються практично в усіх сферах суспільного життя, та навіть в економіці держави, що дає змогу висувати проблему боротьби з кібершахрайством у число основних.

 Окрім того, що може наноситись безпосередня шкода від неавторизованого доступу до інформації, або її розповсюдження чи модифікації, то кібершахрайство може бути джерелом загрози національній безпеці, економіці та інтересам людини. Проблемою є й те, що загроза таких діянь є не до кінця усвідомленою, причиною цьому є те, що відсутня наукова розробленість фундаментальних понять, що пов’язані з нею.

 Інтернет є місцем, у якому вчинити кримінальні правопорушення дуже легко, адже існує анонімність та необмеженість мережі, яку можна використовувати у своїх протиправних діях.

 Жодні терміни із частиною «кібер» ще досі не отримали сформованого визначення ані на науковому, ані на нормативно-правовому рівнях, через що залишаються предметом дискусій.

 На даному етапі поняття «боротьба з кібершахрайством» є новим для вітчизняної науки, навіть попри те, що протиправні діяння із застосуванням Всесвітноьої павутини мають високий рівень суспільної небезпеки.

 Отже, відсутність належного законодавчого закріплення поняття «боротьба з кібепшахрайством» є однією із причин наявності проблем у його повному розумінні та науковому тлумаченні.

 Щодо боротьби із кібершахрайством в Україні, за загальним правилом вона здійснюється Департаментом кіберполіції, шляхом законодавчого врегулювання та іншими суб’єктами, що зацікавлені у подоланні даного явища. У свою чергу держава здійснює свою діяльність у законодавчому та організаційному напрямах, а Департамент кіберполіції у профілактичному.

 Основним аспектом встановлення даного терміну є рівень небезпеки, який характеризує вчинене діяння. Але саме поняття «кібершахрайство» не дає зрозуміти масштаб небезпечності дії та середовища її вчинення. Доцільно розглядати кібершахрайство як специфічний вид протиправної діяльності, що здійснюється у комп’ютерних мережах.

 Важливо звернути увагу й на те, що не можна ототожнювати кібершахрайство та інформаційні кримінальні правопорушення. Оскільки в нашій державі кібершахрайство існує у вигляді потенційної загрози, то важливим є впровадження попереджувальних заходів. Це все є поштовхом для створення ефективної системи запобігання та виявлення такої діяльності, що буде базою для успішною боротьби з кібершахрайством в Україні.

 Загалом протидія кібершахрайству має включати в себе загальнодержавні заходи економічного, виховного, політичного характеру, а також комплекс вузько спрямованих заходів, спрямованих на безпосереднє подолання протиправних діянь. Оскільки злодіяння у кіберпросторі мають міжнародний характер, то й боротьба з ними вимагає гармонізації національних законодавств.

Така гармонізація повинна відповідати регіональним вимогам та можливостям. Глобальна програма кібербезпеки базується на п’ятьох принципах: правові заходи; технічні й процедурні заходи; організаційні структури; створення потенціалу; міжнародна співпраця;

Для дієвої протидії з кібершахрайством усі ці принципи повинні бути врахованими. Найважливішим принципом є перший, який передбачає запровадження певних правових заходів. Дані заходи вимагають прийняття основних положень кримінального законодавства, що передбачатимуть кримінальну відповідальність за такі дії, як кібершахрайство, неавторизований доступ до інформації, її пошкодження, порушення авторських прав тощо. Інструменти, необхідні для розслідування протиправних діянь у кіберпросторі, можуть істотно відрізнятися від тих, які використовуються при розслідуванні «традиційних» кримінальних правопорушень.

 У зв’язку з міжнародним масштабом кібершахрайства необхідно вдосконалювати основи національного законодавства, зокрема й для того, щоб мати можливість співпрацювати з правоохоронними органами за кордоном. Для того, щоб боротьба з кібершахрайством була ефективною, на належному рівні має бути розвинена організаційна структура, адже не маючи належної системи відповідних органів, яка чітко розподіляє повноваження, навряд чи можна чекати на комплексне вирішення юридичних, технічних та соціальних аспектів даної проблеми.

 Для того, аби мати змогу ефективно розслідувати кримінальні правопорушення пов’язані з віртуальним простором, необхідною є не тільки гармонізація законодавства, а й розробка відповідних механізмів співпраці. Тому, надзвичайним аспектом є рівень довіри, який має бути не тільки між державами, а й між громадянином та державою [19, с. 126-128].

Одним з головних і найперших елементів в попередженні кібершахрайства є обізнаність користувачів платформи Інтернет у її функціонуванні та дотримання усіх вимог безпеки: встановлення паролів, використання спеціальних символів тощо.

 Оскільки ми вже згадували про те, що кібершахрайство є транснаціональним явищем, то йому характерний максимальний рівень латентності. Головними факторами латентності кібершахраїв є:

1. таємниця процесу вчинення протиправних діянь, що поєднується з різними сферами та наслідками їх вчинення, а також «комп’ютерна необізнаність» переважної більшості жертв кібершахраїв, їх нехтування своєю безпекою;
2. байдужа поведінка жертв та/або свідків кримінального правопорушення – не звертання жертви та осіб, яким відомо про кримінальне правопорушення, до правоохоронних органів;
3. недоліки в діяльності правоохоронних органів щодо реагування на звернення та повідомлення про кібершайхства.

Запобігання кібершахрайству на загально соціальному рівні передбачає перелік дієвих соціально-економічних, організаційно-управлінських, ідеологічних, культурно-виховних та інших заходів, спрямованих на вирішення важливих соціальних проблем та суперечок в країні.

 Сама реалізація загально соціальних заходів запобіганню кібершахрайству дає змогу мінімізувати випадки вчинення кримінальних правопорушень даного виду, а також запобігати формуванню особистості правопорушника.

 Для належної розробки відповідних заходів протидії кібершахрайству, необхідним аспектом є організація діяльності правоохоронних органів, а також вищих органів держави, що відповідає вимогам, які мають існувати у правовій, незалежній, демократичній державі. До того ж, потрібно усувати фактори, що несуть позитивний вплив на існування та розвиток злочинності.

 У свою чергу, спеціально-кримінологічне запобігання безпосередньо стосується роботи Національної поліції України та спрямовуються в основному на соціальні групи, що привертають увагу учасників запобіжної діяльності. Основними заходами запобігання кібершахрайству, які повинна реалізовувати Національна поліція (в особі департаменту кіберполіції), слід виділяти такі:

1. розроблення та затвердження Стратегії МВС щодо протидії кібершахрайству, яка у свою чергу повинна містити концепцію кримінально-запобіжної діяльності, а також заходи анти кримінального впливу та моніторингові механізми його забезпечення;
2. збільшення кількості планових та позапланових перевірок названими органами поліції підприємств, установ, організацій, робота яких має зв’язок з використанням комп’ютерних технологій або надання інформаційних послуг;
3. посилення відповідальності уповноважених осіб, які за своїми посадовими або функціональними обов’язками відповідають за безпечне функціонування комп’ютерів та комп’ютерних мереж;
4. встановлення жорсткого нагляду за обігом технічних засобів, які є забороненими у вільному використанні, наприклад, технічні засоби для негласного знаття інформації з каналів зв’язку, перехоплення інформації, добору паролів, тощо;
5. впровадження позитивного досвіду діяльності правоохоронних органів інших країн у даній сфері (перш за все для аналізу технічного забезпечення та технології, які використовуються для запобігання вчиненню таких кримінальних правопорушень);
6. участь працівників кіберполіції у міжнародних семінарах, круглих столах, проведення яких присвячено вказаній проблемі, а також ініціювання відповідними органами нашої держави проведення таких заходів на території України.

Важливим елементом діяльності щодо протидії вчиненню кібершахрайств є виявлення осіб, що вчиняють дані протиправні діяння, або ж схильні до вчинення таких злодіянь. Ключовим показником того, що особа схильна до таких діянь є системний перезапис даних без наявної необхідності, їх заміна або видалення, поява фальшивих записів, а також випадки, коли працівник безпричинно починає працювати наднормово. Окремим заходом запобігання вчиненню кібершахрайств є виявлення діяльності кібертерористів, осіб, що використовують комп’ютери для вчинення терористичних актів. [20, с. 164-166]

3.2 Специфіка правового регулювання боротьби з кібершахрайсвом у зарубіжних країнах

 Увесь масштаб Інтернету вказує на те, що певні аспекти кібершахрайства не обмежуються територією певної країни, тому законодавство на міжнародному рівні має регулювати дане питання, відповідати загальновизнаним стандартам, аби його діяльність була ефективною.

 Більше того, процес становлення злагодженої системи правового регулювання боротьби з кібершахрайством неможливий без урахування досягнень до недоліків, що були надбані іноземними державами при формуванні даного інституту.

 У зв’язку з активним розвитком кібершахрайства, запобігання йому має бути актуальним завданням для держави. Проте, у багатьох зарубіжних країнах дана система вже давно налагоджена та приносить свої позитивні результати. Тому, проаналізувавши сучасні вітчизняні реалії, ми можемо відзначити незавершеність даного процесу в Україні та необхідність подальших трансформацій.

Розпочнемо з досвіду Сполучених Штатів Америки, як держави, яка потерпіла чимало атак від кібершахраїв і є чи не найпершою в історії, що розробляла відповідні норми для регулювання злодіянь даного типу. Головними нормами Національної стратегії національної безпеки США, прийнятої у 2015 році, є ті, що встановлюють необхідність захисту від кібератак у кіберпросторі. Сполучені Штати Америки, які проголосили себе батьківщиною Інтернету, взяли на себе відповідальність забезпечення кібербезпеки у всьому Інтернет-просторі. Крім того, було проголошено курс щодо оптимізації законодавчої бази та підвищення її стандартів захисту прав та інтересів громадян [21, с. 78-82].

Таким чином Сполучені Штати Америки є однією з провідних країн-дослідників у галузі досвіду. Оскільки у цій країні триває активна діяльність з протидії таким негативним явищам, як кримінальні правопорушення у віртуальному просторі, зокрема, кібершахрайству, то багато уваги приділено безпеці громадян. США можна назвати головною мішенню кібершахраїв, тому досвід саме цієї країни надзвичайно корисний для розробки правових інструментів протидії даному явищу. Незважаючи на все вище зазначене, в США переважає методика саморегуляції Інтернету, як результат законодавство в цій галузі представлено лице кількома нормативно-правовими актами.

Зокрема, це Закон про електронний підпис, що прийнятий у 2000 р. Основною його метою є забезпечення правового регулювання використання електронного підпису в комерційних відносинах. Найбільша кількість нормативно-правових актів діє у сфері випуску цінних паперів, захисту інтелектуальної власності, а також від неавторизованого доступу до інформації, авторських прав, тощо. Для прикладу, у США кримінальна відповідальність за неналежне зберігання, обробку, знищення особистої інформації, у формі, що непередбачена законодавством. Для порівняння, у країнах Європейського Союзу кримінальні справи порушуються лише у випадку шкоди безпеці держави або основним правам громадян, що вказує на те, що соціальний аспект правового регулювання боротьби з кібершахрайством має велике значення.

Цікаво також звернути увагу на досвід регулювання такої проблеми у країні, яка як і наша входила до колишнього СРСР, у якій було створено спеціальний орган для боротьби з кримінальними правопорушення у віртуальному просторі Міністерства внутрішніх справ Республіки Білорусь. 27 лютого 2001 року у структурі кримінальної поліції МВС з’явилося управління оперативно-організаційної діяльності, у складі якого до листопада 2002 року діяло відділення по розкриттю кримінальних правопорушень у сфері новітніх інформаційних технологій.

Даний орган має статус самостійного оперативно-розшукового підрозділу Міністерства, яке здійснює координацію підрозділів головного управління кримінальної поліції МВС і органів внутрішніх справ при виявленні ними злочинів проти інформаційної безпеки Для здійснення взаємодії з іншими правоохоронними органами і організаціями застосовується умовне найменування Управління «К» МВС Республіки Білорусь.

 Загалом законодавча боротьба з кримінальними правопорушеннями у сфері високих технологій представлена невеликою кількістю норм та законів: Глава Кримінального кодексу Республіки Білорусь, Закон про електрозв’язок, закон про інформацію, інформатизацію і захист інформації, Конвенція про кіберзлочини, Додатковий протокол до Конвенції про кіберзлочини, Указ «Про заходи щодо вдосконалення використання національного сегменту мережі Інтернет», Указ «Про деякі питання розвитку інформаційного суспільства в Республіці Білорусь», Указ «Про затвердження Положення про порядок взаємодії операторів електрозв’язку з органами, які проводять оперативно-розшукову діяльність». У цілому варто відзначити схожість законодавчої основи Республіки Білорусь та України, проте особливим є Указ «Про затвердження Положення про порядок взаємодії операторів електрозв’язку з органами, які проводять оперативно-розшукову діяльність» [22, с. 35-44].

Проаналізувавши правове регулювання боротьби з кібершахрайством, можна стверджувати про спроби встановлення контролю за Всесвітньою мережею, проте важливим аспектом є те, що наявні заборони не містять порушення прав та свобод людини і громадянина. У досліджуваних країнах існує взаємозв’язок між державою та суспільство, який позитивно впливає на розуміння суспільством проблем та необхідністю встановлення меж для їх вирішення. Доцільно відзначити й роль міжнародного законодавства та міждержавних угод, що мають значний вплив на відносини громадян у різних державах. Це ще раз вказує на те, що їх роль у вітчизняному праві необхідно оптимізувати до вищого рівня.

**ВИСНОВКИ**

 Проаналізувавши увесь викладений вище матеріал, можна зробити наступні висновки: виникнення кіберзлочинності пов’язане з виникненням самого простору у якому дані протиправні діяння вчиняються – комп’ютерної мережі, адже її стрімкий розвиток зацікавив людей, які володіли навичками, що дозволяли їм мати доступ до чужої інформації.

 Також, проаналізувавши становлення та розвиток кіберзлочинності ми можемо висувати припущення щодо того, що дане явище є новим, а тому значний його розвиток може чекати нас попереду, якщо кожна держава не буде сприяти його запобіганню належним чином.

Щодо новизни та небезпечності такого поняття як «кібершахрайство», то сьогодні воно є чи не найнебезпечнішим проявом кіберзлочинності, адже найчастіше зустрічається у соціальних мережах, якими наразі користуються мільярди людей і через свою необізнаність можуть потрапляти у руки кібершахраїв.

Нами запропоновано авторське визначення кібершахрайства, яке полягає в наступному: «це дії, направлені на заволодіння чужим майном або придбання права на майно, або заподіяння іншої майнової шкоди шляхом навмисного спотворення або приховування інформації, що заносяться до комп’ютерної системи чи інший вплив на процес обробки інформації, що має на меті отримання матеріальної вигоди для себе або інших осіб».

Разом з розвитком соціальних мереж зросли і види діяльності в них, хтось просто ділиться своїм життям з аудиторією, а хтось набуває статусу «Інфлюенсера», завойовує довіру своєї аудиторії, та для розвитку свого блогу проводить Giveaway, які, на жаль, все більше стають нечесними, обіцяних призів учасники не виграють, а блогери мають корисливі мотиви проведення даних розіграшів.

Проте, усіх цих проблем можна уникнути, якщо вибрати правильну систему їх запобіганню: налагодити систему законодавства у цій сфері, а також підвищити рівень довіри між державою та її громадянами, і, що не менш важливо, нарешті по-справжньому оцінити небезпеку таких діянь, адже через те, що ми не можемо побачити своїх реальних збитків, ми не надаємо їй особливого значення. У зв’язку з цим нами розроблено програму запобігання кібершахрайству в Україні (Додаток А).

Важливим аспектом при подоланні такої проблеми є позитивний досвід інших держав, які страждають від подібної проблеми, адже спираючись на нього, ми можемо бачити реальні результати у подоланні даної проблеми.

У зв’язку зі стрімким поширенням та розвитком кібершахрайства в Україні та світі пропонуємо виключити із ч. 3 ст. 190 КК України фразу «шляхом незаконних операцій з використанням електронно-обчислювальної техніки» та доповнити КК України статтею 363-4 наступного змісту:

«1. Заволодіння чужим майном або придбання права на майно, або заподіяння іншої майнової шкоди шляхом навмисного спотворення або приховування інформації, що заносяться до комп’ютерної системи (кібер[шахрайство](https://zakon.rada.gov.ua/laws/show/2341-14?find=1&text=%D1%88%D0%B0%D1%85%D1%80%D0%B0%D0%B9%D1%81%D1%82%D0%B2%D0%BE#w1_3)) -

карається штрафом від двох тисяч до трьох тисяч неоподатковуваних мінімумів доходів громадян або громадськими роботами на строк від двохсот до двохсот сорока годин, або виправними роботами на строк до двох років, або обмеженням волі на строк до трьох років.

2. [Кібершахрайство](https://zakon.rada.gov.ua/laws/show/2341-14?find=1&text=%D1%88%D0%B0%D1%85%D1%80%D0%B0%D0%B9%D1%81%D1%82%D0%B2%D0%BE#w1_5), вчинене у великих розмірах, -

карається позбавленням волі на строк від трьох до восьми років.

3. [Кібершахрайство](https://zakon.rada.gov.ua/laws/show/2341-14?find=1&text=%D1%88%D0%B0%D1%85%D1%80%D0%B0%D0%B9%D1%81%D1%82%D0%B2%D0%BE#w1_6), вчинене в особливо великих розмірах, -

карається позбавленням волі на строк від п’яти до дванадцяти років з конфіскацією майна».

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ**

1. Основні завдання Департаменту кіберполіції Національної поліції України. URL https://www.cybercrime.gov.ua/contacts (дата звернення 12.12.2020)

2. Вехов Б. В., Голубев В.А. Расследование компьютерных преступлений в странах СНГ. Монография. Под ред. Б. П. Смагоринского. Волгоград : ВА МВД России, 2004. 304 с.

3. Всесвітній огляд економічних злочинів. URL: https:/ /www.pwc.com/ua/uk/ Україна (дата звернення 12.12.2020).

4. Голубєв В. О. Розслідування комп’ютерних злочинів. Монографія. Запоріжжя. Гуманітарний університет «ЗІДМУ», 2003. 296 с.

5. Конвенція про кіберзлочинність: міжнародний документ : від 23.11.2001 URL: http://zakon5.rada.gov.ua/laws/show/994\_575(дата звернення 12.12.2020).

6. Голубєв В. О. Комп’ютерні злочини в банківській діяльності. З. Павел, 1997. 118 с.

7 Кравцова М. А. Понятие киберпреступности и ее признаки. *Часопис Київського університету права.* 2015. № 2. С. 320–324.

8. Бутузов В. М. Співвідношення понять «комп’ютерна злочинність» та «кіберзлочинність». *Інформаційна безпека людини, суспільства, держави*. 2010. № 1 (3). С. 18.

9. Пивоваров В. В., Терещенко К.В. Шахрайство її банківськими картками: окремі питання віктимологічної профілактики. *Карпатський приватний часопис*. 2015. Вип. 2. С. 132–137.

10. Про ратифікацію Конвенції про кіберзлочинність : Закон України : від 07.09.2005 № 2824-ІV URL: http:// zakon2.rada.gov.ua/laws/show/2824-15(дата звернення 12.12.2020).

11. Що таке Instagram? URL:<https://www.businessinsider.com/instagram-2010-11>(дата звернення 12.12.2020).

12. Блог Пономарева: як українською «інфлюенсер». URL: <https://www.bbc.com/ukrainian/blog-olexandr-ponomariv-48826130>(дата звернення 12.12.2020).

13.  [У Instagram вже більше 1 млрд користувачів](https://web.archive.org/web/20180622011030/https%3A/npvua.com/u-instagram-vzhe-bilshe-1-mlrd-korystuvachiv-sotsmerezha-zapuskaye-novyj-servis-igtv-dlya-vertykalnyh-video-tryvalistyu-do-godyny-itc-ua.html). URL: [https://web.archive.org/web/20180622011030/https://npvua.com/u-instagram-vzhe-bilshe-1-mlrd-korystuvachiv-sotsmerezha-zapuskaye-novyj-servis-igtv-dlya-vertykalnyh-video-tryvalistyu-do-godyny-itc-ua.html](https://web.archive.org/web/20180622011030/https%3A/npvua.com/u-instagram-vzhe-bilshe-1-mlrd-korystuvachiv-sotsmerezha-zapuskaye-novyj-servis-igtv-dlya-vertykalnyh-video-tryvalistyu-do-godyny-itc-ua.html)(дата звернення 12.12.2020).

 14. Рудой К.М. Протидія кіберзлочинності як напрям забезпечення міжнародної безпеки ОВС України. *Публічне право : науково-практичний юридичний журнал.* Всеукр. громадська організація «Майбутнє країни». Ужгород. нац. ун-т. Київ, 2015. № 3 (19). C. 144-149.

 15. Савчук Н.В. Кіберзлочинність: зміст та методи боротьби. *Теоретичні та прикладні питання економіки: збірник наукових праць.* МОНУ. КНУ імені Тараса Шевченка; Ін-т конкурентного суспільства. Київ, 2009. Вип. 19. С. 338-342.

 16. Сервецький І. В. Деякі проблеми захисту персональних даних в Україні *Боротьба з організованою злочинністю і корупцією (теорія і практика).* К. МНДЦ, 2014. № 9. С. 193-199.

 17. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування. Аналітична записка URL: http:// [www.niss.gov.ua/articles/454](http://www.niss.gov.ua/articles/454) (дата звернення 18.10.2020)

 18. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. *Юридичний журнал*. 2009. № 5. С. 45–46.

 19. Солодка О. М. Боротьба з комп’ютерною злочинністю як пріоритетний напрям забезпечення інформаційної безпеки України. *Актуальні проблеми управління інформаційною безпекою держави: зб. Матеріалів наук.-практ. конф*., 17 берез. 2010 р., м. Київ. К. Нац. акад. СБУ України, 2010. С. 126-128.

 20. Якубівська Ю. Є. Кібератаки у сфері інформаційної безпеки: тенденції на євразійському просторі. *Вітчизняна система охорони і захисту інтелектуальної власності в умовах приєднання до Європейського Союзу: Збірник тез доповідей Всеукраїнської науково-практичної конференції*, м. Тернопіль, 24-25 квітня 2015 р., ТНЕУ. Тернопіль, 2015. С. 164-166.

 21. Тихомиров О.О. Протидія кіберзлочинності як складова державного забезпечення інформаційної безпеки. *Актуальні проблеми управління інформаційною безпекою держави : зб. матНПК*, (Київ, 22 берез. 2011 р.). Ч. 2. К. Вид-во НА СБ України, 2011. С. 78-82.

 22. Сорокин В. Д. Правовое регулирование: предмет, метод, процесс. Правоведение. 2000. №4 (231). С. 35-44.

**ДОДАТОК А**

**Програма запобіганню кібершахрайству в Україні**

 Стрімкий розвиток такого явища як «кібершахрайство» є беззаперечним на сьогодні. Створюється все більше кібершахрайських груп, а масштаби розвитку даної проблеми з кожним днем збільшуються. Державна політика України має розвиватися у цьому напрямку, тим самим створюючи нові методи боротьби з кібершахрайством. Саме тому ми пропонуємо на рівні Кабінету Міністрів України розробити та затвердити відповідну Державну програму по запобіганню кібершахрайству в Україні.

|  |  |
| --- | --- |
| **Мета програми** | Становлення напрямів розвитку державної політики у сфері кіберзлочинності, зокрема приділення уваги проблемі виду кіберзлочинності – кібершахрайству, створення передумов для зменшення поширення даного явища, належна оцінка небезпеки кібершахрайства. |
| **Шляхи і способи розв’язання проблеми** | Необхідно залучити фахівців та спеціалістів для комплексного аналізу та вирішення даної проблеми. Розв’язання цієї проблеми включає в себе систему заходів, які б проводилися відповідними державними органами. Насамперед, необхідно вдосконалити кримінальне законодавство щодо цього питання та внести відповідні зміни та доповнення. При цьому, до вирішення цієї проблеми необхідно залучати навчальні заклади, соціальні служби. |
| **Завдання і заходи** | 1. Запровадження у школах, гімназіях, ліцеях інформаційних лекцій щодо явища «кібершахрайства», роз’яснення способів та методів його діяльності, мети, сутності.2. Проведення на рівні навчальних закладів заходів щодо всебічного розвитку дітей, створення відповідних гуртків, секцій для розвитку їх умінь, навичок та знань.4. Створення при навчальних закладах центрів з надання належної цифрової освіти, базові навички про безпеку в Інтернеті, загальні засади діяльності в мережі.5. Залучення IT фахівців для вдосконалення програми контролю за блогерами, а також для створення подібних програм, які б забезпечили безпечне використання Інтернету усіма користувачами. |
| **Очікувані результати** | Виконання Програми сприятиме ефективному і просторово збалансованому розвитку державної політики в сфері запобігання «кібершаїрайству» та дасть можливість забезпечити:- інформування та усвідомлення користувачами сутності «кібершахрайства»;- всебічний розвиток умінь, навичок користувачів, забезпечення їх безпеки у використанні Інтернет-ресурсів;- забезпечення надання кваліфікованої цифрової освіти користувачам;- забезпечення додаткового контролю з боку правоохоронних органів за блогерами;- створення IT-програм щодо контролю за інтернет-контентом блогерів.  |
| **Фінансове забезпечення** | Фінансове забезпечення Програми здійснюється за рахунок коштів, що передбачаються у державному бюджеті на відповідний рік, коштів місцевих бюджетів, а також за рахунок міжнародної фінансової і технічної допомоги та інших джерел, не заборонених законодавством. |

**Рекомендовані заходи**

|  |  |
| --- | --- |
| **Органи, відповідальні за проведення заходів** | **Заходи** |
| Міністерство освіти і науки | 1. Запровадження у школах, гімназіях, ліцеях інформаційних лекцій щодо «кібершахрайства», роз’яснення способів та методів його діяльності, мети, сутності.2. Проведення на рівні навчальних закладів заходів щодо всебічного розвитку дітей, створення відповідних гуртків, секцій для розвитку їх умінь, навичок та знань.3. Запровадження у навчальних закладах предметів, які б готували школярів до життя в інформаційному суспільстві.4. Залучення фахівців, які б надавали належні цифрові навички. |
| Кіберполіція | 1. Впровадження програмних засобів для систематизації та аналізу інформації про діяльність «кібершахраїв», їх поширення.2. Проведення заходів щодо боротьби з «кібершахраями». 3. Проведення контролю чисельності «кібершахраїв».4. Здійснення постійного моніторингу та нагляду за створенням нових «груп кібершахраїв».5. Завчасне реагування на будь-які випадки вчинення чи спроби вчинення кримінальних правопорушень з ознаками «кібершахрайства» |
| Міністерство внутрішіх справ | 1. Проведення наукових, кримінологічних і соціологічних досліджень щодо боротьби з «кібершаїрайством».2. Залучення IT фахівців для вдосконалення програми контролю за блогерами, а також для створення подібних програм, які б забезпечили безпечне використання інтернету усіма користувачами. |
| Міністерство юстиції | 1. Проведення заходів щодо інформування суспільства з діяльністю «кібершахраїв», формування правової свідомості і культури громадян.  |