2.3 Актуальні проблеми протидії кіберзлочинності в Україні

Останні двадцять років характеризуються активним розвитком комп'ютерних технологій. Комп'ютер грає велику роль, як в повсякденному житті кожного з нас, так і діяльності цілої держави. Але, швидка комп'ютеризація потягнула за собою виникнення нового виду суспільних відносин – відносин у кіберпросторі. Кіберпростір в свою чергу має низьку негативних, кримінально-правових характеристик, як порушення авторських прав, розповсюдження комп'ютерних вірусів, втручання в роботу інформаційних носіїв, незаконне використання інформації, та багато інших, як традиційних, так і інших видів кримінальних правопорушень, які були названі кіберзлочинами.

Кіберзлочиність є великою проблемою XXI століття. Дослідження внутрішньої структури, понятійного складу та аналіз інформаційних правопорушень, як суспільно негативного явища у наші часи є вкрай важливим аспектом, оскільки саме він допоможе побудувати ефективні механізми виявлення, розслідування та протидії комп'ютерній злочинності.

Кіберзлочинність, що набула суттєвого розвитку на сучасному етапі розвитку людства, спричиняє серйозне занепокоєння у системи правоохоронних та правозахисних органів держав світу. Систематичне зростання кількості інформаційних злочинів та динаміка їх поширення актуалізує питання дослідження проблем протидії кіберзлочинності та створення ефективної схеми розбудови належного рівня кібербезпеки нашої держави. Водночас систематичне розповсюдження програм-вірусів, фактів несанкціонованого доступу до інформаційних ресурсів кіберпростору, протиправне викрадення важливої інформації з баз даних, що не перебуває у загальному доступі, спричиняє дедалі більше негативних наслідків та несе небезпеку для суспільства.

Аналізуючи ситуацію, що склалася у нашій державі та у світі загалом в період боротьби з COVID-19, варто наголосити на тому, що світовий інформаційний простір під час карантину зазнав численних негативних явищ. Антисуспільний елемент, що являє собою велику кількість спроб вчинення

комп'ютерного шахрайства, привернув увагу спеціалістів та оперативних підрозділів, головною метою яких є боротьба з інформаційною злочинністю, що шириться світом [67, с. 135]. Існує потреба аналізу тієї неоднозначної ситуації, яка склалася в Україні щодо кіберпростору та протиправних посягань на інформаційні ресурси, що знаходяться в ньому. Передусім нагальною потребою є огляд світового досвіду протидії інформаційній та комп'ютерній злочинності з метою наслідування перспективних шляхів удосконалення системи забезпечення кібербезпеки нашої держави.

Терміни «кіберзлочинність», «злочини у сфері комп’ютерних технологій», «злочини у сфері комп’ютеризації» є такими, що пояснюють однакове злочинне явище, та в сучасному нормативному забезпеченні не визначені, однак сама концепція була сформульована завдяки активній роботі правоохоронних служб розвинутих країн Європи, ще в ХХ столітті, та стосується правопорушень у сфері комп’ютерного інформування та телекомунікації, незаконного введення в обіг нелецензованого комп’ютерного товару та багато інших правопорушень.

На сьогоднішній день комп’ютерні злочини є найбільш динамічною групою суспільно небезпечних посягань. Темпи поширення даних правопорушень напряму залежать від розвитку науки та технічного програмування населення, а також постійного поліпшення комп’ютерної техніки.

М.В. Карчевський та В.В. Невгад зазначають, що кіберзлочинність, кібершахрайство та викрадання інформаційних даних стало зворотнім ефектом суспільного розвитку у сфері комп’ютеризації. Так, наприклад в 2000 році фактів використання комп’ютера для вчинення кримінального правопорушення, зокрема, викрадення чужих персональних даних, або заволодіння банківськими рахунками, не було виявлено, але вже в 2001 році, за даними МВС, таких злочинів було зареєстровано 5, у 2002 році кількість зросла до 30, 2007 році- 146, а вже у 2020 році їх кількість суттєво зросла до 108474, що скоріш за все було зумовлено карантинними заходами від COVID-19 [68].

Кіберзлочини – це вид злочинів, що вчиняються в інтернет просторі (кіберпросторі), за допомогою математичних, цифрових або символічних прийомів, що знаходяться в постійній динаміці [69].

На відміну від інших груп злочинів, що в своєму розвитку нараховують декілька століть: крадіжка, шахрайство, вбивство, злочини у сфері комп'ютерного забезпечення є відносно молодим суспільно небезпечним явищем , що починає своє існування з появою мережі Інтернет. Такі ознаки, як масштабність; анонімність, швидкість передачі інформації; глобальність аудиторії, велика кількість сервісів, що пов'язані між собою, робить інтернет сприятливим для здійснення злочинних дій, оскільки виявити такі дії є більш складною задачею для правоохоронної системи.

Інформаційна злочинність у сучасному світі є найбільш динамічним видом кримінального правопорушення. Швидка тенденція у розвитку, зумовлена постійним розвитком комп'ютерних технологій. Кіберзлочинність – це вид кримінальних правопорушень, при вчиненні якого, особа використовує електронно-обчислювальні машини (комп'ютери), автоматизовані системи чи мережі електрозв'язку. Відповідальність за даний вид неправомірних дій передбачені Розділом XVI КК України.

Історичний розвиток кіберзлочинності починається з 60-х років XX століття, та нараховує наступні етапи:

– виникнення перших Інтернет серверів;
– виникнення перших Інтернет вірусів;
– застосування вперше відповідальності до кіберзлочинця, США 1983 р.
– прийняття першого нормативно – правового акту, що забороняв розповсюдження інтернет вірусів, США 1986 рік.
– прийняття Конвенції про кіберзлочинність Ради Європи, 2001 р.

Питання теоретичного визначення кіберзлочинності, полягає у криміналістичному дослідженні даного явища. Таким чином, об'єктом кіберзлочинів є сфера суспільних відносин що існує у межах інформаційного поля. Тобто, такі відносини, що виникають у процесі використання електронно-

обчислювальних мереж автоматизованих систем та мереж електрозв'язку. Суб'єкт кримінального правопорушення є загальним –фізична осудна особа що досягла віку кримінально-правової відповідальності. Деякі склади злочинів передбачені Розділом XVI КК України передбачають наявність спеціального суб'єкта злочину. Спосіб вчинення кіберзлочинів може різниться залежно від засобів скоєння кримінального правопорушення. Таким чином способами можуть бути: безпосередній доступ до інформації що містить на інформаційних носіях та способи віддаленого доступу до цієї ж інформації.

Отже можна виділити основні ознаки кіберзлочинності як суспільно небезпечного явища:

– сферою вчинення таких правопорушень є кіберпростір;

– дана група правопорушень включає в себе низьку відносин пов'язаних з використанням електронно-обчислювальних мереж автоматизованих систем та мереж електрозв'язку;

– у своїй більшості кіберзлочини передбачають наявність у правопорушники прямого умислу;

– засобами їх вчинення є комп'ютерні системи автоматизовані системи та мережі електрозв'язку.

Не менш важливим є визначення класифікації інформаційної злочинності оскільки саме вона повинна стати у нагоді при дослідженні сутності супільно-небезпечного діяння. Розуміння видів кіберзлочинів є важливим для побудови механізму виявлення розслідування та протидії злочинів у сфері комп'ютеризації.

Проаналізувавши нормативну базу та наукові погляди щодо класифікації кіберзлочинів ми можемо зробити висновок що найбільш доцільний поділ міститься у Конвенції Ради Європи про кіберзлочинність. Саме вона будується на родовому об'єкті досліджуваного виду правопорушення та є основою для побудови законодавства розвинутих країн. У наукових кругах існує дуже багато поглядів щодо поділу кіберзлочинів найбільш відомим з них є поділ у відповідності з родовим об'єктом:

– правопорушення відповідальність за які наступає на підставі Розділу XVI КК України;

– правопорушення відповідальність за які передбачена різними Розділами КК України.

КК України не містить чіткого поділу правопорушень у сфері комп'ютеризації. Це не є позитивним аспектом оскільки виникають труднощі у процесі кваліфікації дій осіб які вчинили правопорушення. Так, у більшості випадків відповідальність наступає за кримінальні правопорушення, передбачені ст.361 КК України, а найменш застосованою, на сьогоднішній день, є ст. 363 КК України.

Ще однією проблемою є застосування судами для осіб більш м'яких покарань, ніж передбачає стаття КК України, а також не застосування додаткових видів покарань, у вигляді конфіскації майна, особливо для речей, за допомогою яких було вчинено кримінальне правопорушення . Статистика показала, що рівень судимості, по відношенню до рівня скоєних правопорушень є дуже низьким.

Ми вважаємо, що сучасна правова система України повинна бути модернізована, у відповідності з Європейськими стандартами, а саме у сфері виявлення, розслідування та протидії кіберзлочинності. Модернізована правова система, допомогла б нам уникнути проблем у сфері розуміння внутрішньої структури, досліджуваного явища, кваліфікації дій осіб, які вчинили правопорушення та призначенні для них покарання.

Сьогодні актуальності набуває питання забезпечення кібербезпеки, що являє собою рівень захищеності інтересів людини та громадянина, суспільства та держави під час використання кіберпростору, а також можливості виявлення, запобігання і нейтралізація реальних і потенційних загроз кібербезпеці. Основоположними засадами, на яких базується чинне законодавство України у сфері протидії кіберзлочинності є загальні та міжнародні принципи: верховенство права, законність, забезпечення національних інтересів держави, пропорційність та адекватність заходів кібербезпеки реальним та потенційним

ризикам, пріоритет запобіжних заходів, взаємна допомога щодо правил про взаємну допомогу та інші.

Організаційні основи розслідування інформаційних та комп'ютерних злочинів сьогодні в Україні складають слідчі дії на початковому та наступному етапі розслідування. Відтак з метою запобігання поширення злочинів у кіберпросторі (правове регулювання передбачено відповідними статтями Кримінального кодексу України) оперативні та слідчі групи, по-перше, повинні здійснити повний збір необхідної інформації з локального пристрою чи комп'ютера злочинця, по-друге, організувати затримання особи злочинця, провести допит свідків, підозрюваних та, за наявності, співучасників у здійсненні конкретного кіберзлочину.

Перед Україною постає низка актуальних проблем, що сприяють зниженню ефективності протидії інформаційним злочинам, кількість та різноманітить яких з плином часу лише зростає. Основними питаннями, які потребують вирішення, є, по-перше, відсутність закріплення у чинних нормативно-правових актах України категоріального апарату у сфері кіберзлочинності, по-друге, відсутність спеціальних охоронних механізмів, призначених для здійснення контролю за інформаційним середовищем та явищами, що відбувають в ньому, по-третє, недостатність кадрового забезпечення правоохоронних органів держави й оперативних підрозділів розслідування транснаціональної кіберзлочинності, по-четверте, несвоєчасне повідомлення про вчинення кіберзлочинів з доку державних та комерційних структур, що зазнали нападу з боку кіберзлочинців**.**

Теоретичний аналіз світового досвіду боротьби з кіберзлочинністю вказує на беззаперечну роль США, ЄС та Канади у розвитку даної сфери. Необхідно зазначити про величезний внесок США, що створили Департамент кіберполіції у штаті Нью-Йорк, основними функціями якого є реалізація та розробка довгострокової національної політики щодо захисту держави від атак кіберзлочинців, та проєкт «Безпечне дитинство», котрий забезпечує протидію сексуальній експлуатації дітей у мережі Інтернет. Позитивним також є досвід

Європейського Союзу, що вирізняється створенням єдиної уніфікованої системи Центрів оперативної безпеки, котрі діють на території усього союзу демократичних європейських країн, та запровадженням системи так званих «кіберсанкцій». Успіхів у реалізації національної політики у сфері протидії кіберзлочинності досягла Канада, котра посприяла створенню сталої системи підрозділів муніципальної поліції, на які було покладено законом додаткові функції щодо ведення боротьби з кіберзлочинністю.

Задля вдосконалення протидії боротьби з кіберзлочинністю Україні варто посприяти реалізації нововведень передусім на нормативно-правовому та інституціональному рівнях. Доречним буде першою чергою сформувати категоріальний апарат, визначити державний орган, який би здійснював координації дій усіх оперативних підрозділів, обмежити обсяг повноважень державних оперативних підрозділів, посприяти закріпленню на законодавчому рівні можливості проведення незалежних перевірок суб'єктів, що надають цифрові послуги населенню, наділити підрозділи української муніципальної поліції новими функціями щодо протидії кіберзлочинності виданням відповідного нормативного акту, сприяти налагодженню тісного співробітництва з інституціями ЄС, спільній діяльності громадськості та наукових центрів з державними інституціями боротьби з кіберзлочинністю, запровадити режим «кіберсанкцій» на основі законодавства ЄС.