МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Київський національний торговельно-економічний університет

Кафедра міжнародного публічного права

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Міжнародно-правове співробітництво держав у сфері забезпечення кібербезпеки»

Студентки 2 курсу магістратури, 12м групи,
денної форми навчання
спеціальності Бондарєвої
«Міжнародне право» _____ Катерини Дмитрівни

Науковий керівник Дешко
д. ю. н., доцент _____ Людмила Миколаївна

Керівник освітньо-професійної
програми Дешко
д. ю. н., доцент _____ Людмила Миколаївна

2018

ЗМІСТ

ВСТУП

Актуальність теми. В сучасному світі технології розвиваються дуже стрімко. Виникн

це складні питання, які обговорювалися з моменту впровадження цієї технології і лишаються актуальними на сьогоднішній день. Сама держава не може справитися із цією проблемою, адже кіберзлочинність носить міжнаціональний характер: хакерські атаки можуть проводиться з використанням ресурсів з будь-яких куточків світу, тим самим значно ускладнюючи ідентифікацію та локалізацію нападників. Саме тому налагодження системи міжнародно-правового співробітництва держав є надзвичайно важливим кроком до забезпечення кібербезпеки.

Основними напрямами співпраці між національними урядами в сфері кібербезпеки є обмін інформацією, розслідування нападів або злочинів, запобігання або зупинка шкідливої поведінки, надання доказів і навіть організація передачі осіб до запитуючої держави.

Однак, з розвитком співпраці держав у сфері забезпечення кібербезпеки, створюються нові юридичні виклики. Величезна проблема полягає в невизначеності застосування правил, що регламентують фізичну силу до використання кібератак. Це створює масу юридичних викликів на шляху до забезпечення кібербезпеки. Положення Статуту ООН не дозволяють чітко встановити рівнозначність хакерській атаці, яку здійснила одна держава проти іншої, збройному нападу, що дає нації право на силові дії у відповідь. Крім того, концепція Статуту ООН щодо «застосування сили» не охоплює дії терористів та інших недержавних суб’єктів, які часто стоять за хакерськими атаками.

До того ж що не єдиним міжнародним договором у цій сфері є Конвенція Ради Європи про кіберзлочинність 2001 року. Конвенція являє собою правоохоронний договір, призначений для розробки спільної кримінально-правової політики, спрямованої на визначення, покарання та тим самим стримування злочинів, пов'язаних із кіберзлочинністю. Потенціал Конвенції щодо забезпечення кібербезпеки обмежується тим фактом, що його правоохоронна система діє у багатьох випадках у такий часовий діапазон, який занадто довгий, щоб захистити жертви кібернетичної атаки від шкоди. Натомість Конвенція розглядає види злочинів і процедуру реагування на кібератаки, інші злочинні дії, які уже сталися. І не розглядає як запобігти кіберзлочинам. Більше того, у договорі немає механізму встановлення або перегляду практик або стандартів кіберсистеми, які могли б загалом підвищити рівень безпеки. Тому, потенціал цього договору у забезпеченні загальної прихильності зменшується завдяки відображенню у ній зусиль, спрямованих на покарання поведінки на основі обмежень вмісту (таких як шахрайство та дитяча порнографія), а не на намаганні покарати за кіберзлочини, які потенційно можуть завдати шкоди самій кіберінфраструктурі.

Також варто взяти до уваги, що більшість країн серед яких країни, що розвиваються та країни з меншим рівнем розвитку взагалі не визнають кіберзлочинність у своєму національному законодавстві. Це полегшує умови для розвитку і процвітання кіберзлочинів, а також знижує у свідомості людей розуміння того, що неправомірні діяння в Інтернеті це серйозні злочини, які мають бути криміналізовані. І що покарання також має бути відповідним.

Більшість людей не усвідомлюють що таке кіберзлочини і як вони можуть вплинути на їх життя. Найпопулярнішими кіберзлочинами є крадіжка баз даних підприємств та шантажування щодо повернення файлів за гроші. Минулого року така ситуація сталася в Україні, від чого збитки понесли не лише українські підприємства і організації, а й представництва

іноземних компаній. Також представники індустрії кіно, музики, художнього мистецтва, розробники комп'ютерних ігор, програм та програмних забезпечень постійно несуть збитки через Інтернет піратство.

Наступним прикладом кіберзлочину є виведення з ладу або часткове призупинення роботи критично важливих інфраструктур. Зачасту до таких дій вдаються інші держави як прихована погроза з метою вирішення політичних суперечок. Це глобальна проблема, адже якщо злочинці можуть контролювати наприклад подачу світла, електроенергії в місті, то це може призвести навіть до захоплення і окупаціїї. Крім того, справа може дійти найжахливіших наслідків у випадку кібертероризму. Сьогодні в світі тероризм це дуже актуальна проблема. Випадки тероризму збільшились і рано чи пізно це може перейти на новий рівень – кібертероризм.

Саме тому зростає потреба у розвитку цієї галузі, розвитку національного законодавства за допомогою міжнародного права, яке держави мають розробляти у ході своєї співпраці.

Розвиток цифрових технологій в поєднанні з проблемою анонімності і обмеженнями, що накладаються принципом територіальної юрисдикції, невизначеність такого явища як кібератака безумовно є найсерйознішими перепонами на шляху до забезпечення кібербезпеки.

Теоретико-методологічну основу дослідження становлять праці вчених, наковців, політичних діячів, які торкались питань міжнародної співпраці у сфері забезпечення кібербезпеки та інших правових аспетів кіберзлочинності: М. С. Вільям, К. М. Віткомб, М. Герке, С. Гордон, С. Гранджер, Дж. Дароу, М. Джемінані, К. С. Джойнер, М. Е. Кабей, Л. П. Кураков, П. Ліндольм, Дж. В. Маклафін, Ф. А. Манель, С. Х. Нікум, П. Перник, Р. Рейберг, У. Сайбер, Р. Т. Слівка, М. Смітт, П. Стівен, П. А. Тейлор, О. Ткаченко, Р. Форд, Р. Н. Фрід, Н. Холмов, А. Черепанов.

Питання відносин в Інтернеті, а також розвиток законодавства в даній сфері досліджували С. А. Бабкін, Ю. М. Батурін, І. Л. Бачило, С. Д.

Бражник, В. В. Воробьов, А. В. Гелер, М. Д. Гудман, А. М. Доронін, А. А. Жмихов, А. М. Жодзишкий, Е. В. Краснєнкова, С. В. Молчанов, Д. С. Пушкін, Т. Г. Смірнова, Т. Л. Тропіна, С. І. Ушаков, В. П. Числін, А. Е. Шарков, Д. А. Ястрєбов.

Нормативну базу дослідження становлять нормативно-правові акти України та зарубіжних країн, міжнародні договори, правотворчі рішення міжнародних організацій і органів.

Емпіричною базою дослідження є матеріали судової практики, декларації та резолюції міжнародних міжурядових організацій, звіти органів державної влади, офіційні статистичні дані з досліджуваної проблематики.

Мета і задачі дослідження. *Метою* дослідження є розроблення концепції забезпечення кібербезпеки на міжнародному та національному рівнях за допомогою застосування міжнародно-правових норм, що були вироблені в результаті міжнародного співробітництва держав.

Для досягнення зазначеної мети визначено такі дослідницькі *задачі*:

виявити етапи генези міжнародно-правового співробітництва держав у сфері забезпечення кібербезпеки;

уточнити поняття кіберзлочинів, класифікувати їх;

виявити особливості нормативного регулювання міжнародного співробітництва держав у сфері забезпечення кібербезпеки;

виявити особливості організаційно-правового механізму міжнародного співробітництва держав у сфері забезпечення кібербезпеки на світовому рінві;

виявити особливості організаційно-правового механізму міжнародного співробітництва держав у сфері забезпечення кібербезпеки на регіональному рівні;

охарактеризувати участь України в міжнародно-правовому співробітництві у сфері забезпечення кібербезпеки;

розробити пропозиції з вдосконалення міжнародно-правового регулювання співробітництва держав у сфері забезпечення кібербезпеки шляхом створення єдиної міжнародної системи захисту та моніторингу;

розробити пропозиції з вдосконалення міжнародно-правового регулювання співробітництва держав у сфері забезпечення кібербезпеки шляхом вдосконалення національного законодавства держав.

Об'єктом дослідження є суспільні відносини, які виникають при міжнародно-правовому співробітництві держав у сфері забезпечення кібербезпеки.

Предметом роботи є міжнародно-правове співробітництво держав у сфері забезпечення кібербезпеки.

Методи дослідження. Методологічною основою проведеного дослідження стали загальні методи наукового пізнання, а також такі, що застосовуються в юридичній науці: методи аналізу і синтезу, формально-логічний, порівняльно-правовий, статистичний тощо. Зокрема, завдяки історико-правовому методу досліджено еволюцію відносин співпраці у сфері забезпечення кібербезпеки, а також виявлено основні періоди становлення та розвитку міжнародних відносин у сфері забезпечення кібербезпеки (підрозділ 1.1). Логіко-семантичний метод допоміг обґрунтувати визначення кіберзлочину, його видів (підрозділ 1.2). Методи аналізу та синтезу застосовано для поглиблення загального понятійно-дефініційного апарату (підрозділи 2.2, 2.3). За допомогою формально-логічного методу проведено аналіз взаємозв'язку нормативної бази міжнародних організацій та належного здійснення правосуддя, аналіз законодавства України, відповідних міжнародних установ та відповідних органів міжнародних організацій з метою виявлення його недоліків і розроблення пропозицій щодо їх усунення (підрозділи 1.3, 2.3, 3.2). Порівняльно-правовий метод дав змогу проаналізувати положення

вітчизняного та зарубіжного законодавства щодо досліджуваного права (підрозділ 1.3, 2.3). Статистичний метод застосовувався для опису загальної картини кіберзлочинів у світі (підрозділ 1.1).

Наукова новизна одержаних результатів зумовлена тим, що в магістерській роботі вперше у вітчизняній правовій науці на основі наукових здобутків, міжнародних договорів, правотворчих рішень міжнародних організацій і органів, декларацій і резолюцій міжнародних міжурядових організацій, законодавства України і зарубіжних країн та практики його застосування проведено системне, комплексне дослідження відносин міжнародної співпраці у сфері забезпечення кібербезпеки, що дало змогу обґрунтувати цілісну наукову концепцію цих відносин, а також нові теоретичні та прикладні положення і висновки.

Наукова новизна результатів дослідження конкретизується в таких положеннях, висновках, рекомендаціях та пропозиціях:

виявлено етапи генези міжнародно-правового співробітництва держав у сфері забезпечення кібербезпеки: 1. 1960-1970 роки - правопорушення зосереджувалися на фізичному пошкодженні комп'ютерних систем та знищенню збережених даних. Вони підпадали під юрисдикцію національного законодавства. 2. 1970-1080 роки - поява інтрнету, зародження кіберзлочинів (незаконне використання комп'ютерних систем, комп’ютерне шахрайство). застосування чинного законодавства у випадках комп'ютерної злочинності спричинило труднощі, обговорення правових рішень розпочалося в усьому світі. 3. 1980 - 1990 роки - збільшення кількості користувачів компютерних систем. Поява хакерів. Країни розпочали процес оновлення свого законодавства з метою задоволення вимог мінливого злочинного середовища. Поява першого міжнародного документу у сфері забезпечення кібербезпеки (хоч і на регіональному рівні) - розроблена спеціальним комітетом експертів Ради Європи у 1989 році Рекомендація №89. 4. 1990 - 2000 роки - розвиток

кіберзлочинності. Початок роботи таких міжнародних організацій як ОЕСР, Рада Європи, Велика вісімка, ООН над питаннями кібербезпеки. Як наслідок, кожна з цих організацій розробили певні рекомендації, які описувались вище, поведінки держав у випадку кіберзлочинів. Поява перших серйозних прицедентів міжнародних кіберпорушень та кіберзлочинів. 5. 2000 - 2010 роки - прийняття найважливіших рішень у сфері забезпечення кібербезпеки міжнародним співтовариством. Прийняття Радою Європи 23 листопада 2001 року у Будапешті Конвенції Ради Європи про кіберзлочинність, в 2004 році Європейським парламентом створено європейське агентства по мережевій і інформаційній безпеці (ENISA), в 2008 році ITU розробили Глобальну програму кібербезпеки ("GCA"). Призначення ITU статусу міжнародної організації, що має координуючу роль у всіх аспектах кібербезпеки. 6. 2010 - теперішній час - у сфері кіберзлочинності зявляються такі види злочинів, як кібертероризм. Міжнародна спільнота вдається до створення ценрів боротьби з кіберзлочинністю з філіалами в країнах.

уточнено поняття кіберзлочинів, класифікувати їх: кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечується сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенціальних загроз національній безпеці України у кіберпросторі», де «кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікації з використанням мережі Інтернет та або інших глобальних мереж передачі даних;

виявлено особливості нормативного регулювання міжнародного співробітництва держав у сфері забезпечення кібербезпеки: Найважливішою багатосторонньою угодою, яка конкретно стосується аспектів кібератак, є Конвенція Ради Європи про кіберзлочинність (Council of Europe Convention on Cybercrime – «CEC») 2001 року. Конвенція являє собою правоохоронний договір, призначений для розробки спільної кримінально-правової політики, спрямованої на визначення, покарання та тим самим стримування злочинів, пов'язаних із кіберзлочинністю;

виявлено особливості організаційно-правового механізму міжнародного співробітництва держав у сфері забезпечення кібербезпеки на світовому рівні. Співробітництво зумовлено такими всесвітніми міжнародними організаціями: ООН, Група 8, Міжнародний союз електрозв'язку, ОЕСР, Інтерпол.

виявлено особливості організаційно-правового механізму міжнародного співробітництва держав у сфері забезпечення кібербезпеки на регіональному рівні: Рада Європи, ЄС, Азіатсько-тихоокеанське економічне співробітництво (АТЕС), Співдружність, Ліга арабських держав (ЛАД), Організація американських держав (ОАД), Організація Східнокарибських держав, Тихоокеанський регіон;

охарактеризувано участь України в міжнародно-правовому співробітництві у сфері забезпечення кібербезпеки: Окрім роботи над національним законодавством, Україна визнає необхідність міцного міжнародного співробітництва та розбудови спроможності для вирішення потреб та загроз, пов'язаних із кібербезпекою, яка також висвітлена в новій Стратегії. Україна співпрацює з багатьма партнерами в кібер-сфері. Україна є партнером спільних проектів Європейського Союзу та Ради Європи "CyberCrime EAP II" та "CyberCrime EAP III", які мають регіональний аспект та включають

країни Східного партнерства. Перший проект спрямований на вдосконалення взаємної правової допомоги для міжнародної співпраці з питань кіберзлочинності та електронних доказів; посилення ролі 24/7 контактних пунктів;

розроблено пропозиції з вдосконалення міжнародно-правового регулювання співробітництва держав у сфері забезпечення кібербезпеки шляхом створення єдиної міжнародної системи захсту та моніторингу: створення міжнародної організації із забезпечення кібербезпеки. А також розробка і впровадження Конвенції із забезпечення кібербезпеки, яка була би написана під егідою цієї ж організації. Метою організації є забезпечення кібербезпеки як на національному, так і на міжнародному рівнях та всебічна співпраця між державами у сфері забезпечення кібербезпеки. Основна стратегія міжнародної організації із забезпечення кібербезпеки – створення єдиних стандартів забезпечення кібербезпеки і їх уніфікація державами;

розроблено пропозиції з вдосконалення міжнародно-правового регулювання співробітництва держав у сфері забезпечення кібербезпеки шляхом вдосконалення національного законодавства держав. Кожна держава повинна прийняти стратегію із забезпечення кібербезпеки і втілювати її в життя, приділити увагу законодавству у цій сфері, визначити та конкретизувати перелік кіберзлочинів та покарань, налагодити роботу відповідних органів із забезпечення кібербезпеки, активно співпрацювати з іншими державами та міжнародними організаціями.

Структура магістерської роботи зумовлена метою та задачами дослідження. Магістерська робота складається зі вступу, трьох розділів, що поділяються на 8 підрозділів, висновків, списку використаних джерел (156 найменувань). Загальний обсяг дисертаційної роботи становить 130 сторінки, з них основного тексту – 112 сторінок.

РОЗДІЛ 1 СТАНОВЛЕННЯ МІЖНАРОДНО-ПРАВОВОГО СПІВРОБІТНИЦТВА ДЕРЖАВ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

1.1 Генеза міжнародно-правового співробітництва держав у сфері забезпечення кібербезпеки

Виникнення і розвиток нового виду злочинності у світі інформаційних технологій та необхідна правова відповідь це складні питання, які обговорювалися з моменту впровадження цієї технології і лишаються актуальними на сьогоднішній день. Протягом останніх 50 років на національному та регіональному рівнях було запропоновано та реалізовано чимало різних ідей вирішення цих питань. Однією з причин, чому питання кібербезпеки залишаються відкритими, - це постійний технологічний розвиток, а також зміна методів та способів здійснення правопорушень.

У 1960-і роки впровадження комп'ютерних систем на базі транзисторів, які були меншими і дешевшими, ніж системи, які до цього створювались на основі електровакуумних ламп, призвели до збільшення використання комп'ютерних технологій [1]. На цьому ранньому етапі правопорушення зосереджувалися на фізичному пошкодженні комп'ютерних систем та знищенню збережених даних [2]. Такі випадки траплялись, наприклад, у Канаді, де в 1969 році студентський бунт викликав пожежу, яка призвела до знищення комп'ютерних даних університету [3].

Кіберзлочинність, як така зародилась з появою інтернету. В 1957 році у відповідь на запуск радянського супутника, США створюють Агентство передових дослідницьких проектів (ARPA). Зусилля організації були спрямовані на дослідження у сфері комп'ютерних технологій, які очолив доктор Дж. Ліклайдер. Джозеф Ліклайдер вперше висловив ідею про необхідність створення комп'ютерів, що працюють в режимі реального часу. В 1965 році вчений опублікував свою концепцію комп'ютерної мережі «Galactic network». Ідея цієї концепції полягала в необхідності об'єднання комп'ютерів в мережу з вільним доступом будь-якої людини з будь-якої точки світу до її ресурсів. Ліклайдера називають духовним батьком всесвітньої мережі, людиною, що посіяла насіння Інтернету.

В середині 1960-х років Сполучені Штати розпочали дискусію щодо створення надійного, на випадок війни, центрального сховища даних, яким змогли би користуватись всі міністерства. В 1969 році за дорученням Міністерства оборони США декілька наукових установ починають розробляти мережу, що вважається початком інтернету – ARPAnet (Advanced Research Projects Agency Network). Першочерговим завданням ARPAnet Міністерство оборони США вбачало об'єднати в єдину мережу науково-дослідницькі та військові інститути в США задля збільшення швидкості та покращення зручності обміну інформацією між ними. В умовах Холодої війни також стала задача створити інфраструктуру, спроможну пережити атомний удар. Отже, можна сказати, що поштовхом до інформаційно-технологічного прогресу, створення Інтернету послужили політичні протистояння двох наддержав – Радянського Союзу та США.

У 1970-х роках використання комп'ютерних систем та комп'ютерних даних зростало [4]. Наприкінці десятиріччя в США було засновано приблизно 100 000 комп'ютерів [5]. З падінням цін комп'ютерні технології почали активніше використовуватись в межах адміністративного та громадського секторів, а також в бізнесі. 1970-ті роки характеризувалися зміщенням від традиційних майнових злочинів проти комп'ютерних систем

[6], які переважали у 1960-х роках, до нових форм злочинності [7]. Хоча фізичний збиток продовжував залишатись актуальною формою кримінального переслідування проти комп'ютерних систем, [8] були визнані нові форми комп'ютерної злочинності. Вони включали в себе незаконне використання комп'ютерних систем [9] та маніпулювання електронними даними. Перехід від ручних до комп'ютерних операцій призвів до ще однієї нової форми злочинності комп'ютерного шахрайства [10]. Вже в цей час багатомільйонні втрати були спричинені такими шахрайськими операціями [11].

Зокрема, комп’ютерне шахрайство стало справжнім викликом для правоохоронних органів, яким доводилось розслідувати дедалі більше подібних випадків [12]. Оскільки застосування чинного законодавства у випадках комп'ютерної злочинності спричинило труднощі, обговорення правових рішень розпочалося в усьому світі. В той же час Інтерпол розпочав активну роботу аналізу явищ комп’ютерного шахрайства та пошуку можливості юридичної відповіді.

У 1980-х роках персональні комп'ютери стали все більш популярними. Відповідно, знову зростає кількість комп'ютерних систем і, отже, кількість потенційних цілей для злочинців. Вперше цілі включали широкий спектр критично важливих інфраструктур [13]. Одним із побічних ефектів розповсюдження комп'ютерних систем стало підвищення інтересу до програмного забезпечення, що призвело до появи перших форм програмного піратства та злочинів, пов'язаних із патентами. Мережі дозволяли правопорушникам входити в комп'ютерну систему, не перебуваючи на місці злочину. В 1983 році в штаті Мілуокі, США стався перший арешт Інтернет-злочинця. Приводом до цього послужив перший зареєстрований Інтернет-злам, здійснений шістьма підлітками, які називали себе «Група 414» (414 – міжміський телефонний код Мілуокі). Протягом дев’яти днів ними було зламано 60 комп’ютерів, серед яких були комп’ютери Лос-Аламоської державної лабораторії. Після арешту один з

членів групи дав свідчення і інші її учасники отримали умовний термін покарання [14].

Крім того, можливість розповсюдження програм через мережі дозволила правопорушникам розповсюджувати шкідливе програмне забезпечення та комп'ютерні віруси [15]. Країни розпочали процес оновлення свого законодавства з метою задоволення вимог мінливого злочинного середовища [16]. Сполучені Штати почали розробку законопроекту, спеціально для боротьби з кіберзлочинністю. У 1986 році в США вступив в дію перший комп'ютерний закон «The Computer Fraud and Abuse Act», згідно якого було заборонено неавторизований доступ до будь-якої комп'ютерної системи і отримання секретної військової інформації. Окрім цього, закон захищав такі види несекретної інформації: інформація, що належить фінансовим установам (наприклад, про кредитні картки і рахунки); дані, що належать урядовим установам; інформація, яка належить міжнародним та міжштатовим організаціям. Пошкодження даних і розповсюдження вірусів також було під забороною. Закон одразу показав свою ефективність. Цього ж року було заарештовано члена групи «Legion of Doom» Лойда Бланкеншипа, також відомого під ніком «The Mentor». Пізніше, у в'язниці Бланкеншип написав знаменитий Маніфест хакера – «Hacker Manifesto».

В цей час починає зароджуватись міжнародні відносини у сфері забезпечення кібербезпеки. Зокрема, перші кроки до встановлення міжнародної співпраці було зроблено Радою Європи. Спеціальний комітет експертів Ради Європи у 1989 році розробив рекомендацію № 89, затверджену комітетом Міністрів ЄС. Рекомендація містить ряд правопорушень, пов'язаних з інформаційними технологіями для розробки країнами-учасницями ЄС карної стратегії у відповідь на такі злочини. Документ також вказує на необхідність досягнення міжнародного консенсусу з питань криміналізації деяких злочинів, пов'язаних з комп'ютерами. Рекомендація містить два списки злочинів - «мінімальний»

і «факультативний (додатковий)». «Мінімальний» список включає діяння, які обов'язково мають бути заборонені міжнародним законодавством і підлягають переслідуванню в судовому порядку. «Додатковий» список містить ті правопорушення, по яких досягнення міжнародної згоди представляється скрутним [17].

ОЕСР та Рада Європи створили навчальні групи для аналізу явищ та оцінки можливостей юридичної відповіді. На 22-му саміті (Ліон, 1996) «Велика вісімка» затвердила підготовлені Експертною групою з транснаціональної організованої злочинності «Рекомендації боротьби з транснаціональною злочинністю», в які також увійшли пропозиції щодо протидії високотехнологічним і комп'ютерним злочинам. Рекомендації закликають до мобілізації міжнародного співробітництва по розслідуванню кіберзлочинів, перегляду матеріального і процесуального національного законодавства з метою забезпечення адекватного кримінального переслідування на місцевому рівні. Однак, дані рекомендації не містять конкретних керівних принципів щодо забезпечення кібербезпеки і не мають обов'язкового характеру.

Введення в дію графічного інтерфейсу ("WWW") в 1990-х роках призвело до стрімкого зростання кількості користувачів Інтернету. Інформа

навіть у країнах, де оприлюднення такої інформації було незаконним [18]. Ще одне питання, пов'язане з онлайн-службами, яке виявилося особливо складним у розслідуванні транснаціо

це швидкість обміну інформацією. Врешті решт, розповсюдження дитячої порнографії перемістилося з фізичного обміну книгами та стрічками на інтернет-розповсюдження через веб-сайти та Інтернет-послуги [19]. Хоча комп'ютерні злочини були загалом місцевими злочинами, Інтернет перетворив електронні злочини на транснаціональні. У результаті перед міжнародним співтовариством постала потреба у вирішенні нових питань.

У 1990 році VIII Конгрес ООН з попередження злочинності і поводження з правопорушниками ухвалив резолюцію, що закликає держави-члени ООН збільшити зусилля із боротьби з комп'ютерною злочинністю, модернізуючи національне карне законодавство, сприяти розвитку в майбутньому структури міжнародних принципів і стандартів запобігання, судового переслідування і покарання в області комп'ютерної злочинності [20]. 14 грудня 1990 року Генеральна Асамблеєю ООН ухвалила резолюцію, що закликає уряди держав-членів керуватися рішеннями, прийнятими на VIII Конгресі ООН.

Першим великим фінансовим злочином з використанням Інтернету стала «справа Володимира Левіна». Йдеться про аферу, яку в 1994 році провернув пітерський хакер Володимир Левін та його прибічники. Міжнародна організована злочинна група у складі 12 людей зламала систему управління рахунками корпоративних клієнтів американського "Сітібанку" [21]. Таким чином було викрадено понад 12 мільйонів доларів. Судовий розгляд завершився 24 лютого 1998 року. Суд південного округу Нью-Йорка призначив Левіну 36 місяців в'язниці (замість обіцяних спочатку шістдесяти років). Цей гучний та інтернаціональний злочин продемонстрував, що кіберзлочини можуть завдати серйозного фінансового збитку.

У 1995 році в Ліоні (Франція) була проведена міжнародна конференція Інтерполу з комп'ютерної злочинності. Учасники конференції підкреслили, що викликає тривогу відсутність міжнародного механізму для раціонального і ефективного протистояння цьому виду злочинності. За підсумками конференції був зроблений висновок, що у більшості країн світу спостерігається усе зростаюче використання інформаційних технології в кримінальній діяльності. Це викликає необхідність постійного вивчення цього кримінального прояву, оскільки розвиток комп'ютерних технології призводить до використання цих інновацій при скоєні комп'ютерних злочинів [22].

Підхід Інтерполу до боротьби з кіберзлочинністю полягає в тому, щоб використовувати досвід його членів у боротьбі із злочинами у сфері інформаційних технологій шляхом функціонування робочих груп або експертних груп. Робочі групи створюються для вивчення регіонального досвіду і існують в Європі, Азії, Африці і Північній і Південній Америці.

Оцінка наступного факту привела до появи таких термінів, як «Інтернет-тероризм», «комп'ютерний тероризм», «кібертероризм». У 1998 році 12-річний хакер проник в комп'ютерну систему, яка контролювала водоспуск дамби Теодора Рузвельта в Арізоні. Небезпека його дій полягала в тому, що у разі відкриття зливних воріт дамби вода могла затопити міста Темп і Месе із загальною чисельністю населення в 1 млн. людей.

Наступним етапом розвитку кіберзлочинності стало використання мережі Інтернет в політичних цілях. Так, 21 грудня 1995 року група активістів «Strano Network» здійснили перший в історії Інтернет-страйк проти політики уряду Франції, щодо ядерних програм та соціальної сфери. В ході протесту учасники групи зі всього світу одночасно заходили на урядові сайти, що обмежувало доступ до сайтів і навіть виводило їх з ладу на деякий час.

Ще один яскравий приклад виник з конфлікту в Косово. Різні групи комп'ютерних активістів дуже активно викладали в Інтернеті інформацію для засудження військових дій Югославії та НАТО, порушували при цьому роботу урядових комп'ютерів і утримували контроль над сайтами з подальшою зміною вмісту. За допомогою широкого розповсюдження історій про небезпеки і жахи війни, викладання фактів і думок політиків, громадських діячів, ця подія стала відомою на весь світ. Даний конфлікт вважається першою в світі Інтернет-війною. Проте, на мою думку, подібні випадки складно віднести до серйозних кіберзлочинів. У кожній демократичній країні дозволяються мирні протести. Тому і це свого роду я вважаю одним з видів мирних протестів та пропаганди, яка не несе абсолютно ніякої шкоди. Якщо велика група людей, об'єднаних по всьому

світу прагнуть добитися справедливості шляхом розповсюдження інформації – це не є загрозою для людства. Скоріше за все, це схоже на революцію з боку суспільства по відношенню до злочинних дій правління. Якщо порівнювати мирні протести у класичному вигляді, якими ми звикли їх бачити, коли люди виходять на вулиці з протестами в Інтернеті, можна сказати, що в останньому виді унеможливлюється каліцтво, фізична жорстокість та інші неправомірні заходи, які можуть бути застосовані з боку урядовців, поліції та просто неадекватних людей.

Як і кожне попереднє десятиліття, 21 століття характеризується новими тенденціями в галузі комп'ютерної злочинності та кіберзлочинності. Змінились не тільки методи, але і вплив. Оскільки правопорушники змогли автоматизувати атаки, кількість правопорушень збільшилася. Країни, регіональні та міжнародні організації мусили реагувати на зростаючі виклики та надавали відповідь на кіберзлочинність як пріоритет. У сфері кіберзлочинності з’являються нові суб’єкти. Окрім фізичних осіб, інтернаціональних груп людей, активістів, комп’ютерні злочини стають притаманними для терористів, які виводять з ладу критично важливі інфраструктури і держав, які ведуть кібернетичні війни шляхом розповсюдження вірусів, пропаганди, зомбування та шпіонаж. Віруси виводять з ладу роботу підприємств, що тягне за собою величезні фінансові збитки.

Прогресом в міжнародно-правовому забезпеченні кібербезпеки стало прийняття Радою Європи 23 листопада 2001 року у Будапешті Конвенції Ради Європи про кіберзлочинність. Це один з найважливіших документів, що регулюють правовідносини у сфері глобальної комп'ютерної мережі і доки єдиний документ такого рівня. Прийняття його - це своєрідна віха в історії боротьби з кіберзлочинністю [23]. Наша країна ратифікувала цю конвенцію 7 вересня 2005 року [21].

Підготовка Конвенції була тривалим процесом - за чотири роки було складено 27 проектів. Остання версія, що містить преамбулу і чотири

глави, датована 25 травня 2001 року, була представлена Європейській комісії з боротьби з кіберзлочинністю на 50-му пленарному засіданні 18-22 червня 2001 року.

Конвенція класифікує злочини в кіберпросторі на 4 групи. У першу групу злочинів, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних даних і систем входять: незаконний доступ (ст. 2), незаконне перехоплення (ст. 3), дія на комп'ютерні дані (ст. 4) або на системи (ст. 5). Також до цієї групи злочинів входить протизаконне використання спеціальних технічних пристроїв (ст. 6). Об'єктом злочину виступають не лише комп'ютерні програми, розроблені або адаптовані для скоєння злочинів, передбачених в статтях 2-5 Конвенцій, але і комп'ютерні паролі, коди доступу і їх аналоги, за допомогою яких може бути отриманий доступ до комп'ютерної системи в цілому або будь-якій її частині (з урахуванням злочинного наміру). Норми ст. 6 Конвенцій застосовні тільки у тому випадку, якщо використання (поширення) спеціальних технічних пристроїв спрямоване на здійснення протиправних діянь.

До другої групи входять злочини, пов'язані з використанням комп'ютерних засобів : підлог і шахрайство з використанням комп'ютерних технологій (статті 7, 8 Конвенцій).

Третю групу складають злочини, пов'язані з контентом (змістом) даних. До четвертої групи увійшли порушення авторського права і суміжних прав.

Крім того, на початку 2002 р. до Конвенції ухвалив протокол, що додає в перелік злочинів поширення інформації расистського і іншого характеру, що підбурює до насильницьких дій, ненависті або дискримінації окремої особи або групи осіб, що ґрунтуються на расовій, національній, релігійній або етнічній приналежності.

Таким чином, перший розділ Конвенції присвячений видам діянь, що підлягають криміналізації. Її другий розділ освітлює процесуальні аспекти боротьби з кіберзлочинністю.

У Конвенції піднімається одна із основних проблем правового регулювання Інтернету - визначення юрисдикції (ст. 22). Конвенція пропонує традиційне рішення проблеми юрисдикції : карна юрисдикція визначається відповідно до територіальної ознаки (територія держави; борт судна або літака держави).

Зважаючи на відсутність кордонів в глобальних мережах, Конвенція уточнює ситуацію колізії юрисдикції декількох держав: у такому разі, згідно п. 5 ст. 22, держави повинні проводити консультації для визначення відповідної юрисдикції для судового переслідування.

Глава III Конвенції – «Міжнародна співпраця» - присвячена питанням екстрадиції, спільній діяльності держав-учасників у сфері боротьби з комп'ютерними злочинами і досягнення узгодженості для збору доказів в електронній формі.

Конвенція про кіберзлочинність на сьогодні є одним з базових міжнародно-правових актів у сфері права телекомунікацій, але і цей документ не позбавлений недоліків. Ще до підписання Конвенції деякі групи по захисту громадянських прав і провайдери інтернет-послуг приводили серйозні аргументи проти укладення цього договору, який на їх погляд має неясні формулювання і пред'являє провайдерам непосильні вимоги.

У число організацій, що підписали протест проти прийняття Конвенції, увійшли «Фонд Електронних Меж» (Electronic Frontier Foundation, США), міжнародна організація «Суспільство Інтернет» (Internet Society), «Організація кіберправа і кіберсвободи» (Cyber - Rights & CyberLiberties, Великобританія), «Кріптополіс» (Kriptopolis, Іспанія) і інші. У протесті відзначається, що Конвенція несе в собі загрозу для норм захисту особи, що встановилися, невиправдано розширює поліцейські

функції уряду, а також знижує відповідальність держави в правоохоронній діяльності.

Звичайно, єдиним критерієм ефективності Конвенції, так само як і справедливості заперечень критично налагоджених опонентів, являється практика її застосування положень. Окремі положення Конвенції (наприклад, що стосуються процесуальних питань, визначення юрисдикції і класифікації кіберзлочинів) надалі будуть переглянуті. Але сьогодні можна констатувати, що прийняття Конвенції послужить фундаментом для міжнародного законодавства, що формується. Навіть ті країни, які з яких-небудь причин не підписали Конвенцію можуть використовувати досвід, що накопичується, по правовому регулюванню нової предметної області – кіберпростір.

10 березня 2004 року європейським парламентом створено європейське агентства по мережевій і інформаційній безпеці (ENISA). Це агентство Євросоюзу, створено з метою підвищення ефективності функціонування внутрішнього ринку. Агентство виступає в ролі консультанта і центру передових технології у сфері мережевої і інформаційної безпеки для країн-членів і інститутів Євросоюзу. Крім того, агентство сприяє розвитку зв'язків між країнами-членами Євросоюзу, інститутами Євросоюзу, господарюючими суб'єктами і приватним бізнесом [24].

У той же час починає активно діяти ITU - Міжнародний союз електрозв'язку. Діючи згідно з щорічними закликами Генеральної Асамблеї ООН для більшого міжнародного співробітництво у боротьбі з кібер-загрозами та після численних конференцій та досліджень різноманітних приватних, національних, регіональних та міжнародних груп ITU скликало Всесвітній саміт з інформаційного суспільства (WSIS), на якому уряди та світові лідери закликали ITU стати єдиним "фасилітатором дій" у визначеній лінії дій 5: "Створення впевненості та безпеки в застосуванні ІКТ [Інформаційні та комунікаційні технології]". Після проведення низки

зустрічей, декларацій, програм та значних зусиль експерти та підтримуючі уряди, ІКТ, розпочаті 17 травня 2007 року, а також оголосили в 2008 році свою Глобальну програму кібербезпеки ("GCA") "забезпечити заходи, в рамках яких міжнародна відповідь на зростаючі виклики для кібербезпеки може бути узгоджена та вирішена". GCA підкреслює бажаність узгоджених зусиль всіх зацікавлених сторін "для зміцнення довіри та безпеки в інформаційному суспільстві, "Але він вважає, що ITU є "унікальним місцем", щоб бути лідером у цих зусиллях. В ITU входять 191 держава-член, а його сектори операцій (радіозв'язок, стандартизація та розвиток телекомунікацій) швидко розширюються, включивши в них питання, пов'язані з кібер-технологіями. Організація здійснює свою сприйняту роль через широкий спектр заходів з освіти в галузі кібербезпеки та розробки та оприлюднення широкого кола планів та протоколів, спрямованих на створення безпечної кіберінсталяції шляхом боротьби з кіберзлочинністю, технічними стандартами, вимогами безпеки, потенціалом будівництво та навіть популяризація дитячої онлайнової безпеки. GCA закликає до постійного залучення всіх існуючих зацікавлених сторін до зусиль у сфері кібербезпеки. В той же час, однак, це чітко свідчить про свою рішучість шукати впровадження стандартів, виданих власним органом з розробки стандартів (MCE-D) та ISO, а також його наміром відігравати провідну, чи не єдину координуючу роль у всіх аспектах кібербезпеки.

У січні 2013 року в Гаазі відкрився Європейський центр боротьби з кіберзлочинністю (EC3). Завдання EC3 - присікати дії організованих злочинних мереж. На даний момент об'єкти уваги EC3 обмежені трьома онлайн-шахрайство, що заподіює великий збиток фінансовим організаціям і їх клієнтам; поширення дитячої порнографії, кібератаки на ключові інфраструктури і інформаційні системи [25].

Отже, можна виділити такі етапи появи та розвитку кіберзлочинності:

1. 1960-1970 роки - правопорушення зосереджувалися на фізичному пошкодженні комп'ютерних систем та знищенню збережених даних. Вони підпадали під юрисдикцію національного законодавства.
2. 1970-1080 роки - поява інтрнету, зародження кіберзлочинів (незаконне використання комп'ютерних систем, комп’ютерне шахрайство). застосування чинного законодавства у випадках комп'ютерної злочинності спричинило труднощі, обговорення правових рішень розпочалося в усьому світі.
3. 1980 - 1990 роки - збільшення кількості користувачів компютерних систем. Поява хакерів. Країни розпочали процес оновлення свого законодавства з метою задоволення вимог мінливого злочинного середовища. Поява першого міжнародного документу у сфері забезпечення кібербезпеки (хоч і на регіональному рівні) - розроблена спеціальним комітетом експертів Ради Європи у 1989 році Рекомендація №89.
4. 1990 - 2000 роки - розвиток кіберзлочинності. Початок роботи таких міжнародних організацій як ОЕСР, Рада Європи, Велика вісімка, ООН над питаннями кібербезпеки. Як наслідок, кожна з цих організацій розробили певні рекомендації, які описувались вище, поведінки держав у випадку кіберзлочинів. Поява перших серйозних прицедентів міжнародних кіберпорушень та кіберзлочинів.
5. 2000 - 2010 роки - прийняття найважливіших рішень у сфері забезпечення кібербезпеки міжнародним співтовариством. Прийняття Радою Європи 23 листопада 2001 року у Будапешті Конвенції Ради Європи про кіберзлочинність, в 2004 році Європейським парламентом створено європейське агентства по мережевій і інформаційній безпеці (ENISA), в 2008 році ITU

розробили Глобальну програму кібербезпеки ("GCA"). Призначення ITU статусу міжнародної організації, що має координуючу роль у всіх аспектах кібербезпеки.

6. 2010 - теперішній час - у сфері кіберзлочинності зявляються такі види злочинів, як кібертероризм. Міжнародна спільнота вдається до створення ценрів боротьби з кіберзлочинністю з філіалами в країнах.

Основними напрямами співпраці між національними урядами в сфері кібербезпеки, як уже було сказано, є обмін інформацією, розслідування нападів або злочинів, запобігання або зупинка шкідливої поведінки, надання доказів і навіть організація передачі осіб до запитуючої держави.

Однак, з розвитком співпраці держав у сфері забезпечення кібербезпеки, створюються нові юридичні виклики. Величезна проблема полягає в невизначеності застосування правил, що регламентують фізичну силу до використання кібератак. Це створює масу юридичних викликів на шляху до забезпечення кібербезпеки. Положення Статуту ООН не дозволяють чітко встановити рівнозначність хакерській атаці, яку здійснила одна держава проти іншої, збройному нападу, що дає нації право на силові дії у відповідь. Крім того, концепція Статуту ООН щодо «застосування сили» не охоплює дії терористів та інших недержавних суб'єктів, які часто стоять за хакерськими атаками. Оскільки акти кіберагресії не піддаються традиційній класифікації відповідно до міжнародно-визнаних норм ведення бойових дій, як правило, прийнято вважати, що держави повинні ставитися до міжнародних хакерських атак як до різновиду кримінального правопорушення. Навіть в тому випадку, якщо хакерська атака здійснена державою або його агентами, в рамках чинного міжнародного правового режиму забороняються несанкціоновані односторонні дії. Таким чином, потерпіла держава, домагаючись справедливості, з великою часткою ймовірності, буде змушена вдаватися до кримінального переслідування. Ситуація ще більше ускладнюється тим

фактом, що обсяг правил застосування сили далеко не загально узгоджений.

Ще одним юридичним викликом є те, що хакерські атаки зазвичай мають мало спільного з традиційною злочинною діяльністю; як правило, буває важко встановити злочинний характер подібних діянь, на відміну від актів війни або тероризму. Хакерські атаки в значній мірі не піддаються простій класифікації видів озброєнь, яка використовується в міжнародному праві, що серйозно ускладнює застосування традиційних визначень злочинності, тероризму та агресії, наведених в існуючих правових нормах [26].

Потерпілі держави, перш ніж вжити заходів в рамках існуючих міжнародно-правових норм, повинні попередньо з'ясувати джерело і характер конкретних випадків хакерських атак. При цьому, кібератака повинна розглядатися або як збройний напад, або як кримінальний злочин.

Значним юридичним викликом є також встановлення законодавства за яким слід судити кіберзлочинців. За самою природою кібепростору, хакерські атаки можуть проводиться з використанням ресурсів з будь-яких куточків світу, тим самим значно ускладнюючи ідентифікацію та локалізацію нападників. Крім того, країни, що не володіють розвиненою цифровою інфраструктурою, аби замаскувати джерело нападу, можуть де завгодно укласти договір оренди відповідного устаткування, що дає можливість здійснювати хакерську атаку проти визначеної мети. Встановлення відповідальних сторін також ускладнюється прискореним прогресом комп'ютерних технологій, що ставить правоохоронні органи в дуже невигідне становище.

Розвиток цифрових технологій в поєднанні з проблемою анонімності і обмеженнями, що накладаються принципом територіальної юрисдикції, невизначеність такого явища як кібератака безумовно є найсерйознішими перепонами на шляху до забезпечення кібербезпеки.

1.2 Поняття та види кіберзлочинів

Більшість звітів, довідників чи публікацій про кіберзлочинність починаються з визначення термінів "комп'ютерна злочинність" та "кіберзлочинність". В останні десятиліття були прийняті різні підходи для розробки точного визначення для обох термінів[27]. Перед тим, як надати оцінку існуючим підходам, корисно визначити зв'язок між "кіберзлочинністю" та "злочином, пов'язаним з комп'ютерними програмами". Термін "кіберзлочинність" є вужчим, ніж злочин, пов'язаний з комп’ютером, оскільки мова йде про вчинення злочину за допомогою комп'ютерної мережі. Злочини, пов'язані з комп'ютером, охоплюють навіть ті правопорушення, які не мають ніякого відношення до мережі, але стосуються лише автономних комп'ютерних систем.

Під час 10-го Конгресу Організації Об'єднаних Націй із запобігання злочинності та поводження з правопорушниками у рамках відповідного

семінару було розроблено два визначення [28]. Кіберзлочинність у вузькому значенні (комп'ютерна злочинність) охоплює будь-яку незаконну поведінку, спрямовану на безпеку комп'ютерних систем та оброблюваних ними даних за допомогою електронних операцій. Кібернетичні злочини в ширшому сенсі (злочини, пов'язані з комп'ютером) охоплюють будь-яку незаконну поведінку, здійснену за допомогою або в зв'язку з комп'ютером чи мережею, включаючи такі злочини, як незаконне володіння, надання або розповсюдження інформації за допомогою комп'ютерної системи чи мережі. Ще одне більш широке визначення наведене в статті 1.1 Стенфордського проекту Міжнародної конвенції про посилення захисту від кіберзлочинності та тероризму ("Стенфордський проект"), яка вказує на те, що кіберзлочинність відноситься до дій стосовно кіберсистем. Термін "кіберзлочинність" використовується для опису низки злочинів, включаючи традиційні комп'ютерні злочини, а також мережеві злочини.

Закон України про основні засади забезпечення кібербезпеки України від 5 жовтня 2017 року визначає «кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечується сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенціальних загроз національній безпеці України у кіберпросторі», де «кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з’єднаних) комунікаційних систем та забезпечення електронних комунікації з використанням мережі Інтернет та або інших глобальних мереж передачі даних». «Кіберзахист – це сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від

кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем» [29].

Термін "кіберзлочинність" використовується для охоплення широкого кола злочинних дій. Оскільки визнані злочини включають широке коло різноманітних правопорушень, важко розробити типологію чи систему класифікації кіберзлочинності [30]. Один підхід можна знайти в Конвенції про кіберзлочинність, яка розрізняє чотири різні види правопорушень:

1. Правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних та систем.

2. Правопорушення, пов'язані з комп'ютером.

3. Правопорушення, пов'язані зі змістом.

4. Правопорушення, пов'язані з порушенням авторських та суміжних прав.

Ця типологія не є повністю послідовною, оскільки вона не базується на єдиному критерії диференціації категорій. Три категорії зосереджені на об'єкті правового захисту: "злочини проти конфіденційності, цілісності та наявності комп'ютерних даних та систем"; правопорушення, пов'язані з вмістом; та правопорушенням пов'язані з авторським правом. Четверта категорія "злочини, пов'язані з комп'ютером" зосереджена не на об'єкті правової охорони, а на методі, що використовується для вчинення злочину. Крім того, деякі терміни, які використовуються для опису злочинних дій (таких як "кібертероризм" або "фішинг"), охоплюють дії, які відносяться до кількох категорій. Тим не менше, ці чотири категорії можуть служити корисною основою для обговорення явищ кіберзлочинності. Для того, щоб зрозуміти суть і значення кіберзлочинів, потрібно розглянути їх види.

Злочини проти конфіденційності, цілісності та наявності комп'ютерних даних та систем. Усі правопорушення у цій категорії спрямовані проти (як мінімум) одного з трьох правових принципів конфіденційності, цілісності та доступності. На відміну від злочинів, які протягом століть охоплюються кримінальним законодавством (наприклад,

крадіжка чи вбивство), комп'ютеризація правопорушень є порівняно недавньою, оскільки комп'ютерні системи та комп'ютерні дані були розроблені лише приблизно 60 років тому. Ефективне переслідування цих дій вимагає від існуючих норми кримінального права не тільки захищати матеріальні речі та фізичні документи від маніпуляцій, але також адаптуватись, застосовуючи нові правові принципи. Під цю категорію злочинів підпадає незаконний доступ, незаконне отримання даних, незаконне перехоплення, перешкода передачі даних, втручання в систему.

Незаконний доступ являє собою хакерство, взлом і стосується незаконного доступу до комп'ютерної системи. Це один з найстаріших злочинів, пов'язаних із комп'ютерними злочинами [31]. Після розвитку комп'ютерних мереж (особливо Інтернету) цей злочин став масовим явищем. Найвідомішими об’єктами хакерських атак є Національне управління з аеронавтики і дослідження космічного простору США (НАСА), Військово-повітряні сили США, Пентагон, Yahoo, Google, eBay та урядові сайти Німеччини [32].

Приклади таких правопорушень включають взлом пароля захищених веб-сайтів та обхід захисту комп'ютерних систем. Але акти, пов'язані з терміном "хакерство", також включають в себе підготовчі дії, такі як використання несправного програмного забезпечення чи програмного забезпечення для незаконного отримання пароля для входу в комп'ютерну систему, створення "підробки" веб-сайтів, щоб користувачі розкривали свої паролі та поширення програмних засобів кілогінгу (наприклад, "клавіатурних шпигунів"), які записують кожне натискання клавіші.

Мотивація правопорушників може бути різною. Деякі обмежують свою діяльність обходом заходів безпеки тільки для того, щоб довести свої здібності. Інші діють через політичну мотивацію (відома під назвою "хактивізм"). Деякі правопорушники використовують доступ для здійснення подальших злочинів, таких як шпіонаж даних, маніпулювання даними або атаки служб (DoS). У більшості випадків незаконний доступ

до комп'ютерної системи є лише найважливішим першим кроком. Збільшенню кількості хакерських атак сприяють такі чинники: недостатній та неповний захист комп'ютерних систем, розробка програмних засобів, які автоматизують атаки і зростаюча роль приватних комп'ютерів як мети хакерських атак.

Незаконне отримання даних прирівнюється до шпіонажу даних. Якщо комп'ютерна система підключена до Інтернету, правопорушники можуть намагатися отримати доступ до цієї інформації через Інтернет з майже будь-якого місця світу. Інтернет все частіше використовується для отримання комерційної таємниці [33]. Значення конфіденційної інформації та можливості доступу робить дані шпіонажу надзвичайно цікавими. У 1980-х роках німецьким хакерам вдалося зламати доступ до сайтів уряду США та військових комп'ютерних систем, отримуючи секретну інформацію та продаючи цю інформацію агентам з іншої країни.

Зловмисники використовують різні методи для доступу до комп'ютерів потерпілих, включаючи програмне забезпечення для сканування, незахищені порти або обхідні заходи захисту, а також за допомогою "соціальної інженерії" [34]. Останній підхід, зокрема, стосується нетехнічного виду вторгнення, яке багато в чому залежить від взаємодії людини і часто притягує інших людей до порушення процедур безпеки [35]. У контексті незаконного доступу описується маніпуляція людьми з наміром отримати доступ до комп'ютерних систем. Соціальна інженерія зазвичай є дуже успішною, оскільки найслабша ланка комп'ютерної безпеки часто є користувачами, що експлуатують комп'ютерну систему. Одним із прикладів є "фішинг", який нещодавно став ключовим злочином, скоєним у кіберпросторі, і описує спроби шахрайства отримувати конфіденційну інформацію (наприклад, паролі) шляхом представлення себе як надійної особи чи бізнесу (наприклад, фінансової установи) у начебто офіційному електронному повідомленні. Хоча людська вразливість користувачів відкриває двері для ризику

шахрайства, вона також пропонує рішення. Освічені користувачі комп'ютерів не є легкими жертвами для злочинців, які використовують соціальну інженерію. Як наслідок, освіта користувача повинна бути суттєвою частиною будь-якої стратегії боротьби з кіберзлочинністю.

Крім того, технічні заходи можуть бути зроблені для запобігання незаконного доступу. ОЕСР підкреслює важливість криптографії для користувачів, оскільки криптографія може допомогти поліпшити захист даних. вид захисту інформації, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо. Такий захист може бути більш ефективним, ніж будь-який фізичний захист. Успіх злочинців в отриманні конфіденційної інформації часто обумовлений відсутністю захисних заходів.

Хоча правопорушники зазвичай націлені на комерційну інформацію, все частіше трапляються випадки злочинів із даними, що зберігаються на приватних комп'ютера [36]. Приватні користувачі часто зберігають інформацію про банківський рахунок та кредитну картку на своєму комп'ютері. Порушники можуть використовувати цю інформацію для своїх цілей (наприклад, дані банківського рахунку для здійснення грошових переказів) або продати її третій стороні. Записи кредитних карток, наприклад, продаються на суму до 60 доларів США. Звичайно, прибутки від ділової таємниці, як правило, перевищують прибуток від одержання або продажу одиночної інформація про кредитну картку. Однак, оскільки приватні комп'ютери, як правило, менш захищені, шпіонаж даних на основі приватних комп'ютерів, ймовірно, стане ще більш вигідним.

Є два підходи до отримання інформації. Правопорушники можуть отримати доступ до комп'ютерної системи або пристрою зберігання даних і витягувати інформацію; або спробуйте маніпулювати користувачем, щоб

вони розкривали інформацію або коди доступу, які дозволяють злочинцям отримати доступ до інформації ("фішинг").

Правопорушники часто використовують комп'ютерні інструменти, встановлені на комп'ютерах жертв або шкідливі програми, які називаються шпигунськими програмами, для передачі даних їм. Класичне антишпигунське та антивірусне програмне забезпечення в значній мірі не завжди може їх ідентифікувати.

Незаконне перехоплення є наступним підвидом злочинів проти конфіденційності, цілісності та допустимості комп’ютерних даних та систем. Правопорушники можуть перехоплювати зв'язок між користувачами (наприклад, електронною поштою) або іншими формами передачі даних (коли користувачі завантажують дані на веб-сервери або отримують доступ до веб-зовнішніх носіїв даних) для запису інформації, якою вони обмінюються. У цьому контексті правопорушники взагалі можуть націлюватися на будь-яку комунікаційну інфраструктуру (наприклад, фіксовані лінії або бездротовий зв'язок) та будь-яку інтернет-службу (наприклад, електронну пошту, чат або через голосовий зв'язок).

Більшість передач даних серед постачальників Інтернет-інфраструктури або Інтернет-провайдерів є добре захищеними та важко перехопленими. Однак злочинці шукають слабкі місця в системі. В даний час готелі, ресторани та бари пропонують клієнтам доступ до Інтернету через точки бездротового доступу. Проте сигнали в обміні даними між комп'ютером і точкою доступу можуть бути отримані в радіусі до 100 метрів. Порушники, які бажають перехопити процес обміну даними, можуть робити це з будь-якого місця в межах цього радіуса. Навіть там, де бездротові з'єднання зашифровані, правопорушники можуть розшифрувати записані дані. Щоб отримати доступ до конфіденційної інформації, деякі правопорушники встановлюють точки доступу поблизу місцевостей, де існує високий попит на бездротовий доступ (наприклад, поблизу ресторанів та готелів). Більшість країн перейшли до захисту використання

телекомунікаційних послуг шляхом криміналізації незаконного перехоплення телефонних розмов. Однак, зважаючи на зростаючу популярність послуг на основі IP
це ідентифікатор (унікальний числовий номер) мережевого рівня, який використовується для адресації комп'ютерів чи пристроїв у мережах, які побудовані з використанням інтернету), законодавцям, можливо, доведеться оцінити, як можна встановити подібний захист для послуг, що базуються на IP.

Перешкода передачі даних: передача даних є життєво важливим для приватних користувачів, підприємств та адміністрацій, і всі вони залежать від цілісності та доступності даних. Відсутність доступу до даних може призвести до значного (фінансового) збитку. Порушники можуть порушувати цілісність даних та втручатися в них, видаляючи, пригнічуючи або змінюючи комп'ютерні дані. Одним із поширених прикладів видалення даних є комп'ютерний вірус. Починаючи з часу розробки комп'ютерних технологій, комп'ютерні віруси загрожували користувачам, які не встановили належний захист [37]. З тих пір кількість комп'ютерних вірусів значно зросла. Відтоді не тільки кількість вірусних атак збільшилася, але також змінилися методи та функції вірусів.

Раніше комп'ютерні віруси поширювалися за допомогою пристроїв зберігання даних, таких як гнучкі диски, в той час як сьогодні більшість вірусів поширюються через Інтернет як додатки до електронних поштових повідомлень або до файлів, які завантажують користувачі. Ці ефективні нові методи розповсюдження значно прискорили вірусні інфекції та значно збільшилася кількість заражених комп'ютерних систем. За оцінками експертів, за допомогою комп'ютерного черв'яка SQL Slammer було інфіковано 90% вразливих комп'ютерних систем протягом перших 10 хвилин його розповсюдження [38].

Сучасні віруси здатні здійснювати віддалене управління комп'ютером жертви або шифрувати файли, щоб жертви не мали доступу до власних файлів, доки вони не заплатять гроші, щоб отримати ключ.

Наступним підвидом є системне втручання. Якщо правопорушники вдаються до запобігання безперебійної роботи комп'ютерних систем, це може призвести до значних фінансових втрат для жертв. Якщо правопорушники мають доступ до комп'ютерної системи, вони можуть знищити апаратне забезпечення. Для більшості кримінально-правових систем такі випадки не становлять серйозних проблем, оскільки вони схожі на класичні випадки пошкодження або руйнування майна. Однак для високорентабельних підприємств електронної комерції фінансові збитки, завдані нападами на комп'ютерну систему, набагато перевищують витрати на комп'ютерні апарати.

Більш складним завданням для правових систем є шахрайство в Інтернеті. Приклади цих віддалених атак на комп'ютерні системи включають комп'ютерні хробаки та атаки, результатом яких є відмова комп’ютера в обслуговуванні. Комп'ютерні хробаки є підгрупою зловмисного програмного забезпечення (наприклад, комп'ютерні віруси). Вони є самореплікаційними комп'ютерними програмами, які шкодять мережі, ініціюючи кілька процесів передачі даних. Вони можуть впливати на комп'ютерні системи, перешкоджаючи плавному функціонуванню комп'ютерної системи, використовуючи системні ресурси для реплікації себе через Інтернет або створення мережевого трафіку, що може призвести до закриття доступності певних сервісів (таких як веб-сайти).

Такі комп'ютерні атаки створюють серйозні проблеми для більшості систем кримінального права, оскільки ці напади не можуть мати жодного фізичного впливу на комп'ютерні системи. Для вирішення питання про запобігання та судове переслідування подібних нападів на критичну інфраструктуру, необхідний окремий законодавчий підхід.

До злочинів, пов’язаних зі змістом відносять: еротичні або порнографічні матеріали, дитячу порнографію, расизм, пропаганда насильства, правопорушення, пов’язані з релігією, незаконні онлайн-ігри, наклеп та фальшиві відомості, спам та пов'язані з ними загрози, інші форми незаконного вмісту.

Розвиток правових інструментів для боротьби з цією категорією суттєво впливає на національні підходи, які можуть враховувати фундаментальні культурні та правові принципи. Нелегальний контент, системи цінностей та правові системи значно відрізняються між собою у різних країнах. Поширення ксенофобних матеріалів є незаконним у багатьох європейських країнах, але може бути захищеним принципом свободи слова у Сполучених Штатах. Використання принизливих зауважень стосовно Святого Пророка є кримінальним у багатьох арабських країнах, але не в деяких європейських країнах [38].

Юридичні підходи до криміналізації незаконного змісту не повинні втручатися у право на свободу вираження поглядів. Право на свободу вираження поглядів, наприклад, визначається принципом 1 (b) Йоханнесбургських принципів національної безпеки та свободи вираження [40]. Однак принцип 1 (c) пояснює, що право на свободу вираження поглядів може бути обмеженим. Тоді як криміналізація незаконного контенту не може бути закритою, вона повинна суворо обмежуватися. Особливо обговорювались такі обмеження щодо криміналізації наклепу. Спільна декларація Спеціального доповідача ООН про свободу думки та вираження 2008 року вказує на те, що неточні поняття, такі як передача повідомлень та прославляння тероризму або екстремізму, не повинні підлягатись криміналізації.

Ці юридичні виклики є складними, оскільки інформація, доступна одному комп'ютерному користувачеві в одній країні, доступна майже з будь-якої точки світу. Якщо "правопорушники" створюють вміст, який є незаконним у деяких країнах, але не в країні, з якої вони працюють,

кримінальне переслідування "правопорушників" важко здійснити або взагалі неможливо.

Є багато невизначеності щодо змісту матеріалу та в якій мірі конкретні дії повинні бути криміналізовані. Різні національні погляди та труднощі у переслідуванні порушень, здійснених поза межами території країни, що досліджує, сприяли блокуванню певних типів контенту в Інтернеті. Якщо існує угода про недопущення доступу до веб-сайтів із незаконним вмістом, розміщеним за межами країни, держави можуть підтримувати суворі закони, блокувати веб-сайти та фільтрувати вміст [41].

Існують різні підходи до систем фільтрування. В деяких державах від постачальників доступу вимагається встановлювати програми, що аналізують відвідувані веб-сайти та блокують веб-сайти з чорного списку [42]. Ще одне рішення встановлення програмного забезпечення для фільтрів на комп'ютерах користувачів (корисний підхід для батьків, які хочуть контролювати вміст, який можуть переглядати діти, а також для бібліотек та загальнодоступних інтернет-терміналів).

Спроби керувати вмістом в інтернеті не обмежуються певними типами вмісту, які широко визнані незаконними. Деякі країни використовують технологію фільтрів для обмеження доступу до веб-сайтів, що стосуються політичних тем. Фахівці повідомляють, що в даний час цензура застосовується приблизно двома десятками країн [43].

Вміст сексуального характеру був одним із перших незаконних контентів, який комерційно поширювався через інтернет. Торгівля в інтернеті еротичними та порнографічними матеріалами має багато переваг, включаючи: обмін носіями (такими як картинки, фільми, пряма трансляція) без необхідності витрат на доставку; набагато більша кількість клієнтів, ніж в роздрібних магазинах; анонімність аспект, який споживачі порнографії цінують, з урахуванням переважаючих соціальних поглядів. Недавні дослідження виявили 4,2 мільйони порнографічних веб-

сайтів, які є доступними в інтернеті в будь-який час. Крім веб-сайтів, матеріали порнографічного характеру можуть бути розповсюджені через системи обміну файлами та системи обміну миттєвими повідомленнями. Різні країни криміналізують еротичний та порнографічний матеріал, як правило так: дозволяють обмінюватися порнографічними матеріалами серед дорослих та обмежують криміналізацію випадків, коли неповнолітні отримують доступ до такого роду матеріалів. Дослідження показують, що доступ до порнографічного матеріалу для дітей може негативно вплинути на їх розвиток. Деякі країни визнають кримінальну відповідальність за будь-який обмін порнографічними матеріалами навіть у дорослих, не орієнтуючись на конкретні групи (такі як неповнолітні). Але, знову ж таки, велику роль грає глобалізація інтернету. Навіть якщо органи влади можуть ідентифікувати веб-сайти з інших куточків світу, що містять порнографічні матеріали, вони можуть не мати жодних повноважень для примусового виконання вилучення образливого вмісту постачальниками. Принцип національного суверенітету, як правило, не дозволяє країні проводити розслідування на території іншої країни без дозволу місцевої влади [44].

Інтернет став основним каналом для розповсюдження дитячої порнографії. У 1970-х і 1980-х роках правопорушники, які брали участь в обміні дитячої порнографії, зіткнулися з серйозними загрозами [45]. У той час комерційний ринок дитячої порнографії зосереджувався головним чином на Європі та США , а матеріал був дорогим і його було важко отримати. У минулому виробники не мали можливості самостійно робити фотографії та фільми. Вони були залежними від послуг, що пропонуються підприємствами. Це підвищувало шанси працівників правоохоронних органів виявляти дитячу порнографію за допомогою звітів від підприємств, що займаються розробкою.

Доступність відеокамер на ринку змінило цю ситуацію. Але ризики були пов'язані не тільки з виробництвом. Засоби зв'язку між продавцем та колекціонером, а отже, і самим ринком, були обмеженими. Ситуація

суттєво змінюється з появою інтернет-додатків для обміну даними. Виникли проблеми з точки зору виявлення та розслідування випадків дитячої порнографії. Інтернет сьогодні є основним каналом для торгівлі порнографією, а також дитячою порнографією [46]. Одним із наслідків цього розвитку є те, що навіть коли правопорушник, який видав матеріал, заарештований і його файли конфісковані, стає важко видаляти файли після того, як вони були продані через інтернет.

На відміну від різних поглядів на дорослу порнографію, дитяча порнографія широко засуджена, а правопорушення, пов'язані з дитячою порнографією, в більшості країнах визнані злочинними [47]. Міжнародні організації займаються боротьбою проти дитячої порнографії в інтернеті, з низкою міжнародно-правових ініціатив, серед яких: Конвенція Організації Об'єднаних Націй про права дитини 1989 року [48]; Рамкове рішення Ради Європи Європейського Союзу 2003 року про боротьбу з сексуальною експлуатацією дітей та дитячою порнографією [49], Конвенція Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства 2007 р. [50].

На жаль, ці ініціативи, спрямовані на контроль над поширенням порнографії в мережі, мало стримують злочинців, які використовують інтернет для обміну дитячою порнографією. Дослідження поведінки правопорушників дитячої порнографії показує, що 15 % арештованих осіб, які мають у своєму розпорядженні дитячу порнографію в інтернеті, мали понад 1000 фотографій на своєму комп'ютері; 80 % мали фотографії дітей у віці від 6 до 12 років [51], 19 % мали зображення дітей віку молодше 3 років 344; 21 % мали зображення з насильством. Складність притягнення до відповідальності злочинців полягає в тому, що більшість матеріалів є захищеними паролем, або знаходяться на закритих форумах, до яких звичайні користувачі та правоохоронні органи можуть рідко отримувати доступ. Тому таємні операції є життєво важливими у боротьбі з дитячою порнографією.

Расизм, ненависні висловлювання та пропаганда насильства зараз не такі популярні, як були в 2000 роках. Радикальні групи використовують такі системи масової комунікації, як Інтернет для розповсюдження пропаганди. У 2006 році в інтернет існувало понад 6 000 таких веб-сайтів, що сприяють расовій ненависті, насильству та ксенофобії.

Приклади веб-сайтів підбурювання до ненависті включають веб-сайти, що містять інструкції щодо побудови бомб. Крім пропаганди, Інтернет використовується для продажу певних товарів, наприклад, предмети, пов'язані з нацистами, такі як прапори з символікою, уніформа та книги, легко доступні на аукціонних платформах та спеціалізованих веб-магазинах. Інтернет також використовується для надсилання електронних повідомлень та інформаційних бюлетенів та поширення відеокліпів та телевізійних шоу через популярні архіви, такі як YouTube. Не всі країни визнають кримінальними правопорушення для цих правопорушень [52]. У деяких країнах такий зміст може бути захищений принципами свободи слова.

Думки різняться щодо того, наскільки далеко випливає принцип свободи слова в певних темах, що часто перешкоджає міжнародним розслідуванням. Одним із прикладів конфлікту законів є справа, що стосується постачальника послуг Yahoo! у 2001 році, коли французький суд наказав Yahoo! (заснований у США) заблокувати доступ французьких користувачів до матеріалу, пов'язаного з нацистами [53]. На підставі першої поправки до Конституції Сполучених Штатів продаж таких матеріалів є дозволеним законодавством США. Після першої поправки американський суд вирішив, що французький порядок не може бути застосований проти Yahoo! у Сполучених Штатах.

Диспропорції між країнами з цих питань були очевидними під час розробки Конвенції Ради Європи про кіберзлочинність. Конвенція про кіберзлочинність спрямована на гармонізацію законів, пов'язаних із кіберзлочинністю, для забезпечення того, щоб міжнародні розслідування

не розв’язували конфлікти законів. Не всі сторони, що беруть участь у переговорах, могли б узгодити загальну позицію щодо криміналізації поширення ксенофобних матеріалів, тому ця тема була виключена з Конвенції про кіберзлочинність. Інакше деякі країни (включаючи Сполучені Штати), можливо, не підписали би Конвенцію про кіберзлочинність.

До злочинів з незаконним змістом також належить правопорушення проти релігії. Такими є веб-сайти, які представляють матеріали, що схиляють до підписання антирелігійних письмових заяв. Також іншими прикладами можуть слугувати наклеп на релігію.

Проте, не варто забувати, що багато дискусійних груп ґрунтуються на принципі свободи слова. Свобода слова є ключовим чинником успіху в інтернеті. Хоча для сучасних розвинутих держав дуже важливо охороняти принцип свободи слова, навіть найбільш ліберальні країни певною мірою регулюють умовами та законами цей принцип. Найбільшим успіхом в цій справі для держави є знайти баланс між обмеженнями та дозволеним при застосуванні свободи слова.

Різні юридичні стандарти щодо незаконного контенту відображають проблеми регулювання змісту. Навіть там, де публікація контенту охоплюється положеннями, що стосуються свободи слова в країні, де вміст доступний, цей матеріал можна отримати в країнах з більш жорсткими правилами. "Мультиплікаційний спір" у 2005 році продемонстрував потенціал для конфлікту. Публікація дванадцяти редакційних мультфільмів у датській газеті «Jyllands-Posten» призвела до широкомасштабних протестів у мусульманському світі [54].

Як і у випадку незаконного змісту, наявність певної інформації чи матеріалів є кримінальним правопорушенням у деяких країнах. Захист різних релігій та релігійних символів у різних країнах відрізняється. Деякі країни визнають кримінальну відповідальність за використання принизливих висловлювань стосовно релігії, тоді як інші країни можуть

прийняти більш ліберальний підхід і не вживати криміналізацію подібним діям.

Інтернет-ігри та азартні ігри є однією з найбільш розвинутих сфер в інтернеті. Деякі оцінки передбачають зростання обсягів прогнозованих надходжень від онлайн-азартних ігор в 3.1 до 24 млрд. Дол. США у 2010 році (хоча в порівнянні з доходами від традиційних азартних ігор вони залишаються відносно невеликими [55]).

Регулювання азартних ігор поза межами Інтернету між країнами дуже різниться. Інтернет дозволяє людям обходити обмеження щодо азартних ігор. Інтернет-казино широко доступні. Більшість з них розміщується в країнах з ліберальними законами чи взагалі з відсутністю правил щодо азартних ігор в інтернеті. Користувачі можуть з легкістю відкривати рахунки в інтернеті, переказувати гроші та грати в азартні ігри.

Інтернет-казино також можуть бути використані для фінансування тероризму та боротьби із зароблянням грошей. Якщо правопорушники використовують онлайн-казино, яке не веде обліку, правоохоронним органам важко визначити походження коштів. Було здійснено декілька спроб законодавства запобігти участі в онлайн-азартних іграх [56], зокрема, Закон США про захист Інтернет-азартних ігор у 2006 році, спрямований на обмеження незаконних онлайн-азартних ігор переслідуючи провайдерів фінансових послуг, якщо вони здійснюють розрахунки за транзакції, пов'язані з незаконними азартними іграми. На мою думку, це найоптимальніший шлях боротьби з таким видом кіберзлочину.

Інтернет може бути використаний для поширення дезінформації. Веб-сайти можуть представляти фальшиву інформацію або наклеп особливо в форумах і чатах, де користувачі можуть публікувати повідомлення без перевірки модераторами. Неповнолітні користувачі все частіше використовують веб-форуми та соціальні мережі, де така інформація може бути розміщена також. Кримінальна поведінка може включати публікацію

інтимних фотографій або фальшивих відомостей про сексуальні вчинки [57].

У більшості випадків правопорушники користуються перевагами того факту, що постачальники, які пропонують дешеві або безкоштовні публікації зазвичай не вимагає ідентифікації авторів або може не підтверджувати ідентифікатор. Це ускладнює ідентифікацію правопорушників. Крім того, модератори форуму можуть не мати ніяких обмежень щодо вмісту. Ці переваги не завадили розробці цінних проектів, таких як онлайн-енциклопедія Wikipedia, де існують суворі процедури регулювання вмісту. Проте така ж технологія може використовуватися правопорушниками для публікації неправдивих відомостей (наприклад, про конкурентів) або розголошення секретної інформації (наприклад, публікації державної таємниці).

Важливо підкреслити підвищену небезпеку, надану фальшивою або оманливою інформацією. Дезінформація може серйозно зашкодити репутації та гідності потерпілих у значній мірі, оскільки онлайн-заяви є доступними для всесвітньої аудиторії. Навіть якщо інформація виправляється або видаляється незабаром після публікації, можливо, вона вже була дубльована людьми, які не бажають скасувати чи видалити їх. У цьому випадку інформація може бути доступною в інтернеті, навіть якщо вона була вилучена чи виправлена оригінальним джерелом. Приклади включають випадки інтернет розсилки мільйонам людей непристойних, оманливих чи хибних електронних повідомлень про людей чи організації. Шкода репутації в такому випадку колосальна і ніколи не може бути відновлена, незалежно від істинності чи іншої вихідної електронної пошти. Тому свобода слова та захист потенційних жертв від наклепу повинні бути добре збалансовані.

"Спам" описує отримання небажаних масових повідомлень. Хоча існують різноманітні шахраї, найпоширеніші це спам-повідомлення по електронній пошті. Правопорушники надсилають мільйони електронних

повідомлень користувачам, часто містять рекламу продуктів і послуг, але часто також мають шкідливе програмне забезпечення. Перша електронна пошта спаму була відправлена в 1978 р. і відтоді приплив спамових повідомлень різко збільшився [58]. Сьогодні постачальники послуг електронної пошти повідомляють, що від 85 до 90 % усіх електронних листів є спамом.

Більшість постачальників електронної пошти реагують на зростаючі рівні спам-повідомлень, встановивши технологію антиспам-фільтрів. Ця технологія визначає спам за допомогою фільтрів ключових слів або "чорних списків" IP-адрес спамерів. Хоча технологія фільтрів продовжує розвиватися, спамери виявляють шляхи використання цих систем, наприклад, уникаючи ключових слів. Так, спамери знайшли багато способів описати "Віагру", одну з найпопулярніших продуктів, що пропонуються в спамі, без використання назви бренду [59].

Успіх у виявленні спамових повідомлень залежить від змін у способі розповсюдження спаму. Спам-повідомлення є надзвичайно вигідними, оскільки витрати на надсилання мільярдів електронних повідомлень є низькими. Деякі фахівці вважають, що єдиним реальним рішенням у боротьбі зі спамом є підвищення витрат на передачу для відправників.

Інтернет використовується не лише для вищезазначених злочинів та правопорушень, але також як форум для залучення, пропозицій та підбурювання до злочинів незаконного продажу товарів та надання інформації та інструкцій щодо незаконних дій (наприклад, як створити вибухові речовини).

Різні країни застосовують різні національні правила та торговельні обмеження для різних продуктів, таких як військове спорядження. Аналогічна ситуація існує і в лікарських засобах ліки, які доступні без обмежень, в деяких країнах можуть потребувати рецепту в інших. Транскордонна торгівля може ускладнити забезпечення обмежень доступу до певних продуктів на території тієї чи іншої держави [60].

Інтернет-магазини, що працюють у країнах без обмежень, можуть продавати товари клієнтам інших країн з обмеженнями. До появи та розвитку Інтернету більшості людей було важко отримати інструкції щодо створення зброї. Необхідна інформація була доступною (наприклад, в книгах, що стосуються хімічних аспектів вибухових речовин), але здобуття такої інформації забирало багато часу, необхідного для пошуку. Сьогодні інформація про те, як побудувати вибухові речовини, доступна через Інтернет, і легкість доступу до інформації підвищує вірогідність нападів. Це і є приклади злочинів та правопорушень, які пов’язані зі змістом.

Наступну категорію кіберзлочинів складабють правопорушення, пов'язані з авторськими правами та товарними знаками. Однією з життєво важливих функцій Інтернету є поширення інформації. Компанії використовують Інтернет для розповсюдження інформації про свої продукти та послуги. Їх імідж брендів та корпоративний дизайн можуть бути використані для збуту контрафактної продукції: фальшивомонетники копіюють логотипи, а також продукти та намагаються зареєструвати домен, пов'язаний з цією конкретною компанією. Компанії, які розповсюджують продукти безпосередньо через Інтернет, можуть мати юридичні проблеми з порушенням авторських прав. Їхні продукти можуть бути завантажені, скопійовані та розповсюджені.

Основою сучасних порушень авторських прав є швидке та точне відтворення. Сьогодні можна дублювати цифрові джерела без втрати якості, а також, як результат, робити копії з будь-якої копії. Найбільш поширені порушення авторських прав включають обмін піснями, файлами та програмним забезпеченням, захищеними авторським правом, у системах спільного використання файлів [61] або через послуги зі створення власних ресурсів та обхід системи керування цифровими правами.

Технологія, що використовується для обміну файлами, дуже складна і дозволяє короткочасно обмінюватися великими файлами. Децентралізована концепція мереж обміну файлами другого покоління

ускладнює запобігання їх роботі. Правоохоронні органи мали певний успіх у розслідуванні порушень авторських прав у системах з файлообмінниками. Більш пізні версії систем обміну файлами дозволяють створювати анонімні повідомлення та ускладнюють розслідування.

Технологія спільного використання файлів використовується не тільки звичайними людьми та злочинцями, а й звичайними підприємствами. Проте, не всі файлообмінники порушують авторські права. Прикладом є обмін авторизованими копіями або творами мистецтва всередині суспільства.

Тим не менше, використання систем обміну файлами створює проблеми для індустрії розваг. Дослідження виявляють мільйони користувачів спільного використання файлів та мільярди завантажених файлів [62]. Копії фільмів з'являються в системах обміну файлами, перш ніж вони офіційно випускаються в кінотеатрах. Розробка анонімних систем обміну файлами робить роботу власників авторських прав значно складнішою, а також правоохоронних органів.

Дискусії криміналізації порушень авторських прав спрямовано не лише на обмін файлами та обхід технічного захисту, але також на виробництво, продаж та зберігання "незаконних пристроїв" або інструментів, призначених для того, щоб користувачі могли здійснювати порушення авторських прав.

відомий аспект глобальної торгівлі, схожий на порушення авторських прав. Порушення, пов'язані з товарними знаками перейшли в кіберпростір з різним ступенем криміналізації відповідно до національного законодавства тієї чи іншої держави. Найбільш серйозні правопорушення включають використання товарних знаків у злочинній діяльності з метою введення в оману користувачів та злочинів, пов'язаних із доменним ім'ям. Гарна репутація компанії часто пов'язана безпосередньо з її товарними знаками. Порушники використовують фірмові назви та торговельні марки

шахрайським чином у ряді заходів, включаючи фішинг, про який згадувалось раніше.

Ще однією проблемою, пов'язаною з порушеннями торговельних марок, є правопорушення, пов'язані з доменом. У більшості випадків правопорушники прагнуть продати домен за високу ціну компанії, яка безпосередньо володіє назвою домену, або використовувати його для продажу товарів чи послуг, що вводять в оману користувачів через їх передбачуваний зв'язок із товарним знаком. Іншим прикладом злочину, пов'язаного з доменом, є "викрадення домену".

Комп'ютерне шахрайство є одним із найпопулярніших злочинів в Інтернеті, оскільки це дозволяє правопорушнику використовувати автоматизацію та програмні засоби для маскування ідентичностей злочинців. Автоматизація дозволяє правопорушникам отримувати великі прибутки від ряду малих дій. Однією зі стратегій, що використовуються правопорушниками, є забезпечення того, щоб кожна потерпіла жертва зазнала фінансових втрат нижче певної межі. З "маленькими" втратами жертви рідше витрачають час та енергію на звернення до поліції та розслідуванні таких злочинів. Хоча ці правопорушення здійснюються за допомогою комп'ютерних технологій, більшість кримінальних правових системи класифікують їх не як комп'ютерні правопорушення, а як просте шахрайство.

Головною відмінністю між комп'ютерним та традиційним шахрайством є мета шахрайства. Якщо правопорушники намагаються вплинути на особу, злочин зазвичай визнається шахрайством. Якщо правопорушники спрямовані на комп'ютер або системи обробки даних, злочини часто класифікуються як шахрайство, пов'язане з комп'ютером. Найпоширеніші злочинні дії, пов'язані з шахрайством, включають фальсифікацію онлайн-аукціону (правопорушники пропонують неіснуючі товари для продажу та вимагають від покупців сплатити завдаток перед відправленням товару або купують товари та вимагають спершу

реалізувати доставку, без наміру платити) та шахрайство, пов’язане з виманюванням номерів картки або перерахунку коштів, ніби то відсоткову вартість за виграний приз.

Наступним підвидом правопорушень проти авторських прав є підробка. Підробка, з використанням комп'ютерних технологій являє собою маніпулювання цифровими документами [63]. Порушення може бути, наприклад, здійснене шляхом створення документа, який, як видається, походить від надійної установи; маніпулювання електронними зображеннями (наприклад, зображення, що використовуються як докази в суді) або зміна текстових документів . Часто правопорушники надсилають електронні листи, які виглядають як повідомлення від законних фінансових установ, про фінансову заборгованість та погрози арештом чи судовим слідством у випадку, якщо отримувач такого листа не сплатить свою заборгованість.

Також, електронні листи закликають одержувача розкривати та/або підтвердити певну конфіденційну інформацію. Багато потерпілих дотримуються порад та розкривають інформацію, що дозволяє правопорушникам здійснювати онлайн-трансляцію тощо.

У минулому судове переслідування, пов'язане з комп'ютерною підробкою, було рідкістю, оскільки більшість юридичних документів перебували в матеріальному вигляді. На сьогоднішній день цифрові документи відіграють все більш важливу роль і використовуються частіше. Заміна класичних документів цифровими документами підтримується правовими засобами їх використання, наприклад, законодавством, що визнає цифрові підписи. Злочинці завжди намагалися маніпулювати документами. Завдяки цифровим підробкам документи тепер можуть бути скопійовані без втрати якості та легко маніпулювати. Для судових експертів важко довести цифрові маніпуляції, крім випадків, коли технічний захист використовується для захисту документа від фальсифікації.

За підробкою даних слідує їх крадіжка. Термін "крадіжка ідентифікаційних даних" описує кримінальні діяння обманного отримання та використання ідентичності іншої особи [64]. Процес трансформації від промислово розвинених країн до інформаційних технологічних має великий вплив на розвиток правопорушень, пов'язаних з крадіжкою особистих даних.

Взагалі, правопорушення, яке описується як крадіжка особистих даних, складається з трьох різних етапів. На першому етапі правопорушник отримує інформацію, що стосується особистих даних. Цю частину злочину можна, наприклад, виконувати за допомогою шкідливого програмного забезпечення або фішингу. Другий етап характеризується взаємодією з інформацією, що стосується особистості, використання інформації в рамках кримінальних правопорушень. Прикладом є продаж інформації, що стосується особистих даних. Третій етап використання інформації, пов'язаної з особистістю, у зв'язку з кримінальним правопорушенням. Найбільш цінними даними для злочинців є номери паспортів, дати народження, адреси, номери телефонів та паролі.

Окрім усіх вищезазначених правопорушень та злочинів, існує кілька термінів, які використовуються для опису складних шахрайств, які поєднують в собі цілий ряд різних правопорушень. Приклади включають в себе використання Інтернету в терористичних цілях, відмивання грошей за допомогою Інтернету та фішинг. Загальну категорію змішаних злочинів складають: кібертероризм, кібервійни,

На рахунок кібертероризму відомо, що терористи використовують Інтернет для:

- пропаганди;
- збору інформації;
- підготовки реальних нападів;
- публікації навчального матеріалу;
- спілкування;

- фінансування тероризму;
- нападу на критичні інфраструктури [65].

Незважаючи на важливість комплексного підходу, загроза Інтернет-атак на критичну інфраструктуру не повинна виключатися з центральної зони обговорення. Вразливість та зростаюча залежність від інформаційних технологій обумовлюють необхідність включення атак Інтернету на критичну інфраструктуру в стратегії запобігання та боротьби з кібертерроризмом. Проте, незважаючи на більш інтенсивні дослідження, боротьба з кібертерроризмом залишається складною пролемою. Розвиток співпраці держав в цьому питанні полягає в тому, що міжнародні спільноти визнали, що загрози міжнародного тероризму вимагають глобальних рішень.

Здійснювати акти комп'ютерного терору здатні багато організацій екстремістського спрямування: ІГІЛ, різні релігійні рухи та інші незаконні збройні формування. Їх атаки підтримують міжнародну напруженість в ряді регіонів і провокують виникнення глобальних криз в економіці та дипломатичних відносинах між багатьма країнами.

Деякі аспекти кібертероризму можна розглянути на прикладі кібератаки на кіностудію Sony Pictures в грудні 2015 року. Кібератака на Sony пройшла через вихід нового фільму кіностудії під назвою «Інтерв'ю», в якому описувалась змова проти лідера Північної Кореї, що дало підставу припустити про залучення цієї країни в те, що трапилося. Хакери намагалися тиснути на Sony, щоб заблокувати показ фільму. Для цього вони проникли в систему корпорації, зламали електронну пошту керівництва компанії, вкрали п'ять відеофайлів і перетворили на купу мотлоху настільні комп'ютери і сервери у всій корпорації.

Потім вони опублікували вибрані електронні листи, чим дуже сильно збентежили керівництво компанії, і шляхом оприлюднення персональних даних викликали хвилювання серед працівників компанії (деякі з них подали позови до суду). Система компанії була виведена з ладу, що

змусило співробітників працювати з ручкою і папером. Витрати на відновлення системи спочатку оцінювалися від 40 мільйонів доларів до 100 мільйонів.

Після цього Sony не змінила своїх планів випустити фільм в прокат до Різдва. Через кілька тижнів після кібератаки хакери підвищили ставки, погрожуючи реальною терористичною атакою, на зразок 9/11, на кінотеатри, що демонструють фільм і, отже, на глядачів. Чотири великі кіномережі відмовилися показувати фільм. Зрештою, Sony, втративши 80% внутрішнього ринку, зняла фільм з показу.

До великої кількості традиційних методів відмивання грошей додається цілий ряд методів за допомогою Інтернету. Інтернет-фінансові послуги пропонують можливість ведення декількох фінансових операцій у всьому світі.

Виявлення підозрілих операцій з відмиванням грошей ґрунтуються на зобов'язаннях фінансових установ. Регулювання грошових переказів в даний час обмежено і Інтернет пропонує правопорушникам можливість дешевих і неоподаткованих грошових переказів закордон. Сучасні труднощі у дослідженні інтернет-методів боротьби з відмиванням грошей часто випливають із використання віртуальних валют та використання інтернет-казино.

Останнім, але не менш популярним видом кіберзлочинів є так названий «фішинг». вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі персональних даних клієнтів онлайн аукціонів, сервісів з переказу або обміну валюти, інтернет-магазинів. Шахраї використовують усілякі схеми, які найчастіше змушують користувачів самостійно розкрити конфіденційні да наприклад, посилаючи електронні листи із пропозиціями підтвердити реєстрацію облікового запису, що містять посилання на веб-сайт в Інтернеті, зовнішній вигляд якого повністю копіює дизайн відомих ресурсів.

Це один з різновидів соціальної інженерії, заснований на незнанні користувачами основ мережевої безпеки. Зокрема, багато хто не знає простого факту: сервіси не розсилають листів з проханнями повідомити свої облікові дані, пароль та інше.

Для захисту від фішингу виробники основних інтернет-браузерів домовилися про застосування однакових способів інформування користувачів про те, що вони відкрили підозрілий сайт, який може належати шахраям. Нові версії браузерів вже володіють такою можливістю, яка відповідно іменується «антифішинг». За даними компанії

вони шифрують дані на жорсткому диску та вимагають гроші від жертви за їхнє розшифрування.

1.3 Нормативне регулювання міжнародного співробітництва держав у сфері забезпечення кібербезпеки

Нещодавні дискусії на міжнародних форумах, що стосуються кібербезпеки, вказують на "кібер-норми" або "кібер-норми поведінки" як найбільш підходящі засоби для керування поведінкою держав у

кіберпросторі. Вважається, що основні цілі узгодження норм включають підвищену передбачуваність, довіру та стабільність у використанні інформаційно-комунікаційних технологій. Саме норми розглядаються як керівні принципи формування внутрішньої та зовнішньої політики, а також мають визначати основи для формування міжнародних партнерських відносин.

Міжнародним співтовариством було визначено, що відповідно до кіберзлочинів будуть застосовуватись не тільки ті міжнародні угоди, які пов’язанні напряму з кібербезпекою, а й інші міжнародні угоди, які потенційно можуть вплинути на діяльність з кібербезпеки (Статут ООН та Женевські конвенції) та загальноприйняті правила поведінки (звичаєве право). Наприклад, кібернетичні удари, які мають кінетичні ефекти, еквівалентні фізичному застосуванню сили, можуть розглядатися як «збройні напади» за Статутом ООН у тій же мірі, що й фізичне застосування сили. США запропонували таку концепцію в якості керівного принципу [66].

Відповідно до статті 2.4 Статуту ООН всі держави-учасники утримуються в їхніх міжнародних відносинах від загрози силою або її застосуванні як проти територіальної недоторканності або політичної незалежності будь-якої держави. Таким чином, застосування державою збройних сил є злочином проти миру, оголошеним поза законом з боку міжнародного співтовариства, і допускається тільки в тому випадку, коли нація здійснює невід'ємне право на самооборону або було санкціоновано Радою Безпеки ООН. Таким чином, кібератака, наслідки якої можна прирівняти до наслідків застосування сили або погрози силою, або порушення миру, прирівнюється до порушення основних принципів міжнародного права, зазначених в Статуті ООН.

Крім того, право держав на здійснення самооборони або прийняття контрзаходів у відповідь на такі напади буде залежати від їх потенційних наслідків. Міжнародне право також передбачає правила, пов'язані з

застосуванням сили під час збройного конфлікту, які, ймовірно, застосовуються до кібератак, включаючи, наприклад, вимоги про те, що некомбатанти та цивільні установи, такі як лікарні, не будуть навмисно атаковані, і що використання сили обмежується такими критеріями як необхідність та пропорційність.

Перша рекомендація щодо багатостороннього договору боротьби з кіберзлочинністю була опублікована Центром міжнародної безпеки і співробітництва Стенфордського університету у 2000 році. У цьому проекті пропонувалось створити міжнародне агентство з регуляторним органом, аналогічне створенню спеціалізованих установ в інших сферах транснаціональної діяльності, але з великою залежністю від приватної експертизи [67]. США виступили проти такого підходу, але підтримка багатосторонніх домовленостей та заходів зросла [68].

Резолюції Генеральної Асамблеї (ГА), що починаються в 1998 році (GA Res. 53/70), приймаються щороку, відзначаючи різні аспекти та проблеми кібербезпеки, включаючи злочинність, тероризм, захист критичної інфраструктури, спам, напади на кіберінфраструктуру та потреби у розбудові потенціалу. Крім того, конференції, за підтримки ООН, окремими урядами, регіональними організаціями тощо, неодноразово проводились в різних місцях світу, що призвело до активних закликів про посилення міжнародного співробітництва в боротьбі з загрозами кібербезпеки [69]. 6 січня 2006 року Генеральна Асамблея прийняла резолюцію 60/45, в якій, зокрема, закликала Генерального секретаря призначити "групу урядових експертів, яка буде створена у 2009 році на основі справедливого географічного розподілу", до продовжуватимуть вивчати "існуючі та потенційні загрози в галузі інформаційної безпеки та можливі спільні заходи для їх подолання" та "представлять доповідь про результати цього дослідження Генеральній Асамблеї на її шістдесят п'ятій сесії" [70]. Таким чином, 10 липня 2010 року Група урядових експертів, що представляють 15 держав, включаючи

Китай, Індію, Росію та США, представили доповідь, що узагальнила загрози на той час перед інформаційними та комунікаційними технологіями (ІКТ) та рекомендації наступних "подальших кроків щодо розвитку заходів зміцнення довіри та інших заходів, спрямованих на зменшення ризику перешкод на шляху до ІКТ":

- ведення подальшого діалогу між державами для обговорення норм, що стосуються державного використання ІКТ, для зменшення колективного ризику та захисту найважливіших національних та міжнародних інфраструктур;
- впровадження заходів щодо зміцнення довіри, стабільності та зменшення ризику для подолання наслідків використання ІКТ державного характеру, включаючи обмін національними поглядами на використання ІКТ в конфлікті;
- обмін інформацією щодо національного законодавства, національних стратегій та технологій в галузі ІКТ, політики та передового досвіду;
- визначення заходів щодо підтримки розвитку потенціалу в менш розвинутих країнах;
- пошук можливостей розробки загальних понять та визначень, що стосуються резолюції 64/25 Генеральної асамблеї ООН [71].

Цей набір рекомендацій не є важливим кроком до договору про кіберзахист. Тим не менш, цей звіт представляє собою прорив у ситуації «глухого кута», яка склалася внаслідок вимог деяких держав щодо широкомасштабних домовленостей з кібербезпеки, пов'язаних, зокрема, із збройним конфліктом, та протистоянням США міжнародним переговорам щодо кібервійни та інших аспектів кібербезпеки. Готовність США почати дискусії на рахунок поведінки держави, норм, оборонних стратегій, передових практик та створення потенціалу є значним зрушенням. Це, очевидно, випливає з тодішньої готовності адміністрації президента Обами

розглянути міжнародні заходи щодо посилення стримування через міжнародне співробітництво.

Найважливішою багатосторонньою угодою, яка конкретно стосується аспектів кібератак, є Конвенція Ради Європи про кіберзлочинність (Council of Europe Convention on Cybercrime – «CEC») 2001 року. Конвенція являє собою правоохоронний договір, призначений для розробки спільної кримінально-правової політики, спрямованої на визначення, покарання та тим самим стримування злочинів, пов'язаних із кіберзлочинністю. Згідно CEC держави мають прийняти закони, що передбачають кримінальну відповідальність за наступними п'ятьма видами дій проти цілісності кіберсистем: незаконний доступ; нелегальне перехоплення; втручання у дані; втручання у систему; зловживання пристроями [72]. Вона також визначає види поведінки, пов'язані з експлуатацією кіберсистем, включаючи шахрайство, підробку, дитячу порнографію та порушення законів про авторські права [73]. Держави-члени зобов'язані надавати своїм національним правоохоронним органам повноваження розслідувати кримінальну поведінку та співпрацювати з іншими державами-членами у їх виконанні через договори про видачу та MLAT (Договори взаємної правової допомоги) [74]. Держави мають право робити застереження, які звільняють себе від судового переслідування окремих злочинів та утримуватися від співпраці у справах, які вважаються невідповідними їх державній політиці або безпеці [75].

Конвенція про кібербезпеку визначає загальні принципи міжнародного співробітництва. Сторони співробітничають між собою у найширших обсягах відповідно до принципів Конвенції шляхом застосування відповідних міжнародних документів щодо міжнародного співробітництва у кримінальних питаннях, угод, укладених на основі єдиного чи взаємного законодавства, і внутрішньодержавного законодавства, з метою розслідування або переслідування кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними або з

метою збирання доказів у електронній формі, які стосуються кримінальних правопорушень [76]. СЕС визначає та тлумачить принципи екстрадиції та взаємної допомоги.

Принцип екстрадиції застосовується при кримінальному порушенні, пов'язаному з комп'ютерами, за умови, що вони підлягають покаранню позбавлення волі, максимальний строк якого складає щонайменше один рік, або більш суворому покаранню, відповідно до законодавства обох заінтересованих сторін. При чому, якщо у законодавствах держав не сходяться строки позбавлення волі, застосовується той з них, який є мінімальним. Для того, щоб цей принцип діяв максимально ефективно, держави повинні підписувати двосторонні договори про екстрадицію. Однак, у випадку відсутності двостороннього договору можна вважати Конвенцію юридичною основою для екстрадиції відносно будь-якого кримінального правопорушення, на яке міститься посилання в Конвенції [77]. Якщо сторона, до якої надійшов запит на екстрадицію відмовила в цьому на підставі громадянства особи, стосовно якої надходить запит про екстрадицію, або тому, що сторона, яку запитують, вважає, що вона має юрисдикцію стосовно такого правопорушення, сторона, яку запитують, на запит сторони, яка запитує, надсилає справу своїм компетентним органам з метою переслідування правопорушення, і належним чином повідомляє його результат стороні, яка запитує. Такі органи приймають свої рішення і проводять свої розслідування і переслідування таким же чином, як і у випадку будь-якого іншого правопорушення подібної природи відповідно до законодавства такої сторони [78].

Сторони надають одна іншій взаємну допомогу у найширшому обсязі з метою розслідування або переслідування кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів у електронній формі щодо кримінального правопорушення [79]. За надзвичайних умов держава може зробити запит про взаємну допомогу або повідомлення, пов'язане з допомогою за допомогою термінових засобів

інформації (факс, електронна пошта). Засіб комунікації має бути належним до забезпечення форм безпеки та підтвердження достовірності, можуть використовуватись кодування, де це необхідно [80]. Як і у випадку з принципом екстрадиції, якщо між сторонами немає договору про взаємну допомогу, Конвенція може служити підставою до надання допомоги.

СЕС також визначає конкретні принципи взаємної допомоги. Серед них принцип термінового збереження комп'ютерних даних, які зберігаються (Сторона може запитати іншу Сторону видати ордер чи іншим чином провести термінове збереження комп'ютерних даних, які зберігаються за допомогою комп'ютерної системи, яка знаходиться на території такої іншої Сторони, і відносно якої Сторона, яка запитує, має намір надіслати запит про взаємну допомогу щодо обшуку чи подібного доступу, арешту чи подібних дій або розголошення таких даних [81.) та принцип термінового розкриття збережених даних про рух інформації (Якщо стає відомо, що постачальник послуг в іншій державі був залучений до передачі такої інформації, Сторона, яку запитують, терміново повідомляє Стороні, яка запитує, обсяг інформації про рух даних, достатній для ідентифікації такого постачальника послуг і шляху передачі такої інформації [82]).

До Конвенції може приєднатись будь-яка держава, яка не є членом Ради Європи на запрошення Комітету Міністрів Ради Європи. Таке рішення ухвалюється більшістю та одностайним голосуванням представників Договірних Держав, які мають право брати участь у засіданнях Комітету Міністрів [83].

Аналізуючи Конвенцію можна дійти висновку, що її метою є заохочення укладення або доповнення державами двосторонніх, багатосторонніх договорів, зокрема мова йде про Європейську конвенцію про екстрадицію, відкритої для підписання у Парижі 13 грудня 1957 року, Європейську конвенцію про взаємну допомогу у кримінальних справах, відкриту для підписання у Страсбурзі 20 квітня 1959 року та

Додатковий протокол до Європейської конвенції про взаємну допомогу у кримінальних справах, відкритого для підписання у Страсбурзі 17 березня 1978 року. Якщо держави підписують двосторонню або багатосторонню угоду, то вона вважається такою, яка має примат над Конвенцією, але така угода не має суперечити її цілям та принципам.

У випадку виникнення спорів, щодо тлумачення або застосування норм СЕС, сторони можуть звернутись до Європейського комітету з проблем злочинності, до арбітражного суду, рішення якого є обов'язковим для виконання сторонами, або до міжнародного суду, за домовленістю сторін [84].

Потенціал СЕС щодо забезпечення кібербезпеки обмежується тим фактом, що його правоохоронна система діє у багатьох випадках у такий часовий діапазон, який занадто довгий, щоб захистити жертви кібернетичної атаки від шкоди. Натомість Конвенція розглядає види злочинів і процедуру реагування на кібератаки, інші злочинні дії, які уже сталися. І не розглядає як запобігти кіберзлочинам. Більше того, у договорі немає механізму встановлення або перегляду практик або стандартів кіберсистеми, які могли б загалом підвищити рівень безпеки. Тому, потенціал СЕС у забезпеченні загальної прихильності зменшується завдяки відображенню у ній зусиль, спрямованих на покарання поведінки на основі обмежень вмісту (таких як шахрайство та дитяча порнографія), а не на намаганні покарати за кіберзлочини, які потенційно можуть завдати шкоди самій кіберінфраструктурі.

Ще однією міжнародною угодою, яка має важливе значення є Довгостроковий план дій з інформаційної безпеки в рамках Шанхайської організації співробітництва, прийнятий на сьомій нараді глав урядів (Китай, Росія, Казахстан, Киргизька Республіка, Таджикистан, Узбекистан), яка відбулась 16 серпня 2007 року у Киргизькій Республіці.

багатостороннє об'єднання, діяльність якого спрямована на забезпечення безпеки і підтримання

стабільності на великому Євро-Азіатському просторі, на спільне протистояння новим викликам і загрозам, зміцнення торговельно-економічного та культурно-гуманітарного співробітництва. В рамках ШОС питання інформаційної безпеки вже давно стоїть на порядку денному. В Довгостроковому плані дій з інформаційної безпеки прописані необхідні заходи для протидії використання інформаційних технологій в терористичних цілях, забезпечення безпечного, стабільного функціонування та інтернаціоналізації управління глобальною мережею Інтернет. У 2009 році між членами організації було підписано Міжурядову угоду про основні напрямки взаємодії держав з протидії кіберзагрозам. Принципи, зазначені в Угоді ШОС узгоджуються з правоохоронним підходом СЕС, оскільки вони стосуються забезпечення кіберсистем від нападу, але вони суттєво відрізняються від Конвенції Ради Безпеки, підкреслюючи намір Членами забезпечити національний контроль над кіберсистемами та змістом [85]. Угода підписана шістьма державами-членами, і, як СЕС, вона може бути схвалена іншими державами.

Багато інших міжнародних організацій розглядають питання кібербезпеки. Така тенденція у деякій мірі ускладнює процес уніфікації норм міжнародного права в сфері забезпечення кібербезпеки. Про це попереджає Центр стратегічних і міжнародних досліджень (The Center for Strategic and International Studies, CSIS), який являє собою аналітичний інститут в США. На засадах Центру створюється Комісія (CERT) з кібербезпеки для надання консультацій президентам США щодо створення та підтримки комплексної стратегії кібербезпеки. У Звіті політики кіберпростору за 2009 рік Комісія зазначає, що деякі з зусиль міжнародних організацій можуть призвести до суперечливості їх норм та стандартів. Прикладом є одночасний розвиток стандартів криміналістики Міжнародного союзу електрозв'язку (ITU) з одного боку, та Міжнародної організації стандартів (ISO) з другого боку [86]. Доповідь Рахункової палати США (GAO) від липня 2010 року рішуче підтримує ці висновки,

зазначаючи: "Величезна кількість міжнародних організацій, які беруть участь у реагуванні на інциденти, також можуть перешкоджати міжнародній координації" [87]. Це створює великі труднощі співпраці держав та міжнародних організацій на шляху до створення єдиного міжнародного документу, який би регулював відносини у сфері кібербезпеки та передбачав загрози кібератак. Можна зробити висновок, що координуючі органи не мають продемонстрованої спроможності "надати законну глобальну службу інформаційної безпеки для всіх учасників. . . " [87].

Міжнародною організацією, яка найбільше пов’язана з кіберпростором є Міжнародний союз електрозв’язку (ITU). ITU прийняв кілька рішень, пов'язаних з кібербезпекою:

- Резолюція Повноважної ради ITU 130 (Rev. Guadalajara, 2010 р.) "Про збільшення ролі ITU у зміцненні довіри та безпеки при використанні інформаційних та комунікаційних технологій";
- Повноважна конференція ITU 149 (Анталія, 2006 р.) "Дослідження визначень та термінології, що стосуються зміцнення довіри та безпеки при використанні інформаційних та комунікаційних технологій";
- Резолюція 45 (Доха, 2006 р.) Всесвітньої конференції з розвитку електрозв'язку (WTDC) про механізми посилення співпраці у сфері кібербезпеки, включаючи боротьбу зі спамом, та доповідь з наради щодо механізмів співробітництва з кібербезпеки та боротьби зі спамом (31 серпня - 1 вересня 2006 р.);
- Резолюція 50 (Йоганнесбург, 2008 р.) Всесвітньої асамблеї стандартизації електрозв'язку (WTSA) з питань кібербезпеки;
- Резолюція 52 (Йоганнесбург, 2008 р.) Всесвітньої асамблеї стандартизації електрозв'язку (WTSA) з питань протидії спаму та боротьби зі спамом;

- Резолюція 58 (Йоганнесбург, 2008 р.) Всесвітньої асамблеї стандартизації електрозв'язку (WTSA) про заохочення створення національних команд з реагування на інциденти, особливо для країн, що розвиваються.

Варто також зазначити, що інститут співробітництва держав у сфері забезпечення кібербезпеки є міжгалузевим, адже регулюється джерелами міжнародного права у різних сферах.

Як висновок, можна сказати, що в даний час не існує всеосяжної міжнародно-правової бази щодо кібербезпеки. Міжнародні зусилля концентруються на вузькій сфері питань, в першу чергу стосуються конфіденційності даних і прав людини, замість реалізації більш широких заходів, спрямованих на встановлення і диференціацію різних рівнів кіберагресії і кодифікацію міжнародних підходів до вирішення цієї проблеми. Ці недоліки можуть бути частково обумовлені самою природою хакерської атаки, яка кидає виклик концептуальним категоріям, які ми досі використовуємо для недопущення хаосу і підтримки порядку в нашому суспільстві і в нашому житті. Без всеосяжного міжнародного визначення типів кіберагресій, країни будуть продовжувати стикатися з труднощами в оцінці законності своєї реакції на такі атаки. На довершення всього, не існує міжнародних органів, уповноважених розслідувати і переслідувати в судовому порядку випадки кіберагресії, які при виробленні відповіді на хакерські атаки були б не обмежені принципом територіальної юрисдикції, прийнятим в правовій системі країни нападу. Протидії кіберагресії заважає той факт, що міжнародне право не визнає обов'язок надавати допомогу іншим державам в розслідуванні випадків подібного роду за відсутності відповідної домовленості між сторонами.

РОЗДІЛ 2 ОРГАНІЗАЦІЙНО-ПРАВОВИЙ МЕХАНІЗМ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА ДЕРЖАВ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

2.1 Співробітництво держав на світовому рівні

Ряд міжнародних організацій постійно працюють, щоб аналізувати останні події в галузі кіберзлочинності та створили робочі групи для розробки стратегій боротьби з цими злочинами (рис 2.1).

Рис.2.1. Всесвітні міжнародні організації

Так, у 1997 році група восьми (G8) створила "Підкомітет з боротьби проти злочинів у сфері інформаційних технологій", присвячений боротьбі з кіберзлочинністю. Під час зустрічі у Вашингтоні, округ Колумбія, міністри юстиції та внутрішніх справ "Великої вісімки" прийняли Основні принципи та план дій для боротьби з комп'ютерними злочинами [88]. Зокрема, глави «великої вісімки» виокремили такі принципи:

- не повинно бути безпечних притулків для тих, хто зловживає інформаційними технологіями;
- розслідування та кримінальне переслідування міжнародних злочинів у галузі інформаційних технологій повинні координуватися між усіма зацікавленими державами незалежно від того, які держави зазнали шкоди;
- співробітники правоохоронних органів повинні бути навчені та обладнані належними засобами для вирішення проблем кіберзлочинів.

У 1999 році "Велика вісімка" визначила свої плани щодо боротьби проти кіберзлочинів на Конференції міністрів з питань боротьби з транснаціональними організованими злочинами в Москві [89]. Вони висловили свою стурбованість щодо злочинів (таких як дитяча порнографія), а також відстеження транзакції та транскордонний доступ до збережених даних. У їхньому комюніке міститься ряд принципів боротьби з кіберзлочинністю, які сьогодні знаходяться в ряді міжнародних стратегій.

Одним з практичних досягнень роботи експертних груп була розробка міжнародної 24/7-мережі контактів що вимагає від країн-учасниць встановлення контактних пунктів для транснаціональних розслідувань, які доступні 24 години на добу, 7 днів на тиждень.

У 2001 році G8 обговорила процедурні механізми боротьби з кіберзлочинністю на семінарі, що відбувся в Токіо [90], присвячений тому, чи повинні виконуватися зобов'язання з утримання даних. У 2004 році міністри юстиції та внутрішніх справ "Великої вісімки" видали комюніке, в якому вони розглянули необхідність створення глобальних можливостей у боротьбі проти злочинного використання Інтернету. Під час зустрічі 2006 року в Москві міністри юстиції та внутрішніх справ "Великої вісімки" обговорили питання, що стосуються боротьби з кіберзлочинністю, та питань кіберпростору, і особливо необхідність вдосконалення ефективних контрзаходів [91].

Під час зустрічі міністрів юстиції та міністрів внутрішніх справ країн Великої вісімки у Мюнхені 2007 року терористичне використання Інтернету було додатково обговорено, і учасники погодились визнати злочинним використання Інтернету терористичними групами [92]. Ця угода не включала конкретні дії, які державам слід криміналізувати.

На засіданні міністрів юстиції та внутрішніх справ 2009 року у Римі було обговорено декілька питань, пов'язаних із кіберзлочинністю. В остаточній заяві зазначається, що, на думку Великої вісімки, блокування веб-сайтів дитячої порнографії на основі чорних списків, оновлених та

розповсюджених міжнародними організаціями, повинно виконуватися [93]. Що стосується кіберзлочинів в цілому, то остаточна декларація підкреслює зростаючу загрозу та вказує на що необхідна тісніша співпраця між постачальниками послуг та правоохоронними органами, а також необхідно зміцнювати існуючі форми співпраці, такі як Контактні органи з питань високої технології 24 години на добу (G8) [94].

Кіберзлочинність та кібербезпека стали питаннями, які обговорювалися на наступних форумах G8, де делегації обговорювали теми, пов'язані з Інтернетом. Але, хоча темы кіберзлочинності приділялася велика увага, остаточні декларації, на відміну від попередніх років, не містили конкретних рекомендацій. Група "Великої двадцятки" погодилася лише на загальні принципи, такі як важливість безпеки та захист від злочинів, що є основою міцного та процвітаючого Інтернету.

Організація Об'єднаних Націй також виробила кілька підходів для вирішення проблеми кіберзлочинів. Хоча спочатку діяльність ООН обмежувалася загальними керівними принципами, організація останнім часом інтенсивніше займалася проблемами та юридичними відповідями.

Конвенція ООН про права дитини 1989 року містить норми, спрямовані на захист дітей. Стаття 34 закликає держави-члени запобігати експлуатаційному використанню дітей у порнографічних виставах. Однак, Конвенція не визначає дитячу порнографію, а також не містить положень, що узгоджують криміналізацію дитячої порнографії в Інтернеті [95].

Резолюція Генеральної Асамблеї ООН 45/121 прийнята на восьмому засіданні ООН з попередження злочинності та поводження з правопорушниками (що відбулась в Гавані, Куба, 27 серпня - 7 вересня 1990 року) стосується комп'ютерної злочинності. На підставі своєї Резолюції 45/121 (1990) ООН опублікувала в 1994 році посібник із запобігання та контролю за злочинністю, пов'язаною з комп'ютером [96].

У 2000 році Генеральною Асамблеєю ООН був прийнятий Факультативний протокол до Конвенції про права дитини з продажу дітей,

дитячої проституції та дитячої порнографії, який не лише висвітлює проблему дитячої порнографії в цілому, але і прямо вказує на роль Інтернету у поширенні такого матеріалу. Стаття 3 Факультативного протоколу зобов'язує сторони криміналізувати дії, пов'язані з дитячою порнографією.

Під час десятого Конгресу Організації Об'єднаних Націй з попередження злочинності та поводження з правопорушників, який відбувся у Відні у 2000 році обговорювався вплив комп'ютерних злочинів. Дебати зосереджувалися, зокрема, на категоріях злочинів та транснаціональних розслідуваннях, а також юридичних відповідях на це явище [97]. Висновки семінару містять основні елементи дискусії, яка все ще триває: від держав вимагається криміналізація кіберзлочинів, законодавство має включати процедурні інструменти, а партнерство між державним та приватним секторами повинно бути посилено. Крім того, було наголошено на важливості розвитку потенціалу - питання, яке було знову піднято в наступні роки. Віденська декларація закликала Комісію з попередження злочинності та кримінального правосуддя зайнятися роботою в таких напрямках: розробка рекомендацій щодо запобігання та контролю злочинів, пов'язаних із комп'ютером; працювати над покращенням здатності запобігати, досліджувати та переслідувати інформаційні та комп'ютерні злочини.

У тому ж році Генеральна Асамблея ООН прийняла резолюцію про боротьбу зі злочинним використанням інформаційних технологій, яка демонструє деяку схожість з "Планом дій десяти пунктів" Великої вісімки 1997 року [98]. У своїй резолюції Генеральна Асамблея визначила низку заходів, спрямованих на недопущення злочинного використання інформаційних технологій, в тому числі: обов’язок держав робити усе, щоб їхні закони та практика унеможливлювали існування безпечних притулків для тих, хто зловживає інформаційними технологіями; співробітництво в галузі правоохоронної діяльності при розслідуванні та переслідуванні

міжнародних справ про злочинне використання інформаційних технологій має узгоджуватися між усіма зацікавленими державами; співробітники правоохоронних органів повинні бути навчені та обладнані для подолання злочинного використання інформаційних технологій. Резолюція 55/63 пропонує державам вжити необхідних заходів для боротьби з кіберзлочинністю на регіональному та міжнародному рівнях. Це включає розробку національного законодавства з метою усунення "безпечних" місць для злочинного використання технологій, поліпшення спроможності правоохоронних органів співпрацювати через кордони при розслідуванні та кримінальному переслідуванні міжнародних справ про злочинне використання інформаційних технологій злочинним шляхом, покращення обміну інформацією, посилення безпеки даних і комп'ютерних систем, навчання правоохоронних органів для вирішення конкретних проблем, пов'язаних з кіберзлочинністю, створення режиму взаємодопомоги та підвищення обізнаності громадськості про загрозу кіберзлочину.

56/121 [99]. У резолюції згадуються існуючі міжнародні підходи у боротьбі з кіберзлочинністю та висвітлюються різні рішення.

Відзначаючи роботу міжнародних та регіональних організацій у боротьбі з високотехнологічними злочинами, включаючи роботу Ради Європи щодо розробки Конвенції про кіберзлочинність, а також роботу цих організацій у поширенні діалогу між урядом та приватним сектором щодо безпеки та довіри в кіберпросторі, резолюція:

- пропонує державам-членам при розробці національного законодавства, політики та практики боротьби з злочинністю використання інформаційних технологій, враховувати, у відповідних випадках, роботу та досягнення Комісії з попередження злочинності і кримінального правосуддя та інших питань міжнародні та регіональні організації;

- приймає до уваги цінність заходів, викладених в її резолюції 55/63, і знову пропонує державам-членам враховувати їх в їх зусиллях в боротьбі зі злочинним використанням інформаційних технологій;
- постановляє відкласти розгляд цього питання, в очікуванні роботи, передбаченої Планом дій проти високотехнологічних та комп'ютерних злочинів Комісії з попередження злочинності і кримінального правосуддя.

Резолюції 57/239 і 58/199 є двома основними резолюціями Генеральної Асамблеї ООН, що стосуються кібербезпеки. Не вдаючись до деталей щодо кіберзлочинності, вони нагадують резолюції 55/06 та 56/121. Обидві резолюції, крім того, підкреслюють необхідність міжнародного співробітництва в боротьбі з кіберзлочинністю, визнаючи, що прогалини доступу держав та використання інформаційних технологій можуть послабити ефективність міжнародного співробітництва у боротьбі з злочинністю використання інформаційних технологій.

Кіберзлочинність обговорювалася під час одинадцятого Конгресу ООН з попередження злочинності і кримінального правосуддя в Бангкоку, Таїланд, в 2005 році. У рамках підготовчих засідань до початку з'їзду деякі країни-члени, такі як Єгипет, закликали до створення нової конвенції ООН проти кіберзлочинності, а регіональна підготовча нарада Західної Азії вимагала переговорів щодо таких Конвенція [100]. Можливість ведення переговорів про конвенцію була включена в керівництво по обговоренню для одинадцятого Конгресу ООН зі злочинності. Однак, держави-члени наразі не можуть вирішити питання щодо ініціювання гармонізації законодавства. Отже, Бангкокська декларація стосується лише існуючих підходів.

Тема кіберзлочинів також обговорювалася на дванадцятому Конгресі ООН з попередження злочинності та кримінального правосуддя, що відбулася в Бразилії в 2010 році [101]. У рамках чотирьох регіональних підготовчих нарад на з'їзді для Латинської Америки та Карибського басейну, країн Азії, Тихого океану та Африки, країни закликали до

розробки міжнародної конвенції про кіберзлочинність. На самих конгресах держави-члени зробили значний крок до більш активного залучення Організації Об'єднаних Націй до дебатів з питань комп'ютерної злочинності та кіберзлочинів. Той факт, що делегації обговорили ці теми протягом двох днів і що організували додаткові заходи, підкреслює важливість теми, яка була інтенсивніше обговорена, ніж під час минулих конгресів [102].

Обговорення зосереджувалися на двох основних питаннях: як можна досягти гармонізації правових норм та як підтримувати країни, що розвиваються, у боротьбі з кіберзлочинністю? Перше питання особливо актуальне, якщо ООН розробляє комплексні правові стандарти або пропонує, щоб держави-члени добримувались Конвенції Ради Європи про кіберзлочинність. Після інтенсивних дебатів, де зокрема обговорювалася обмеженість охоплення Конвенцією про кіберзлочинність, держави-члени вирішили не пропонувати ратифікувати Конвенцію про кіберзлочинність, а зміцнювати роль ООН у двох важливих напрямках:

- вимога до Управління Організації Об'єднаних Націй з наркотиків та злочинності, у відповідь на запит, у співпраці з державами-членами, відповідними міжнародними організаціями та приватним сектором надавати технічну допомогу та підготовку держав для вдосконалення національного законодавства та розбудови спроможності національних органів влади з метою боротьби з кіберзлочинністю, включаючи запобігання, виявлення, розслідування та кримінальне переслідування такого злочину у всіх його формах та підвищення безпеки комп'ютерних мереж

- вимога до Комісії з попередження злочинності та кримінального правосуддя розглянути питання про скликання відкритої міжурядової експертної групи для проведення всебічного вивчення проблеми кіберзлочинів та відповідей на неї державами-членами, міжнародним співтовариством та приватним сектором, включаючи обмін інформацію

про національне законодавство, найкращі практики, технічну допомогу та міжнародне співробітництво, з метою вивчення можливостей для зміцнення існуючих та надання нових національних та міжнародних юридичних чи інших заходів проти кіберзлочинів.

У березні 2010 року Генеральна Асамблея ООН прийняла нову резолюцію в рамках ініціативи "Створення глобальної культури кібербезпеки" [103]. Резолюція 64/211 посилається на дві основні резолюції про кіберзлочинність [104], а також на дві головні резолюції з кібербезпеки [105]. Добровільний інструмент самооцінки національних зусиль із захисту критично важливих інформаційних інфраструктур, що міститься в додатку до резолюції, закликає країни переглянути та оновити юридичні повноваження (у тому числі ті, що стосуються кіберзлочинності, конфіденційності, захисту даних, комерційного права, цифрових підписів та шифрування), які можуть бути застарілими або застарілими внаслідок швидкого засвоєння та залежності від нових інформаційних та комунікаційних технологій. Резолюції також закликає держави використовувати регіональні міжнародні конвенції, механізми та прецеденти у цих оглядах.

Після рішення держав-членів запропонувати Управління ООН з наркотиків і злочинності (УНЗ ООН) створити міжурядову робочу групу, перше засідання групи відбулося у Відні у січні 2011 року [106]. Група експертів включала представників держав-членів, міжурядових та міжнародних організацій, спеціалізованих установ, приватних організаційних секторів та академічного кола. Під час зустрічі члени експертної групи обговорили проект структури для комплексного дослідження, що аналізує проблему кіберзлочинів, а також можливі юридичні відповіді [107]. Що стосується юридичної відповіді, то декілька учасників підкреслили корисність існуючих міжнародно-правових документів, включаючи Конвенцію Організації Об'єднаних Націй проти транснаціональної організованої злочинності (UNTOC) та Конвенцію Ради

Європи про кіберзлочинність, а також бажаність розробки глобального правового інструменту, спрямованого на вирішення конкретної проблеми кіберзлочинності. Результатом роботи групи став величезний рапорт під назвою «Всебічне вивчення кіберзлочинності» 2013 року, в якому зазначається природа кіберзлочинів, юридичні виклики та рішення забезпечення кібербезпеки у світі. Зокрема, йдеться про криміналізацію кіберзлочинів, постійне адаптування національних систем права під норми міжнародного права у сфері забезпечення кібербезпеки у відповідності до появи нових видів злочинної діяльності в даній сфері, введення поняття та процедури електронних доказів та електронного розслідування, посилення співпраці держав задля забезпечення кібербезпеки як на регіональному, так і на глобальному рівнях та нові стратегії, які повинні застосовуватися державами для забезпечення кібербезпеки не тільки для покарання злочинців, а і для запобігання таким злочинам.

Наступна всесвітня міжнародна організація, яка поширює співпрацю у сфері забезпечення кібербезпеки це Міжнародний союз електрозв’язку (ITU). Це спеціалізоване агентство в рамках Організації Об'єднаних Націй, що відіграє провідну роль у стандартизації та розвитку телекомунікацій, а також у питаннях кібербезпеки.

Серед інших видів діяльності, ITU була головною організацією Всесвітнього саміту з питань інформаційного суспільства (ВСІС), який проходив у два етапи в Женеві, Швейцарії (2003 рік) та Тунісі (2005 рік). Уряди, політики та експерти з усього світу поділилися думками та досвідом щодо найкращого вирішення проблем, пов'язаних із розвитком глобального інформаційного суспільства, включаючи розробку сумісних стандартів та законів. Висновки Саміту містяться в Женевській декларації принципів, Женевському плані дій; Туніських зобов'язань та Туніському порядку денному для інформаційного суспільства [108].

Женевський план дій підкреслює важливість заходів боротьби з кіберзлочинністю: уряди у співпраці з приватним сектором повинні

запобігати, виявляти та реагувати на кіберзлочинність та неправомірне використання інформаційних технологій шляхом: розробки керівних принципів, що враховують зусилля, які здійснюються в цих сферах; розглядаючи законодавство, яке дозволяє ефективно розслідувати і переслідувати зловживання; заохочення ефективних зусиль взаємодопомоги; зміцнення інституційної підтримки на міжнародному рівні для попередження, виявлення та відновлення таких інцидентів; заохочення освіти та підвищення обізнаності [109].

Кіберзлочинність також розглядалася на другому етапі ВСІС в Тунісі в 2005 році. Туніський порядок денний для інформаційного суспільства підкреслює необхідність міжнародного співробітництва у боротьбі з кіберзлочинністю та посилається на існуючі законодавчі підходи, такі як резолюції Генеральної Асамблеї ООН та Конвенцію Ради Європи про кіберзлочинність: уряди держав-учасниць підкреслюють важливість кримінального переслідування кіберзлочинів, включаючи кіберзлочинність, що здійснюється в одній державі, але мають наслідки в інших державах. Вони далі підкреслюють необхідність ефективних інструментів та дій на національному та міжнародному рівнях для сприяння міжнародному співробітництву серед, зокрема, правоохоронних органів з питань кіберзлочинності. Учасники закликають уряди у співпраці з іншими зацікавленими сторонами розробляти необхідні законодавчі акти для розслідування та кримінального переслідування кіберзлочинності, відзначаючи існуючі рамки, наприклад резолюції Генеральної Асамблеї ООН 55/63 та 56/121 "Про боротьбу з злочинним використанням інформаційних технологій" та регіональними ініціативами в тому числі, але не обмежуючись, Конвенцію Ради Європи про кіберзлочинність [110].

Як результат ВСІС, ITU був призначений єдиним посередником, спрямованим на зміцнення довіри та безпеки використання інформаційних та комунікаційних технологій [111]. На другій зустрічі з питань сприяння ВСІС у 2007 році Генеральний секретар ITU підкреслив важливість

міжнародного співробітництва у боротьбі з кіберзлочинністю та оголосив про запуск Глобальної програми з кібербезпеки. Глобальна програма кібербезпеки побудована на п'яти стратегічних стовпах, включаючи розробку стратегій вдосконалення законодавства для забезпечення кібербезпеки та складається з семи основних завдань:

1. Розробити стратегії створення глобального, сумісного з існуючими національними та регіональними законодавчими документами, типового закону про кіберзлочинність.

2. Створення відповідних національних і регіональних організаційних структур та політики щодо кіберзлочинів.

3. Розробка стратегії встановлення загальноприйнятих мінімальних критеріїв безпеки та схем акредитації для програмних застосувань та систем.

4. Розробка стратегій створення глобальної системи спостереження, попередження та реагування на інциденти для забезпечення транскордонної координації між новими та існуючими ініціативами.

5. Розробка стратегій створення та затвердження загальної та універсальної системи цифрової ідентичності та необхідних організаційних структур для забезпечення визнання цифрових повноважень для фізичних осіб через географічні кордони.

6. Розробка глобальної стратегії, спрямованої на сприяння формуванню людського та організаційного потенціалу з метою покращення знань та ноу-хау у всіх секторах та у всіх вищезгаданих сферах.

7. Консультації щодо потенційної основи глобальної стратегії зацікавлених сторін для міжнародного співробітництва, діалогу та координації у всіх вищезгаданих сферах.

Для аналізу та розробки заходів та стратегій щодо Глобальної програми з кібербезпеки Генеральний секретар ITU створив експертну групу високого рівня (HLEG), яка об'єднала представників держав-членів,

промисловості та наукової галузі. У 2008 році група експертів завершила переговори та опублікувала «Глобальну стратегічну доповідь» [112]. На додаток до огляду різних регіональних та міжнародних підходів у боротьбі з кіберзлочинністю, в доповіді також зазначаються правові заходи стосовно кіберзлочинів [113] Також наведено огляд норм кримінального права, процедурних документів, нормативних актів, що регулюють відповідальність постачальників послуг Інтернету та гарантії захисту основних прав користувачів Інтернету.

Під егідою Глобальної програми з кібербезпеки ITU працює над наданням країнам допомоги у здійсненні гармонізованої діяльності в галузі кібербезпеки на національному, регіональному та міжнародному рівнях. Мандат ITU щодо розбудови спроможності було підкреслено Резолюцією 130 Повноважної конференції ITU в Гвадалахарі, 2010 р.. На підставі цієї резолюції ITU має повноваження надавати державам-членам, зокрема, країнам, що розвиваються, допомогу у виробленні відповідних та дієвих правових заходів, що стосуються захисту від кіберзлочинців. Це включає в себе заходи з нарощування потенціалу у розробці національних стратегій, законодавчих та виконавчих заходів, організаційних структур (наприклад, спостереження, попередження та реагування на інциденти) серед інших областей. Разом із партнерами з державного та приватного секторів ITU розробив інструменти кібербезпеки для надання державам-членам допомоги у підвищенні національної обізнаності, проведення національного аналізу кібербезпеки, перегляду законодавства та розширення можливостей спостереження, попередження та реагування на інциденти.

Ще однією організацією, яка має вагому роль у міжнародно-правовому регулюванні співробітництва держав у забезпеченні кібербезпеки є Інтерпол. Інтерпол взяв на себе зобов'язання щодо глобальної боротьби з кіберзлочинністю.

Більшість кіберзлочинів носять транснаціональний характер, тому Інтерпол є першочерговим партнером для будь-якого правоохоронного органу, який намагається розслідувати ці злочини на кооперативному рівні. Працюючи з приватною промисловістю, Інтерпол може забезпечити правоохоронну діяльність на місцевому рівні з цілеспрямованим кіберінтелектом, отриманим шляхом об'єднання даних у глобальному масштабі.

Основними ініціативами Інтерполу у сфері кіберзлочинів є:

- оперативна і слідча підтримка;
- кібер-інтелект і аналіз;
- цифрова криміналістика
- інновації та дослідження;
- нарощування потенціалу.

Інтерпол прагне бути глобальним координаційним органом для виявлення та попередження цифрових злочинів через Глобальний комплекс інновацій INTERPOL (IGCI) у Сінгапурі. Цей передовий об'єкт дослідження та розробки, який відк

-

консолідація зусиль правоохоронних органів різних країн у боротьбі з кіберзлочинністю. Робота центру сконцентрована на чотирьох основних напрямках: оперативна підтримка і сприяння розслідуванням, інновації, дослідження і комп'ютерна безпека, підготовка поліцейських кадрів, міжнародне партнерство і розвиток. Інтерпол має унікальну позицію, спрямовану на поглиблення боротьби з кіберзлочинністю у глобальному масштабі, шляхом активного вивчення нових злочинів, новітніх методів навчання та розробки інноваційних інструментів поліцейської діяльності.

Діяльність Організації економічного співробітництва і розвитку, розпочата за тематикою комп’ютерної злочинності ще 1983 року,

спрямовується на проведені досліджень, пов'язаних із можливістю гармонізації кримінального законодавства щодо комп'ютерних злочинів. У 1992 році радою ОЕСР було прийнято «Керівні принципи з інформаційної безпеки». У 2002 році нова версія принципів «Керівні принципи ОЕСР із забезпечення безпеки інформаційних систем і мереж: до культури безпеки» була рекомендована Радою ОЕСР. Керівними принципами є:

1) Обізнаність. Учасники повинні усвідомлювати необхідність забезпечення безпеки інформаційних систем та мереж і що вони можуть зробити для підвищення безпеки.

2) Відповідальність. Всі учасники відповідають за безпеку інформаційних систем та мереж.

3) Відповідь на злочини або правопорушення. Учасники повинні діяти своєчасно та кооперацийно, щоб запобігти, виявляти та реагувати на інциденти в сфері безпеки.

4) Етика. Учасники повинні поважати законні інтереси інших.

5) Демократія. Безпека інформаційних систем та мереж повинна бути сумісною з основними цінностями демократичного суспільства.

6) Оцінка ризику. Учасники повинні проводити оцінку ризику.

7) Розробка та реалізація безпеки. Учасники повинні включати безпеку як важливий елемент інформаційних систем та мереж.

8) Управління безпекою. Учасники повинні прийняти комплексний підхід до управління безпекою.

9) Переоцінка. Учасники повинні переглянути та переоцінити безпеку інформаційних систем та мереж та внести відповідні зміни в політику, практику, заходи та процедури безпеки. Також на зустрічах ОЕСР доповіді були присвячені темам боротьби зі спамом (2005 рік), та законодавчих рішень держав щодо проблеми кібертероризму (2007 рік).

2.2. Співробітництво в рамках регіональних об`єднань

На додаток до міжнародних організацій, які в усьому світі активно співпрацюють у сфері забезпечення кібербезпеки, ряд міжнародних організацій в окремих регіонах також зосереджені на діяльності вирішення питань, пов'язаних з кіберзлочинністю.

Рис.2.2. Регіональні міжнародні організації

Рада Європи відіграє активну роль у вирішенні завдань кіберзлочинності. У 1976 році Рада Європи підкреслила міжнародний характер злочинів, пов'язаних із комп'ютерами, і обговорила цю тему на конференції, присвяченій аспектам економічних злочинів. Ця тема з тих пір залишається на порядку денному.У 1985 році Рада Європи призначила Комітет експертів для обговорення правових аспектів комп'ютерних злочинів [114]. У 1989 році Європейським комітетом з проблем злочинності було прийнято "Експертний звіт про комп'ютерну злочинність", що аналізує основні кримінально-правові норми, необхідні для боротьби з новими формами електронних злочинів, включаючи комп'ютерне шахрайство та підробку. Комітет міністрів у 1989 р. прийняв рекомендацію [115], в якій особливо висвітлено міжнародний характер комп'ютерної злочинності:

«Комітет міністрів відповідно до положень статті 15.b Статуту Ради Європи, вважаючи, що метою Ради Європи є досягнення більшої єдності між її членами; Визнаючи важливість адекватного та швидкого реагування

на нові юридичні виклики, пов'язані з комп'ютерною злочинністю; Враховуючи те, що злочини, пов'язані з комп'ютерами, часто мають транскордонний характер; Усвідомлюючи необхідність подальшої гармонізації законодавства, практики та удосконалення міжнародного правового співробітництва, рекомендує урядам держав-членів:

1. Враховувати при перегляді свого законодавства чи ініціювання нового законодавства доповідь про злочини пов'язані з комп'ютерами, розробленим Європейським комітетом з проблем злочинності, і, зокрема, керівних принципів для національних законодавчих органів;

2. Доповісти Генеральному секретарю Ради Європи протягом 1993 року про будь-які події в їх законодавстві, судову практику та досвід міжнародно-правового співробітництва в галузі комп'ютерної злочинності.»

У 1995 році Комітет міністрів прийняв ще одну рекомендацію стосовно проблем, що виникають у зв'язку з транснаціональними комп'ютерними злочинами [116]. Керівні принципи для розробки відповідного законодавства були підсумовані в Додатку до Рекомендації.

Європейський комітет з проблем злочинності у 1996 році вирішив створити комітет експертів з питань кіберзлочинності. У період з 1997 по 2000 рік комітет провів десять пленарних засідань та п'ятнадцять засідань його Редакційної групи відкритого складу. Асамблея прийняла Проект конвенції про кіберзлочинність в квітні 2001 року. Завершений Проект конвенції був представлений на затвердження Комітету з проблем злочинності та Комітету міністрів для прийняття та відкриття до підписання [117]. Конвенція про кіберзлочинність була відкрита до підписання під час церемонії підписання в Будапешті 23 листопада 2001 року, під час якої 30 країн підписали Конвенцію про кіберзлочинність (вкл Канаду, Сполучені Штати, Японію та Південну Африку, які брали участь у переговорах). До квітня 2012 року підписано 47 держав, і 33 держави ратифікували Конвенцію

Ради Європи про кіберзлочинність. Конвенція про кіберзлочинність сьогодні визнана важливим регіональним інструментом боротьби з кіберзлочинністю та підтримується різними міжнародними організаціями.

Під час переговорів щодо тексту Конвенції про кіберзлочинність з'ясувалося, що криміналізація расизму та розповсюдження ксенофобних матеріалів є особливо суперечливими питаннями. Деякі країни в яких принцип свободи вираження поглядів був сильно захищений, висловили стурбованість тим, що, якщо положення будуть включені до Конвенції про кіберзлочинність, що порушують свободу вираження поглядів, вони не зможуть підписати Конвенцію [118]. У четвертому проекті редакції від 1998 року Конвенція все ще що містила положення, яке вимагало від учасників криміналізації нелегалів що стосується, зокрема, таких питань, як дитяча порнографія та расова ненависть. Щоб уникнути ситуації, коли країни не зможуть підписати Конвенцію через свободу вираження поглядів, ці питання були вилучені з Конвенції про кіберзлочинність, а під час розробки проекту вони інтегрували в окремий протокол. До січня 2012 року було підписано 35 держав, та ще 20 держав ратифікували Додатковий протокол.

В даний час Конвенція Ради Європи про кіберзлочинність як і раніше є інструментом, що має найширший вплив, підтримуваний різними міжнародними організаціями. Однак дебати на дванадцятому конгресі Ради Європи про боротьбу зі злочинністю підкреслили, що через десять років після відкриття для підписання вплив Конвенції залишається обмеженим.

США є єдиною країною за межами Європи, яка ратифікувала цей документ. Це правда, що вплив Конвенції не можна вимірювати виключно кількістю підписів чи ратифікацій, оскільки такі країни як Аргентина, Пакистан, Філіппіни, Єгипет, Ботсвана та Нігерія використовували цю Конвенцію як модель при уніфікації їх законодавства без формального приєднання до неї. Проте навіть у випадку з цими країнами незрозуміло,

наскільки вони використовували Конвенцію як модель. Адже деякі з них також використовували інші тексти законів, такі як Директива ЄС щодо атак проти інформаційних систем.

Одним із ключових намірів Конвенції було надання всебічного правового підходу, який стосується всіх відповідних областей кіберзлочинності. Але порівнюючи Конвенцію з іншими підходами, зокрема, Типовим законом Співдружності про кібербезпеку, що стосується комп'ютерної злочинності, а також Директива ЄС з електронної комерції, показують, що в Конвенції відсутні важливі аспекти. Наприклад, були упущені такі питання: положення, що стосуються прийнятності електронних свідчень або відповідальності постачальників послуг Інтернету. Особливо відсутнє забезпечення, принаймні, базової регуляторної бази щодо прийнятності електронних доказів. Це має суттєві наслідки, оскільки електронні докази широко характеризуються як нова категорія доказів [119]. І якщо країна не має інших документів, або її суди не визнають такі докази прийнятними, країна, можливо, не зможе засудити жодних правопорушників, незважаючи на повну імплементацію цієї Конвенції.

Наступною регіональною організацією, яка бере активну участь в міжнародно-правовому регулюванні кібербезпеки є Європейський Союз (ЄС). Протягом останнього десятиліття ЄС розробив кілька правових документів, що стосуються аспектів кіберзлочинність. Хоча ці інструменти загалом є обов'язковими для 28 держав-членів, деякі країни та регіони використовують стандарти ЄС як орієнтир у своїх національних та регіональних дискусіях щодо гармонізації законодавства.

Ще в 1996 році ЄС розглянув ризики, пов'язані з Інтернетом, в повідомленні, присвяченому незаконному та шкідливому контенту в Інтернеті [120]. ЄС підкреслив важливість співпраці між державами-членами для боротьби проти незаконного контенту в Інтернеті. У 1999 році Європейський Парламент і Рада прийняли план дій щодо сприяння більш

безпечному використанню Інтернету та боротьби з незаконним та шкідливим вмістом у глобальних мережах [121]. План дій зосереджувався на саморегуляції, а не на криміналізації. Також в 1999 році ЄС розпочав ініціативу "eEurope", прийнявши повідомлення Європейської Комісії "eEurope - інформаційне суспільство для всіх" [122]. Ця ініціатива визначає основні цілі, але не розглядає криміналізацію незаконних дій, скоєних з використанням інформаційних технологій. У 2001 році Європейська Комісія (ЄК) опублікувала повідомлення "Створення безпечного інформаційного суспільства шляхом покращення безпеки інформаційних інфраструктур та боротьби зі злочинністю, пов'язаною з комп'ютерними злочинами" [123] У цьому повідомленні ЄК проаналізувала та вирішила проблему кіберзлочинності та загострення необхідності ефективних дій для боротьби із загрозами цілісності, доступності та надійності інформаційних систем та мереж.

Окрім повідомлення про злочини, пов'язані з комп'ютером, ЄС опублікував в 2001 році повідомлення "Мережа та інформаційна безпека" [124], в якому було проаналізовано проблеми безпеки в мережі та складено стратегічний план дій у цій сфері. Повідомлення ЄК підкреслюють необхідність наближення матеріального кримінального права в рамках Європейського Союзу, особливо щодо нападів на інформаційні системи.

Гармонізація матеріального кримінального права в рамках Європейського Союзу у боротьбі з кіберзлочинністю визнається ключовим елементом усіх ініціатив на рівні ЄС. У 2007 році ЄС оприлюднив повідомлення щодо загальної політики боротьби з кіберзлочинністю [125]. Повідомлення підсумовує поточну ситуацію та підкреслює важливість Конвенції Ради Європи про кіберзлочинність як переважаючий міжнародний інструмент боротьби з кіберзлочинністю. Крім того, в повідомленні вказуються питання, які ЄК зосереджує на майбутніх заходах. Серед них:

- зміцнення міжнародного співробітництва у боротьбі з кіберзлочинністю;
- покращення координації фінансової підтримки навчальних заходів;
- організація наради правоохоронних експертів;
- посилення діалогу в галузі забезпечення кібербезпеки;
- моніторинг еволюційних загроз кіберзлочинності для оцінки необхідності подальшого законодавства.

Директива ЄС про електронну торгівлю [126], зокрема, стосується відповідальності постачальника послуг Інтернету за дії, вчинені третіми особами (стаття 12 та наступні). Беручи до уваги виклики, що випливають з міжнародного виміру мережі, розробники вирішили розробити правові стандарти, щоб забезпечити рамки для загального розвитку інформаційного суспільства та підтримувати загальний економічний розвиток, а також роботу правоохоронних органів [127]. Директива грунтується на тому, що розвиток інформаційно-комунікаційних послуг ускладнюється низкою правових перешкод належному функціонуванню внутрішнього ринку, що дає Європейському Співтовариству свій мандат. Хоча Директива підкреслює, що не має наміру гармонізувати сферу кримінального права як такої, вона також регулює відповідальність за кримінальним законодавством [128].

У 2000 році Рада Європейського Союзу прийняла підхід до вирішення проблем дитячої порнографії в Інтернеті. Рішення, яке було прийнято, є подальшим кроком у зв'язку з повідомленням 1996 року про незаконний і шкідливий вміст в Інтернеті та відповідний план дій 1999 року щодо сприяння безпечному використанню Інтернету та боротьби з незаконним та шкідливим вмістом у глобальних мережах [129]. Проте Рішення не містить зобов'язань щодо прийняття конкретних положень кримінального права.

У 2001 році ЄС прийняв першу правову базу, яка безпосередньо стосується аспектів кіберзлочину. Рамкове рішення ЄС щодо боротьби з шахрайством та підробкою безготівкових коштів містить зобов'язання щодо гармонізації законодавства про кримінальне законодавство щодо конкретних аспектів комп'ютерного шахрайства та виробництва інструментів, таких як комп'ютерні програми, спеціально прийняті з метою вчинення злочинів, зазначених в Рамковому рішенні [130].

Стаття 3 Рамкового рішення проголошує: «Кожна держава-член вживає необхідних заходів для забезпечення того, щоб наступна поведінка підпадала під кримінальне правопорушення у разі вчинення навмисно: виконання або заподіяння передачі грошової вартості та тим самим заподіяння несанкціонованого збитку майну іншої особи, з наміром забезпечити несанкціоновану економічну вигоду особи, яка вчинила правопорушення, або для третьої сторони шляхом:

- без права внесення, зміни, видалення або припинення комп'ютерних даних, зокрема ідентифікаційних даних, або

- без права на втручання у функціонування комп'ютерної програми чи системи.»

У 2005 році Рада прийняла Директиву щодо збереження даних ЄС. Вона містить зобов'язання Інтернет-провайдерів зберігати певні дані про трафік, необхідні для ідентифікації злочинців у кіберпросторі. Той факт, що ключова інформація про будь-яке спілкування в Інтернеті буде охоплена Директивою, призвела до інтенсивної критики з боку правозахисних організацій та може призвести до перегляду Директиви та її використання конституційними судами [131]. Радник Європейського суду, генеральний адвокат Джуліан Кокот, зазначив, що сумнівно, чи можна виконувати зобов'язання щодо збереження даних без порушення основних прав. Потенціал труднощів, пов'язаних з виконанням таких положень, вже був висвітлений "Великою вісімкою" в 2001 році.

У 2007 році Європейський Союз розпочав дискусію щодо проекту поправки до Рамкового рішення про боротьбу з тероризмом [132]. У вступі до проекту поправки ЄС наголошують, що існуюча правова база передбачає кримінальну відповідальність за сприяння або заохочення та підбурювання, але не криміналізує поширення експертиза тероризму через Інтернет. З поправкою, ЄС прагне вживати заходів для подолання розбіжностей та наближення законодавства у всьому ЄС до Конвенції Ради Європи про запобігання тероризму.

«Стаття 3 - Злочини, пов'язані з терористичною діяльністю 1. Для цілей цього Рамкового рішення: (a) "громадська провокація вчинення терористичного злочину" означає розповсюдження або іншим чином повідомлення суспільству з наміром підбурювати до вчинення одного з дій, зазначених у частині 1(a)-(h) статті 1, якщо така поведінка, незалежно від того, чи прямо закріплює терористичні правопорушення, спричиняє небезпеку, що може бути скоєно один чи декілька таких правопорушень; (b) "вербування до тероризму" означає закликати іншу особу до здійснення одного з дій, зазначених у статті 1 (1) або в статті 2 (2); (c) "підготовка до тероризму" означає надання інструкцій щодо виготовлення або використання вибухових речовин, вогнепальної зброї та інших видів зброї, шкідливих та небезпечних речовин або інших спеціальних методів або методів для здійснення одного з дій, зазначених у статті 1 (1), знаючи, що надані навички призначені для використання з цією метою. 2. Кожна держава-член вживає необхідних заходів для забезпечення того, щоб правопорушення, пов'язані з тероризмом, містили наступні навмисні дії: (a) громадську провокацію вчинення терористичного злочину; (b) вербування для тероризму; (в) підготовка тероризму; (d) крадіжка з метою здійснення одного з дій, зазначених у статті 1 (1); (д) вимагання з метою здійснення одного з дій, зазначених у статті 1 (1); (f) складання фальшивих адміністративних документів з метою здійснення одного з дій, зазначених у підпунктах (a) -h) статті 1 (1) та статті 2 (2) (b). 3. Для того, щоб акт

вважався покараним, як зазначено у пункті 2, не потрібно, щоб фактично вчинили терористичне правопорушення."»[132].

Таким чином, на підставі статті 3 (1) (c) Рамкового рішення держави-члени, зобов'язані криміналізувати публікацію інструкцій щодо використання вибухових речовин, знаючи, що ця інформація призначена для використання у зв'язку з тероризмом. Необхідність доказів того, що інформація призначена для використання в цілях, пов'язаних з тероризмом, найімовірніше обмежує застосування цього положення стосовно більшості інструкцій щодо використання зброї, доступних в Інтернеті, оскільки їх публікація не пов'язує їх безпосередньо до терактів. Оскільки більшість зброї та вибухових речовин можуть використовуватися для здійснення "регулярних" злочинів, а також злочинів, пов'язаних із тероризмом (подвійне використання), сама інформація навряд чи може бути використана для доведення того, що особа, яка їх опублікувала, знала про способи подальшого використання такої інформації. Тому слід враховувати контекст публікації (наприклад, на веб-сайті, що експлуатується терористичною організацією).

Азіатсько-тихоокеанське економічне співробітництво (АТЕС) визначило кіберзлочинність як важливу сферу діяльності, а лідери АТЕС закликали до тіснішої співпраці між посадовими особами, які беруть участь у боротьбі з кіберзлочинністю. Декларація засідання 2008 року міністрів зв'язку та інформації АТЕС в Бангкоку, Таїланд, підкреслив важливість продовження співпраці у боротьбі з кіберзлочинними. До цих пір АТЕС не надав юридичну основу щодо кіберзлочинів, але згадав про такі міжнародні стандарти, як Будапештська конвенція про кіберзлочинність. Крім того, АТЕС тісно вивчила національне законодавство про кіберзлочинність у різних країнах під час обстеження законодавства в галузі кіберзлочинного законодавства та розробило базу даних про підходи до надання допомоги країнам у розробці та перегляді

законодавства [133]. Підходи базуються на законодавчій базі Будапештської конвенції про кіберзлочинність.

це одне з питань, що розглядаються Співдружністю націй. Діяльність організації зосереджена, зокрема, на гармонізації законодавства. Беручи до уваги зростаючу важливість кіберзлочинності, міністри Співдружності прийняли рішення доручити експертній групі розробити правову основу боротьби з кіберзлочинністю на основі Конвенції Ради Європи про кіберзлочинність. Група експертів представила свою доповідь і рекомендації у березні 2002 року. Надалі в 2002 році був представлений проект типового закону про комп'ютерні злочини [134]. Завдяки чіткій інструкції, а також визнанні групою експертів Конвенції Ради Європи про кіберзлочинність як міжнародного стандарту, типовий закон значною мірою відповідає стандартам, визначеним цією Конвенцією.

На засіданні 2000 року міністри законів та генеральні прокурори невеликих юрисдикцій Співдружності вирішили створити експертну групу для розробки типового законодавства щодо цифрових доказів. Типовий закон був представлений у 2002 році. На додаток до законодавчого забезпечення, Співдружність організувала декілька навчальних заходів. Співтовариство мережі інформаційних технологій та розвитку (COMNET-IT) спільно організувала тренінги з кіберзлочинністю у квітні 2007 року. У 2009 році на Мальті, за підтримки Фонду Співдружності для технічних питань, відбулася Програма навчання третіх країн Співдружності з правових рамок для ІКТ. Ще одне тренування було організовано в 2011 році. Ціль політики Співдружності у сфері забезпечення кібербезпеки полягає в тому, щоб дозволити всім країнам Співдружності ефективно співпрацювати у глобальному бою з кіберзлочинністю.

Під час позачергової конференції міністрів Африканського Союзу, відповідального за комунікацію та інформаційні технології, яка відбулася в Йоганнесбурзі в 2009 році, міністри розглянули різні теми, пов'язані з

посиленням використання ІКТ в африканських країнах. Було вирішено, що Комісія Африканського Союзу повинна - спільно з Економічною комісією ООН для Африки - розробити правові рамки для африканських країн, що стосуються таких питань, як електронні угоди, кібернетична безпека та захист даних. У 2011 році Африканський Союз представив проект Концепції Африканського Союзу про створення надійної правової бази для кібербезпеки в Африці. Метою розробників є зміцнення чинного законодавства в державах-членах щодо інформаційно-комунікаційних технологій. Що стосується мандату, то це не обмежується кіберзлочинністю, а також включає в себе інші питання інформаційного суспільства, такі як захист даних та електронні транзакції.

Конвенція є всеосяжною, ніж більшість інших регіональних підходів. Вона містить чотири частини. Перша частина стосується електронної комерції: різних аспектів, таких як договірна відповідальність електронного постачальника товарів та послуг, зобов'язань за договором в електронній формі та безпека електронних операцій. Друга частина стосується питань захисту даних. Третя частина стосується боротьби з кіберзлочинністю.

Концепція міжнародної співпраці особливо виражена статтями 21 та 25:

«Стаття 21: Міжнародне співробітництво

Кожна держава-член приймає такі заходи, які вона вважає необхідними для сприяння обміну інформацією та обміну швидкими, оперативними та взаємними даними органами держав-членів та подібними організаціями інших держав-членів, відповідальними за застосування закону на двосторонній або багатосторонній основі.

Стаття 25: Модель міжнародного співробітництва

Кожна держава-член приймає такі заходи та стратегії, які вона вважає необхідними для участі у регіональному та міжнародному співробітництві в галузі кібербезпеки. Резолюції, спрямовані на сприяння участі держав-

членів в рамках цих відносин, були прийняті великою кількістю міжнародних урядових органів, включаючи Організацію Об'єднаних Націй, Африканський Союз, Європейський Союз, Велику вісімку та ін. Організації, такі як Міжнародний союз електрозв'язку, Рада Європи, Співдружність Націй та інші, створили модельні рамки для міжнародного співробітництва, які держави-члени можуть прийняти в якості керівництва.»

Наступною регіональною міжнародною організацією, яка бере участь в забезбеченні кібербезпеки є Організація арабських держав і Рада з питань співробітництва в Перській затоці. Ряд країн арабського регіону вже прийняли національні заходи та підходи до боротьби з кіберзлочинністю. Приклади таких країн включають Пакистан, Єгипту та Об'єднані Арабські Емірати (ОАЕ). Для гармонізації законодавства в регіоні ОАЕ подали типовий законодавчий акт до Ліги арабських держав (Керівний закон боротьби зі злочинністю у сфері інформаційних технологій) [135].

Організація американських держав. З 1999 року Організація американських держав (ОАД) активно займається питанням кіберзлочинності в регіоні. Загалом питаннями кіберзлочинів в ОАД займається REMDA - провідний політичний та технічний форум з питань правосуддя та міжнародно-правового співробітництва.

У 2010 році REMDA звернувся до питання про кіберзлочинність на своєму восьмому засіданні. Учасники коротко обговорили важливість продовження консолідації та оновлення Міжамериканського порталу співпраці в галузі кіберзлочинності через Інтернет-сторінку ОАД та посилення спроможності держав розробляти законодавство та процесуальні заходи, пов'язані з кіберзлочинністю та електронними доказами. Крім того, в рекомендаціях наради висвітлено бажання посилити механізми, що дозволяють обмінюватися інформацією та співпрацювати з іншими міжнародними організаціями та установами в галузі кіберзлочинності, такими як Рада Європи, ООН, ЄС, АТЕС, ОЕСР, Великої

вісімки, Співдружності та Інтерполу, так що держави-члени ОАД можуть скористатися перевагами розвитку цих МО.

Організація Східнокарибських держав. У грудні 2008 року МСЕ та ЄС розпочали проект "Посилення конкурентоспроможності в Карибському басейні шляхом гармонізації політики, законодавства та регуляторних процедур у сфері ІКТ. Цей проект є частиною програма "ІКТ-інформаційні та комунікаційні технології" та дев'ятий Європейський фонд розвитку. Мета проекту - допомогти таким країнам гармонізувати свою політику та правові рамки в області ІКТ. В рамках даного проекту було визначено дев'ять напрямків роботи, в яких розроблена типова політика та типові законодавчі тексти для сприяння розробці та узгодженню законодавства в регіоні. Кіберзлочинність була однією з дев'яти робочих областей.

Розробка типового законодавчого тексту відбувалася у три етапи. На першому етапі було зібрано та переглянуто діюче законодавство країн-бенефіціарів. Паралельно було визначено кращі практики регіонального та міжнародного характеру. Пріоритет надається стандартам, які безпосередньо застосовуються принаймні в деяких країнах-бенефіціаріях (наприклад, Типовий закон Співдружності від 2002 року). Однак огляд також включав найкращі практики з інших регіонів, таких як ЄС та Африка.

Звіт містив огляд існуючого законодавства, а також порівняльний аналіз законодавства, який порівнював існуюче законодавство з найкращим регіональним та міжнародним досвідом. З метою підготовки аналізу пробілів у звіті було визначено також особливі потреби регіону (наприклад, законодавство про спам), які не обов'язково розглядаються найкращою міжнародною практикою. На основі звіту та аналізу пробілів зацікавлені сторони склали типові директивні принципи політики. На другому етапі розроблено типовий законодавчий текст з урахуванням політичних керівних принципів.

На другому семінарі експерти з питань політики, розробники законодавства та інші зацікавлені сторони країн-бенефіціарів обговорили та внесли зміни до проекту типового законодавчого тексту, який був підготовлений до зустрічі, і прийняли його. Типовий законодавчий текст має такі основні цілі: відображає особливі вимоги регіону і розробляється з урахуванням практики законодавства в регіоні, з тим щоб забезпечити безперебійну реалізацію. У типовому законодавчому тексті міститься складний набір визначень та основні положення кримінального права, включаючи положення, що стосуються питань, таких як спам, які мають високий пріоритет для регіону, але не обов'язково містяться в регіональних рамках, таких як Конвенція Ради Європи про кіберзлочинність.

«Стаття 15 (2) Країна може обмежити криміналізацію стосовно передачі кількох електронних повідомлень у рамках клієнтських або ділових відносин. Країна може вирішити не криміналізувати поведінку в розділі 15 (1) (a) за умови наявності інших ефективних засобів правового захисту.» - в тексті містяться положення процесуального права та положення про відповідальність постачальників послуг Інтернету.

Тихоокеанський регіон. Паралельно з проектом спільного фінансування МСЕ та ЄС також і у Карибському басейні розпочали проект гармонізації політики, законодавства та регуляторних процедур у сфері ІКТ. Проект зосереджується на створенні людських та інституційних можливостей у сфері ІКТ шляхом проведення заходів з навчання та обміну знаннями та досвідом.

У березні 2011 року у Вануату відбувся семінар, присвячений нинішньому законодавству в галузі кіберзлочинного законодавства в Тихому океані. Під час семінару був представлений комплексний порівняльний юридичний аналіз, який містив огляд існуючого законодавства в регіоні а також порівняння з найкращими практиками з інших регіонів. Наступним кроком була проведена конференція, присвячена методам розробки політики та законодавства в галузі

кіберзлочинів, в серпні 2011 року на Самоа. Під час конференції були представлені кращі практики з інших регіонів та структури для гармонізованої політики та законодавства. Вони адресовані матеріальному кримінальному праву, процесуальному законодавству, міжнародному співробітництву, відповідальності Інтернет-провайдера, електронним доказам та заходам із попередження злочинності. У квітні 2011 року Секретаріат Тихоокеанського співтовариства організував конференцію, присвячену боротьбі з кіберзлочинністю в Тихому океані. Цей захід було спільно організовано з Радою Європи. Під час конференції обговорювалися питання, пов'язані з матеріальним кримінальним правом, процесуальним правом та міжнародним співробітництвом.

2.3 Участь України в міжнародно-правовому співробітництві у сфері забезпечення кібербезпеки у сфері забезпечення кібербезпеки

Відповідно до Кримінального кодексу України, до інформаційних злочинів (кіберзлочинів) відносяться: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку; створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут; Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї; Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється; Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку [140].

У відповідь на масштабні кібератаки в останні роки, в 2016 році в Україні було прийнято Національну стратегію кібербезпеки. Створення Національного координаційного центру з кібербезпеки та оновлення законодавства в галузі кіберзлочинності у відповідності до вимог Будапештської конвенції є двома основними кроками у підвищенні кібер-

стійкості країни. Ці заходи супроводжуються налагодженням сильної співпраці з міжнародними партнерами в кібер-сфері, у тому числі з питань кіберзлочинності та кіберзахисту.

Збільшення оцифрування послуг та дуже активне використання Інтернету призвело до еволюції кіберпростору, що також викликало значні проблеми для безпеки урядів у всьому світі щодо злочинів за допомогою комп'ютерних систем.

В Україні це було продемонстровано кібератаками на енергетичні компанії у грудні 2015 р., нападами на основні українські телеканали в день місцевих виборів у 2017 р. 27 червня 2017 року сталась масштабна хакерська атака хробаком-винищувачем NotPetya, яка вразила майже 80 % підприємств в Україні а також перекинулась на підприємства закордоном. Зловмисники викрадали інформацію з підприємств та відкривали доступ до їх комп'ютерних мереж.

Заступник голови адміністрації Президента України Дмитро Шимків, колишній директор представництва фірми Microsoft в Україні, заявив, що внаслідок атаки хробаком NotPetya було виведено з ладу близько 10 % персональних комп'ютерів в Україні (особистих, в державних та не державних установах і підприємствах). Усунення наслідків атаки вірусом-винищувачем NotPetya забрало істотні зусилля та час. Так, наприклад, компанія Reckitt Benckiser заявила, що частина комп'ютерних систем відновить свою нормальну роботу лише у серпні 2017 року [141]. За оцінками концерну Maersk втрати компанії, особливо її підрозділів Maersk Line, Damco та APM Terminals разом будуть складати 200 - 300 млн. доларів. Технічний персонал був вимушений протягом 10 днів заново встановлювати і налаштувувати все програмне забезпечення на 4000 серверах, 45000 робочих станціях. Робітники були вимушені вручну опрацьовувати інформацію про виробничі процеси. У вересні 2017 року американська логістична та поштова компанія FedEx оприлюднила оцінку збитків у своєму дочірньому підприємстві у Нідерландах TNT Express. Так,

через порушення нормальних робочих процесів підприємство оцінює свої збитки на рівні до 300 млн. доларів за перше півріччя 2017 року. Внаслідок цієї проблеми американська фармацевтична компанія Merck заявила про тимчасову зупинку виробництва вакцини проти вірусу папіломи людини [142].

На думку деяких експертів з міжнародного права - Майкла Шмітта та Джефрі Білера невибірковий характер поширення вірусу та свідомий вибір цивільних об'єктів для початку атаки свідчать про те, що організатори атаки порушили міжнародне право звичаїв військового конфлікту, тобто, такий вчинок може вважатись воєнним злочином. Оскільки від атаки постраждали треті країни, а отже атака ще й порушує міжнародні норми стосовно нейтральності країн [142].

Ці інциденти відповідають загальним тенденціям, які Україна спостерігає за останні роки:

- посилене використання атак "Distributed Denial of Service" (напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена);

- вразливості "нульового дня"*, використовуваного для проникнення та виведення з ладу важливих інфраструктур.

Аналіз ситуації також вказує на цільові напади на дипломатів, правоохоронні органи, державні підприємства, засоби масової інформації, політиків та громадських діячів, а також дезінформаційні кампанії через Інтернет для впливу на людей заради лобіювання власними інтересами. Вплив цих нападів може бути дуже істотним, оскільки пошкодження критичних інформаційних інфраструктур та перешкоджання ефективному функціонуванню національних органів влади може призвести до жахливих наслідків [143]. Також, не слід забувати про кібератаки ініційовані урядами інших держав. Інформаційно-психологічна війна спрямована на

дискредитацію державної влади та сприяє дестабілізації соціально-політичної ситуації.

У відповідь на ці виклики, Указом Президента Україна прийняла свою національну стратегію кібербезпеки від 15 березня 2016 року. Стратегія, також включає річний План дій для її реалізації та має загальну мету створити умови, які б забезпечили відповідні умови кіберпростору та його використання в інтересах осіб, суспільства та уряду [144]. Увага Стратегії зосереджується на трьох основних завданнях:

1. Розвиток національної системи кібербезпеки.
2. Сприяння новим можливостям в секторі безпеки та оборони.
3. Забезпечення кібербезпекою критичні інформаційні інфраструктури та державні інформаційні ресурси.

Національна система кібербезпеки, запроваджена Стратегією, забезпечує співпрацю між усіма державними установами, місцевими органами влади, військовими підрозділами, правоохоронними органами, науково-дослідними та навчальними закладами, цивільними групами, підприємствами та організаціями, незалежно від форм власності, або осіб, що є власниками критичної інформаційної інфраструктури [145

міжрегіональний територіальний орган Національної поліції України, який забезпечує реалізацію державної політики у сфері протидії кіберзлочинності, здійснює інформаційно-аналітичне забезпечення керівництва Національної поліції України та органів державної влади про стан вирішення питань, віднесених до його компетенції. Завданнями Департаменту кіберполіції є участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, учинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку [146]. Департамент також сприяє іншим підрозділам Національної поліції

України у попередженні, виявленні та припиненні кримінальних правопорушень [147]. Щорічно кількість виявлених кіберзлочинів завдяки Департаменту збільшується в середньому на 2500. У 2017

виключно кіберзлочини.

Ключовим кроком у реалізації Стратегії було створення Національного координаційного центру з кібербезпеки у червні 2016 р., який є робочим органом Ради національної безпеки і оборони. Серед основних завдань Центру: аналіз стану кібербезпеки; результатів проведення огляду національної системи кібербезпеки; стану готовності суб'єктів забезпечення кібербезпеки до виконання завдань з питань протидії кіберзагрозам; стану виконання вимог законодавства щодо кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також критичної інформаційної інфраструктури; даних про кіберінциденти стосовно державних інформаційних ресурсів в інформаційно-телекомунікаційних системах тощо. Центр прогнозує та виявляє потенційні та реальні загрози у сфері кібербезпеки України, узагальнює міжнародний досвід у сфері забезпечення кібербезпеки; оперативне, інформаційно-аналітичне забезпечення РНБО з питань кібербезпеки.

Центр бере участь в організації і проведенні міжнаціональних і міжвідомчих кібернавчань та тренінгів, розробляє відповідні методичні документи і рекомендації. Центр має право запитувати та одержувати від органів виконавчої влади, органів місцевого самоврядування, підприємств, установ і організацій статистичні дані, інформацію, довідкові та інші матеріали, необхідні для вирішення питань, що належать до його компетенції; користуватися інформаційними базами даних державних органів, державними, в тому числі урядовими, системами зв'язку і комунікацій, мережами спеціального зв'язку та іншими технічними засобами тощо. Керівником Центру за посадою є Секретар Ради

національної безпеки і оборони України, секретарем – керівник структурного підрозділу Апарату Ради національної безпеки і оборони України, до відання якого віднесені питання кібербезпеки.

В 2017 році Верховна Рада України ухвалила законопроект "Про основні засади забезпечення кібербезпеки України" – робота над ним тривала понад два роки. Закон є надзвичайно важливим з точки зору створення системи забезпечення кібербезпеки держави в цілому. У ньому визначено, кого і що мають захищати від кібератак та хто це має робити. Під захист потрапляють комунікаційні системи, якими, зокрема, користуються органи влади і правопорядку, та ресурси у сферах електронного урядування і комерції. Крім того, захищеними мають бути "критично важливі об'єкти інфраструктури" [148], під якими законодавці розуміють цілу низку підприємств і установ, наприклад, у галузі енергетики, інфраструктури, банківського сектору, стратегічних підприємств. Перевіряти дотримання інформаційної безпеки будуть за допомогою незалежного аудиту, що має проходити за стандартами ЄС та НАТО.

Крім того, як держава-учасниця Будапештської конвенції про кіберзлочинність, Україна прагне до повної імплементації Конвенції [149; 150]. Проект законодавства був підготовлений і в даний час обговорюється в Парламенті, що передбачає посилення відповідальності за кіберзлочинність, а також визначає важливу термінологію та оновлену відповідальність постачальників послуг Інтернету відповідно до Конвенції.

Окрім роботи над національним законодавством, Україна визнає необхідність міцного міжнародного співробітництва та розбудови спроможності для вирішення потреб та загроз, пов'язаних із кібербезпекою, яка також висвітлена в новій Стратегії. Україна співпрацює з багатьма партнерами в кібер-сфері. Україна є партнером спільних проектів Європейського Союзу та Ради Європи "CyberCrime EAP II" та "CyberCrime EAP III", які мають регіональний аспект та включають країни

Східного партнерства. Перший проект спрямований на вдосконалення взаємної правової допомоги для міжнародної співпраці з питань кіберзлочинності та електронних доказів; посилення ролі 24/7 контактних пунктів [151; 152]. Другий проект, який був започаткований у Києві у квітні 2016 року, полягає у вирішенні питань державного та приватного співробітництва [153]. За рекомендаціями Ради Європи встановлюється співпраця між національній владою та Інтернет-провайдерами. Така співпраця сприятиме структурованому діалогу з Інтернет-провайдерами, що допоможе встановити засоби довіри до розуміння та реагування на потреби кожного.

Крім того, британські та естонські партнери надавали українським правоохоронним органам сучасне обладнання та програмне забезпечення, щоб провести професійну комп'ютерну кримінальну експертизу і більш ретельно вивчити кіберзлочини.

В сфері кібербезпеки Україна також співпрацює з Цільовим фондом НАТО з питань к

НАТО з питань кібербезпеки». Зокрема, угодою передбачено розбудову в Україні мережі ситуаційних центрів реагування на комп'ютерний інцидент та розгалуженої мережі автоматизованих датчиків подій, інтегрованих в інформаційні мережі об'єктів критичної інформаційної структури [154]. Також, було схвалено рішення про подальший напрямок розбудови національної системи кібербезпеки з урахуванням можливостей Трастового фонду, а саме: підвищення технічних можливостей України у сфері кібербезпеки шляхом її оснащення автоматизованими датчиками подій та підключення до національної мережі ситуаційних центрів Держспецзв'язку; створення центрів кібернетичної безпеки в системі Збройних сил України та Національної поліції з їх подальшим інтегруванням в національну мережу ситуаційних центрів. Разом з

партнерами НАТО, Україна проводила заняття та тренінги з кіберзахисту, в рамках якої учасники навчаються, як реагувати на великі кібернапади національної оборонної інфраструктури.

Україна не тільки бере участь в міжнародних ініціативах у сфері протидії кібернетичним загрозам, але також сприяє розвитку регіональних ініціатив. За ініціативи на чолі з Україною в рамках Організації за демократію та економічний розвиток (до якої також входять Азербайджан, Грузія, Молдова, Україна) була створена робоча група з питань кібербезпеки. Група зараз обговорює розробку Меморандуму про взаєморозуміння для прийняття її урядами. Організація вже запровадила захищену систему зв'язку, яка, зокрема, забезпечує безпечний обмін данними в Інтернеті та проведення відеоконференцій.

Досвід України показує, що для подолання постійних к

між

національними органами, приватним сектором та міжнародними партнерами з метою створення необхідних можливостей та ефективного реагування на такі загрози.

РОЗДІЛ 3. ШЛЯХИ ВДОСКОНАЛЕННЯ МІЖНАРОДНОГО ПРАВА У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

3.1 Створення єдиної міжнародної системи захисту і моніторингу

В попередніх розділах описувались кроки, які були зроблені міжнародними організаціями та державами задля забезпечення кібербезпеки. Загалом їхні дії були дуже схожими: уніфікація національного законодавства з нормами міжнародного права (як правило з нормами Конвенції Ради Європи про кібербезпеку), створення на основі міжнародних норм і принципів власних стратегій та політики забезпечення кібербезпеки, заохочення до міжнародної співпраці, допомога державам, що розвиваються шляхом проведення навчань, тренінгів, впровадження у таких державах досвіду та законодавства розвинених країн, створення центрів 24/7 і т. д.

Але також описувались і виклики, з якими стикаються держави і міжнародні організації під час забезпечення кібербезпеки. Було виявлено, що міжнародні джерела права у сфері кіберзлочинності не зовсім відповідають сучасним реаліям і в основному стосуються заклику держав співпрацювати та самостійно налаштовувати своє законодавство таким чином, щоб воно ефективно допомагало боротися з кіберзлочинами.

Проте, на мою думку дана сфера надто делікатна, щоб прирівнювати кіберзлочини до звичайних злочинів і орієнтуватись лише на національне

кримінальне право. Враховуючи це, а також те, що ще досі не існує жодної міжнародної організації, яка би займалась виключно забезпеченням кібербезпеки, варто розглянути таку можливість як стратегію розвитку та вдосконалення міжнародного права у сфері забезпечення кібербезпеки.

Отже, шляхом вдосконалення міжнародного права в даній сфері я бачу за доцільне створення міжнародної організації із забезпечення кібербезпеки. Членамии організації можуть ставати будь-які держави, які підписали Конвенцію із забезпечення кібербезпеки, яка була би написана під егідою цієї ж організації. Метою організації є забезпечення кібербезпеки як на національному, так і на міжнародному рівнях. Цілі організації являють собою попередженння кіберзлочинів, розлідування та боротьбу з ними. Завданнями організації є:

1. Посилити захист критично важливої інформаційної інфраструктури (КІІ) проти кібер-атак. КІІ - це комп'ютерні системи, безпосередньо задіяні у наданні основних послуг. Кібер-атаки на КІІ можуть мати неабиякий вплив на економіку та суспільство. Метою організації буде забезпечити рамки для визначення КІІ та надання власникам КІІ чіткого уявлення про свої зобов'язання щодо активного захисту КІІ від кібер-атак. Це створювало би стійкість до КІІ, захищаючи економіку держав та наш спосіб життя в цілому. Сектори КІІ: енергетика, вода, банківська справа та фінанси, охорона здоров'я, транспорт (до яких належать наземний, морський та авіа- транспорт), інформаційно-комунікаційні засоби, засоби масової інформації, служби безпеки та надзвичайних ситуацій, а також уряди.

2. Запобігання та реагування на загрози та інциденти, пов'язані з кібербезпекою одним з органів Органзації – міжнародною кіберполіцією Організації. Спеціально створені групи експертів в рамках цього органу проводитимуть розслідування загроз та інцидентів, пов'язаних із кібербезпекою, для визначення їх впливу та запобігання подальшій шкоді або інцидентам кібербезпеки.

3. Полегшення обміну інформацією, що стосується кіберзлочинів та кібербезпеки шляхом створення представництва в кожній державі-члені. Це є надзвичайно важливим, оскільки своєчасна інформація допомагає урядам та власникам комп'ютерних систем виявляти вразливі місця та запобігати ефективним випадкам кібер-інцидентів.

4. Беручи до уваги міжнародний характер кіберзлочинності, гармонізація національних законів і технік. Проте гармонізація повинна враховувати регіональний попит та потенціал. Тому варто було би створити консультацыйны групи для держав. Це не тільки допоможе вирішити проблеми урядів, що пов'язані з кіберзлочинністю, а й підкреслить важливість розробки та вдосконалення відповідного законодавства, міжнародного співробітництва та підвищення обізнаності про безпеку інформації серед кінцевих користувачів.

5. Впровадження правових, технічних та процесуальних заходів в боротьбі з кіберзлочинністю.

6. Допомога країнам у вирішенні законодавчих завдань, спричинених злочинною діяльністю, яка здійснюється через мережі ІКТ шляхом розроблення Конвеції, яка у порівнянні з Конвенцією Ради Європи була би чіткішою по відношенню до покарання кіберзлочинців. Розробка законодавства для криміналізації певної поведінки або запровадження розслідувальних документів є досить незвичайним для більшості країн. Регулярна процедура полягає в першу чергу в запровадженні стратегії, яка визначає різні інструменти, що використовуються для вирішення проблеми. В рамках різноманітних підходів до гармонізації законів про кіберзлочинність мало уваги приділялося не лише інтеграції законодавства в національну законодавчу базу, а й включенні його у існуючу політику або розробку такої політики вперше. Як наслідок, деякі країни, які запровадили законодавство про кіберзлочинність без розробки стратегії боротьби з кіберзлочинністю, а також політики на рівні уряду, зіткнулися з серйозними труднощами. В основному це було результатом відсутності

заходів щодо попередження злочинності, а також дублювання різних заходів.

На мою думку, Організація із забезпечення кібербезпеки повинна мати таку структуру:

- Рада міністрів – вищий керівний орган, що складатиметься з представників держав, а саме міністрів юстиції, зв'язку, національної безпеки. Які саме міністри будуть членами Ради міністрів вирішує сама держава. Але вони повинні бути обізнані у даній сфері, добре володіти інформацією щодо правових аспектів забезпечення кібербезпеки. Рада скликатиметься раз на рік та звітуватиме про гармонізацію національного законодавства відповідно до Конвенції та інші кроки до забезпечення кібербезпеки. Також Рада міністрів визначає стратегії розвитку забезпечення кібербезпеки та вирішує важливі питання;

- Генеральна рада – виконавчий орган Організації, що здійснює загальне керівництво органами, уповноваженими спостерігати за дією урядів та угод складених під егідою організації. У числі функцій Ради - організація роботи Органу з вирішення спорів і Органу з безпеки. Рада також слідкує за виконанням рішень Органу з вирішення спорів державами-членами;

- Секретаріат – адміністративний орган, що очолюватиметься генеральним директором і складатиметься з уповноважених представників держав – експертів у сфері правових аспектів забезпечення кібербезпеки. Окрім адміністративних питань, цей орган також вирішуватиме питання стосовно політики забезпечення кібербезпеки та способів запобігти кіберзлочинам. Спеціальні експертні групи Секретаріату будуть працювати над розробкою рішень та відповідей на кіберзагрози, а також завдання які поставить перед ними Рада міністрів;

- Орган з безпеки – орган, що буде подібним до Інтерполу. Функції органу з безпеки пердбачають вжиття заходів попередження та ліквідацію

кібератак, розслідування кіберзлочинів шляхом створення слідчих груп. На основі розслідування Орган з вирішення спорів буде виносити рішення;

- Орган з вирішення спорів – не важко здогадатись, що цей орган подібний міжнародному суду буде вирішувати суперечки на міжнародному рівні. При цьому, спори будуть стосуватись як тлумачення Конвенції та інших міжнародних угод в рамках Організації, застосування національного законодавства щодо забезпечення кібербезпеки, так і самих кіберзлочинів.

3.2 Вдосконалення національного законодавства держав

Для того, щоб запровадити найбільш ефективну систему забезпечення кібербезпеки, окрім міжнародної співпраці також необхідно постійно вдосконалювати національне законодавство. На даному етапі ця сфера дуже молода та не розвинута. В Україні приміром діє лише Конвенція Ради Євпропи про кібербезпеку, ЗУ «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 та XVI Розділ кримінального кодексу України присвячений. Злочиниам у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Ця кількість джерел є маленькою, враховуючи, що Україна в останні роки стала простором для тестувань хакерами нових кібер-атак.

На нашу думку, кожна держава повинна прийняти стратегію із забезпечення кібербезпеки і втілювати її в життя, приділити увагу законодавству у цій сфері, визначити та конкретизувати перелік кіберзлочинів та покарань, налагодити роботу відповідних органів із

забезпечення кібербезпеки, активно співпрацювати з іншими державами та міжнародними організаціями.

Якою ж має бути національна стратегія? Національні стратегії в галузі кібербезпеки можуть мати різні форми і можуть змінювати рівень деталізації залежно від цілей та рівня розвитку конкретної країни. Тому не існує встановленого і загально узгоджених критеріїв визначення того, що становить національну стратегію кібербезпеки.

Опираючись на існуючі дослідження в цій галузі, цей документ заохочує зацікавлених сторін сформувати національну стратегію кібербезпеки як:

- вираження бачення, цілей, принципів та пріоритетів на високому рівні;
- рішення питань кібербезпеки;
- вдосконалення кібербезпеки;
- опис кроків, програм та ініціатив, які матиме країна;
- зобов'язання захищати свою національну кібер-інфраструктуру та

У сучасному глобалізованому світі право складається з безлічі національних, регіональних та міжнародних правових систем. Взаємодія між цими системами відбувається на декількох рівнях. Як наслідок, положення національних законів держав іноді суперечать один одному, що призводить до зіткненням законодавства або не збігання з достатньою часткою, що виключає юрисдикційні прогалини, адже кібербезпека має галузевий характер і може стосуватися кількох держав одночасно. Ці відмінності між національними законами приводять до питання про те, наскільки важливо гармонізувати закони про кіберзлочинність? Це можна зробити кількома способами, в тому числі за допомогою як обов'язкових, так і необов'язкових міжнародних або регіональних ініціатив.

Основою гармонізації може бути єдиний національний підхід (причому всі інші ретельно переглядають їхні закони) або, частіше,

загальні правові стандарти, визначені в законодавстві ряду держав, або виражені в рамках багатосторонньої угоди [155].

Одним із головних аргументів на користь гармонізації права у різних юрисдикціях є уникнення безпечних притулків і штрафних притулків для злочинців. Отже, якщо шкідливі дії, пов'язані з Інтернетом, визнаються кримінальними, наприклад, в країні А, але не в країні В, правопорушник у країні В може вільно здійснювати правопорушення в країні А через Інтернет. У таких випадках держава А не може самотужки ефективно захищати від наслідків такої транснаціональної діяльності. Навіть якщо її кримінальне законодавство дозволяє заявляти про юрисдикцію над виконавцем у державі В, він все одно буде вимагати допомоги від держави В - щодо збору доказів або екстрадиції виявленого злочинця. З метою захисту осіб, що знаходяться в межах своєї юрисдикції, держава В навряд чи допомагатиме в тому випадку, якщо така поведінка також буде криміналізована в її законодавстві.

Гармонізація процесуального права є другою неодмінною вимогою для ефективного співробітництва в міжнародному праві. Таким чином можна створити єдину систему доказів. Або укладати двосторонні угоди щодо доказів у справах, що стосуються порушення кібербезпеки. Ці угоди за своєю суттю та змістом мають бути схожими на договори про взаємну правову допомогу. У наведеному вище прикладі, якщо держава В не має необхідних процесуальних повноважень для прискореного збереження комп'ютерних даних, то, наприклад, держава А не зможе вимагати цей об'єкт через взаємну правову допомогу.

Через труднощі, що виникають при спробі визначити та повідомити про кіберзлочинність, національні та міжнаціональні порівняльні статистичні дані зустрічаються набагато рідше ніж про інші види злочинів. Саме тому зростає потреба у спеціальних центрах на державному рівні, які могли би розпізнати та повідомити міжнародне співтовариство про кібер-загрозу.

Дослідження UNDOC передбачає, що 80 % жертв кіберзлочинства не повідомляють про злочин у поліцію [156]. Це виникає через брак усвідомлення віктимізації та механізмів звітності. Важливо підкреслити ініціативи щодо збільшення звітності, у тому числі системи звітування в режимі он-лайн та гарячої лінії, посилення поліцейської діяльності та обміну інформацією. Реакція на кіберзлочинність, що супроводжується середньостроковими та довгостроковими тактичними дослідженнями, може успішно визначати кримінальні ринки та кримінальні схеми, що означає краще розуміння ситуацій, які потребують регулювання.

До тих пір, поки правоохоронні органи не матимуть сукупну картину жертв кіберзлочинності та їх правопорушників, залишатиметься незрозумілим питання про те, хто вони (чи є вони фізичними особами або корпорацією чи урядами), спосіб їх віктимізації та обсяг поліцейських ресурсів, які повинні бути виділеними на ліквідацію проблеми. Неможливість побудувати профіль злочинця призводить до неможливості ізолювати мотивацію правопорушника з метою криміналізації.

ВИСНОВКИ

У роботі було досліджено генезу розвитку міжнародних відносин у сфері забезпечення кібербезпеки, зокрема було виділено етапи становлення міжнародного співробітництва:

1. 1960-1970 роки - правопорушення зосереджувалися на фізичному пошкодженні комп'ютерних систем та знищенню збережених даних. Вони підпадали під юрисдикцію національного законодавства.
2. 1970-1080 роки - поява інтрнету, зародження кіберзлочинів (незаконне використання комп'ютерних систем, комп’ютерне шахрайство). застосування чинного законодавства у випадках комп'ютерної злочинності спричинило труднощі, обговорення правових рішень розпочалося в усьому світі.
3. 1980 - 1990 роки - збільшення кількості користувачів компютерних систем. Поява хакерів. Країни розпочали процес оновлення свого законодавства з метою задоволення вимог

мінливого злочинного середовища. Поява першого міжнародного документу у сфері забезпечення кібербезпеки (хоч і на регіональному рівні) - розроблена спеціальним комітетом експертів Ради Європи у 1989 році Рекомендація №89.

4. 1990 - 2000 роки - розвиток кіберзлочинності. Початок роботи таких міжнародних організацій як ОЕСР, Рада Європи, Велика вісімка, ООН над питаннями кібербезпеки. Як наслідок, кожна з цих організацій розробили певні рекомендації, які описувались вище, поведінки держав у випадку кіберзлочинів. Поява перших серйозних прецедентів міжнародних кіберпорушень та кіберзлочинів.
5. 2000 - 2010 роки - прийняття найважливіших рішень у сфері забезпечення кібербезпеки міжнародним співтовариством. Прийняття Радою Європи 23 листопада 2001 року у Будапешті Конвенції Ради Європи про кіберзлочинність, в 2004 році Європейським парламентом створено європейське агентства по мережевій і інформаційній безпеці (ENISA), в 2008 році ITU розробили Глобальну програму кібербезпеки ("GCA"). Призначення ITU статусу міжнародної організації, що має координуючу роль у всіх аспектах кібербезпеки.
6. 2010 - теперішній час - у сфері кіберзлочинності зявляються такі види злочинів, як кібертероризм. Міжнародна спільнота вдається до створення ценрів боротьби з кіберзлочинністю з філіалами в країнах.

Проаналізувавши історію становлення і розвитку міжнародних відносин і міжнародного права у сфері забезпечення кібербезпеки можна дійти висновку, що юридичними викликами у цій сфері є: проблема класифікації та визнання кіберзлочину. В більшості країнах відсутній чіткий перелік кіберзлочинів; хакерські атаки зазвичай мають мало

спільного з традиційною злочинною діяльністю. Як правило, буває важко встановити злочинний характер подібних діянь, на відміну від актів війни або тероризму. Хакерські атаки в значній мірі не піддаються простій класифікації видів озброєнь, яка використовується в міжнародному праві, що серйозно ускладнює застосування традиційних визначень злочинності, тероризму та агресії, наведених в існуючих правових нормах; проблема встановлення законодавства за яким слід судити кіберзлочинців. За самою природою кібепростору, хакерські атаки можуть проводиться з використанням ресурсів з будь-яких куточків світу, тим самим значно ускладнюючи ідентифікацію та локалізацію нападників; відсутність чітко сформованого переліку покарань кіберзлочинців; відсутність налагодженої системи постраждалий – правоохоронні органи. Більшість людей, які зазнали шкоди в результаті кібератак не звертаються до правоохоронних органів.

2. Уточнено поняття кіберзлочину – це у вузькому значенні (комп'ютерна злочинність) охоплює будь-яку незаконну поведінку, спрямовану на безпеку комп'ютерних систем та оброблюваних ними даних за допомогою електронних операцій. Кібернетичні злочини в ширшому сенсі (злочини, пов'язані з комп'ютером) охоплюють будь-яку незаконну поведінку, здійснену за допомогою або в зв'язку з комп'ютером чи мережею, включаючи такі злочини, як незаконне володіння, надання або розповсюдження інформації за допомогою комп'ютерної системи чи мережі.

За такими критеріями кіберзлочини класфіковано на такі види: злочини проти конфіденційності, цілісності та наявності комп'ютерних даних та систем (незаконний доступ, н езаконний шпіонаж, незаконне перехоплення, незаконне втручання у данні і/або систему); злочини, пов’язані зі змістом (еротичні або порнографічні матеріали, дитяча порнографія, расизм, пропаганда насильства, равопорушення, пов’язані з релігією, незаконні онлайн-ігри, наклеп та фальшиві відомості, спам та

пов'язані з ними загрози); правопорушення, пов'язані з авторськими правами та товарними знаками (порушення, пов'язані з авторськими правами, порушення, пов'язані з авторськими правами); злочини, пов'язані з використанням комп'ютерів (шахрайство, підробка, крадіжка особистих даних); комбіновані кіберзлочини (кібертероризм, кібервійна).

3. Виявлено такі особливості нормативного регулювання міжнародного співробітництва держав у сфері забезпечення кібербезпеки: Найважливішою багатосторонньою угодою, яка конкретно стосується аспектів кібератак, є Конвенція Ради Європи про кіберзлочинність (Council of Europe Convention on Cybercrime – «CEC») 2001 року. Конвенція являє собою правоохоронний договір, призначений для розробки спільної кримінально-правової політики, спрямованої на визначення, покарання та тим самим стримування злочинів, пов'язаних із кіберзлочинністю. Згідно CEC держави мають прийняти закони, що передбачають кримінальну відповідальність за наступними п'ятьма видами дій проти цілісності кіберсистем: незаконний доступ; нелегальне перехоплення; втручання у дані; втручання у систему; зловживання пристроями.

Конвенція про кібербезпеку визначає загальні принципи міжнародного співробітництва. Сторони співробітничають між собою у найширших обсягах відповідно до принципів Конвенції шляхом застосування відповідних міжнародних документів щодо міжнародного співробітництва у кримінальних питаннях, угод, укладених на основі єдиного чи взаємного законодавства, і внутрішньодержавного законодавства, з метою розслідування або переслідування кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними або з метою збирання доказів у електронній формі, які стосуються кримінальних правопорушень.

Аналізуючи Конвенцію можна дійти висновку, що її метою є заохочення укладення або доповнення державами двосторонніх, багатосторонніх договорів, зокрема мова йде про Європейську конвенцію

про екстрадицію, відкритої для підписання у Парижі 13 грудня 1957 року, Європейську конвенцію про взаємну допомогу у кримінальних справах, відкриту для підписання у Страсбурзі 20 квітня 1959 року та Додатковий протокол до Європейської конвенції про взаємну допомогу у кримінальних справах, відкритого для підписання у Страсбурзі 17 березня 1978 року. Якщо держави підписують двосторонню або багатосторонню угоду, то вона вважається такою, яка має примат над Конвенцією, але така угода не має суперечити її цілям та принципам.

Як висновок, можна сказати, що в даний час не існує всеосяжної міжнародно-правової бази щодо кібербезпеки. Міжнародні зусилля концентруються на вузькій сфері питань, в першу чергу стосуються конфіденційності даних і прав людини, замість реалізації більш широких заходів, спрямованих на встановлення і диференціацію різних рівнів кіберагресії і кодифікацію міжнародних підходів до вирішення цієї проблеми. Ці недоліки можуть бути частково обумовлені самою природою хакерської атаки, яка кидає виклик концептуальним категоріям, які ми досі використовуємо для недопущення хаосу і підтримки порядку в нашому суспільстві і в нашому житті. Без всеосяжного міжнародного визначення типів кіберагресій, країни будуть продовжувати стикатися з труднощами в оцінці законності своєї реакції на такі атаки. На довершення всього, не існує міжнародних органів, уповноважених розслідувати і переслідувати в судовому порядку випадки кіберагресії, які при виробленні відповіді на хакерські атаки були б не обмежені принципом територіальної юрисдикції, прийнятим в правовій системі країни нападу. Протидії кіберагресії заважає той факт, що міжнародне право не визнає обов'язок надавати допомогу іншим державам в розслідуванні випадків подібного роду за відсутності відповідної домовленості між сторонами.

4. Виявлено такі особливості організаційно-правового механізму міжнародного співробітництва держав у сфері забезпечення кібербезпеки на світовому рівні: Основними напрямами співпраці між національними

урядами в сфері кібербезпеки, як уже було сказано, є обмін інформацією, розслідування нападів або злочинів, запобігання або зупинка шкідливої поведінки, надання доказів і навіть організація передачі осіб до запитуючої держави.

Всесвітніми організаціями, які працюють у сфері забезпечення кібербезпеки є ООН, Група 8, Міжнародний союз електрозв'язку, ОЕСР, Інтерпол. Вони вирішують глобальні питання, що стосуються забезпечення кібербезпеки.

5. Виявлено такі особливості організаційно-правового механізму міжнародного співробітництва держав у сфері забезпечення кібербезпеки на регіональному рівні. На додаток до міжнародних організацій, які в усьому світі активно співпрацюють у сфері забезпечення кібербезпеки, ряд міжнародних організацій в окремих регіонах також зосереджені на діяльності вирішення питань, пов'язаних з кіберзлочинністю. Так, на регіональному рівні цими питаннями займаються Рада Європи, ЄС, Співдружність, Азіатсько-тихоокеанське економічне співробітництво (АТЕС), Ліга арабських держав (ЛАД), Організація американських держав (ОАД), Організація Східнокарибських держав, Тихоокеанський регіон.

6. Охарактеризовано участь України в міжнародно-правовому співробітництві у сфері забезпечення кібербезпеки. Була ухвалена Національна стратегія україни із забезпечення кібербезпеки. Ключовим кроком у реалізації Стратегії було створення Національного координаційного центру з кібербезпеки у червні 2016 р., який є робочим органом Ради національної безпеки і оборони. В 2017 році Верховна Рада України ухвалила законопроект "Про основні засади забезпечення кібербезпеки України" – робота над ним тривала понад два роки. Закон є надзвичайно важливим з точки зору створення системи забезпечення кібербезпеки держави в цілому. У ньому визначено, кого і що мають захищати від кібератак та хто це має робити. Під захист потрапляють комунікаційні системи, якими, зокрема, користуються органи влади і

правопорядку, та ресурси у сферах електронного урядування і комерції. Крім того, захищеними мають бути "критично важливі об'єкти інфраструктури", під якими законодавці розуміють цілу низку підприємств і установ, наприклад, у галузі енергетики, інфраструктури, банківського сектору, стратегічних підприємств. Перевіряти дотримання інформаційної безпеки будуть за допомогою незалежного аудиту, що має проходити за стандартами ЄС та НАТО. В сфері кібербезпеки Україна також співпрацює з Цільовим фондом НАТО з питань кіберзахисту, є партнером спільних проектів Європейського Союзу та Ради Європи "CyberCrime EAP II" та "CyberCrime EAP III", які мають регіональний аспект та включають країни Східного партнерства.

7. Розроблено такі пропозиції з вдосконалення міжнародно-правового регулювання співробітництва держав у сфері забезпечення кібербезпеки шляхом створення єдиної міжнародної системи захисту і моніторингу: створення міжнародної організації із забезпечення кібербезпеки. Метою організації є забезпечення кібербезпеки як на національному, так і на міжнародному рівнях. Цілі організації являють собою попередженння кіберзлочинів, розлідування та боротьбу з ними. Завданнями організації є:

1. Посилити захист критично важливої інформаційної інфраструктури (КІІ) проти кібер-атак. 2. Запобігання та реагування на загрози та інциденти, пов'язані з кібербезпекою одним з органів Органзації – міжнародною кіберполіцією Організації. Спеціально створені групи експертів в рамках цього органу проводитимуть розслідування загроз та інцидентів, пов'язаних із кібербезпекою, для визначення їх впливу та запобігання подальшій шкоді або інцидентам кібербезпеки. 3. Полегшення обміну інформацією, що стосується кіберзлочинів та кібербезпеки шляхом створення представництва в кожній державі-члені. Це є надзвичайно важливим, оскільки своєчасна інформація допомагає урядам та власникам комп'ютерних систем виявляти вразливі місця та запобігати ефективним випадкам кібер-інцидентів. 4. Беручи до уваги міжнародний характер

кіберзлочинності, гармонізація національних законів і технік. Проте гармонізація повинна враховувати регіональний попит та потенціал. 5. Впровадження правових, технічних та процесуальних заходів в боротьбі з кіберзлочинністю. 6. Допомога країнам у вирішенні законодавчих завдань, спричинених злочинною діяльністю, яка здійснюється через мережі ІКТ шляхом розроблення Конвеції, яка у порівнянні з Конвенцією Ради Європи була би чіткішою по відношенню до покарання кіберзлочинців. Розробка законодавства для криміналізації певної поведінки або запровадження розслідувальних документів є досить незвичайним для більшості країн. Регулярна процедура полягає в першу чергу в запровадженні стратегії, яка визначає різні інструменти, що використовуються для вирішення проблеми. В рамках різноманітних підходів до гармонізації законів про кіберзлочинність мало уваги приділялося не лише інтеграції законодавства в національну законодавчу базу, а й включенні його у існуючу політику або розробку такої політики вперше. Як наслідок, деякі країни, які запровадили законодавство про кіберзлочинність без розробки стратегії боротьби з кіберзлочинністю, а також політики на рівні уряду, зіткнулися з серйозними труднощами. В основному це було результатом відсутності заходів щодо попередження злочинності, а також дублювання різних заходів.

8. Розроблено пропозиції з вдосконалення міжнародно-правового регулювання співробітництва держав у сфері забезпечення кібербезпеки шляхом вдосконалення національного законодавства держав. Кожна держава повинна прийняти стратегію із забезпечення кібербезпеки і втілювати її в життя, приділити увагу законодавству у цій сфері, визначити та конкретизувати перелік кіберзлочинів та покарань, налагодити роботу відповідних органів із забезпечення кібербезпеки, активно співпрацювати з іншими державами та міжнародними організаціями.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. R. T. Slivka. Methods and Problems in Computer Security // Journal of Computers and Law. – 1975. – p. 217.
2. V. McLaughlin. Computer Crime: The Ribicoff Amendment to United States Code // Criminal Justice Journal. – 1978. – №2. – p. 217.
3. M. E. Kabay. A Brief History of Computer Crime: An Introduction for Students. 2008. – p. 5. available at:www.mekabay.com/overviews/history.pdf.
4. Quinn. Computer Crime: A Growing Corporate Dilemma // The Maryland Law Forum. – 1978. – №8. – p. 48.
5. Stevens. Identifying and Charging Computer Crimes in the Military // Military Law Review. – 1985. – p. 59.
6. Gemignani. Computer Crime: The Law in ’80 // Indiana Law Review. – 1980. – №13. – p. 681.

7. V. McLaughlin. Computer Crime: The Ribicoff Amendment to United States Code // Criminal Justice Journal. – 1978. – №2. – p. 217.
8. Kabay. A Brief History of Computer Crime: An Introduction for Students, 2008, page 5, available at: www.mekabay.com/overviews/history.pdf.
9. Freed, Materials and cases on computer and law, 1971, page 65.
10. McLaughlin, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, Vol. 2, page 217 et seq.; Bequai, Computer Crime: A Growing and Serious Problem, Police Law Quarterly, Vol. 6, 1977, page 22.
11. Nycum. Legal Problems of Computer Abuse // Washington University Law Quarterly, 1977, page 527.
12. Schjolberg. Computers and Penal Legislation, A study of the legal politics and a new technology, 1983, page 6, available at: www.cybercrimelaw.net/documents/Strasbourg.pdf.
13. Elizabeth A. Glynn. Computer Abuse: The Emerging Crime and the Need for Legislation, Fordham Urban Law Journal, 1983, page 73.
14. Лукацкий А. Хакеры управляют реактором [Електрон. ресурс] / А. Лукацкий; Центр исследований компьютерной преступности - Режим доступу : http://www.crime-research.ru/library/Lukac0103.html
15. Kabay. A Brief History of Computer Crime: An Introduction for Students, 2008, page 23, available at: www.mekabay.com/overviews/history.pdf.
16. Schjolberg. Computer-related Offences, Council of Europe, 2004, page 4, available at: www.cybercrimelaw.net/documents/Strasbourg.pdf.
17. European committee on crime problems (1990) “Computer-related crime. Recommendation No. R (89) 9 on computer-related crime and final report of European committee on crime problems”. Stasbourg 1990. p. 60 (Accessed 30 April 2014).
18. Sofaer/Goodman, Cyber Crime and Security – The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7.

19. Child Pornography, CSEC World Congress Yokohama Conference, 2001, page 17; Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 9.
20. Резолюція 45/113 Генеральної Асамблеї ООН від 14 грудня 1990 року / [Електронний ресурс] – Режим доступу: http://zakon4.rada.gov.ua/laws/show/995_204
21. Кураков Л. П. Информация как обьект правовой защиты // Москва: Гелиос, 1998 - С. 220-221
22. Goodman M. D., Brenner S. W. The Emerging Consensus on Criminal Conduct in Cyberspace // UCLA J.L. & Tech. – 2002. №3 [Електронний ресурс] – Режим доступу: http://www.lawtechjournal.com/articles/ 2002/03_020625_goodmanbrenner.php
23. Про киберпреступления: Европейская Конвенция от 23 ноября 2001 г. / [Електронний ресурс] – Режим доступу: http://www.eos.ru/eos_delopr/eos_law/detail.php?ID=32003&SECTION_ID=671
24. Государственные стратегии кибербезопасности [Електронний ресурс] – Режим доступу: http://www.bezpeka.com/ru/lib/sec/gen/government-cybersecurity-strategy.html
25. Европейский центр борьбы с киберпреступностью отчитался за первый год работы / [Електронний ресурс] – Режим доступу: http://www.interfax.ru/world/357250
26. William M. Stahl. The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity, 40 Ga. J. Int'l & Comp. L. 247 (2011). Available at: http://digitalcommons.law.uga.edu/gjicl/vol40/iss1/9
27. Nhan/Bachmann in Maguire/Okada (eds). Critical Issues in Crime and Justice, 2011, page 166.

28. Crimes related to computer networks. Background paper for the workshop on crimes related to the computer network, // 10th UN Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.187/10, page 5; available at: www.uncjin.org/Documents/congr10/10e.pdf.
29. Про Основні засади забезпечення кібербезпеки України: Наказ від 05.10.2017 № 2163-19 Режим доступу: http://zakon3.rada.gov.ua/laws/show/2163-19 (дата звернення: 10.10.2017)
30. Gordon/Ford. On the Definition and Classification of Cybercrime // Journal in Computer Virology. Vol. 2, No. 1, 2006, page 13-20.
31. Taylor. Hacktivism: In Search of lost ethics? // Crime and the Internet. 2001, page 61.
32. Joyner/Lotrionte. Information Warfare as International Coercion: Elements of a Legal Framework // EJIL 2002, No5 – page 825.
33. Annual Report to Congress on Foreign Economic Collection and Industrial Espionage – 2003, page 1, available at: www.ncix.gov/publications/reports/fecie_all/fecie_2003/fecie_2003.pdf.
34. Granger. Social Engineering Fundamentals, Part I: Hacker Tactics // Security Focus. 2001. available at: www.securityfocus.com/infocus/1527
35. High-Level Experts Group:Global Strategic Report. ITU Global Cybersecurity Agenda. 2008, page 31, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.
36. Sieber. Council of Europe Organised Crime Report 2004, page 102
37. Kabay. A Brief History of Computer Crime // An Introduction for Students. 2008. p. 23. available at: www.mekabay.com/overviews/history.pdf.
38. Critical Infrastructure Protection Department Of Homeland Security Faces Challenges In Fulfilling Cybersecurity Responsibilities // GAO,

2005 GAO-05-434, page 12, available at: www.gao.gov/new.items/d05434.pdf.

39. Cohen. Freedom of Speech and Press: Exceptions to the First Amendment // CRS Report for Congress. 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf
40. Johannesburg Principles on National Security, Freedom of Expression and Access to Information. §§ 3.2.6 and 3.2.7.
41. Reidenberg. States and Internet Enforcement // University of Ottawa Law & Technology Journal. Vol. 1, No. 213, 2004, page 213 et seq., available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965
42. Stadler. Multimedia und Recht 2002, p. 343 et seq.
43. Haraszti, Preface. In Governing the Internet Freedom and Regulation in the OSCE Region, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.
44. Roth. State Sovereignty // International Legality and Moral Disagreement. 2005. p. 1, available at: www.law.uga.edu/intl/roth.pdf.
45. Lanning. Child Molesters // A Behavioral Analysis. 2001. p. 63.
46. US House of Representatives. Sexual Exploitation of Children over the Internet // Report for the use of the Committee on Energy and Commerce. 109th Congress.2007. p. 8.
47. Eneman. A Critical Study of ISP Filtering Child Pornography, 2006, page 1.
48. ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 34, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.
49. United Nations Convention on the Right of the Child, A/RES/44/25, available at: www.hrweb.org/legal/child.html.
50. Council Framework Decision on combating the sexual exploitation of children and child pornography, 2004/68/JHA, available at: http://eur-

lex.europa.eu/LexUriServ/site/en/oj/2004/l_013/l_01320040120en00440048.pdf.

51. Wolak, Finkelhor, Mitchell. Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online // Victimization Study, 2005, page 5, available at: www.missingkids.com/en_US/publications/NC144.pdf
52. Tsesis. Prohibiting Incitement on the Internet // Virginia Journal of Law and Technology. Vol. 7. 2002, available at: www.vjolt.net/vol7/issue2/v7i2_a05-Tsesis.pdf.
53. Van Houweling. Enforcement of Foreign Judgements // Michigan Journal of International Law, 2003, page 697.
54. The Times Online, 70.000 gather for violent Pakistan cartoons protest, available at: www.timesonline.co.uk/tol/news/world/asia/article731005.ece
55. Landes. The Prohibition Of Internet Gambling And A Proposed System Of Regulation // Layovers And Cargo Ships. p. 915, available at: www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf
56. Olson. Betting No End to Internet Gambling, Journal of Technology Law and Policy, Vol. 4, Issue 1, 1999, available at: http://grove.ufl.edu/~techlaw/vol4/issue1/olson.html.
57. Sieber. Council of Europe Organised Crime Report 2004, page 105
58. Sunner. Security Landscape Update 2007, page 3, available at: www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/session2-sunner-C5-meeting-14-may-2007.pdf.
59. Lui, Stamm. Fighting Unicode // Obfuscated Spam. 2007. p. 1, available at: www.ecrimeresearch.org/2007/proceedings/p45_liu.pdf.
60. De Clippele. Legal aspects of online pharmacies // Acta Chir Belg. 2004. p. 364, available at: www.belsurg.org/imgupload/RBSS/DeClippele_0404.pdf

61. Sieber. Council of Europe Organised Crime Report 2004, page 148.
62. The Recording Industry 2006 // Privacy Report, page 4, available at: www.ifpi.org/content/library/piracy-report2006.pdf.
63. ITU Global Cybersecurity Agenda // High-Level Experts Group, Global Strategic Report, 2008, page 39, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.
64. ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 39, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.
65. Gercke. Cyberterrorism, How Terrorists Use the Internet // Computer und Recht. 2007, page 62
66. John Markoff. Step Taken to End Impasse Over Cybersecurity Talks // New York Times. July 17. 2010,
67. Abraham D. Sofaer and Seymour E. Goodman. A Proposal for an International Convention on Cyber Crime and Terrorism // CISAC, Aug. 2000
68. Richard A. Clarke and Robert K. Knake. Cyber War // New York: Harper Collins 2010. p. 270.
69. Citizen's guide to the 2010 financial report of the united states government // Government Accountability Office Auditor's Report. 2010. p. 8-17.
70. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: Резолюция 60/45, принятая Генеральной Ассамблеей Организации Объединенных Наций.
71. Developments in the field of information and telecommunications in the context of international security: Item 94 of the provisional list (A/65/100).
72. Про кіберзлочинність: Конвенція від 23 листопада 2001 р. – Ст. 2-6.
73. Про кіберзлочинність: Конвенція від 23 листопада 2001 р. – Ст. 7-10.
74. Про кіберзлочинність: Конвенція від 23 листопада 2001 р. – Ст. 14.

75.Про кіберзлочинність: Конвенція від 23 листопада 2001 р. – Ст. 42.
76.Про кіберзлочинність: Конвенція від 23 листопада 2001 р. – Ст. 23.
77.Про кіберзлочинність: Конвенція від 23 листопада 2001 р. – Ст. 24, п. 1-3.
78.Про кіберзлочинність: Конвенція від 23 листопада 2001 р. – Ст. 24, п. 6.
79.Про кіберзлочинність: Конвенція від 23 листопада 2001 р. – Ст. 25, п. 1
80.Про кіберзлочинність: Конвенція від 23 листопада 2001 р. – Ст. 25, п. 3.
81.Про кіберзлочинність: Конвенція від 23 листопада 2001 р. – Ст. 29, п.1.
82.Про кіберзлочинність: Конвенція від 23 листопада 2001 р. – Ст. 30, п. 1.
83.Про кіберзлочинність: Конвенція від 23 листопада 2001 р. – Ст.37, п. 1.
84.Про кіберзлочинність: Конвенція від 23 листопада 2001 р. – Ст. 45, п. 2.
85.О сотрудничестве в области обеспечения международной информационной безопасности: соглашение между правительствами государств — членов шанхайской организации сотрудничества от 5 января 2012 г. – Ст. 4
86.Cyberspace Policy Review // Border Security Publications2009. p. 20-21 // Електронний режим доступу: https://www.dhs.gov/publication/2009-cyberspace-policy-review
87.Citizen’s guide to the 2010 financial report of the united states government // Government Accountability Office Auditor’s Report. 2010. p. 36-37

88. United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005. Chapter 6. page 233. available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.
89. Communique of the Ministerial Conference of the G8 Countries on Combating Transnational Organized Crime // Moscow, 19-20 October 1999.
90. G8. Government-Industry Workshop on Safety And Security In Cyberspace, Tokyo, May 2001.
91. United States National Research Council, Information Technology for Counterterrorism: Immediate Actions and Future Possibilities. 2003. p. 11
92. ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 17, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.
93. Final Declaration of the 2009 G8 ministerial meeting of Justice and Home Affairs, Rome, p. 6, available at: www.g8italia2009.it/static/G8_Allegato/declaration1giu2009,0.pdf.
94. Final Declaration of the 2009 G8 ministerial meeting of Justice and Home Affairs, Rome, page 7, available at: www.g8italia2009.it/static/G8_Allegato/declaration1giu2009,0.pdf.
95. A/RES/44/25, adopted by the UN General Assembly on 12 December 1989
96. 1008 A/RES/45/121, adopted by the UN General Assembly on 14 December 1990. The full text of the resolution is available at: www.un.org/documents/ga/res/45/a45r121.htm.
97. Report of the tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.185/15, No. 165, available at: www.uncjin.org/Documents/congr10/15e.pdf.
98. Report of the tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 2000. A/RES/55/63.

99. Report of the tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 2000. A/RES/56/121. The full text of the resolution is available at: http://daccessdds.un.org/doc/UNDOC/GEN/N01/482/04/PDF/N0148204.pdf.

100. Report of the Western Asian Regional Preparatory Meeting for the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, A/CONF.2003/RPM.4/1, No. 14.

101. Declaration Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice, available at: www.unodc.org/pdf/crime/congress11/BangkokDeclaration.pdf.

102. Contribution of the Secretary General of the Council of Europe to the twelfth United Nations Congress on Crime Prevention and Criminal Justice, Information Documents SG/Inf(2010)4, 16.02.2010, page 17 et seq.

103. Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructure // Contribution of the Secretary General of the Council of Europe to the twelfth United Nations Congress on Crime Prevention and Criminal Justice, Information Documents A/RES/64/211.

104. Contribution of the Secretary General of the Council of Europe to the twelfth United Nations Congress on Crime Prevention and Criminal Justice, Information Documents // Resolutions 55/63 and 56/121.

105. Contribution of the Secretary General of the Council of Europe to the twelfth United Nations Congress on Crime Prevention and Criminal Justice, Information Documents // Resolutions 57/239 and 58/199.

106. The report on the meeting of the open-ended working group (UNODC/CCPCJ/EG.4/2011/3) is available at: www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2

011/UNODC_CCPCJ_EG4_2011_3/UNODC_C
CPCJ_EG4_2011_3_E.pdf.

107. Draft topics for consideration in a comprehensive study on the impact of and response to cybercrime, UNODC/CCPCJ/EG.4/2011/2. The document is available at:
www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/UNODC_
CCPCJ_EG4_2011_2/UNODC_CCPCJ_EG4_2011_2_E.pdf.

108. ECOSOC Resolution 2004/26, on International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes

109. WSIS Geneva Plan of Action, 2003, available at: www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1160|0.

110. WSIS Tunis Agenda for the Information Society, 2005, available at: www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0.

111. For more information on Action Line C5, see: www.itu.int/wsis/c5/, and also the meeting report of the second Facilitation Meeting for WSIS Action Line C5, 2007, p. 1, available at:
www.itu.int/osg/csd/cybersecurity/pgc/2007/events/docs/meetingreport.pdf

112. Gercke. Zeitschrift fuer Urheber- und Medienrecht, 2009, Issue 7, page 533.

113. Gercke. National, Regional and International Approaches in the Fight against Cybercrime // Computer Law Review International, 2008, Issue 1, page 7

114. United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at:
www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

115. Recommendation No. R (89) 9, adopted by the Committee of Ministers on 13 September 1989 at the 428th Meeting of the Ministers Deputies.

116. Recommendation No. R (95) 13, adopted by the Committee of Ministers on 11 September 1995 at the 543rd Meeting of the Ministers Deputies.

117. Gercke. The Slow Awake of a Global Approach Against Cybercrime // Computer Law Review International, 2006, 140 et seq.; Gercke, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 et seq.; Aldesco,

118. United Nations Conference on Trade and Development, Information Economy Report 2005 // UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 234, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

119. Whitcomb, An Historical Perspective of Digital Evidence: A Forensic Scientist's View // International Journal of Digital Evidence. 2002, Vol. 1, No. 1.

120. Stockholm Programme, An open and secure Europe serving and protecting the citizens, 2009, No. 3.3.1.

121. Decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999.

122. Communication of 8 December 1999 on a Commission initiative for The Lisbon Special European Council, 23 and 24 March 2000 – eEurope – An information society for all – COM 1999, 687.

123. Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions – Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, 26.1.2001, COM(2000) 890.

124. Network and Information Security – A European Policy approach – adopted 6 June 2001.

125. ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 17, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

126. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000.

127. Lindholm, Maennel. Computer Law Review International 2000, 65.

128. Gercke. Impact of the Lisbon Treaty on Fighting Cybercrime in the EU // Computer Law Review International, 2010, page 75 et seq.

129. Decision No. 276/1999/EC of the European Parliament and of the Council of 25, January 1999.

130. Art. 4 of the Framework Decision of the European Parliament and of the Council of 25, January 1999.

131. Gercke. The Development of Cybercrime Law in 2005 // Zeitschrift fuer Urheber- und Medienrecht 2006, page 286.

132. Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism.

133. Report to Leaders and Ministers on Actions of the Telecommunications and Information Working Group to Address Cybercrime and Cybersecurity, 2003/AMM/017.

134. United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

135. Regional Conference Booklet on: Cybercrime, Morocco, 2007, page 6, available at: www.pogar.org/publications/ruleoflaw/cybercrime-09e.pdf.

136. Deshko L. Structural Elements of International Legal Mechanisms for Ensuring The Everyone's Right to Seek Rights Protection in International Judicial Institutions or in the Relevant Bodies of

International Organizations // Закон и жизнь. – 2013. – №12/3. – С. 64-67.

137. Дешко Л. Критерії ефективності національного засобу юридичного захисту щодо невиконання чи затримок у виконанні рішень національних судів (за матеріалами практики Європейського суду з прав людини) / Л. Дешко // Правничий часопис Донецького Університету. – 2012. – №1. – С. 84-91.

138. Deshko L. The Subjective Legal Right Structure to Apply to the International Judicial Institutions or to the Relevant Bodies of International Organizations / Материалы Международной научно-практической конференции «Ценности и интересы современного общества» (14 ноября 2013 г., г. Москва) [Електронний ресурс]. – Режим доступу: http://www.mesi.ru/our/ events/detail/124931/

139. Дешко Л.М. Конституційне право на звернення до міжнародних судових установ та міжнародних організацій: монографія / Л.М. Дешко. – Ужгород, 2016. – 486 с.

140. Кримінальний кодекс України: Закон України від 05.04.2001 р. // Відомості Верховної Ради України. – 2001. – №25. – Ст. 131.

141. Anton Cherepanov. Analysis of TeleBots' cunning backdoor. // We livesecurity magazine. – 2017. – 4 July. [Електронний ресурс]. – Режим доступу: https://www.welivesecurity.com/2017/07/04/analysis-of-telebots-cunning-backdoor/

142. Michael Schmitt and Lieutenant Colonel Jeffrey Biller (2017-07-11). The NotPetya Cyber Operation as a Case Study. [Електронний ресурс]. – Режим доступу: https://medium.com/@rsatter/cyberattacks-healthcare-and-international-law-65f09e259d8.

143. Пирет Перник. What Ukraine needs to defend against cyber, information and psychological operations. // International centre for defense and security – 2014. – September. [Електронний ресурс]. –

Режим доступу: https://www.icds.ee/ru/blog/article/what-ukraine-needs-to-defend-against-cyber-information-and-psychological-operations/

144. Про Стратегію кібербезпеки України: Указ президента від 27 січня 2016 р. // Відомості Верховної Ради України. – 2016. – № 96 – Ст. 4.

145. Oleksii Tkachenko. Cybersecurity in Ukraine: National Strategy and international cooperation // The Global Cyber Expertise Magazine. – 2017. – May. – 3d issue.

146. Про Національний координаційний центр кібербезпеки: Указ Президента України від 7 червня 2016 р. // Відомості Верховної Ради України. – 2016. – №242.

147. Про національну поліцію: Закон України від 2 липня 2015 р. // Відомості Верховної Ради України. – 2015. – №40-41. – Ст. 379.

148. Nikolai Holmov. Cyber security/cyber defence Ukraine // Structural changes ahead. – 2017. – November. [Електронний ресурс]. – Режим доступу: http://www.odessatalk.com/2017/11/cyber-securitycyber-defence-ukraine-structural-changes-ahead/

149. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. // Відомості Верховної Ради України. – 2017. – №45. – Ст. 1, п. 15.

150. Про кіберзлочинність: Конвенція від 23 листопада 2001 р. // Відомості Верховної Ради України. – 2001.

151. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 7 вересня 2005 року. // Відомості Верховної Ради України. – 2005. – № 2824-IV.

152. Assessment report on international cooperation in cybercrime in the EAP region, September 2016 // Reports under CybeCrime EAP II – 2016. – September. – P. 3-4.

153. Cybercrime strategies, procedural powers and specialised institutions in the Eastern Partnership region – state of play, June 2017 // Reports under CybeCrime EAP III – 2017. – June. – P. 6.

154. Про реалізацію Трастового фонду Україна ? НАТО з питань кібербезпеки між Службою безпеки України та Румунською службою інформації: Угода від 23 липня 2015 р. // Відомості Верховної Ради України. – 2015. – Ст. 5.

155. Comprehensive Study on Cybercrime // United nations office on drugs and crime: Draft—February 2013. P. 56-57.

156. Comprehensive Study on Cybercrime // United nations office on drugs and crime: Draft—February 2013. P. 58.