Київський національний торговельно-економічний університет

Кафедра міжнародного публічного права

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

МІЖНАРОДНО-ПРАВОВЕ РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Студентки 2 курсу, 10мз групи,
спеціальності 293 «Міжнародне право»,
спеціалізації «Міжнародне право» _____ Домченко Олесі Олександрівни

Науковий керівник
кандидат юридичних наук, доцент _____ Буличева Наталія Анатоліївна

Керівник освітньо-професійної програми
доктор юридичних наук, доцент _____ Дешко Людмила Миколаївна

Київ 2018

ЗМІСТ

Перелік умовних позначень

AES – алгоритм симетричного ключа

API – прикладний програмний інтерфейс

ARPANET – Мережа Агентства передових досліджень(англ. Advanced Research Projects Agency Network).

CERT – Команда реагування на комп'ютерні надзвичайні події (англ. Computer Emergency Response Team)

ENIAC – електронний цифровий інтегратор і комп'ютер

ENISA – Європейське агентство з питань мережевої та інформаційної безпеки

GGE – Група урядових експертів

IEC – Міжнародна електротехнічна комісія

IP – міжмережевий протокол, набір протоколів мережі Інтернет (англ. Internet Protocol).

ISACA – Асоціація аудиту і контролю інформаційних систем

ISO – Міжнародна організація зі стандартизації (англ. International Organization for Standardization)

NCP – перший стандарт мережевого протоколу мережі ARPANET (Network Control Protocol)

TCP –протокол керування передаванням (англ. Transmission Control Protocol)

ATEC – форум економік Тихоокеанського узбережжя (англ. The Asia-Pacific Economic Cooperation)

АТР – Азіатсько-Тихоокеанський регіон

ІБ – інформаційна безпека

ІКТ – інформаційно-комунікаційні технології

ІС – інформаційна система

ІТ – інформаційні технології

ККУ – Кримінальний кодекс України

КСЗІ – комплексна система захисту інформації

МАГАТЕ – Міжнародне агентство з атомної енергії

НД ТЗІ – державний стандарт технічного захисту інформації

ОАД – Організація Американських Держав (англ. Organization of American States,)

ОЕСР – Організація економічного співробітництва і розвитку

ПЕК – Паливно-енергетичний комплекс

ПК – персональний комп’ютер

ППОС – Процесу планування та оцінки сил

СУІБ – системи управління інформаційною безпекою

ШОС – Шанхайська організація співробітництва

ЮНДП – Програма розвитку ООН (англ. UNDP, United Nations Development Programme)

ЮНЕСКО – Організація Об'єднаних Націй з питань освіти, науки і культури

ЮНКТАД – Конференція ООН з торгівлі та розвитку

ВСТУП

Актуальність теми. Широке використання інформаційних технологій, практично в усіх сферах людської діяльності, було викликано «комп'ютеризацією суспільства». Багато хто називає цей період «інформаційною ерою». Актуальність теми полягає в тому, що в міжнародному співтоваристві країн, на різних рівнях, визнано факт подвійного використання високих (найновіших, найпрогресивніших) технологій сучасності, тобто існує необхідність обмеження військового застосування досягнень науки й техніки і запобігання неконтрольованому поширенню інформаційних озброєнь. Співробітництво у сфері інформаційної безпеки потребує пошуку спільних рішень щодо протидії інформаційним і кіберзагрозам. Сьогодні все більше поєднуються інформаційні та комунікаційні технології, пристрої та послуги для повсякденного життя. Глобальна спільнота все частіше використовує ІКТ, як для суспільного, так і для економічного розвитку. Уряди у всьому світі визнають що ІКТ мають силу впливати на подальше процвітання та благополуччя їх громадян. Також вони визнають що інформаційна безпека повинна бути невід'ємною і нерозривною частиною технологічного прогресу. Однак, як і в реальному світі, кібер-світ зазнає впливу різноманітних небезк та загроз, які можуть спричинити до великих збитків.

Внаслідок зростаючої залежності світу від інформаційних систем, створюються нові проблеми інфомаційної безпеки. Це вимагає дуже серйозної уваги не тільки з боку кожної держави, а й з боку всього міжнародного співтовариства. Досягнення щодо інформаційної безпеки будуть втілені завдяки міжнародній співпраці. Ключова проблема полягає у відсутності повноцінної міжнародно-правової бази, яка б регулювала діяльність держав в даній сфері. Це створює серйозні проблеми для правоохоронних органів у всьому світі.

Масштаб інформаційних та кіберзлочинів, за останній час, значно зріс, потрібно розвивати інформаційну безпеку, щоб зменшити загрози та підвищити довіру до використання електронних комунікацій. Тому зрозуміло, що існує

прямий причинно-наслідковий принцип між розвитком ІКТ і їх незаконним та шкідливим використанням. Щоб протидіяти цьому ефекту, інформаційна безпека стає дедалі актуальнішим поняттям.

Наразі приймають різні рішення та доктрини, пов'язані з інформаційною та кібербезпекою майже у всіх країнах світу для захисту цих сфер.

Проте між країнами все ще існує помітний розрив з точки зору поінформованості, розуміння, знання та, нарешті, здатність розгортати відповідні стратегії, можливості та програми для забезпечення і належного використання ІКТ як сприятливих умов для економічного розвитку.

Питання в сфері інформаційної безпеки аналізуються у працях В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа, О.А. Баранов, Д. Франсело, І.В. Діордіца, Д. Дубова, Ю.Ю. Орлов, Я. Малик, Б.А. Кормич.

Мета та завдання дослідження. *Мета роботи* полягає в тому, щоб на основі аналізу наукових джерел, розробок, а також узагальнення та систематизації міжнародно-правового регулювання інформаційної безпеки держави, сформулювати пропозиції та рекомендації з удосконалення законодавства України щодо впровадження нових та підвищення ефективності існуючих механізмів інформаційної безпеки, протидії інформаційним та кіберзагрозам.

Для досягнення мети дипломної роботи необхідно вирішити такі *завдання*:

1. охарактеризувати становлення та розвиток «інформаційного простору» в міжнародному праві;
2. визначити поняття та зміст інформаційної безпеки та кібербезпеки;
3. обґрунтувати різницю між кібербезпекою та інформаційною безпекою;
4. проаналізувати міжнародно-правові акти в сфері інформаційної безпеки та кібербезпеки;
5. виявити особливості організаційно-правового механізму міжнародного співробітництва держав у сфері забезпечення інформаційної безпеки;
6. з’ясувати сутність кіберзлочинності та кібертероризму як загроз інформаційній безпеці у міжнародному праві;

7. проаналізувати стан державної політики у сфері інформаційної безпеки в Україні;
8. навести пропозиції щодо удосконалення міжнародного співробітництва в сфері інформаційної безпеки;
9. сформулювати рекомендації з удосконалення законодавства України у сфері інформаційної безпеки.

Об'єкт дослідження – міждержавні відносини, які виникають при здійсненні інформаційної безпеки.

Предмет дослідження – міжнародно-правове регулювання забезпечення інформаційної безпеки держави.

Методи дослідження. Методологічною основою дослідження стали загальні методи наукового пізнання, а також такі, що застосовуються в юридичній науці: методи аналізу і синтезу, історико-логічний, моделювання, логіко-симантичний тощо. Для теоретичного осмислення застосуємо методи: аналізу і синтезу (для поглиблення загального понятійного апарату), історико-логічний метод (становлення та розвиток інформаційного простору). До наукового осмислення застосуємо методи: логіко-семантичний метод (обґрунтувати визначення інфомаційної бепеки та кібербезпеки, поняття кіберзлочину та його види), моделювання (визначення моделі інформаційної безпеки у світі), порівняльно-правовий метод (поріняння положеннь вітчизняного та зарубіжного законодавства), абстрагування й узагальнення (визначення шляхів вдосконалення державної політики України щодо інформаційної безпеки).

Нормативну базу дослідження становлять міжнародні договори, міжнародні конвенції, правотворчі рішення міжнародних організацій та їх органів, нормативно-правові акти, пов'язані з реалізацією міжнародної та державної політики у сфері інформаційної безпеки, наукові дослідження учених в сфері інформаційної безпеки та кібербезпеки, закони України.

Наукова новизна одержаних результатів полягає в наведенні положеннь, висновків, рекомендацій та пропозицій спрямованих на вдосконалення міжнародного співробітництва та державної політики України в сфері

інформаційної безпеки. Основні результати, які були отримані в процесі вирішення поставлених завдань та становлять наукову новизну дослідження, полягають у наступному:

– виявлено та охарактеризовано процес становлення та розвитку інформаційного простору. Міжнародний інформаційний простір це сукупність складних інформаційних технологій, які є основою і визначальним компонентом промислово-економічного комплексу транснаціональних спільнот, які впливають на формування світоглядних процесів у суспільстві. Головними періодами становлення інформаційного простору є: 1940-1960 рр. – пов'язані з винаходом і впровадженням в практичну діяльність електронно-обчислювальних машин (комп'ютерів); 1970-1980 рр. – поява перших персональних комп'ютерів, було створено «Інтернет» та почався розвиток інформаційної безпеки; 1990-2000 рр. – Інтернет став загальнодоступним для звичайних користувачів, з'явився знаменитий Веб-браузер NCSA Mosaic. Всесвітня павутина ставала дедалі популярнішою;
– уточнено поняття інформаційної безпеки та кібербезпеки і обґрунтувано різницю між кібербезпекою та інформаційною безпекою: кібербезпека – це інформаційні технології, пов'язані з безпекою комп'ютерних систем та інформації (обладнання та програм), тоді як інформаційна безпека – це практика захисту інформації, зазвичай організації чи компаній, у тому числі в IT системах, від несанкціонованого доступу, використання, розкриття, порушення, модифікації, перегляду, перевірки, запису або знищення. Кібербезпека є частиною Інформаційної безпеки;
– проаналізовано міжнародно-правові акти в сфері інформаційної безпеки та кібербезпеки: найважливішою на данний час є Будапештська конвенція 2001 року про кіберзлочинність. Дана конвенція є правоохоронним договором, спрямована на визначення, покарання та тим самим

стримування злочинів, пов'язаних з інформаційною безпекою та кібербезпекою;

- виявлено особливості організаційно-правового механізму міжнародного співробітництва держав у сфері забезпечення інформаційної безпеки на міжнародному рівні. Співробітництво зумовлено такими міжнародними організаціями: ЮНЕСКО (в рамках свого мандата сприяє політиці в галузі створення інформаційного простору на міжнародному рівні), ENISA (допомагає країнам ЄС бути краще оснащеним та підготовленим до запобігання, виявлення та реагування на проблеми інформаційної безпеки) і також БРІКС, ЮНКАД та ЮНДП;
- з’ясовано сутність кіберзлочинності та кібертероризму як загроз інформаційній безпеці у міжнародному праві; кібертероризм – це використання комп'ютерів та інформації, зокрема через Інтернет, для заподіяння фізичної, реальної шкоди або суттєвого порушення інфраструктури. кіберзлочинність – це використання комп'ютера як інструменту до незаконного доступу для здійснення фальсифікації, незаконний оборот інтелектуальної власності, крадіжка ідентичності або порушення конфіденційності;
- проаналізовано стан державної політики у сфері інформаційної безпеки в Україні. В Україні розроблено деякі нормативно-правові акти які регулюють данну сферу, але не в повному обсязі. Створено орган який забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність. Цим органом є Кіберполіція Національної поліції України. Триває імплементація Будапештської конвенції 2001 року до законодавства України;
- розроблено рекомендації та пропозиції з вдосконалення державної політики у сфері інформаційної безпеки шляхом створення Інформаційного кодексу України в якому б поєднувалися інформаційна

безпека і кібербезпека та були зазначені шляхи регулювання, забезпечення інформаційної безпеки та відповідальність за скоєні злочини в ІТ сфері;

– розроблено пропозиції з вдосконалення міжнародно-правового регулювання співробітництва держав у сфері забезпечення інформаційної безпеки шляхом створення єдиної міжнародної системи. Повинна розпочатися робота по розробці міжнародних принципів (наприклад, режим, кодекс поведінки для держав) з метою зміцнення міжнародної інформаційної безпеки. Перш за все, ці принципи могли б прийняти форму багатосторонньої декларації, вони згодом будуть включені в багатосторонній міжнародно-правовий документ. У той же час міжнародне співтовариство повинне розглянути і прийняти вищезазначені принципи в пакеті, тобто, маючи на увазі загрози військового, терористичного або кримінального характеру з метою застосування цих принципів, як до військової, так і цивільної сфери.

Дипломна робота складається з переліку умовних поначень, вступу, трьох розділів, що включають 9 підрозділів, висновків та списку використаних джерел. Загальний обсяг роботи становить 122 сторінок.

РОЗДІЛ 1. ОСНОВНІ ЗАСАДИ СТАНОВЛЕННЯ ТА РОЗВИТКУ ІНФОРМАЦІЙНОГО ПРОСТОРУ

1.1. Генеза становлення та розвитку інформаційного простору

Експоненціальне зростання використання інформаційних та комунікаційних технологій з другої половини XX століття значно послаблює тенденції розвитку суспільства. Сучасні інформаційні та комунікаційні технології істотно розширили можливості та збільшили ефективність методів взаємодії між географічно віддаленими суб'єктами від різних галузей суспільства та економіки. Зростаюча кількість користувачів інформаційно-комунікаційних технологій призводить до посилення залежності як від державного, так і від приватного секторів від цих технологій, що робить їх більш вразливими.

Окрім високої залежності суспільства від інформаційних та комунікаційних технологій, початок 21-го століття ознаменувався значною зміною глобального середовища безпеки та збільшенням кількості несиметричних загроз з вищим ступенем витонченості та наслідків впливу. Широкий спектр потенційних методів зловживання та пошкодження електронних систем інформації, зв'язку та контролю, а також негативного впливу на соціальні та економічні процеси в рамках міжнародного кібер-середовища, таким чином, кібер-загрози є серед потенційно серйозних глобальних загроз, таких як міжнародний тероризм, розповсюдження зброї масового знищення тощо.

На сьогодні існує декілька підходів до розуміння світового інформаційного простору. Міжнародний інформаційний простір можна розглядати як середовище буття людини, яке забезпечує діяльність будь-якої системи, зокрема – системи міжнародних інформаційних відносин. Також світовий інформаційний простір визначається як система спільного використання національних інформаційних ресурсів за узгодженими сферами і напрямками діяльності. У вузькому значенні міжнародний інформаційний простір розуміють як суму складних інформаційних технологій, які є основою і визначальним компонентом промислово-економічного комплексу транснаціональних спільнот, які впливають на формування

світоглядних процесів у суспільстві [35]. Міжнародний інформаційний простір можна характеризувати такими чинниками:

- територія розповсюдження інформації за допомогою глобальної системи комунікацій;
- інфраструктура або технологічні засоби і можливості зберігання, обробки і розповсюдження інформації по вертикалі та горизонталі;
- наявність міжнародної та національної інформаційної політики, комплексу норм і принципів, що регулюють функціонування та використання міжнародної інформації;
- наявність міжнародних угод в галузі комунікацій, які базуються на розумінні світової ролі інформаційних процесів, і їх впливу на розвиток цивілізацій;
- доступ до інформації світової громадськості і участь суб'єктів міжнародних відносин у загальній системі зв'язку [35].

Подолання проблем при створенні єдиного інформаційного простору залежать від співробітництва між всіма учасниками міжнародного співтовариства.

Інформаційний простір та безпека розвивалася на період Другої світової війни і навіть в період давніх часів. Отже почнемо розгляд історії інформаційної безпеки з давніх методів приховування повідомлень до відомої машини Enigma та сучасної криптографії.

1. Від античності до другої світової війни. Інформаційна безпека як наука сама по собі є відносно новою. Практика отримання інформації залежала від потреб збереження таємниць людьми. Наприклад, стародавні греки робили татуювання на головах рабів, які згодом заростали волоссям, щоб сховати повідомлення. Рабів потім відправляли до призначеного одержувача і голили голови, щоб розкрити таємницю.

Леонардо да Вінчі славився написанням текстів в зворотному напрямку у своїх зошитах, використовуючи дзеркало, щоб інші люди не змогли зрозуміти, що він пише.

2. Шифр Цезара. Кілька стародавніх культур, у тому числі греки, римляни та євреї, використовували прості замінники шифрів. Це було в основному для дипломатичного та військового спілкування. Юліус Цезар історично зараховує найбазифікованіший замінний шифр, який носить його ім'я і донині. Шифр Цезаря кодує повідомлення шляхом перекладу алфавіту на заздалегідь визначену кількість букв і заміни нової літери на кожну букву в повідомленні.

Оскільки шифри ускладнювалися, часто поєднуючи декілька шифрів заміщення, загальний ключ між відправником і отримувачем теж був довшим. Це ускладнювало та забирало багато часу для людей, щоб кодувати та декодувати повідомлення.

3. Машина Enigma. Криптографія зробила великий стрибок з винаходом механічних роторних машин на початку 20 століття. Машини складалися з приєднаних передач і роторів, які можна було встановити на заздалегідь визначений ключ і автоматично шифрувати повідомлення, послідовно об'єднуючи декілька шифрів заміщення. Найвідомішою криптографічною роторною машиною була машина Enigma, яка використовувалася німцями під час Другої світової війни.

Витокам комп'ютерів і сучасних інформаційних технологій багато століть. Еволюція математики привела до створення засобів для надання допомоги розрахунку. Першою людиною, яка побудувала одну із перших лічильних машин був Блез Паскаль (Франція, 17 століття).

ENIAC (електронний цифровий інтегратор і комп'ютер), перший електронний цифровий комп'ютер, був розроблений для армії США в 1946 році. З тих пір, комп'ютери і комп'ютерне програмування розвивалися дуже швидко. Перехід від вакуумних трубок до транзисторів значно зменшив розмір і вартість обчислювальних пристроїв і підвищення їх надійності. Так як комп'ютери стали меншими, дешевшими і швидшими, слово «неможливо» стало просто вираженням.

Оскільки розвиток комп’ютерів призвів до революції в обробкці, зберіганні та обміні інформації, ставки з приводу інформаційної безпеки виросли.

Необхідність захисту особистої, фінансової та секретної інформації призвела до швидкого розвитку математичних та обчислювальних методів захисту інформації. Перший офіційний стандарт шифрування, відомий як стандарт шифрування даних (DES), був опублікований у 1975 році і був заснований в 1977 році.

Можна виділити такий приклад періодизації інформаційної безпеки:

1946 рік – пов'язаний з винаходом і впровадженням в практичну діяльність електронно-обчислювальних машин (комп'ютерів). Завдання інформаційної безпеки вирішувалися, в основному, методами і способами обмеження фізичного доступу до устаткування засобів добування, переробки і передачі інформації [11].

У 1962 році Джозеф Ліклайдер, керівник Агентства передових оборонних дослідницьких проектів США висловив ідею Всесвітньої комп'ютерної мережі.

У 1965 році відбулося становлення та розвиток локальних інформаційно-комунікаційних мереж. Завдання інформаційної безпеки також вирішувалися, в основному, методами і способами фізичного захисту засобів добування, переробки і передачі інформації, об'єднаних в локальну мережу шляхом адміністрування і управління доступом до мережевих ресурсів [11].

У 1969 році Міністерство оборони США започаткувало розробку проекту, котрий мав на меті створення надійної системи передачі інформації на випадок війни. Агентство (англ. DARPA) запропонувало розробити для цього комп'ютерну мережу. Розробка була доручена Каліфорнійському університету Лос-Анджелеса, Стенфордському дослідному центрові, Університету штату Юта та Університету штату Каліфорнія в Санта-Барбарі. Ця мережа була названа ARPANET (англ. Advanced Research Projects Agency Network, Мережа Агентства передових досліджень). У рамках проекту мережа об'єднала названі заклади. Всі роботи фінансувались за рахунок Міністерства оборони. ARPANET почала активно рости й розвиватись, її дедалі ширше почали використовувати вчені із різних галузей науки. Перший сервер ARPANET було встановлено 1 вересня 1969 року у Каліфорнійському університеті в Лос-Анджелесі. Комп'ютер «Honeywell 516» мав 12 кілобайт оперативної пам'яті [14].

У 1970-х роках з'явилися перші персональні комп'ютери:

– машини були автономними та керованими однією людиною;

– програмне забезпечення було унікальним.

В кінці 1970-х роках зросла інформаційна загроза після розвитку дешевого та стандартизованого програмного забезпечення. За допомогою розвитку апаратного та програмного забезпечення стає більш доступним і ефективним захист інформації а не лише комп'ютерів, що обробляють інформацію. Отже, цілі захисту інформації змінилися, тоді як раніше надійність комп'ютера були домінуючими, на цьому етапі конфіденційність, цілісність і доступність стали набувають значення. Зміна фокусу від захисту комп'ютерів до захисту інформації ознаменувало появу інформаційної безпеки.

Також у 1970-х роках мережа загалом використовувалась для пересилки електронної пошти, тоді з'явилися перші списки поштових розсилок, групи новин та дошки оголошень. Але в ті часи мережа ще не могла легко взаємодіяти з іншими мережами, котрі були побудовані на інших технічних стандартах. До кінця 1970-х років почали активно розвиватись протоколи передачі даних, що були стандартизовані у 1982-1983 роках.

У 1973 році до мережі через трансатлантичний кабель були підключені перші іноземні організації з Великобританії та Норвегії мережа стала міжнародною [14].

1973 рік – пов'язаний з використанням надмобільних комунікаційних пристроїв з широким спектром завдань. Загрози інформаційній безпеці стали набагато серйознішими. Для забезпечення інформаційної безпеки в комп'ютерних системах з безпровідними мережами передачі даних потрібно було розробити нові критерії безпеки. Утворилися співтовариства людей–хакерів, що ставлять собі за мету нанесення збитку інформаційній безпеці окремих користувачів, організацій і цілих країн. Інформаційний ресурс став найважливішим ресурсом держави, а забезпечення його безпеки – найважливішою і обов'язковою складовою національної безпеки. Формується інформаційне право – нова галузь міжнародної правової системи [11].

У 1975 році Джером Зальцер (Jerome Saltzer) та Майкл Шредер (Michael Schroeder) виділяють три категорії загроз для інформації:

- несанкціоноване вивільнення інформації (конфіденційність);
- неавторизована модифікація інформації (цілісність);
- несанкціонована відмова в користуванні (доступність).

З тих пір концепція трьох основних категорій загрози та відповідні цілі безпеки стали основною філософією інформаційної безпеки.

Дослідження інформаційної безпеки ще до початку 1980-х років були конференційні та фінансувались військовими відомствами у всіх країнах світу.

У 1980–х р. комп'ютери поступово почали проникати в комерційний сектор. Через виникнення проблем безпеки, 1 січня 1983 року, мережа ARPANET перейшла з протоколу NCP на протокол TCP/IP, який досі успішно використовується для об'єднання інформаціних мереж. Саме у 1983 році за мережею ARPANET закріпився термін «Інтернет» [14].

У 1984 році була розроблена система доменних назв (англ. Domain Name System, DNS). Тоді ж у мережі ARPANET з'явився серйозний суперник – Національний науковий фонд США (NSF) заснував міжуніверситетську мережу NSFNet (англ. National Science Foundation Network), котра була сформована з дрібніших мереж, включаючи відомі на той час Usenet та Bitnet і мала значно більшу пропускну здатність, аніж ARPANET. До цієї мережі за рік під’єдналось близько 10 тисяч комп'ютерів, назва «Інтернет» почала плавно переходити до NSFNet [14].

У 1988 році було винайдено протокол Internet Relay Chat (IRC), завдяки якому в Інтернеті стало можливим спілкування в реальному часі (чат).

У 1989 році в Європі, в стінах Європейського центру ядерних досліджень (франц. Conseil Européen pour la Recherche Nucléaire, CERN) народилась концепція тенет. Її запропонував знаменитий британський вчений Тім Бернерс-Лі, він же протягом двох років розробляв протокол HTTP, мову гіпертекстової розмітки HTML та ідентифікатори URI.

У 1990 році мережа ARPANET припинила своє існування, програвши конкуренцію NSFNet. Тоді ж було зафіксовано перше підключення до Інтернету телефонною лінією (так зване «дозвонювання» англ. Dial-up access).

У 1991 році тенета стали доступні в Інтернеті, а в 1993 році з'явився знаменитий Веб-браузер (англ. web-browser) NCSA Mosaic. Всесвітня павутина ставала дедалі популярнішою [14].

У 1995 році NSFNet повернулась до ролі дослідницької мережі, маршрутизацією всього трафіку Інтернету тепер займались мережеві провайдери (постачальники послуг), а не суперкомп'ютери Національного наукового фонду. В тому ж році тенета стали основним постачальником інформації в Інтернеті, обігнавши за обсягом трафіку протокол передачі файлів FTP та було сформовано Консорціум всесвітньої павутини (англ. WWW Consorcium, W3C). Можна сказати, що тенета перетворили Інтернет і створили його сучасний вигляд. З 1996 року Всесвітнє павутиння майже повністю підмінило собою поняття «Інтернет» [14]. Отже ось такі є етапи зародження та становлення інформаційного простору та інформаційної безпеки.

Процеси формування та розвитку сучасного інформаційного суспільства, факт створення якого офіційно визнали представники держав Великої вісімки в ході Окінавської зустрічі в липні 2000 року, базуються, як відомо, на синтезі двох технологій – комп’ютерної і телекомунікаційної. Ці процеси підпорядковуються двом простим, але дуже змістовним законам. Перший закон сформулював один із засновників корпорації Intel Гордон Мур. В ньому йдеться про кількість транзисторів у процесорах яких збільшуватиметься вдвічі протягом кожних півтора року. Цей закон фактично пояснює виникнення нових, специфічних за формою і способами функціонування суб’єктів та об’єктів інформаційної інфраструктури, гарантоване зростання швидкості обчислень і обсягів оброблюваної інформації, а також формування на рубежі тисячоліть інформаційного простору – глобального інформаційного середовища, яке в реальному масштабі часу забезпечує комплексну обробку відомостей про протиборчі сторони та їх навколишнє оточення з метою підтримання ухвалених

рішень щодо створення оптимального задля досягнення поставлених цілей складу сил і засобів та їх ефективного застосування в різних умовах навколишньої обстановки [3].

Другий закон належить Роберту Меткалфу – винахідникові мережі Інтернет. В ньому йдетья про цінність мережі, яка перебуває у квадратичній залежності від кількості вузлів, що входять до її складу. Отже, цей закон констатує, що основу сучасного інформаційного суспільства становлять мережі різного функціонального призначення, сукупність і взаємозв'язок яких, власне, і створюють інформаційний простір, а також новітні інформаційно-телекомунікаційні (ІТ) технології, які останнім часом: 1) стали важливою складовою суспільного розвитку та розвитку світової економіки в цілому, змінивши значною мірою механізми функціонування багатьох суспільних інститутів та інститутів державної влади; 2) увійшли до групи найбільш істотних факторів, що впливають на формування сучасного високоорганізованого інформаційного середовища й дають змогу на якісно новому рівні інформаційного обслуговування як у віртуальному, так і в реальному просторі вести повсякденну оперативну роботу, здійснювати аналіз стану і перспектив діяльності інформаційно-аналітичних підрозділів, а також добувати вихідні дані, необхідні для ухвалення раціональних і науково-обґрунтованих управлінських рішень [3].

22 липня 2000 року глави восьми держав та урядів промислово розвинених країн підписали Окінавську хартію глобального інформаційного розвитку світової спільноти. У Хартії визначено вільний обмін інформацією та знаннями однієї з демократичних цінностей людства [35].

За останні кілька десятиліть, національні влади і уряди у всьому світі намагалися використовувати інформаційно-комунікаційні технології (ІКТ) для посилення діяльності урядів і комунікацій з суспільством. Протягом короткого періоду часу, інформаційні технології швидко просунулися від основних видів використання ІКТ, як засіб для підтримки адміністративної роботи, до включення урядових заходів ІКТ.

Інформаційні та комунікаційні технології (ІКТ), відносяться до середовища, які забезпечують доступ до інформації через телекомунікації. Вони включають в себе Інтернет, бездротові мережі, мобільні телефони та інші засоби зв'язку. Ці технології принесли великі фінансові та соціальні успіхи і допомогли розвитку суспільства.

1.2. Інформаційна безпека: поняття, зміст та ознаки

Інформаційна безпека – це відносно нове поняття. На сучасному етапі можна виокремити багато термінів значення інформаційної безпеки. Інформаційна безпека – це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, або комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення (у цьому значенні частіше використовують термін «захист інформації») [11]. Інформаційна безпека – це процес захисту даних від несанкціонованого доступу, використання, розголошення, знищення, модифікації або порушення [21]. Отже з приведених вище визначень можна сформувати таке поняття, як інформаційна безпека. Інформаційна безпека – це практика захисту інформації від несанкціонованого доступу, використання, розкриття, порушення, модифікації, перегляду, перевірки, запису або знищення. Це загальний термін, який може бути використаний незалежно від форми даних, яку можуть приймати (електронна, фізична тощо). Терміни інформаційна безпека, безпека комп'ютера та забезпечення інформації часто використовуються взаємозамінно. Ці поняття взаємопов'язані і поділяють загальні цілі захисту конфіденційності, цілісності та доступності інформації, однак між ними є деякі тонкі відмінності. Ці відмінності полягають насамперед у підході до теми, використовуваних методологіях та сферах концентрації. Інформаційна безпека стосується конфіденційності, цілісності та доступності даних, незалежно від форми, яку можуть отримати дані: електронні, друковані чи

інші форми. Також можна зробити висновок що інформаційна безпека – це впевненість і реальність інформаційної системи, яка може функціонувати, як попередження для ворожого середовища.

Сутністю інформаційної безпеки є поняття безпеки, яке характеризує певний процес управління загрозами та небезпеками. Відповідно видове поняття «інформаційна безпека» означає процес управління загрозами та небезпеками в інформаційній сфері. Саме тому інформаційна безпека є невід'ємною частиною загальної безпеки, чи то національної, чи то регіональної, чи то міжнародної. Аналіз інформаційної безпеки передбачає розгляд сукупності таких об'єктивних чинників:

– потреб громадян, суспільства і держави і світового співтовариства;
– уразливість індивідів, суспільства і держави від цифрових технологій;
– наявність широкого кола загроз і небезпек, якими має управляти система забезпечення інформаційної безпеки [30].

Інформаційна безпека є складовим компонентом загальної проблеми інформаційного забезпечення людини, держави і суспільства. Вона орієнтована на захист значимих або вже згаданих суб'єктів інформаційних ресурсів, законних інтересів. Зміст поняття «інформаційна безпека» розкривається у практичній діяльності, наукових дослідженнях, а також нормативно-правових документах [30].

Об’єктами інформаційної безпеки є – інформаційні бази, інформаційні потоки, штатні співробітники.

Можна виділити два основних аспекти інформаційної безпеки:

ІТ-безпека. Іноді називається безпека комп'ютера, інформаційна безпека – це безпека, застосована до технології (найчастіше якась форма комп'ютерної системи). Варто зазначити, що комп'ютери не обов'язково означають домашній робочий стіл. Фахівці з інформаційної безпеки майже завжди знаходяться в будь-якому великому підприємстві / установі через характер і цінність даних у великих підприємствах. Вони несуть відповідальність за захист всієї технології

всередині компанії від шкідливих комп'ютерних нападів, які часто намагаються порушити приватну інформацію або отримати контроль над внутрішніми системами.

Забезпечення інформації. Забезпеченням інформації, як правило, займаються фахівці з інформаційної безпеки. Одним з найпоширеніших методів забезпечення інформаційної безпеки є наявність резервного копіювання даних у разі виникнення проблем, наприклад таких як стихійні лиха, технічні несправності та ін. Тоді дані не втрачаються, коли виникають серйозні проблеми бо мають резервні копії.

Можна виділити п’ять основних методів забезпечення інформаційної безпеки.

Першим методом є теоретичний метод – формалізація процесів, пов’язаних із забезпеченням інформаційної безпеки та обґрунтування коректності та адекватності систем забезпечення інформаційної безпеки.

Другим методом є організаційний методи це – керування ІБ на підприємстві.

Третім методом є правовий метод – відповідальність, робота з держтаємницею, захист авторських прав, ліцензування та сертифікації.

До четвертого методу слід віднести метод сервісу мережної безпеки – ідентифікація та автентифікація, розмежування доступу, протоколювання і аудит, засоби захисту периметра, криптографічні засоби захисту.

Та до останнього п’ятого методу віднесемо інженерно-технічні методи – захист від несанкціонованого зняття інформації під час передавання технічними каналами.

Важливість інформаційної безпеки можна виокремити в так звану тріаду інформаційної безпеки або систему інформаційної безпеки: конфіденційність, цілісність, доступність.

1. Конфіденційність інформації в інформаційних системах (ІС) – унеможливлення отримання інформації неавторизованим користувачем або процесом ІС та збереження її конфіденційності під час виконання певних правил

ознайомлення з нею. Конфіденційність інформації – властивість інформації,що не підлягає розголошенню; надійність, секретність, гарантована приватність [3]. Конфіденційність – захист від несанкціонованого доступу до інформації під час передавання технічними каналами.

При захисті інформації виникає питання чи можна обмежувати доступ до інформації осіб які не претендують на доступ до інформації. Наприклад, закони багатьох країн світу вимагають, щоб університети обмежували доступ до приватної інформації студента. Університет повинен бути впевнений, що тільки уповноважені особи мають доступ до інформацію, для перегляду записів про оцінку та особисті данні студентів.

2. Цілісність інформації – захищеність інформації від несанкціонованої зміни, забезпечення її точності та повноти. Цілісність інформації в ІС – властивість інформації, яка не може бути модифікованою неавторизованим користувачем та зберігати цілісність, якщо дотримуються встановлені правила її модифікації [3]. Тобто цілісність – це гарантія того, що інформація, до якої звертаються, не була змінена і дійсно подається у оригінальному вигляді. Цілісність інформації означає, що інформація справді відображає її передбачуване значення. Інформація може втратити свою цілісність через зловмисний намір, наприклад, коли якась авторизована особа яка навмисно вносить зміни до інформації. Цілісність також може бути втрачена ненавмисно, наприклад, коли прискорення завантаження комп'ютера пошкоджує файл, або хтось, уповноважений робити зміни, випадково видаляє файл або вводить невірну інформацію.

3. Доступність інформації є третьою частиною тріади. Доступність це – можливість використання інформації, коли в цьому постає потреба [3]. Тобто доступність означає, що інформація може бути доступною і модифікованою уповноваженими особами у будь-який термін. Залежно від типу інформації, відповідний термін може означати різні речі. Наприклад, трейдер акції потребує інформацію, щоб вона була доступною та актуальною негайно, щоб вона відображала поточний стан інформації, а продавець може отримати звіти про

продаж наприклад наступного ранку. Такі компанії, як Amazon.com, вимагатимуть наявність своїх серверів цілодобово, сім днів на тиждень. Інші компанії, можливо, не постраждають, якщо їх веб-сервери будуть недоступні деякий короткий час.

Для забезпечення конфіденційності, цілісності та доступності інформації організації можуть вибирати з різних інструментів. Кожен з цих інструментів може бути використаний як частина загальної політики щодо інформаційної безпеки.

Розглянемо технології інформаційної безпеки такі як автентифікація, управління доступом та шифрування.

Організацією довірчої взаємодії в інформаційному просторі є взаємна ідентифікація сторін [3]. Найпоширеніший спосіб ідентифікувати когось є їх зовнішній вигляд. Інструменти для автентифікації використовуються для забезпечення безпеки, людина яка отримує доступ до інформації, дійсно, є тим, ким вона представляється.

Автентифікація може бути виконана шляхом ідентифікації когось через один або декілька чинників. Наприклад, найпоширенішою формою автентифікації сьогодні є ідентифікатор користувача та пароль. У цьому випадку автентифікація здійснюється шляхом підтвердження того, що користувач знає (його ідентифікатор та пароль). Але ця форма автентифікації є ненадійною та іноді потрібні більш жорсткі форми автентифікації. Остаточним чинником є ідентифікація користувача за допомогою фізичних характеристик, такої як сканування очей або відбиток пальців. Визначення когось за своїми фізичними характеристиками називається біометрикою.

Управління доступом. Після того, як користувача буде автентифіковано, наступним кроком буде забезпечення того, щоб він мав доступ до відповідних інформаційних ресурсів. Це робиться за допомогою контролю доступу. Контроль доступу визначає, які користувачі мають право читати, змінювати, додавати та видаляти інформацію.

Безпека нових типів інформаційних ресурсів – захист не тільки окремих документів, файлів або повідомлень, а й інформаційних ресурсів системи в цілому.

Інтеграція захисту в ІС – засоби захисту мають стати невід'ємною частиною засобів, що реалізують інформаційні технології [3]. Захист від засобів нападу – механізми гарантування безпеки системи в умовах взаємодії з програмами, які здійснюють деструктивні дії.

Шифрування. Багато організацій повинні передавати інформацію через Інтернет або передавати її на зовнішніх носіях, таких як компакт-диски або флеш-накопичувачі. У цих випадках, навіть при належній автентифікації та контролю доступу, неавторизована особа може отримати доступ до даних. Шифрування – це процес кодування даних при його передачі чи зберіганні, щоб лише авторизовані особи могли його прочитати. Це кодування виконується за допомогою комп'ютерної програми, яка кодує звичайний текст, який потрібно передавати, також одержувач отримує текст шифру і декодує його (дешифрування). Для того, щоб це працювало, відправник і одержувач повинні узгодити метод кодування, щоб обидві сторони могли правильно спілкуватися. Обидві сторони поділяють ключ шифрування, дозволяючи їм кодувати та декодувати повідомлення один одного. Це називається симетричним шифруванням ключів.

Розглянемо види інформаційної безпеки такі як захист додатків, хмарна безпека та криптографія.

Захист додатків – це широка тема, яка охоплює вразливість програмного забезпечення в веб та мобільних додатках та інтерфейсах прикладного програмування (API). Ці вразливості можуть бути знайдені при автентифікації або авторизації користувачів, цілісності коду та конфігурації, а також розроблених політик та процедур. Вразливі програми можуть створювати точки доступу для значних порушень інформаційної безпеки. Захист додатків є важливою частиною захисту периметру для інформаційної безпеки.

Хмарна безпека – зосереджується на створенні та розміщенні захищених програм у хмарному середовищі та безпечному використанні сторонніх обласних додатків. «Хмара» означає, що програма запускається у спільному середовищі. Підприємства повинні переконатися, що існує адекватна ізоляція між різними процесами в спільних середовищах.

Криптографія. Шифрування даних під час транзиту та відновлення даних допомагають забезпечити конфіденційність та цілісність даних. Цифрові підписи часто використовуються в криптографії для перевірки автентичності даних. Криптографія та шифрування стають дедалі важливішими. Гарним прикладом використання криптографії є розширений стандарт шифрування (AES). AES – алгоритм симетричного ключа, який використовується для захисту секретної державної інформації.

Інфраструктура охоплює захист внутрішніх та екстранет-мереж, лабораторій, центрів обробки даних, серверів, настільних комп'ютерів та мобільних пристроїв.

Реакція на інцидент – це функція, яка відслідковує та досліджує потенційно шкідливу поведінку.

Під час підготовки персоналу IT до загроз, повин бути розроблений план реагування на інцидент та відновлення мережі. Крім того, план повинен створити систему для збереження доказів для криміналістичного аналізу та потенційного судового переслідування. Ці дані можуть допомогти запобігти подальшим порушенням і допомогти виявити зловмисника.

Управління вразливостями – це процес сканування середовища для слабких місць (наприклад, відкачування програмного забезпечення) та визначення пріоритетів для відновлення на основі ризику.

Глави держав і військові командири вже давно усвідомлюють важливість та необхідність захисту інформації про їх військові здібності, кількості військ та військових частин. Така інформація, що потрапляє до рук ворога, може бути катастрофічною. Уряди, військові, фінансові установи, лікарні та приватні компанії отримують велику кількість конфіденційної інформації про своїх

співробітників, клієнтів, продуктів досліджень та фінансового стану. Більша частина цієї інформації збирається, обробляється та зберігається на електронних комп'ютерах та передаються через мережі на інші комп'ютери. Якщо конфіденційна інформація про клієнтів або фінансову компаню, або про нову лінійку продуктів, потрапляє в руки конкурента, таке порушення безпеки може призвести до втрати бізнесу, юридичних справ чи навіть банкрутства бізнесу. Тому конфеденційність, целісність та доспупність є дуже важливими елементами інформаційної безпеки для захсту данних в наш час .

1.3. Кібербезпека: поняття, зміст та ознаки

Упродовж останніх років технологічні інновації виявилися все більш міцно переплетеними в нашому житті. Поширеність мобільних телефонів та планшетів та самого інтернету розширили залежність уявлення щодо безпеки індивідуальної та ділової інформації.

Кіберпростір в даний час є невід'ємною частиною нашого суспільства і економіки, і навіть може стати визначальним фактором у розвитку культури і, можливо, їх зближення з суспільством.

Кіберпростір складається з апаратних засобів, програмного забезпечення, інтернету, інформаційних послуг та системи управління, які забезпечують надання послуг, які необхідні для соціально-економічної діяльності будь-якої держави. Відповідно до міжнародного стандарту кіберпростір – це середовище існування, що виникло в результаті взаємодії людей, програмного забезпечення і послуг в інтернеті за допомогою технологічних пристроїв і мереж, під’єднаних до них, яких не існує в будь-якій фізичній формі. Відповідно до нормативної бази США, кіберпростір – це сфера, що характеризується можливістю використання електронних та електромагнітних засобів для запам’ятовування, модифікування та обміну даними через мережеві системи та пов’язану з ними фізичну інфраструктуру. Відповідно до офіційних документів Євросоюзу, кіберпростір – це віртуальний простір, в якому циркулюють електронні дані світових

персональних комп'ютерів (ПК). Відповідно до офіційних документів Великобританії, кіберпростір – це всі форми мережної, цифрової активності, що включають у себе контент та дії, здійснювані через цифрові мережі. Відповідно до офіційних документів Німеччини, кіберпростір – це вся інформаційна інфраструктура, доступна через інтернет поза будь-якими територіальними кордонами [3]. Отже з наведених визначень можна вивести узагальнене визначення кіберпростору. Кіберпростір – це сукупність засобів і процедур, заснованих на інформаційно-комунікаційних технологіях, який налаштований для надання послуг.

Дійовими особами кіберпростору є легальні користувачі, оператори, адміністратори, хакери, мережеві комбатанти, кіберзлочинці, кібертерористи, підрозділи державних та недержавних структур, що здійснюють інформаційні операції, кібервійська.

Кіберпростір складається з трьох шарів: фізичний рівень, логічний рівень і соціальний шар, які в свою чергу, складається з 5 компонентів: географічний компонент, фізичний компонент мережі, логічні мережеві компоненти, люди і кібер-ідентичність.

Фізичний рівень охоплює географічний компонент і компонент фізичних мереж. Географічний компонент відноситься до фізичного рівеня який охоплює географічний компонент і компонент фізичних мереж. Компонент фізичної мережі складається з апаратних засобів та інфраструктури, підтримки мереж і їх фізичні конектори (кабелі, маршрутизатори, сервери, комп'ютери, і т.д.).

Логічний рівень формується з логічного компонента мережі, ці логічні зв'язки, які існують між вузлами мережі, вузлом може бути будь-який пристрій, що підключений до мережі зв'язку та IT-систем.

Соціальний шар складається з компонентів – людей і кібер-ідентичності. Компонент людина формується з користувачів, які взаємодіють в кібер-просторі. Кібер-ідентичність може бути реальною або підробленою, що дозволяє користувачеві насолоджуватися певною анонімністю і ускладнюють судове переслідування злочинної поведінки, яке відбувається в кібер-просторі.

Кібер-ідентичність формується, серед інших, облікових записів електронної пошти, облікових записів користувачів мережі і профілів в соціальних мережах.

Отже було розглянуто що являє собою кіберпростір та розглянемо суть кібербезпеки.

Як вважає український учений, кандидат технічних наук, старший науковий співробітник Баранов О.А. кібербезпека – це такий стан захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через неповноту, невчасність та невірогідність інформації, що використовує негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації [2]. Деякі експерти, також як і Д. Франсело, вважають, що останнім часом термін кібербезпека все частіше і частіше використовується, але при цьому багато керівників служб безпеки і просто експерти з інформаційної безпеки досі плутаються втому, коли і як використовувати цей термін [2].

Проаналізуємо національні стратегічні документи у деяких країнах світу. У стратегії Франції, присвяченій питанням кібербезпеки, дано таке визначення: кібербезпека – це бажаний стан інформаційної системи, за якого вона може протистояти подіям з кіберпростору, що можуть поставити під загрозу доступність, цілісність або конфіденційність даних, які зберігаються, обробляються або передаються, і пов’язаних з ними послуг, які ці системи пропонують або роблять доступними. Насамперед, треба розуміти, що відповідно до цього визначення кібербезпека – це деякий стан систем, за якого нейтралізуються загрози доступності, цілісності або конфіденційності даних, що циркулюють в інформаційних системах. Крім того, завдяки включенню до переліку об’єктів, на які можуть діяти якісь загрози з кіберпростору, послуг інформаційних систем це визначення терміна дозволяє мати на увазі наявність якихось загроз функціональності систем більш високого порядку, до яких в якості складових елементів входять інформаційні системи. Це положення має важливий

методологічний зміст у розумінні місця і ролі проблеми кібербезпеки в контексті інших видів безпеки [2].

У німецькій стратегії під кібербезпекою розуміється деяка сукупність необхідних і відповідних заходів, в результаті реалізації яких досягається мінімізація ризиків. При цьому в стратегії стверджується, що кібербезпека повинна базуватися на комплексному підході. Це досить прагматична точка зору, яка дозволяє розроблювати практичні кроки щодо забезпечення кібербезпеки, проте вона не надає достатніх методологічних підстав для проектування та оцінки систем, що забезпечують цю безпеку. Про це побічно свідчить зміст десяти стратегічних напрямів у стратегії забезпечення кібербезпеки, оголошених федеральним урядом Німеччини. У Канаді стверджують, що з метою забезпечення найсучаснішого використання кіберпростору, який є стратегічним активом, необхідно передбачати і протистояти кіберзагрозам, що виникають. У канадській стратегії кібербезпеки не міститься чіткого визначення, що являє собою кібербезпека. Відповідно до цього документа під кібербезпекою можна розуміти захист кіберсистем від шкідливого та неправильного використання та від інших деструктивних атак. З іншого боку, надано досить докладне визначення кібератаки, а кібербезпека – це засіб захисту від цих загроз [2].

Одна із найостанніших за часом національних стратегій кібербезпеки (Турецька Республіка) містить таке визначення: кібербезпека – захист інформаційних систем від нападів, що входять до складу кіберпростору, забезпечення конфіденційності, цілісності та доступності інформації, яка обробляється в цьому просторі, виявлення та протидія атакам і кіберінцидентам. При цьому під кіберпростором розуміється середовище, що складається з інформаційних систем, розподілених по всьому світу, в тому числі мереж, що з'єднують ці системи. Національний кіберпростір визначається як простір, який складається з інформаційних систем суб'єктів, що перебувають під юрисдикцією Турецької Республіки.

У Нідерландах також приділяють велику увагу наявності загроз інформаційній інфраструктурі в умовах широкого застосування цифрових

(комп'ютерних) технологій. Кібербезпека – це сукупність зусиль щодо запобігання шкоди, що може бути заподіяна внаслідок збоїв у роботі ІКТ або неправильного їх використання, а також з відновлення ІКТ після реалізації цих загроз. До збоїв стратегія відносить зниження надійності ІКТ, обмеження доступності та порушення конфіденційності та/або цілісності інформації, що зберігається в системах ІКТ. Таке тлумачення робить вельми складним вирішення проблеми визначення критеріїв забезпечення кібербезпеки.Однак у цій стратегії було зроблено вельми важливий в методологічному аспекті висновок – кібербезпека може бути досягнута тільки в системній кореляції з вирішенням проблем захисту та забезпечення основних прав, цінностей і соціально-економічних вигод членів соціуму [2].

Щодо українського законодавства то в законі України «Про основні засади забезпечення кібербезпеки України» прописано таке визначення: «Кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі» [17]. Отже як можна зрозуміти поняття кібербезпеки присутнє як в національному, так і в міжнародному законодавстві.

Таким чином, можна констатувати, що на рівні національних та міжнародних стратегічних документів визначення кібербезпеки значно різняться. А значить, розрізняються і підходи не тільки до змісту відповідних стратегій, а й до змісту планів дій із забезпечення кібербезпеки. Однак транскордонний характер цієї проблеми настійливо диктує необхідність координації зусиль як на національному, так і на міжнародному рівні. Передусім, мова йде про осмислення суті кіберзагроз, змісту робіт щодо забезпечення кібербезпеки, чітке визначення цілей стратегії і власне визначення змісту самого терміна «кібербезпека». Отже розглянувши всі поняття кібербезпеки потрібно сформулювати визначення кібербезпеки. Кібербезпека – це практика захисту систем, мереж та програм від

цифрових атак. Ці атаки, як правило, спрямовані на доступ, зміну або знищення конфіденційної інформації. Кібербезпека включає в себе технології, процеси та елементи керування, призначені для захисту систем, мереж та даних від кібер-атак. Ефективна кібербезпека знижує ризик кібер-атак та захищає організації та приватні особи від несанкціонованої експлуатації систем, мереж та технологій. Кібербезпека – це інформаційні технології, пов'язані з безпекою комп'ютерних систем та інформації. Це охоплює загрози комп'ютерній апаратурі, програмному забезпеченню та даних, включаючи крадіжки, хакерство, віруси тощо. Область комп'ютерної безпеки зросла надзвичайно, оскільки більше пристроїв стає доступним через інтернет, і більше послуг переміщуються в Інтернеті. Кібербезпека – це захист інтернет-підключених систем, включаючи апаратне забезпечення, програмне забезпечення та дані, від кібератак.

Об’єктами кібербезпеки є – органи та канали управління, канали інтерактивної взаємодії, системи моніторингу та збору даних.

Складовими кібернетичної безпеки є захист власної інформаційної сфери, кібернетичні впливи, розвідка інформаційно-телекомунікаційних систем та криптосистем протиборчих сторін.

Сутність кібербезпеки полягає у трьох значеннях: аспекти, сфера дії та рівні. Аспектами кібербезпеки можна виділити: соціальні, технічні, інформаційні та комунікаційні.

Сфера дії: зовнішньополітична, внутрішньополітична, воєнна, економічна, соціальна, екологічна та науково-технічна.

Також можна виділити рівні кібербезпеки: нормативно-правовий, соціальний (біологічний), інфокомунікаційний та соціотехнічний методичні рівні.

У контексті обчислювальної техніки безпека включає кібербезпеку та фізичну безпеку – обидва використовуються підприємствами для захисту від несанкціонованого доступу до центрів обробки даних та інших комп'ютерних систем. Інформаційна безпека, яка призначена для збереження конфіденційності, цілісності та доступності даних, є підмножиною кібербезпеки.

Використання кібербезпеки може запобігти кібератакам, порушенню даних та крадіжці особистих даних та допомогти в управлінні ризиками.

Висновки до розділу 1

Отже інформаційна безпека почала всій розвиток у 20 столітті. Перші спроби збереження інформації розпочались ще зі стародавніх часів. Після створення перших комп’ютерів та мережі інтернет, інформаційна безпека прийняла важливе значення для збереження важливих даних, інформації.

Проаналізувавши поняття кібербезпеки та інформаційної безпеки – стає зрозумілим що кібербезпека – це інформаційні технології, пов'язані з безпекою комп'ютерних систем та інформації (обладнання та програм), тоді як інформаційна безпека – це практика захисту інформації від несанкціонованого доступу, використання, розкриття, порушення, модифікації, перегляду, перевірки, запису або знищення зазвичай організації чи компаній у тому числі в IT системах. Кібербезпека є частиною Інформаційної безпеки.

Об’єктами інформаційної безпеки є – інформаційні бази, інформаційні потоки, штатні співробітники. Об’єктами кібербезпеки є – органи та канали управління, канали інтерактивної взаємодії, системи моніторингу та збору даних.

Термін «інформаційна безпека» вживається в широкому сенсі. У вузькому сенсі доречно застосовувати термін «безпека інформації», що має на увазі просто комплекс заходів щодо захисту інформації. Термін кібербезпека слід розуміти як забезпечення «безпеки інформації».

РОЗДІЛ 2. НОРМАТИВНО-ПРАВОВИЙ ТА ОРГАНІЗАЦІЙНО-ПРАВОВИЙ МЕХАНІЗМ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА В СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Нормативно-правовий механізм інформаційної безпеки держав

Жоден глобальний виклик, що стоїть перед сучасним міжнародним співтовариством, не може бути належним чином вирішений будь-яким окремим міжнародним суб'єктом, незалежно від того, наскільки він є впливовим. Такі складні сучасні явища, як міжнародний тероризм чи кібернетичні загрози, вимагають структури міжнародного співробітництва.

Можна виділити міжнародно правові акти в сфері інформаційної безпеки:

- Резолюції Генеральної Асамблеї ООН.
- Резолюція ГА ООН 54/49 від 1 грудня 1999 р., що вперше вказала на загрози міжнародній інформаційній безпеці стосовно не тільки до цивільної, а й до військової сфери.
- Резолюція ГА ООН 62/17 від 5 грудня 2007 р., яка закликає держави-члени і далі сприяти розгляду на багатосторонньому рівні існуючих та потенційних загроз у сфері інформаційної безпеки, а також можливих заходів по обмеженню загроз, що виникають у цій сфері [25].

У 2011 році Росія, Китай, Узбекистан та Таджикистан висунули пропозиції про створення кодексу інформаційної безпеки. На думку цих країн-учасниць, питання безпеки в сфері Інтернет-діяльності, в зв'язку з їх зростаючою важливістю, повинні розглядатися міжнародним співтовариством. Призначення Кодексу полягає в дотриманні норм, направлених на захист Інтернету і інших комунікаційних технологій від уразливості і інших загроз [26]. Але кодекс так і не був прийнятий.

Значним кроком у створенні захисту інформаційної безпеки стало підписання в рамках Ради Європи Конвенції про кіберзлочинність 23 листопада 2001 р. у Будапешті [27]. Загальна кількість країн, що ратифікували

Конвенцію Ради Європи про кіберзлочинність, сягає 55 та не обмежується країнами-членами РЄ (цю Конвенцію ратифікували також США, Канада, Японія, Мексика, Австралія та багато інших країн). Ще чотири країни підписали, але не ратифікували Конвенцію. Категорично проти її підписання виступають Росія та Китай.

Як зазначено у преамбулі, «Конвенція є необхідною для зупинення дій, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними, шляхом встановлення кримінальної відповідальності за таку поведінку, як це описано у Конвенції, надання повноважень, достатніх для ефективної боротьби з такими кримінальними правопорушеннями шляхом сприяння їхньому виявленню, розслідуванню та переслідуванню, як на внутрішньодержавному, так і на міжнародному рівнях, і укладення домовленостей щодо швидкого і надійного міжнародного співробітництва». При цьому особлива увага звертається на необхідність забезпечити належний баланс між правоохоронними інтересами і повагою до основних прав людини, таких, як право кожного безперешкодно дотримуватись поглядів, а також право на свободу слова, включаючи право на пошук, отримання і передачу будь-якої інформації та ідей, незважаючи на обмеження, права на повагу до приватного життя, а також права на захист особистої інформації.

Конвенція передбачає запровадження на національному рівні кримінальної відповідальності за наступні групи злочинів:

- правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, нелегальне перехоплення, втручання у дані, втручання у систему, зловживання пристроями);
- правопорушення, пов'язані з комп’ютером (підробка, пов'язана з комп'ютерами, шахрайство, пов'язане з комп'ютерами);

- правопорушення, пов'язані зі змістом (правопорушення, пов'язані з дитячою порнографією);
- правопорушення, пов'язані з порушенням авторських та суміжних прав [32]. Конвенція з Кіберзлочинності дає значний поштовх для інформаційної безпеки та кібербезпеки.

Директива 2016/680 Європейського Парламенту та Ради ЄС від 27 квітня 2016 р. про захист фізичних осіб стосовно обробки персональних даних компетентними органами для цілей запобігання, розслідування, виявлення або переслідування кримінальних злочинів або виконання кримінальних покарань та про вільне переміщення таких даних [33].

Створюючи рамки обмежень, закон одночасно гарантує сферу автономії для своїх суб'єктів. У контексті міжнародного права правові норми встановлюють спільні межі прийнятної поведінки у міжнародних відносинах, зберігаючи при цьому важливий простір для маневру, дискрецій та переговорів. Ця ідея лежить в основі відомої презумпції «Lotus», згідно з якою держави можуть діяти вільно, якщо це не суперечить нормам міжнародного права.

Для того, щоб окреслити цю зону свободи для держав та інших міжнародних дійових осіб стосовно нового явища міжнародного значення, необхідно визначити, тлумачити та застосувати до неї відповідні правові норми.

Інформаційний простір, в широкому розумінні, є саме таким явищем. Важливо, що використання і зловживання цим складним віртуальним простором без обмежень впливає на життєво важливі державні інтереси у фізичному світі, включаючи національну безпеку, громадську безпеку чи економічний розвиток. Таким чином, інформаційний простір виходить далеко за межі внутрішніх справ будь-якої держави.

Основні будівельні блоки архітектури Інтернету були закладені більше двох десятиліть тому, представники держав досягли домовленості про те, що міжнародне право фактично застосовується до інформаційного простору.

Важливість даної домовленості є суперечливою. Вона була виражена у формі необов'язкового звіту Групи урядових експертів (GGE), створеної Генеральною Асамблеєю ООН. У той час групу склали представники 15 держав-членів ООН, включаючи три «кібер наддержави» – Китай, Росію та Сполучені Штати. Таким чином, її позиція може бути прийнята як підтвердження спільного розуміння в міжнародній спільноті.

Міжнародне право має застосовуватися, але яке міжнародне право? Незважаючи на те, що група підтримала центральну роль Статуту ООН, деякі її члени сумнівалися в застосуванні «закону збройного конфлікту» на кібер-операції. Можливо, більш важливим є те, як слід застосовувати міжнародне право? Єдина річ, яку потрібно знати це те, що онлайн-сфера не є беззаконним світом, але зовсім іншим, щоб зрозуміти, як її правила точно застосовуються до кібер-феномену.

Виділяються три індикатори очевидної кризи міжнародного права. По-перше, область інформаційної безпеки та кібербезпеки виявляється стійкою до кодифікації застосовних правил у всеосяжному багатосторонньому зобов'язуючому договорі. Вже в 1996 році Франція висунула пропозицію з високим титулом «Хартія міжнародного співробітництва в Інтернеті». Пізніше спільна російсько-китайська ініціатива призвела до двох пропозицій щодо Кодексу поведінки з питань інформаційної безпеки, представленої Генеральної Асамблеї ООН у 2011 та 2015 роках. Однак жодна з цих пропозицій не була задоволена великим ентузіазмом інших держав, і вчені розповіли про перспективи прийняття договору найближчим часом.

По-друге, держави продемонстрували крайнє небажання сприяти розвитку інформаційних та кібер-специфічних міжнародних правил. На додаток до державної практики в цій сфері, яка неминуче охоплена таємницею, держави не хочуть пропонувати чіткі вирази «opinio juris» з питань, пов'язаних з інформаційною безпекою та кібербезпекою. Часом цей підхід, безумовно, може бути зрозумілим, що є наслідком внутрішньої політичної загрози або навіть навмисної стратегії очікування. Це додає певної невизначеності стосовно

конкретної застосовності міжнародного права. Цю тенденцію видно навіть у самих останніх розробках. Репрезентативний приклад іншої втраченої можливості спроба керувати розвитком кібер-простору, що передбачена Посібником «Закони війни» США (англ. «United States (US) Law of War Manual»), прийнятим у липні 2015 року. Незважаючи на те, що в посібнику містяться розділи про кібер-операції, в ньому також наведено практично всі невирішені питання, включаючи стандарти присвоєння, правила націлювання чи вимоги перегляду інформаційної-зброї.

Хоча перші два показники стосуються небажання держав діяти так, як це важливо для створення нових правил, третій – щодо їхньої реальної поведінки у відношенні кібер-управління. Було б неточним стверджувати, що держави повністю відмовилися від встановлення стандартів. Проте, замість того, щоб тлумачити або розвивати норми міжнародного права, представники держави шукали певного сенсу в терміні «норми». Ми можемо побачити цю тенденцію найбільш чітко в контексті роботи GGE ООН. У своїй останній доповіді група оприлюднила переваги добровільних, незв'язаних норм відповідальної поведінки держави. У доповіді зазначалося, що такі норми запобігають виникненню конфліктів у інформаційному просторі, сприяють міжнародному розвитку та зменшують ризики для міжнародного миру та безпеки. У доповіді також рекомендується розгляд таких норм для розгляду державами, одночасно даючи зрозуміти, що ці норми діють на абсолютно незаконному рівні. Незважаючи на їх мінімалізм, норми досі отримали дуже обмежене схвалення їх адресатами. Наприклад, на американсько-китайському саміті у вересні 2015 року два голови-учасники «вітали» звіт, але утримувалися від будь-яких із запропонованих норм.

Разом ці три показники означають тенденцію відходу від створення правових норм міжнародного права в класичному сенсі. Замість розробки обов'язкових договірних або звичних правил, держави вдаються до нормативної діяльності поза рамками традиційного міжнародного права. Незважаючи на те, що ця тенденція, здається, особливо помітна у сфері інформаційної та кібербезпеки, це жодним чином не обмежує її. У правовій теорії це явище було описано як

плюралізація міжнародних нормотворчих процесів, що характеризується зауваженням, що «лише обмежена частина здійснення державної влади на міжнародному рівні матеріалізується сьогодні у створенні норм, які можна вважати міжнародно-правовими правилами відповідно до класичного розуміння міжнародного права». Щоб зрозуміти вплив, який ця ситуація має на міжнародно-правове регулювання інформаційної безпеки та кібербезпеки, ми повинні трохи зменшити масштаб, щоб взяти ширший контекст існуючого міжнародного права.

Відсутність інформаційної конкретної системи норм міжнародного права не означає, що не існує жодних правових норм, які застосовуватимуться до інформаційної та кібер-діяльності. Якщо міжнародне право має бути ефективною структурою управління, вона повинна бути пристосованою до нових явищ без необхідності повторно винаходити повну систему регулювання на кожний випадок.

Як приклад, Статут ООН був завершений, коли винахід ядерної зброї все ще залишався таємницею. Таким чином, цей документ не посилався на цей вид зброї у своїх положеннях про застосування сили. Проте, Міжнародний Суд мав невеликі труднощі у проведеному Консультативному висновку щодо ядерних озброєнь, висловленому десятиліттями пізніше, про те, що ці положення «застосовуються до будь-якого застосування сили незалежно від використовуваної зброї», незважаючи на той факт, що певний вид зброї можливо, ще не був загальновідомим або навіть винайденим, коли Статут був прийнято. Слідом за такою ж логікою, кібер-операції повинні в рівній мірі підпадати під дію міжнародно-правового регулювання застосування сили.

Окрім цих загальноприйнятих норм міжнародного права, окремі секторальні та регіональні договори, взяті разом, забезпечують «розмаїття правил» для інформаційної та кібер-діяльності. Серед них, зокрема, Конституція 1992 року Міжнародного союзу електрозв'язку, Будапештська конвенція 2001 року про кіберзлочинність, Угода про співпрацю в галузі інформаційної безпеки в Шанхайській організації співробітництва 2009 р. та Конвенція 2014 року про

кібербезпеку Африканського Союзу. Хоча ці міжнародні угоди є важливими, вони регулюють лише невелику частину інформаційної безпеки та кібербезпеки, що пов'язано з діяльністю (наприклад, кримінальні правопорушення, вчинені за допомогою комп'ютерних систем чи операції, що перешкоджають існуючим телекомунікаційним мережам), або мають дуже обмежений членський склад (шість держав у випадку домовленості Шанхайської організації співробітництва та їх відсутність в конвенції Африканського Союзу).

Тому, хоча інформаційний простір, безумовно, не є незаконною територією, недоступною міжнародному праву, поки не існує складного регулюючого механізму, що регулює інформаційну та кібернетичну діяльності в державі. Більше того, держави, як видається, неохоче беруть участь у розвитку та тлумаченні міжнародного права, що застосовується до інформаційної безпеки. Цей добровільний відступ спричинив сильний вакуум, який дозволив недержавним суб'єктам перейти до вільного простору та здійснювати різні форми «нормальної підприємницької діяльності».

На державну владу впливають багато факторів, які можуть включати військову потужність, багатство та моральний авторитет. Якщо ми розуміємо владу просто як «здатність змінювати поведінку інших людей, щоб отримувати бажані результати», тоді встановлення юридичних зобов'язань є одним із способів реалізації цієї можливості. При всіх інших рівних умовах, більш важливо, що ці «інші» діятимуть відповідно до певного рівня поведінки, коли це вимагається законом.

Тим не менш, правова невизначеність іноді може вважатися бажаною навіть для «потужних» держав. Наприклад, в перші дні дослідження космосу лише дві держави могли діяти в космічному просторі: США та Радянський Союз. Проте ці дві держави суперечили, протягом значного часу, взяти на себе зобов'язання щодо будь-яких обов'язкових правил, які регулюють космічний простір. Обидві вважали, що прийняття таких правил лише призведе до обмеження їх діяльності в космосі. У цьому контексті законна невизначеність була корисна тим, хто має силу діяти в космосі, для обох сторін холодної війни.

Хоча інформаційний, кіберпростір та космічний простір, хоч і часто об’єднуються як так звані «глобальні надбання», вони відрізняються одне від одного. Це відбувається не тільки тому, що багато держав кидають виклик самій ідеї про інформаційний простір як загальний, прагнучи затвердити більший контроль в Інтернеті. Що ще важливіше, інформаційний простір вже набагато більш багатолюдний, ніж космічний простір. США та Радянський Союз були не тільки єдиними державами, що займалися дослідженням космосу протягом кількох десятиліть, вони також були єдиними акторами, здатними до космічного польоту як такого. Всупереч цьому, в інформаційний та кібер простір в першу чергу проникають неурядові суб’єкти, до яких входять окремі індивіди, корпорації та інші організовані групи. Можливість онлайн-анонімності в поєднанні з відповідною складністю присвоєння кібер-операцій призвели до «драматичного посилення» влади в руках цих недержавних акторів за рахунок їх державних колег.

Недержавні суб’єкти тепер перейшли на територію, вільну від нормотворчості, яку раніше займали виключно держави. Ці події переважно зумовлені приватним сектором та академічними колами, про що свідчить пропозиція Microsoft щодо кібер-норм і так званий проект Талліннського керівництва.

Більш пізніша з двох пропозицій Microsoft, що має назву «Міжнародні норми кібербезпеки: зменшення конфлікту в Інтернет-залежному світі», опублікована в грудні 2014 році. Цікаво, що це не перша така ініціатива приватного сектору. Рівно 15 років тому Стів Кейс, тодішній головний виконавчий директор AOL, закликав держави переглянути свої закони, орієнтовані на країну, і замість цього приймати «міжнародні стандарти», що регулюють важливі аспекти поведінки в Інтернеті, включаючи безпеку, приватне життя та оподаткування. Тим не менше, пропозиція Microsoft – це перша всеосяжна пропозиція про конкретні стандарти поведінки в Інтернеті, яка, незважаючи на її приватне походження, пропонує норми, що мають на меті регулювати виключно поведінку держав.

У 2013 році міжнародна група експертів під керівництвом професора Майкла Шмітта опублікувала Таллінський посібник з міжнародного права, що застосовується до інформаційної війни. Хоча цей проект був здійснений під егідою Центру компетенції кібернетичного співробітництва в Естонії (CCD COE). Посібник дає зрозуміти, що його текст слід розглядати як такий, що відображає думки самих експертів, а не держав або установ, з яких вони походять. Як випливає з його назви, в Посібнику зберігається чітка військова парадигма в усьому, зосереджуючись на закон про застосування сили (jus ad bellum) та закон про збройний конфлікт (jus in bello). В його тексті визначено 95 правил, прийнятих консенсусом між групою експертів, які керувалися амбіціями «тиражувати звичні міжнародні закони». Проте поточний проект «Таллінн 2.0», який завершився в 2016 році, розвів деякі з цих заперечень, звернувши свою увагу на «нижні пороги» операцій та вирішуючи питання державної відповідальності, міжнародне телекомунікаційне право і навіть право на права людини. Як і в документі Microsoft, інтерпритарацією проекту Талліннського керівництва є висовування державно-орієнтовних стандартів поведінки держав.

Зрозуміло, що дві ініціативи дуже важливі. Норми, запропоновані компанією Microsoft, явно означаються лише як широкі пропозиції, а це означає, що державам потрібно перетворити їх у більш конкретні зобов'язання. Наприклад, норма передбачає, що держави повинні мати чітку принципову політику щодо уразливості продуктів та послуг, яка відображає сильний мандат, щоб повідомляти їх постачальникам, а не зберігати, купувати, продавати або використовувати їх. Як визнано у самому документі така політика повинна бути розроблена кожною окремою державою та адаптована до потреб відповідної держави.

На відміну від цього, правилами Талліннського посібника вживаються більш обмежувальні та специфічні форми передбачених звичайними юридичними зобов'язаннями, які держави просто повинні дотримуватися як обов'язкових, без необхідності їх подальшого схвалення або адаптації. Іншими словами, ціль посібника в інтерпретації застосування існуючих правових норм до поведінки в

інформаціному просторі. З огляду на те, що в керівництві часто виникають детальні та нові позиції, не завжди вдається проводити чітку лінію між інтерпретацією та розробкою норм. Тим не менше, передбачувані правила, які він містить, є набагато більш конкретними, ніж норми Microsoft щодо кібербезпеки. Наприклад, правило 37 встановлює заборону на кібератаки проти цивільних об'єктів у контексті збройного конфлікту. Обидва ключових терміна – кібернапади, а також цивільні об'єкти – точно визначені в Інструкції. Хоча деякі розбіжності можуть зберігатися щодо застосування правила в конкретних обставинах, зміст норми є достатньо чітким та точним, щоб створити законні права та обов'язки.

Тим не менше, такі ініціативи як проект Microsoft чи Таллінське керівництво мають не урядове походження і відповідно не несуть обов'язкового характеру. Microsoft усвідомлює свою пропозицію обмеження у цьому відношенні та зазначає, що вона просто закликає держави встановити пропоновані норми щодо траєкторії, з тим щоб зробити їх першими політичними, а потім юридично обов'язковими. Аналогічно, в посібнику на початкових сторінках було зазначено, що він є не обов’язковим документом. Оскільки ці тексти в цілому є продуктами недержавних ініціатив, вони навряд чи можуть бути чимось іншим. Зрештою, з можливими незначними кваліфікаціями у сфері колективної безпеки, все ще вірно, що лише держави є законодавцями міжнародної правової системи.

Якщо ці тексти не є обов'язковими, можна поставити під сумнів їх відповідність з точки зору міжнародного права взагалі. Правда, їх нормативність (у сенсі сили їх претензії на владу) нижча, ніж у міжнародно-правових норм. Це не означає що ці зусилля не мають значення для формування норм міжнародного права, і тим не менше вони документують будь-яку припущену неприйнятність міжнародного права до сфери інформаційної безпеки. Навпаки, недержавні ініціативи такого роду потенційно можуть стати «життєво важливим проміжним етапом для більш жорсткої обов'язкової системи, що дозволяє експериментувати та швидко модифікуватись». Крім того, вони роблять процес законотворення більш багатостороннім та всеосяжним, ніж традиційне державне нормування.

Тому найважливішим питанням є те, чи держави вирішать підхопити ініціативи, запропоновані їх недержавними колегами, і відновити роль головних законодавців.

Кіберпростір – це не перше нове явище, яке протягом деякого часу після його виникнення протистояло розвитку структур глобального управління. Ступінь очікування або припинення може навіть відображати прагнення до кращого розуміння стратегічного потенціалу нового феномену. Проте з покращенням розуміння державою нової ситуації, як правило, зростає також їх бажання підкорятися обов'язковим правилам. Навіть область космічного простору в кінцевому підсумку була піддана обов'язковому правовому режиму, незважаючи на сильне первинне небажання домінуючих держав у космосі.

Тим часом держави керувалися неприйнятними стандартами та критеріями безпеки, більшість з яких були випущені Міжнародним агентством з атомної енергії (МАГАТЕ). Пізніше конвенції з ядерної безпеки об'єднали це нове коло необов'язкових норм та зробили багато відповідних стандартів обов'язковими для всіх держав-членів.

Більш доречно розглядати поточну ситуацію як проміжний етап на шляху до створення «твердого права». Недержавні ініціативи дають можливість державам виявляти дублювання їхніх стратегічних інтересів, і вони можуть служити нормоутворюючими лабораторіями. Їх корисність у цьому сенсі підтверджена недавньою доповіддю Інституту Схід-Захід, яка допоміжним чином розкриває сфери конвергенції за різними пропозиціями норм поведінки держави в інформаційному та кіберпросторі, включаючи ті, що аналізуються.

Останній момент, який слід розглянути – це так звана проблема атрибуції (розуміється як складність визначення ідентичності або місцезнаходження кібер-атакуючого або їх посередника). Певний час це справедливо розглядалося як перешкода для розвитку ефективного правового регулювання інформаційної діяльності. Існуюча анонімність в мережі інтернет ускладнює застосування правил, регулювання та стримування кібер-загроз. Проте нещодавній технічний прогрес підвищив довіру держав щодо кібер-діяльності. Наприклад, США

стверджують, що зараз вона має потенціал щоб знайти своїх кібер-супротивників та здійснити їх затримання. У подібному твердженні Канада зазначила, що вона має надійні системи, що дозволяють локалізувати кібер-загрози, в тому числі ті, що організовуються суб'єктами, що фінансуються державою. Значний прогрес також досягнуто в розуміння правових стандартів присвоєння, які застосовуються до ведення онлайн-процедур. Проблема атрибуції може бути максимально керована, але не вирішена.

Спираючись на виявлену вище сформовану нормативну конвергенцію, держави повинні мати можливість відновити свою центральну роль у міжнародному законодавстві. У найближчому майбутньому вони повинні стати більш готовими, висловлюючи свою думку щодо тлумачення існуючого міжнародного права щодо інформаційної проблеми. Крім того, держави повинні поступово подолати поточне неприйняття до зобов'язань за договорами. Звіти з кінця 2015 року про те, що США та Китай почали вести переговори щодо обов'язкового підписання договору про контроль над озброєннями в інформаційному та кіберпросторі, є можливим раннім знаком того, що цей процес вже триває. І нарешті, цей процес прийняття державою нормотворчості може в кінцевому рахунку цілком імовірно призвести у прийнятті одного чи кількох всеосяжних багатосторонніх зобов'язань, можливо, починаючи з питань визначення, щоб прокласти шлях до майбутнього досягнення консенсусу щодо більш суттєвих питань.

Дві групи урядових експертів (GGE) були створені в 2004 і 2009 роках. Обидві групи зосереджені на існуючих і потенційних небезпеках в інформаційній сфері та вивчають можливі багатосторонні ініціативи щодо їх вирішення. Завдяки «новизні» інформаційної безпеки, перша група не змогла досягти угоди по його остаточній доповіді. Беручи до уваги, друга група успішно затвердила доповідь «A/65/201», опубліковану в 2010 році, яка складалася з цілого ряду рекомендацій, в тому числі:

– діалог для створення норми про те, як держави повинні забезпечити ІКТ;

- заходи щодо зміцнення довіри між державами, в тому числі дискусії по кібервійні;
- інфраструктурний потенціал в менш розвинених країнах;
- розробка загальних визначень і понять, пов'язаних з інформаційною безпекою.

Потім GGE одноголосно прийняли резолюцію «A/RES/66/24», закликаючи до подальшої діяльності за підсумками попередньої групи. дві групи урядових експертів GGE взяли до уваги результати і рекомендації, включені в доповідь і почали свою роботу в 2012 році, через рік, вони представили свою доповідь «A/68/98» на 68 сесії Генеральної Асамблеї ООН. 27 грудня 2013 року Генеральна Асамблея ООН одноголосно прийняла резолюцію «68/243», в якій вона прийняла до уваги результати 2012 та 2013 років. Дві групи урядових експертів GGE та Генеральний секретар закликали створити нову GGE, щоб підготувати доповідь для Генеральної Асамблеї в 2015 році, Група досягла угоди про доповідь в червні 2015 року «A/70/174» за правилами і принципам відповідальної поведінки держав в кібер-сфері. Заходи по зміцненню довіри, міжнародне співробітництво та нарощування потенціалу також є важливими темами обговорення. Зазначена доповідь також відноситься до застосування міжнародного права щодо використання ІКТ і дає рекомендації для майбутньої роботи. Наприклад:

- в їх використанні ІКТ, держави повинні дотримуватися, поряд з іншими принципами міжнародного права, державного суверенітету, вирішувати спори мирним шляхом і невтручання у внутрішні справи інших держав;
- існуючі зобов'язання за міжнародним правом застосовані до державного використання ІКТ, і держави повинні виконувати свої зобов'язання по дотриманню і захисту прав людини і основних свобод;
- держави не повинні використовувати проксі для здійснення міжнародно-протиправних діянь з використанням ІКТ, і повинні прагнути до того, щоб їх територія не використовувалась недержавними суб'єктами для здійснення таких актів;

– ООН повинна відігравати провідну роль у розвитку діалогу з питань безпеки ІКТ в її використанні державами, а також в розробці спільного розуміння з питань застосування норм міжнародного права і норм, правил і принципів відповідної поведінки держав.

Організація економічного співробітництва і розвитку (ОЕСР), запропонувала рекомендації з безпеки інформаційних систем і мереж з тим, щоб сприяти створенню «культуру безпеки» серед своїх держав-членів. Ці принципи, прийняті в 2002 році, сприяння в зміцненні принципів для просування інформаційної безпеки систем і мереж, для направлення фінансів на добробут і соціальний розвиток. У 2012 році ОЕСР ініціювала перегляд цих керівних принципів. На 1 жовтня 2015 року Організація випустила нові рекомендації та подальші пояснення і подробиці з вищезазначеного питання, ОЕСР також опублікувала рекомендації, що стосуються захисту приватного життя та транскордонних потоків персональних даних.

Отже основною стратегією забезпечення інформаційної безпеки в міжнародній сфері є орієнтування на співпрацю з зовнішніми партнерами і зміцнення договірно-правової бази для глобального регулювання даної сфери, також в той же час не забувати про посилення внутрішнього регулювання та орієнтацію на власні ресурси і рішення. Необхідно сконцентрувати увагу на два основні напрямки роботи: зниження ризиків військово-політичного використання ІКТ та формування основ міжнародно-правового режиму відповідальної поведінки держав в інформаційному просторі.

2.2. Організаційно-правовий механізм інформаційної безпеки держав

Зусилля по створенню єдиного інформаційного простору та подолання проблем на цьому шляху у великій мірі залежать від ефективного співробітництва між всіма без винятку учасниками міжнародного співтовариства. Для створення угод з певними межами, щодо розвитку інформаційної сфери на глобальному

рівні у подальшому буде відігравати двостороннє та багатостороннє співробітництво.

З цією метою можна використовувати досвід та діяльність міжнародних фінансових інститутів, включаючи багатосторонні банки розвитку, особливо Всесвітній банк, які можуть займатися фінансуванням та розробкою відповідних програм, направлених на розвиток процесу інформатизації суспільства.

Міжнародна мережа телекомунікацій, ЮНКТАД, ЮНДП та інші міжнародні фонди також можуть відіграти у цьому напрямку важливу роль. Важливим може стати внесок таких міжнародних організацій як Глобальна ініціатива щодо ліквідації електронно-цифрового розриву Всесвітнього економічного форуму та Глобальний діалог бізнесу з питань електронної торгівлі. З цією метою було створено Групу по можливостям інформаційної технології, щоб об'єднати зусилля з метою формування широкого міжнародного підходу у вирішенні питань міжнародного інформаційного співробітництва.

У розвинених країнах світу розроблено спеціальні програми розбудови інформаційної інфраструктури, спрямовані на об'єднання в єдиний інформаційний простір та створення уніфікованої законодавчої бази.

Так на комп'ютерне програмне забезпечення вільного використання у 2002 р. почали переходити установи сфери освіти та науки Німеччини.

Китай з 1990 р. адаптував вільне програмне забезпечення не тільки в урядових установах, а серед інших суб'єктів господарювання на своїй території і зробив це державною політикою.

Аналогічним шляхом йдуть Індія, Перу, країни Скандинавії. Навіть у США – NASA і Військово-морський флот так само, як і значна кількість інших організацій, адаптує програмне забезпечення вільного використання.

Говорячи про світовий інформаційний простір не можна обійти увагою Інтернет, який суттєво впливає на різноманітні сторони соціального життя. З урахуванням швидкості та розмірів поширення комп'ютеризації у світі історію людства навіть поділяють на дві сфери – до та після появи Інтернету. Доступ

населення до Мережі стає однією з важливіших показників розвитку тієї чи іншої країни.

ЮНЕСКО в рамках свого мандата сприяє політиці в галузі створення інформаційного простору на міжнародному рівні. Ще у 1978 р. ЮНЕСКО прийняла Декларацію основних принципів щодо внеску мас-медіа в зміцнення миру і міжнародного взаєморозуміння, підтримки прав людини і запобігання расизму і війни. У 1980 р. важливість цієї декларації ЮНЕСКО була підтверджена важливим документом – публікацією доповіді, видатного політика Шона Макбрайда. Одним з найважливіших аспектів доповіді під назвою «Багато поглядів – один світ» («Many Voices, One World») було засвідчення транснаціонального контролю над міжнародною комунікацією. У ній зазначалося, що для того, щоб громадяни могли ухвалювати свідомі політичні рішення, потрібен широкий спектр інформації і думок з тих чи інших питань. Таким чином, ключовим критерієм свободи інформації є різноманітність її джерел у поєднанні з вільним доступом до цих джерел. Макбрайд пішов навіть далі, наголошуючи, що самої по собі диверсифікації власності замало, потрібна радше диверсифікація джерел інформації та поглядів. Важливим моментом є те, що для реалізації цих положень передбачали впровадження певних різновидів регулювання монополізму і концентрації власності, певною мірою виправдання високих стартових витрат для випуску інформаційної продукції і, можливо, навіть підтримку неприбуткових і громадських комунікаційних структур. Сутність пропозицій, викладених комісією Макбрайда, була підтримана Белградською резолюцією, схваленою XXXII сесією Генеральної конференції ЮНЕСКО у жовтні 1980 р. [35].

На сучасному етапі розвитку міжнародних інформаційних відносин ЮНЕСКО запровадила програму «Інформація для всіх». Вона направлена на зменшення відмінностей між інформаційно багатими та інформаційно бідними країнами підчас створення інформаційного простору для всіх. На її основі проводяться обговорення з питань міжнародної політики і розробки програм, спрямованих на:

- більше розуміння проблем етичного, правового і суспільного характеру, пов'язаних з інформаційно-комунікаційними технологіями;
- поліпшення доступу до інформації, що є суспільним надбанням;
- збереження інформації.

Програма «Інформація для всіх» передбачає загальну схему міжнародної співпраці і партнерства. Вона заохочує розробку загальних стратегій, методів і інструментів для створення інформаційного простору для всіх.

На сьогодні розроблені та ефективно діють такі основні європейські інформаційні сервери:

- CORDIS сервер – https://cordis.europa.eu – інформаційний сервер, що стосується досліджень і розробок в межах Європейського Союзу, містить більше десяти баз даних.
- Council Presidency Service – інформація, що надається державами в ЄС.
- National Research & Development and Innovation Information Service – Національна інформаційна служба з досліджень, розвитку та інновацій. Містить новини в галузі науки та інновацій з держав-членів ЄС, кандидатів та асоційованих країн ЄС.
- ERGO – це каталог національних проектів, проектів ЄС, науково-дослідницьких робіт, що виконуються або виконувались в рамках ЄС. Каталог містить коротку інформацію щодо 91093 проектів з 21 інформаційного джерела.
- CERIF – Загальний європейський дослідницький інформаційний стандарт. Це набір документів для кожного, хто створює або працює з базами даних досліджень та розробок. Він включає перелік важливих базових даних та вибіркові елементи, що можуть використовуватися для опису попередніх даних.
- Regional Research and Innovation Service – Інформація про дослідження та інновації у регіонах Європейського співтовариства. Його мета полягає у створенні динамічного інформаційного простору для дослідницьких,

інноваційних робіт, сервісів та інформаструктури в регіонах та країнах ЄС.

– INCO – Інформаційний пункт спрямований на поширення загальної інформації щодо міжнародної кооперації в рамках програми ЄС з досліджень, технологічного розвитку та демонстраційної активності [35].

Загальноприйнятою практикою у світі є утворення служб та механізмів, що спеціально займаються поширенням відкритих повідомлень про країну. Зазвичай це розглядається як розумний баланс між демократичними принципами права на інформацію й свободи слова і здійснюваним в інтересах суспільства та громадян контролем за нею. Одним із перших прикладів створення таких органів у країнах світу став Комітет стратегічних комунікацій (Strategic Communication Unit) у Великобританії.

В Європі на основі інформаційних технологій формується інформаційний ринок, відбувається стандартизація доступу до адміністративних баз даних, підключення до транс-європейської мережі даних [35]. Отже як стає зрозуміло, було розроблено багато інформаційних програм, що розроблюються по теперішній час, для більшого вдосконалення цієї сфери та для навчання суспільства.

На 2018 р. планувалось провести інформаційні конференції-саміти які допоможуть у розвитку сфери інформаційної безпеки.

1. Щорічний саміт FS-ISAC – розміщується центром обміну та аналізу фінансових послуг, ресурсу, який допомагає членам світової фінансової галузі поділяти та аналізувати інформацію про цифрові та фізичні загрози. Учасники цього щорічного заходу мають можливість почути серію засідань та переговори про новітні загрози, що стоять перед світовим сектором фінансових послуг.

2. Перша щорічна конференція – форум груп реагування на інциденти та небезпеку. Ця п'ятиденна щорічна конференція включає функції реагування на інциденти, управління та технічні сліди, основні презентації і безліч мережевих можливостей. Окрім вивчення найсучасніших стратегій безпеки в управлінні

інцидентами, ті, хто відвідує, можуть заробити до 25 кредитів, що продовжують професійну освіту, і отримати розуміння аналізу мережевої вразливості. Захід проводиться за підтримки Форуму груп ризику та безпеки (FIRST), міжнародної конфедерації з більш ніж 350 довірених груп з реагування з більш ніж 80 країн.

3. Інформаційність Європи (InfoSecurity Europe) – це щорічна конференція, яка перетворилася в один з найбільших і найвидатніших в Європі заходів з інформаційної безпеки. ЇЇ репутація підкріплена вільним відвідуванням. У 2014 році InfoSecurity Europe відвідало приблизно 11500 відвідувачів з більш ніж 70 країн. У минулому році її відвідало понад 19500 відвідувачів.

4. Жінки в галузі кібербезпеки – це один з видів досвіду, розроблений для жінок в галузі кібербезпеки, ця конференція привертає більше уваги кожним новим роком. З різних навчальних досягнень академічних кіл, наукових досліджень та промисловості це чудова можливість організувати та провести ряд семінарів, починаючи від вступу до кібербезпеки до більш технічних тем, таких як цифрова криміналістика.

5. Конференція «Атлантична безпека» – ця конференція об'єднує одні з найяскравіших і найглибших умів у світі, щоб розтягнути межі IT-безпеки. Вона виходить за межі звичайного та говорить про безпеку IT за межами периметру, показуючи людям те, що ще не було виявлено переважною більшістю користувачів.

Міжнародне співтовариство на рівні міжнародних організацій визнало факт подвійного використання високих технологій. Співробітництво у сфері інформаційної безпеки потребує пошуку спільних рішень щодо протидії інформаційним і кіберзагрозам, вироблення міжнародних стратегій інформаційної безпеки щодо кібервоєн, інформаційного тероризму і злочинності. БРІКС – неформальне угруповання, яке об’єднує Федеративну Республіку Бразилію, Республіку Індію, Китайську Народну Республіку, Російську Федерацію і Південно-Африканську Республіку. У сфері інформаційної безпеки країни БРІКС дотримуються стратегій і програм регіональних організацій, до яких вони належать і які демонструють різні підходи до розуміння глобальних

інформаційних загроз і практики протидії викликам високих технологій. Відтак, Бразилія як член Організації Американських Держав підтримує ініціативу США зі створення глобальної культури кібербезпеки і протидії інформаційному тероризму, яка спрямована на запобігання та знешкодження кібератак, боротьбу з кіберзлочинністю, захист критично важливих інфраструктур і мережевих систем. Підсумком цієї ініціативи було створення Міжамериканської мережі груп реагування на надзвичайні ситуації в комп'ютерній сфері, визначення і прийняття єдиних стандартів галузі, здійснено модернізацію нормативно-правової бази для боротьби з кіберзлочинністю, зокрема, приєднання до Європейської конвенції про кіберзлочинність як модельного інструменту в боротьбі з кіберзлочинами в межах асоціації.

Сучасна політика інформаційної безпеки Бразилії пов'язана з концепціями інформаційного протиборства США і пріоритетами співробітництва у форматі «інформаційної парадигми», що передбачає інформаційно-технологічні переваги держави, здатні зберегти досягнуту в докризовий період стабільність і забезпечити посткризовий розвиток, зробити прогнозованими перебіг соціальних конфліктів, запобігти суперечностям у суспільстві. Відповідно, співпраця Бразилії в межах ОАД характеризується поворотом до мілітаризації інформаційної сфери, яка означає тіснішу координацію політичних і силових структур у сфері «кібербезпеки», а також визначенням військових і невійськових аспектів психологічних та інформаційних операцій.

Зокрема, Програми ЄС у сфері інформаційної безпеки стосуються: співробітництва з Радою Безпеки ООН; зміцнення стратегічного партнерства зі США, Росією, Японією, Китаєм, Канадою та Індією; вдосконалення регуляторної політики щодо інформаційної безпеки; розробки і прийняття конвенцій, директив, рекомендацій і резолюцій; розробки доктрин європейської і національної політики інформаційної безпеки та зростання ролі ЄС у забезпеченні регіональної інформаційної безпеки. Так, Індія (у форматі Організації оборонних досліджень і розробок) на рівні стратегічного партнерства підтримує запропоновану Росією концепцію конвенції з інформаційної безпеки з огляду на значне зростання

кількості злочинів у цій сфері, з яких найнебезпечнішими вважаються злочини в кредитно-фінансовій сфері з використанням інформаційних технологій, і Європейську Конвенцію з кіберзлочинності, оскільки формування європейської системи інформаційної безпеки здійснюється на базі загальноприйнятих принципів, тобто, чіткого усвідомлення важливості чинників високих технологій, що впливають на стан національної безпеки, політичних, економічних, військових, етнічних, екологічних та інших складових демократичних процесів, взаємовигідних міждержавних відносин, механізмів колективного реагування на нові загрози, що набули трансконтинентального характеру.

Що стосується Південної Африки, то політика інформаційної безпеки держави передусім відповідає принципам Європейської Конвенції з кіберзлочинності, оскільки в ЮАР було розроблено і 2012 року затверджено відповідний документ про політику кібербезпеки Південної Африки. Крім того, некомерційна організація «Група інформаційної безпеки в Африці», яка була створена у відповідь на збільшення ІТ-безпеки і кібер-злочинності з метою допомоги організаціям з широким спектром інформаційних ризиків, що стоять перед африканським континентом, здійснює впровадження політики кібербезпеки для африканського співтовариства.

Китай і Росія як учасники регіональних об’єднань АТЕС і ШОС розглядають політику інформаційної безпеки як у контексті економічного співробітництва з питань лібералізації торгівлі та інвестицій, так і боротьби з кібертероризмом і використанням високих технологій із злочинною метою. Оскільки АТЕС об’єднує 21 економіку АТР (складається з Австралії, Брунею, В’єтнаму, Гонконгу (Китай), Індонезії, Канади, КНР, Республіки Корея, Малайзії, Мексики, Нової Зеландії, Папуа Нової Гвінеї, Перу, Росії, Сінгапуру, США, Таїланду, Тайваню, Філіппін, Чилі, Японії), політика інформаційної безпеки організації насамперед стосується проблем захисту критично важливої інфраструктури від терористичних загроз. Особливої уваги АТЕС набула проблема кібертероризму, оскільки Інтернет став важливою основою для формування «нової економіки», заснованої на знаннях, розвитку електронної

комерції, електронного уряду, соціального забезпечення потреб суспільств країн АТР на основі ІКТ. Діяльність КНР в АСЕАН стосується стратегії боротьби з кібертероризмом, співробітництва в межах Регіонального форуму з безпеки, який нині є єдиним в АТР механізмом багатостороннього регіонального політичного діалогу з усього спектру питань, пов'язаних з підтриманням миру і стабільності. Його завданням є забезпечення завдяки діалогу і консультацій безконфліктного розвитку Південно-Східної Азії і всього Азіатсько-Тихоокеанського регіону через створення надійної системи інформаційної безпеки [22].

Розглянемо сферу інформаційної безпеки в різних країнах світу.

Австралія. Австралія очолює Групу експертів Організації економічного співробітництва і розвитку (ОЕСР), яка підготувала Керівництво ОЕСР з безпеки інформаційних систем. Австралія також є головою Робочої групи ОЕСР з питань безпеки та конфіденційності інформації, яка несе відповідальність, зокрема, для моніторингу потреби в інформаційній безпеці. Усередині країни, докладні процеси для забезпечення безпеки урядової інформації і стандарти Австралії, в поєднанні зі Стандартами Нової Зеландії розробили спільний стандарт по управлінню інформаційної безпеки, заснований на британському стандарті. Австралійський уряд і промисловість в даний час працюють разом на заходи по захисту національної інформаційної інфраструктури.

Мета інформаційної безпеки, як це визначено в Керівництві ОЕСР з безпеки інформаційних систем є захист інтересів, спираючись на інформаційні системи від шкоди внаслідок відсутності доступності, конфіденційності і цілісність.

З конвергенцією технологій, мета може бути поширена на телекомунікаційні системи, які представляють собою особливий тип інформаційної системи. Будь-яке втручання або використання інформаційних систем буде мати вплив на будь-який вид доступності, конфіденційності та цілісності. Існує небезпека розвитку визначення конкретної технології у швидко мінливому середовищі.

Куба. Куба впродовж десятиліть була піддана агресії з боку Сполучених Штатів в сфері радіо і телебаченні, яка є частиною непохитної політичної агресії з

боку передової військової сфери світу, економічної і політичної влади, чия заявлена мета була в поваленні уряду Куби.

У більшості випадків інформація підбурювала кубинських громадян до здійснення актів громадянської непокори і брати участь в деструктивних і терористичних актах.

Куба завжди була на користь вирішення розбіжностей між державами на основі рівності і поваги національного суверенітету і незалежності, і висловлювати це публічно в різних випадках. Ця позиція залишається незмінною.

Доцільність розробки міжнародних принципів, які б підвищували безпеку глобальних інформаційних і телекомунікаційних систем, а також допомогти в боротьбі з інформаційним тероризмом і злочинністю.

Без сумніву, розвиток нових інформаційних технологій вимагає паралельних зусиль із забезпечення прогресивного розвитку міжнародного права в цій галузі, включаючи розробку адекватної правової бази, яка сприятиме підвищенню безпеки інформаційних систем.

Завдання не буде легким, якщо взяти до уваги той факт, що є ще питання, які зажадають розробці загальноприйнятих визначень з метою сприяння подальшій кодифікації нових принципів, які допомогли б досягти цілей в області безпеки. Сама природа глобальних мереж виходить за межі юрисдикції кожної країни. У багатьох випадках це робить неможливим покладатися на географічні кордони. Крім того, нерівномірний розвиток держав, серед інших чинників, досить важко встановити єдині міжнародні правила, які будуть, застосовуватися до всіх країн.

Тим не менш, не потрібно починати з нуля, оскільки вже існують загальноприйняті принципи і міжнародно-правові документи, які були узгоджені і прийняті державами в різних багатосторонніх форумах відповідно до останніх технічних прогресів. Ці принципи і інструменти були б дуже корисні для зміцнення або розробки нових міжнародних принципів з метою підвищення безпеки глобальних інформаційних та телекомунікаційних систем, а також допомогти в боротьбі з інформаційним тероризмом і злочинністю.

Наведемо лише кілька відповідних прикладів таких угод Куба вважає, що такі повинні бути прийняті до уваги:

- Резолюція 110 Генеральної Асамблеї (II) від 3 листопада 1947, яка засуджує пропаганду, яка може спровокувати або посилити загрозу миру, порушення миру або акт агресії.
- Міжнародна конвенція електрозв'язку, прийнята в Найробі в 1982 році, а також відповідні міжнародно-правові документи, прийняті з питань освіти Організації Об'єднаних Націй, науки і культури та Міжнародного союзу електрозв'язку.
- Принципи, що регулюють використання державами штучних супутників Землі для міжнародного безпосереднього телевізійного мовлення, які були прийняті Генеральною Асамблеєю і які передбачають, що такі заходи повинні проводитися відповідно до норм міжнародного права і в манері, сумісної з розвитком взаєморозуміння і зміцнення дружніх відносин і співробітництва між державами і народами в інтересах підтримання міжнародного миру та безпеки.
- Конвенція про заборону розробки, виробництва, накопичення і застосування хімічної зброї та про її знищення, в додатку до якої містяться положення про захист конфіденційної інформації, яка може також служити в якості корисного довідкового матеріалу для розробки вищевказаних принципів.

І, нарешті, в рамках провідної ролі, яку Організація Об'єднаних Націй, Куба вважає, що повинна рекомендувати державам прийняти закони, які санкціонують розробку та розповсюдження комп'ютерних вірусів і інших шкідливих програм. Крім того, юридично обов'язкові багатосторонні угоди, що забороняють агресію проти інформаційних і телекомунікаційних систем.

Сполучені Штати Америки. США вважають, що інформаційна безпека є широкою і складною темою, що охоплює безліч чинників і зачіпає багато різних видів діяльності окремих осіб, груп і урядів. Хоча загальна тема включає в себе

аспекти, які стосуються міжнародного миру і безпеки (робота Першого комітету), він також включає в себе технічні аспекти, які стосуються глобальних комунікацій, а також не технічних питань, пов'язаних з економічним співробітництвом та торгівлею, прав інтелектуальної власності, правоохоронні органи, антитерористичне співробітництво та інші питання, які розглядаються в другому або шостому комітеті. Дії і програма уряду ні в якому разі не є єдиним відповідним засобом, для інформаційної безпеки також включає в себе важливі проблеми окремих осіб, асоціації, в ході збройного конфлікту, країни використовували різні методи, пов'язані з інформаційною безпекою. Вплив радіочастот та електромагнітні контрзаходи два очевидних приклади; такі методи мають довгу історію. У майбутньому, це буде мати важливе значення для військових сил для захисту своїх власних каналів передачі даних та інші пов'язані з комп'ютером системи. Крім того, держави-члени повинні мати можливості для відновлення основних інформаційних систем в тому випадку, якщо стихійне лихо або катастрофічні аварії відключають основні засоби зв'язку або інші мережі передач даних в державних і приватних секторах. Інформаційна безпека також поширюється на захист інформації, яка стосується військового потенціалу та інших аспектів національної безпеки.

Інформаційна безпека включає в себе необхідність захисту наукових досліджень комерційного характеру, а також технології виробництва та інших видів власних даних (наприклад, маркетингових планів та інформації обслуговування клієнтів).

Інформаційна безпека також пов'язана з необхідністю забезпечення дотримання міжнародних угод з інтелектуальної власності (наприклад, відео та аудіо матеріалів, а також комп'ютерне програмне забезпечення), щоб захистити його від несанкціонованого копіювання та продажу. Захист приватного життя є ще одним аспектом інформаційної безпеки, тобто забезпечення безпеки особистої і комерційної інформації, переданої через публічну міжнародну мережу або через приватні канали передачі даних.

На технічному рівні, правила Міжнародного союзу електрозв'язку і діяльності національних партнерів забезпечити сумісність електронних сигналів, належне використання електромагнітного спектра і широкої надійності міжнародної мережі. Ці функції також відносяться до супутників, які надають широкий спектр послуг, таких як передача голосу і ретрансляції даних, а також даних локаторів та іншої інформації, використовуваної для повітряного і морського судноплавства і для пошуково-рятувальних служб. Крім того, дизайн та стандарти безпеки забезпечують важливу гарантію для виробників і користувачів електронних пристроїв, включаючи комп'ютери. Всі ці нормативні та адміністративні функції можуть бути визначені в широкій концепції інформаційної безпеки.

Широке поширення залежність від інформаційних технологій призвело до безпрецедентного глобального зв'язку і взаємозалежності, в результаті чого багато аспектів національної та міжнародної діяльності, державного і приватного сектора, теоретично можна поставити під загрозу злочинних або терористичних зловживань.

У той час як ступінь залежності від інформаційної технології може варіюватися в залежності від штату, широти діяльності, які покладаються на такі зв'язки – економічні, комерційні, промислові, освітні, юридичні – означає, що всі держави потенційно вразливі до наслідків кримінальної експлуатації. Більш того, ця залежність може бути очікуваною, оскільки такі технології стають все більш і більш центральним значенням для стабільної роботи урядів, а також для підтримки ключових глобальних комерційних і комунікаційних систем, що витримують взаємодії між країнами. Тому Сполучені Штати розглядають злочинне використання інформаційних технологій як виклик інтересам усіх держав і розділяє заклопотаність, висловлену іншими [32].

Сполучені Штати також розглядають будь-яке незаконне вторгнення або спробу порушити або змінити будь-який аспект своїх національних інформаційних систем як потенційну загрозу для її національної інфраструктури і, таким чином, як загрозу своїх національних інтересів. Сполучені Штати,

визнаючи потенційну серйозність цієї загрози, ініціювало на національному рівні, в довгостроковій перспективі, державні і приватні програми, призначені для захисту своєї національної інфраструктури.

Кримінальне законодавство США забороняє втручання в інформаційні інфраструктури Сполучених Штатів. Сполучені Штати визнають відповідне судове переслідування дій, пов'язаних з кримінальним або терористичним використанням інформаційних систем.

Грузія. Грузія прагне розробити систему інформаційної безпеки, яка здатна звести до мінімуму шкідливий вплив будь-яких кібератак і дозволятиме швидке відновлення інформаційної інфраструктури, щоб нормалізувати свою діяльність в період після таких атак.

Грузія має на меті створити таку систему кібербезпеки, яка полегшить з одного боку, захист інформаційної інфраструктури від кібер-загроз (система конфіденційність, цілісність, доступність), а з іншого боку, буде додатковим фактором для економічного та соціального розвитку в країні.

Крім того, метою кібербезпеки Грузії є підвищення критичного опору інформаційних систем проти кібер-атак та викорінення наслідків кібер-інцидентів. Крім того кібербезпека, як невід'ємна частина національної безпеки грузинського законодавства та основні концептуальні документи в галузі національної безпеки визначають кібербезпеку як єдиний з напрямків політики національної безпеки, значення якої надзвичайно зростає паралельно з технологічним прогресом і, крім того, ефективний розвиток держави залежить від кібербезпеки.

Безкомпромісний захист і повага до прав людини та основних свобод – Уряд Грузії розглядає принципи безкомпромісного захисту прав людини в процесі розробки та реалізації політики національної безпеки. Природно, що вищезазначений принцип також має значення для процесу розробки та виконання політики кібербезпеки, оскільки кібербезпека є невід'ємною частиною національної безпеки.

Після російсько-грузинської війни 2008 року Грузія почала поетапний розвиток кібербезпеки. Такий розвиток, на початковому етапі, був зосереджений переважно на створення відповідних інституційних рамок та їх подальшого розвитку. У 2010 році Агентство обміну даними LEPL (англ. «Legal Entity of Public Law»), під керівництвом Міністерства юстиції Грузії було створено Агентство призначене для захисту інформаційних систем країни та запровадження інформаційних стандартів безпеки. Агентство також здійснює моніторинг об'єднаної державної мережі та аудит інформаційних систем.

З метою забезпечення кібербезпеки в галузі оборони, в 2014 році було запроваджено Бюро, яке функціонує в системі Міністерства оборони Грузії.

Бюро в режимі 24/7 відповідає за викорінення та попередження кібер-інцидентів спрямованих проти військової інфраструктури Грузії. Для ефективної реалізації вищезазначених функцій, Бюро забезпечує вивчення існуючої в цій галузі інфраструктури захисту, створення та розвиток механізмів безпеки.

Враховуючи той факт, що Агенція обміну даними та бюро кібербезпеки не виконують правоохоронні функції, було створено Відділ боротьби проти Кіберзлочинності в Департаменті Центральної кримінальної поліції при Міністерстві Внутрішніх справ Грузії. Відділ відповідає за розслідування кібер-інцидентів по всій країні. Відділ також представляє міжнародні контактні пункти, з функціями, пов'язаними з міжнародною співпрацею поліції відповідно до Європейської конвенції «Про кіберзлочинність».

Основні напрями політики кібербезпеки Грузії:

- дослідження та аналіз;
- нова нормативно-правова база;
- підвищення можливостей у сфері кібербезпеки;
- покращення обізнаності громадськості та створення навчальної бази.

Нова законодавчо-нормативна база Грузії. З 2010 року Грузія розробила загальну законодавчу базу, яка спрямована ефективно забезпечувати безпеку у відповідній сфері, що визначає права та відповідальність державного та

приватного секторів у сфері забезпечення інформаційної безпеки і який регулює державні механізми контролю за здійсненням інформаційної безпеки.

Разом з законодавчою базою як такою, вторинне законодавство було розроблено, з метою детального здійснення інформації та кібербезпеки. Відповідні норми передбачають керівні принципи для предметів інформаційної системи в процесі забезпечення кібербезпеки.

Китай. На початку цього року Китай випустив остаточну версію національного стандарту захисту персональних даних, інформаційні технології GB/T 35273-2017 – Специфікація захисту персональної інформації (Специфікація). Специфікація набрала чинності з 1 травня 2018 року.

Специфікація не є законом чи нормативним актом, яка вимагає обов'язкового дотримання. Однак, цілком імовірно, що китайські державні установи покладаються на стандарт, щоб визначити, чи відповідають компанії правилам захисту даних Китаю. Підприємства, які збирають або обробляють особисту інформацію в Китаї, повинні перевіряти свою поточну практику щодо цієї Специфікації для виявлення та мінімізації їхніх потенційних ризиків.

Особиста інформація та чутлива особиста інформація. За Законом про кіберзахист Китаю особиста інформація означає інформацію, яка може бути використана для ідентифікації особи, якщо вона використовується окремо або у поєднанні з іншою інформацією. Ця нова Специфікація розширює це визначення, включивши інформацію, що відображає діяльність людини, таку як історія веб-перегляду.

Чутлива особиста інформація включає в себе інформацію про те, що, якщо її витік, незаконне надання чи невиправдане використання, ймовірно, загрожуватиме особистій та майновій безпекці та може завдати шкоди особистій репутації, фізичному або психічному здоров'ю або призвести до дискримінаційного поводження. Приклади чутливої особистої інформації включають номер посвідчення особи, номер банківського рахунку та особисту інформацію неповнолітніх віком від 14 років.

Контролер даних. У новій специфікації вводиться поняття контролера персональних даних, тобто фізична особа або організація, яка визначає цілі та засоби обробки персональних даних. Контролер даних несе відповідальність за дотримання відповідних законів та правил у зборі, зберіганні, використанні, обміні та передачі особистої інформації, а також при обробці порушень даних.

Збір даних. У новій специфікації зазначається, що збір персональних даних має здійснюватися легально та мінімально. Це вимагає від контролера даних отримати згоду суб'єкта персональних даних (фізична особа, чиї дані збираються), а також вимагає явної згоди, коли збираються конфіденційні дані. Є кілька винятків, коли згода не потрібна. Наприклад, коли збирання та використання персональних даних є необхідними для виконання та виконання контрактів, для кримінального розслідування, або для новинних звітів, коли контролер даних є інформаційним агентством.

Контролер даних також повинен встановити та опублікувати політику конфіденційності відповідно до Специфікації. Політика конфіденційної моделі також додається до Специфікації.

Збереження даних. Особиста інформація повинна зберігатися протягом найближчого періоду часу і лише в тому обсязі, в якому це необхідно. Після того, як особиста інформація була зібрана, контролер даних повинен де-ідентифікувати таку інформацію та зберегти де-ідентифіковану інформацію окремо від будь-якої особистої ідентифікованої інформації. Коли контролер даних припиняє роботу, він повинен припинити збирати особисту інформацію, інформувати відповідні суб'єкти даних, а також видаляти або анонімізувати всю збережену особисту інформацію.

Використання даних. Контролер даних повинен обмежувати доступ до зібраної особистої інформації в мінімальному ступені необхідності. Дані суб'єктів мають право на доступ до даних та виправлення невірних або неповних даних, права на стирання та переносимість даних, а також право на скасування акаунту обміну та передачі даних. Коли контролер даних передає обробку даних третій стороні, контролер даних повинен провести оцінку безпеки, щоб гарантувати, що

сторонні процесори спроможні запропонувати достатню безпеку. Контролер даних повинен також здійснювати нагляд за процесором шляхом аудиту та шляхом застосування контрактних зобов'язань щодо захисту даних.

Якщо контролер даних повинен розповсюджувати або передавати особисту інформацію, він спочатку повинен провести оцінку безпеки, використовувати ефективні заходи для захисту суб'єктів даних, інформувати суб'єктів даних про ціль та одержувача передачі даних та отримати попередню згоду (окрема згода в крім первинної згоди збору та обробки даних). Якщо контролер даних придбаний або об'єднаний з іншими суб'єктами, він повинен повідомити суб'єктів даних про цей факт, а його правонаступник продовжувати виконувати первинні обов'язки та обов'язки контролера даних.

ЄС. В Європейському союзі було створено Європейське агентство з питань мережевої та інформаційної безпеки (ENISA), є центром експертизи для кібербезпеки в Європі. ENISA допомагає країнам ЄС бути краще оснащеним та підготовленим до запобігання, виявлення та реагування на проблеми інформаційної безпеки.

ENISA надає практичні поради та рішення для державного та приватного секторів у країнах та інституціях ЄС. Це включає:

- сприяння розробці національних стратегій кібербезпеки;
- сприяння співпраці між командами з реагування на аварійні ситуації та створення потенціалу.

ENISA також публікує звіти та дослідження щодо питань кібербезпеки. Вона провела дослідження щодо:

- захисту даних;
- підвищення технології забезпечення конфіденційності та забезпечення конфіденційності нових технологій;
- електронна ідентифікація та електронні довірчі послуги виявлення кібер-загроз.

ENISA допомагає розробляти політику та законодавство ЄС щодо мережі та інформаційної безпеки. Це також сприяє економічному зростанню на європейському внутрішньому ринку.

Як викладено в Постанові ЄС № 460/2004 та № 526/2013 стосовно Агентства Європейського Союзу з питань мережевої та інформаційної безпеки, до органів Агентства входять Виконавчий директор, Правління, Виконавча рада та Постійна група зацікавлених сторін.

Щоденна робота ENISA викладена в щорічній робочій програмі Агентства, яка готується щорічно після активних консультацій з керівництвом та виконавчим комітетом ENISA.

ENISA також створила потужну мережу зацікавлених сторін у державному та приватному секторах та прагне досягти наступного:

- Експертиза. Передбачати та підтримувати Європу в умовах виникнення мережевих та інформаційних проблем безпеки, беручи до уваги розвиток цифрового середовища.
- Політика. Полягає у наданні допомоги державам-членам та інституціям Союзу у розробці та реалізації політики, необхідної для законодавчих та нормативних вимог національної безпеки.
- Місткість. Підтримка Європи у покращенні сучасних можливостей мережі та інформаційної безпеки.
- Співтовариство. Посилити співпрацю між державами-членами.

ENISA також тісно співпрацює з спільними дослідженнями та інформацією з Європейською поліцією (Європолом) та Європейським центром комп'ютерних злочинів (EC3).

Агентство також підтримує інші установи ЄС, такі як:

- Агентство з питань правоохоронної підготовки Європейського Союзу (CEPOL).
- Орган європейських регуляторів електронних комунікацій (BEREC).

– Європейське агентство оперативного управління великомасштабними IT-системами у сфері свободи, безпеки та правосуддя (eu-LISA).
– Європейське агентство з авіаційної безпеки (EASA).

Основною цільовою групою ENISA є організації державного сектора, зокрема уряди країн ЄС та Інститути ЄС.

Агентство також обслуговує:

– індустрію ІКТ (телекомунікації, інтернет-провайдери та IT-компанії);
– бізнес-спільноти, особливо малий бізнес;
– спеціалістів з мережевої та інформаційної безпеки, такі як комп'ютерні команди з реагування на надзвичайні ситуації.

Розглянемо декілька країн Європейського союзу.

Нідерланди. Нідерланди, мають найбільш розвинену та зрілу систему інформаційної та кібербезпеки, як з точки зору правового забезпечення, так і з технічного та організаційного. Нідерланди кожні два роки переглядають свою Національну Стратегію кібербезпеки, а Національний Центр кібербезпеки, який являє собою національний CERT з додатковими повноваженнями, розробляє та впроваджує усі процедурні та технологічні питання, що мають відношення до кібербезпеки. Цей же Центр активно співпрацює з Аналітичними та інформаційними центрами (ISACs), які відповідають за безпеку критичної інформаційної інфраструктури за секторами. «Гаряча лінія» meldpunt-kinderporno.nl була ініційована голландськими Інтернет-провайдерами для боротьби з дитячою порнографією як приватна структура, але згодом отримала підтримку Міністерства юстиції Нідерландів. До речі, саме з Нідерландів почалась історія створення загально-європейської мережі «гарячих ліній» – InHope.

Сполучене Королівство Великої Британії. Глобальні інформаційні системи, які засновуються в даний час досягли точки, де багато, якщо не всі держави стикаються з потенційною загрозою для важливих елементів їх критичної інфраструктури від електронного нападу з боку злочинців і терористів. У той час

як небезпека електронного нападу збільшується з часом, як в державному так і в приватному секторі, так стають все більш залежними від комп'ютерних систем, які стають все більш взаємопов'язаними. Крім того, оскільки системи пов'язані на міжнародному рівні, загроза є транскордонною. Кримінальні і терористичні спроби проникнути в системи, зловмисні цілі становлять загрозу для всіх країн світу. Великобританія прийняла заходи від електронної атаки.

Внутрішні заходи включають в себе:

- В рамках уряду, всі критичні системи ідентифіковані.
- Робота з приватним сектором з метою розробки заходів, які удосконалюються з рівнем ризику і забезпечення належних стандартів захисту ключових систем, що входять в критичну національну інфраструктуру.
- Підвищення обізнаності та стандартів інформаційної безпеки в цілому в приватному секторі, проводячи існуючі ініціативи з розвитку передової практики.

У той же час, транскордонне з'єднання означає, що напади на системи в інших державах можуть надавати побічні дії на власну національну інфраструктуру Сполученого Королівства, і що терористи та злочинці, що діють з третіх країн можуть прагнути атакувати системи в Сполученому Королівстві. Тому Сполучене Королівство визнає, що міжнародне співробітництво має важливе значення для боротьби із загрозою зловмисних атак і прагне розвивати існуючі діалоги з цих питань зі своїми міжнародними партнерами.

Великобританія розробила свою комплексну стратегію кібербезпеки. Її виконання забезпечується ефективною правовою базою та наявністю двох Команд реагування на комп'ютерні надзвичайні події (CERT): CERT-UK підтримує операторів, які захищають критичну інфраструктуру, а GovCertUK працює з державними установами. Окрім цього, існують Національна рада Безпеки та Офіс страхування з питань кібернетичної та інформаційної безпеки (Office of Cyber Security and Information Assurance). В країні існує добре розвинена система

державно-приватного партнерства, яке є частиною Стратегії з кібербезпеки. Так, наприклад, Центр захисту національної інфраструктури (CPNI), організовує для компаній, що працюють в 14 секторах економіки, регулярні обміни інформацією за кращими практиками. «Гаряча лінія» Internet Watch Foundation є однією з найстаріших в Європі. Саме у Великобританії розташована штаб-квартира загально-європейської мережі «гарячих ліній» InHope.

Австрія. Австрія також має Стратегію кібербезпеки. Вона є частиною більш загальної Національної стратегії з безпеки інформаційно-комунікаційних технологій. Стратегія являє собою деталізовану програму дій, в якій визначені завдання з кібербезпеки та безпеки інформаційно-комунікаційних технологій, та заходи, що необхідні для їх досягнення. Національна команда реагування на надзвичайні комп'ютерні події CERT.at, має широкі та дуже чітко прописані повноваження. В країні існує декілька інституціолізованих (та багато неформальних) державно-приватних партнерських ініціатив (таких, наприклад, як Австрійський центр безпеки інформаційних технологій – Centre for Secure Information Technology Austria/A-SIT та Kuratorium Sicheres Österreich). Окрім того, існує Austrian Trust Circles, метою якого є обмін інформації щодо захисту критичної інформаційної структури за окремими секторами економіки та розробки специфічних для окремих секторів планів з оцінки ризиків. Austrian Trust Circles є спільною ініціативою CERT.at та австрійського уряду. Існує також «гаряча лінія» stopline.at, куди можна поскаржитись на дитячу порнографію, он-лайн пропаганду символіки націонал-соціалізму та інший небажаний контент.

Іспанія. Іспанія ухвалила Національну Стратегію з кібербезпеки. Це дуже якісний документ, який визначає конкретні цілі та засоби їх досягнення. Ця Стратегія є добре узгодженою як з Планом з національної безпеки, так і з чинним законодавством в галузі кібербезпеки – Стратегія, План та окремі законодавчі акти працюють разом в єдиному пакеті [32].

В Іспанії працюють INTECO-CERT та CCN-CERT, створено Національний Центр з захисту критичної інфраструктури (CNPIC). Цей Центр є державною структурою, яка відповідає за інформаційну безпеку та кібербезпеку, тоді як роль

CERT зводиться до реагування на інциденти кібербезпеки. CNPIC відповідає також за поширення інформації щодо кіберзагроз та кіберінцидентів та забезпечує координацію та співпрацю між різними секторами економіки та між державними та приватними інституціями. Він створює також робочі Групи, які розробляють секторальні плани з кібербезпеки.

В країні існує «гаряча лінія» для захисту дітей від шкідливого контенту, для підвищення обізнаності щодо ризиків кібербезпеці, щодо налагодження співпраці між різними стейкголдерами щодо забезпечення кібербезпеки. Цікаво, що, аби потрапити на сайт цієї «гарячої лінії», потрібно зареєструватись [32].

Як вже зазначалося раніше, інформаційна безпека є широкою і складною темою. Вона має багато аспектів, які пов'язані один з одним в дуже складних відносинах. З огляду на очевидну необхідність проаналізувати всі аспекти інформаційної безпеки і досягти повного розуміння того, як вони взаємодіють між собою, було б передчасно формулювати всеосяжні принципи, що стосуються інформаційної безпеки в усіх її аспектах. Замість цього, міжнародне співтовариство повинне зробити значну кількість систематичного мислення, перш ніж йти далі. Для полегшення роботи, держави повинні шукати ідеї і висновки з широкого кола фахівців.

Вже очевидно, що міжнародне співробітництво має важливе значення для того, щоб ефективно боротися з новим і складним питанням, що піднімаються щодо інформаційного тероризму та організованої злочинності. В даний час існує декілька поточних, багатосторонніх зусиль, присвячених питанням міжнародного співробітництва. Всі ці постійні зусилля заслуговують на увагу і повинні обов'язково мати можливість розроблятися і приносити плоди.

2.3. Кіберзлочинність та кібертероризм як загроза інформаційній безпеці у міжнародному праві

Протягом останніх 50 років обсяг інформаційної безпеки розвивався від систем мейнфреймів до власного пристрою (BYOD), включаючи смарт-мережі.

Мейнфрейм являє собою велику універсальну ЕОМ – високо продуктивний комп'ютер зі значним обсягом оперативної і зовнішньої пам'яті, призначений для організації централізованих сховищ даних великої ємності і виконання інтенсивних обчислювальних робіт [28]. Стратегія державного управління сприяє підвищенню рівня захисту інформації та, таким чином, гарантує надійну та належним чином захищену інформацію.

З точки зору технології мало що розділяє класичну інформаційну безпеку від кібербезпеки. Кібербезпека полягає в забезпеченні даних та систем в глобальному середовищі. Це лише перспектива, яка змінюється. Прийнявши цю точку зору, кібербезпека стала глобальною проблемою визначення. З огляду на характер проблеми, досягнення кібербезпеки, найімовірніше, будуть втілені завдяки політичній співпраці. Кібернетична безпека полягає не лише в крадіжці авторських прав та особистих даних. Вона також має військові аспекти, наприклад, для запобігання діяльності таких організацій, як Wikileaks. WikiLeaks – міжнародна організація, що займається витоками таємної інформації та її подальшою публікацією на своєму сайті. Джерела інформації завжди залишаються анонімними. Організацію було засновано в грудні 2006 зусиллями австралійця Джуліана Ассанжа [4].

Держави також мають дуже різні точки зору на кіберпростір та належне їх використання, де все частіше розвиваються наступальні кібернетичні можливості. Інформаційна безпека стала невід’ємною частиною національної оборони урядів, а також зовнішньої політики та політики безпеки та доктрини, що сприяють побудові інформаційної безпеки як нової сфери бойових дій. Зусилля щодо розробки правил потоків інформації в кіберпросторі зосереджені на застосуванні існуючого міжнародного права, потенційних прогалин, розробці норм, заходах щодо зміцнення довіри та поступу у позиціях стримування. Склався комплекс режимів інформаційної безпеки, який охоплював численні регіональні та міжнародні інституції, які відіграють провідну роль у формуванні відповідних політичних рішень. Отже, існує все більший консенсус щодо того, що стійкість стає одним із ключових елементів загального режиму кібербезпеки, тоді як

операції з викрадення та витоку під час виборів в США відновлювали десятилітні дебати про зв'язок між інформаційними операціями та кібер-операціями.

Вплив інформаційно-комунікаційних технологій (ІКТ) на всі аспекти людського життя, суспільства та держави не можна переоцінити. Окрім очевидних вигод з точки зору економічного, соціального та культурного розвитку, посилення ролі ІКТ у сучасному світі неминуче призводить до нових ризиків для міжнародної та національної безпеки. Є вже реальні докази того, що збитки від використання ІКТ в цілях, які суперечать Статуту Організації Об'єднаних Націй, а також у злочинних та терористичних цілях, можуть бути порівнянними з найбільш руйнівною зброєю. Перелік потенційних цілей інформаційних атак включає в себе не лише інформаційні ресурси Інтернету, а й критичні інфраструктури держав у промисловості, транспорті та енергетичному секторі. Більш того, масштаб і технологічний рівень такого руйнівного впливу постійно зростають. Всі країни без винятку визнають суворість загроз злочинного, терористичного та військово-політичного характеру в інформаційному просторі. Міжнародне співтовариство займається дискусією про те, як забезпечити міжнародну інформаційну безпеку (IIS) більше півтора десятків років. На цьому етапі очевидно ключова проблема полягає у відсутності повноцінної міжнародно-правової бази, що регулює діяльність держав-членів у сфері ІКТ, включаючи їх військові аспекти. Група урядових експертів ООН (GGE) з інформаційних технологій, створена в 2014 р. та відповідно до резолюції «Досягнення в галузі інформації та телекомунікацій в контексті міжнародної безпеки», прийнятої консенсусом на 68-й сесії Генеральної Асамблеї ООН, призначена для вивчення цих питань.

Незаконне використання ІКТ трактується в рамках існуючої системи міжнародно-правових норм таким чином що міжнародне право не має посилання на загальновизнані поняття війни чи збройної боротьби. Більш того, загальноприйнятого визначення інформаційної війни немає, хоча деякі міжнародні акти включають такі визначення. Існує також необхідність вивчення атрибутів інформаційної війни та розробки загальновизнаного визначення,

оскільки деякі особливості незаконного використання ІКТ для вирішення міждержавних відмінностей перешкоджають його правовому регулюванню:

– відсутність «боєголовки» – неможливо простежити момент, коли відбулося застосування військової сили;
– транскордонний характер – сила може бути застосована агресивно через незаконне використання ІКТ проти супротивника без порушення його територіальних кордонів;
– ІКТ не є самою зброєю, що ускладнює класифікацію нападу з використанням ІКТ як озброєного.

Конкретні атрибути ІКТ відповідають тому, що будь-яка війна, що веде до завоювання або перемоги противника, порушує Статут ООН та принцип суверенної рівності держав. Згідно зі статтею 2 Резолюції ООН 3314 «Визначення агресії» 1974 року [7], дії держави кваліфікуються як агресія разом із критеріями застосування сили, першим застосуванням сили, тяжкості та ворожості, незалежно від того, була оголошена війна чи ні. Ці положення можуть застосовуватися до інформаційного простору, хоча деякі норми документа повинні бути адаптовані до конкретних атрибутів ІКТ. На відміну від традиційної інтерпретації агресії, незаконне використання ІКТ не має посилання на введення сили або традиційне використання військової сили, що перешкоджає класифікації комп'ютерних атак як акту агресії.

В інформаційній безпеці розрізняють два види загрози це кіберзлочинність та кібертероризм. Що стосується поняття кібертероризму, наприклад юрист-науковець Діордіца І.В. наводить такий термін «кібертероризм» є синтезом понять «кібер простір» та «тероризм». Під кібертероризмом ми розуміємо протиправне діяння, яке вчиняється з ціллю досягнення негативних наслідків, наприклад отримання матеріальних благ чи загроза інформаційній безпеці держави [8]. Також можна привести ще декілька визначень кібертероризму. Інформаційний тероризм, кібертероризм – використання комп'ютерних та телекомунікаційних технологій (насамперед, інтернету) в терористичних цілях.

Наприклад, акти, спрямовані на залякування з метою досягнення політичних результатів, або завдання шкоди комп'ютерним мережам, особливо персональним комп'ютерам, підключеним до Інтернету, за допомогою таких засобів, як комп'ютерні віруси.

Законодавство України визначає: «Кібертероризм – терористична діяльність, що здійснюється у кіберпросторі або з його використанням». Організація, створена для вироблення узгодженої політики з питань економіки і внутрішньої безпеки (The National Conference of State Legislatures) визначає кібертероризм наступним чином: «Використання інформаційних технологій терористичними групами і терористами-одинаками для досягнення своїх цілей». Може включати використання інформаційних технологій для організації та виконання атак проти телекомунікаційних мереж, інформаційних систем і комунікаційної інфраструктури, або обмін інформацією, а також загрози з використанням засобів електрозв'язку. Прикладами можуть служити злом інформаційних систем, внесення вірусів у вразливі мережі, дефейс веб-сайтів, DoS-атаки, терористичні загрози, спричинені електронними засобами зв'язку [12].

Отже кібертероризм – це використання комп'ютерів та інформації, зокрема через Інтернет, для заподіяння фізичної, реальної шкоди або суттєвого порушення інфраструктури.

Прикладами кібертероризму є:

1. Глобальні терористичні мережі, що руйнують основні веб-сайти, створюють загальні незручності / незручності, або припиняють трафік на веб-сайти, які публікують вміст, з яким хакери не погоджуються.
2. Міжнародні кібертерористи отримують доступ і вимикають або змінюють сигнали, що контролюють військову техніку.
3. Кібертерористи, націлені на системи критично важливої інфраструктури, наприклад, щоб відключити установку для очищення води, спричинити регіональний збиток електроенергії або порушити трубопровід, нафтопереробний завод або переробку нафти. Цей тип кібернетичної атаки може порушити основні міста, спричинити кризу громадського

здоров'я, загрожувати громадській безпеці мільйонів людей, а також викликати масові паніки та загибелі людей.

Отже суб'єктами кібератаки можуть стати політичні організації, державні установи, спеціальні, секретні служби.

Виділяють наступні критерії кібертероризму.

Критерій №1 (фізичний рівень кіберпростору) – характеризується відсутністю або мінімальним ризиком для життя та здоров'я населення, навколишнього середовища й направленістю (спрямованістю) кібератаки на дестабілізацію роботи органів центрального управління. До таких об'єктів можна віднести: мережі зв'язку й інформаційно-обчислювальні мережі, що використовуються державними організаціями під час виконання своїх управлінських функцій; військово-інформаційна інфраструктура, що вирішує завдання управління військами; засоби масової інформації (передусім електронні) тощо.

Критерій №2 (кібертероризм) – характеризується можливістю нанесення значних економічних збитків, великої кількості людських жертв, екологічних катастроф, що призводять до руйнування або виведення з ладу внутрішньодержавної (загальнодержавної) інфраструктури. До таких об'єктів можна віднести: системи керування у галузі транспорту (системи аеропортів, залізниць, метрополітенів, навігації водного транспорту); системи керування газового та газотранспортного комплексу України; системи керування виробництва (АЕС, ГЕС, ТЕЦ), передачі та розподілення електроенергії тощо.

Критерій № 3 (семантичний рівень) – крадіжки, пошкодження даних, що мають критично-важливе значення для держави (ядерні, хімічні, біологічні дослідження, ракетно-космічні технології тощо). До таких об'єктів можна віднести: сервери відомчих інформаційних мереж; інформаційні та керуючі структури банків, промислових підприємств тощо [16].

Ключ до боротьби з кібертероризмом є запобігання. Підприємства повинні переконатися, що їх пристрої в Інтернеті є належним чином захищені, а також

уникати загальних точок доступу. Щоб захистити від викрадення, організації повинні мати повне та своєчасне резервне копіювання своїх систем.

Компанії також повинні розробляти IT-політику для захисту своїх бізнес-даних, в тому числі, які типи файлів співробітники можуть завантажувати, а також що робити у випадку кібератаки. Співробітники мають дотримуватися обмежень щодо встановлення додатків, правил користування паролями та способів виявлення ознак кібер-атаки.

Кіберзлочинність це сукупність злочинів, що вчинюються у віртуальному просторі за допомогою комп'ютерних систем або шляхом використання комп'ютерних мереж та інших засобів доступу до віртуального простору, в межах комп'ютерних мереж, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних [5]. Отже, з даного терміну випливає, що кіберзлочинність – це використання комп'ютера як інструменту до незаконного доступу для здійснення фальсифікації, незаконний оборот інтелектуальної власності, крадіжка ідентичності або порушення конфіденційності. Кіберзлочинність набула широкого розмаху, оскільки комп'ютер став важливим інструментом торгівлі, розваг та державних установ.

Правоохоронні органи в різних країнах світу намагаються вирішити проблему, вона неухильно зростає, і багато людей стали жертвами несанкціонованого доступу, крадіжки особистих даних і шкідливого програмного забезпечення. Одним з кращих способів уникнути, не стати жертвою кібер-злочинів і захисту вашої конфіденційної інформації – є використання непроникної безпеки, яка використовує єдину систему програмного і апаратного забезпечення для автентифікації будь-якої інформації, яка відправляється або отримує доступ через Інтернет.

Існує багато видів та класифікацій кіберзлочинів. Наприклад з 1991 за класифікатором Інтерполу інформаційні злочини поділяються [13]:

– QA – Несанкціонований доступ та перехоплення;

– QD – Зміна комп'ютерних даних;

- QF – Комп'ютерне шахрайство;
- QR – Незаконне копіювання;
- QS – Комп'ютерний саботаж;
- QZ – Інші комп'ютерні злочини.

Також можна виділити ще одну класифікацію:

1. правопорушення проти конфіденційності, цілісності і доступності комп'ютерних даних і систем, зокрема:
   - незаконний доступ, наприклад, шляхом злому, обману та іншими засобами;
   - нелегальне перехоплення комп'ютерних даних; втручання у дані, включаючи навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це;
   - втручання у систему, включаючи умисне створення серйозних перешкод функціонуванню комп'ютерної системи, наприклад, шляхом розподілених атак на ключову інформаційну інфраструктуру;
   - зловживання пристроями, тобто виготовлення, продаж, придбання для використання, розповсюдження пристроїв, комп'ютерних програм, комп'ютерних паролів або кодів доступу метою здійснення кіберзлочинів;
2. правопорушення, пов'язані з комп'ютерами, включаючи підробку і шахрайство, вчинені з використанням комп'ютерів;
3. правопорушення, пов'язані зі змістом інформації, зокрема, дитяча порнографія, расизм і ксенофобія;
4. правопорушення, пов'язані з порушенням авторських та суміжних прав, наприклад незаконне відтворення і використання комп'ютерних програм, аудіо/відео та інших видів цифрової продукції, а також баз даних і книг [34].

У той же час, з урахуванням мотивації злочинців, кіберзлочини представляється можливим умовно розділити на наступні категорії:

Злом – це злочин, при якому вдається отримати доступ до особистої або конфіденційної інформації. У Сполучених Штатах хакерство класифікується як кримінальний злочин і карається як такий. Це відрізняється від етичного злому, який багато організацій використовують для перевірки захисту своєї інтернет-безпеки. При зломі злочинець використовує різноманітне програмне забезпечення для входу на комп'ютер людини, і людина може не знати, що до нього підключений комп'ютер з віддаленого місця.

Піратство – це злочин відбувається, коли людина порушує авторські права і завантажує музику, фільми, ігри та програмне забезпечення. Існують навіть сайти обміну сайтами, які заохочують комп'ютерне піратство, і багато хто з цих веб-сайтів в даний час націлені на ФБР. Сьогодні система правосуддя займається цією кіберзлочинністю, і існують закони, що забороняють людям незаконні завантаження.

Викрадення особистих даних – це стало серйозною проблемою для людей, що використовують Інтернет для операцій з готівкою і банківських послуг. У цьому кіберзлочині злочинець звертається до даних про банківський рахунок, за кредитними картками, за дебетовими картками та іншої конфіденційної інформації, щоб перевести гроші або купити речі в Інтернеті від імені жертви. Це може привести до великих фінансових втрат для жертви і навіть зіпсувати кредитну історію жертви.

Шкідливі програми – це інтернет-програмне забезпечення або програми, які використовуються для руйнування мережі. Програмне забезпечення використовується для доступу до системи для викрадення конфіденційної інформації або даних, або нанесення шкоди програмному забезпеченню, присутнього в системі.

Основним мотивом кіберзлочинців стало вилучення матеріальної вигоди. Практично всі випадки неправомірного доступу до інформації спрямовані на розкрадання грошових коштів.

Кібер-злочини стали реальною загрозою сьогодні і сильно відрізняються від злочинів старої школи, таких як грабіж або крадіжка. На відміну від цих злочинів,

кібер-злочини можуть відбуватися в поодинці і не вимагають фізичної присутності злочинців. Злочини можуть відбуватися в віддаленому місці, і злочинцям не потрібно турбуватися про правоохоронні органи в країні, де вони скоюють злочини. Ті ж системи, які полегшили людям проведення електронної комерції і онлайн-транзакцій, в даний час використовуються кіберзлочинцями.

Кіберзлочинність широко поділяються на три категорії:

- індивідуальна;
- майнова;
- урядова.

Кожна категорія може використовувати різні методи, а використовувані методи варіюються від одного злочинця до іншого.

Індивідуальна. Цей тип кіберзлочинності може бути у вигляді кібер-переслідування, поширення порнографії, торгівля. Сьогодні правоохоронні органи дуже серйозно ставляться до цієї категорії кіберзлочинності і об'єднують сили на міжнародному рівні для захоплення і арешту винних.

Майнова. Також, як в реальному світі, злочинець може вкрасти і пограбувати, навіть в кібер-світі. У цьому випадку вони можуть вкрасти банківські реквізити особи і перевести в готівку гроші; зловживати кредитною карткою, щоб здійснювати численні покупки в Інтернеті; здійснювати шахрайські дії, щоб змусити наївних людей розлучитися зі своїми важко заробленими грошима; використовувати шкідливе програмне забезпечення для доступу до веб-сайту організації або порушити роботу систем організації. Зловмисне програмне забезпечення також може пошкодити програмне забезпечення та комп'ютерне обладнання, так само зробити збитки від хакерів в світі офлайн.

Урядова. Не так часто, як дві інші категорії, злочини проти уряду називаються кібертероризмом. У разі успіху ця категорія може завдати шкоди і викликати паніку серед цивільного населення. У цій категорії злочинці зламують урядові сайти, військові сайти або поширюють пропаганду. Злочинці можуть бути терористичними нарядами або недружніми урядами інших країн.

Було зазначено, що більшість кіберзлочинців мають вільну мережу, в якій вони співпрацюють і співпрацюють один з одним. На відміну від реального світу, ці злочинці не б'ються один з одним за верховенство або контроль. Замість цього вони працюють разом, щоб поліпшити свої навички і навіть допомогти один одному з новими можливостями. Отже, звичайні методи боротьби зі злочинцями не можна використовувати проти кіберзлочинців. Це пов'язано перш за все з тим, що методи, використовувані кіберзлочинцями і технології, занадто швидко змінюються, щоб правоохоронні органи були ефективними.

Ось чому комерційним установам та урядовим організаціям для свого захисту необхідно використовувати інші методи.

Важливим аспектом кіберзлочинності є її нелокальний характер: дії можуть виникати в юрисдикціях, розділених величезними відстанями. Це створює серйозні проблеми для правоохоронних органів, оскільки раніше місцеві або навіть національні злочини то зараз вимагають міжнародного співробітництва. Отже для того, щоб ефективно боротися з кіберзлочинцями через національні кордони, повинні бути ратифіковані міжнародні договори про кіберзлочинність.

У 1996 році Рада Європи разом з представниками уряду Сполучених Штатів, Канади та Японії підготувала попередній міжнародний договір, що охоплює комп'ютерну злочинність. У всьому світі цивільні Лібертаріанські групи негайно опротестували проти положень договору, відповідно до яких інтернет-провайдери (ISP) повинні зберігати інформацію про транзакції своїх клієнтів і передавати цю інформацію за запитом. Проте робота над договором тривала, і 23 листопада 2001 Конвенція Ради Європи про кіберзлочинність було підписано 30 державами. Конвенція набула чинності в 2004 році. Додаткові протоколи, що охоплюють терористичну діяльність, расистські та ксенофобські кіберзлочини, були запропоновані в 2002 році і вступили в силу в 2006 році. Крім того, різні національні закони, такі як Закон США про патріотів в 2001 році, розширили закон правозастосування контролювання і захист комп'ютерних мереж.

Що стосується України то нормативне регулювання цієї сфери не встигає за розвитком технологій, що загострює проблему кібербезпеки. Але протидія кіберзлочинності та кібертероризму є одним із пріоритетних напрямків в політиці держави.

Міжнародне співробітництво України в галузі забезпечення інформаційної безпеки є невід'ємною складовою частиною політичного, військового, економічного, культурного та інших видів взаємодії країн, що входять до світового співтовариства. Таке співробітництво повинно сприяти підвищенню інформаційної безпеки усіх його членів, включаючи Україну.

Особливість міжнародного співробітництва України в галузі забезпечення інформаційної безпеки полягає в тому, що воно здійснюється в умовах загострення міжнародної конкуренції за володіння технологічними та інформаційними ресурсами, за домінування на ринках збуту, в умовах продовження спроб створення структури міжнародних відносин, заснованої на односторонніх рішеннях ключових проблем світової політики, протидії зміцненню ролі України у багатополярному світі, що формується, посилення технологічного відриву провідних держав світу та нарощування їхніх можливостей для створення «інформаційної зброї». Усе це може призвести до нового етапу гонки озброєнь в інформаційній сфері, зростання загрози агентурного та оперативно-технічного проникнення в Україну іноземних розвідок, у тому числі з використанням глобальної інформаційної інфраструктури.

Основними напрямами міжнародного співробітництва України в галузі забезпечення інформаційної безпеки є:

- заборона розробки, поширення та застосування «інформаційної зброї»;
- забезпечення безпеки міжнародного інформаційного обміну, у тому числі зберігання інформації при її передачі національними телекомунікаційними мережами та каналами зв'язку;

– координація діяльності правоохоронних органів країн, що входять у світове співтовариство, із запобігання комп'ютерних злочинів;
– запобігання несанкціонованого доступу до інформації обмеженого доступу у міжнародних банківських телекомунікаційних мережах і системах інформаційного забезпечення світової торгівлі, до інформації міжнародних правоохоронних організацій, що ведуть боротьбу з транснаціональною організованою злочинністю, міжнародним тероризмом, поширенням наркотиків і психотропних речовин незаконною торгівлею зброєю та матеріалами, які розщеплюються, а також торгівлею людьми [36].

Для покращення стану кібербезпеки необхідно:

– забезпечити Україну необхідною підтримкою для впровадження найсучаснішого захисту безпеки на урядових комп'ютерах, зокрема системах, що захищають критичну інфраструктуру України;
– надавати Україні підтримку для зменшення залежності від російських технологій;
– надвати Україні допомогу в нарощуванні спроможності розширити обмін інформацією в галузі кібербезпеки та співпрацювати у міжнародних зусиллях щодо реагування на кібер-загрози.

Висновки до розділу 2

Міжнародне право інформаційної безпеки сьогодні знаходиться в критичному становищі. Це правда, що державні вагання щодо участі у розробці та застосуванні міжнародного права породили сильний вакуум, що дозволяє виникненню недержавних нормотворчих ініціатив. Тим не менше, було б передчасно говорити про ситуацію з кризою.

Кілька історичних паралелей показують, що суміш початкових підходів до м'якого права, поєднаних з зростаючим набором правил обов'язкового зв'язку, може забезпечити логічну та дієву реакцію на нове явище. У XXI столітті

плюралізація нормотворчих процесів із залученням різноманітних державних і недержавних суб'єктів є загальною рисою на міжнародному рівні, і тому її не треба боятися як такої.

Наскільки важливим є те, чи зможуть держави відновити свою традиційну центральну законодавчу роль. Їх поведінка в найближчі кілька років визначатиме, чи ми спостерігатимемо поступовий занепад міждержавного врядування в кіберпросторі або фундаментального перекалібрування правових підходів з державами, що знову стають центром врядування. Якщо вони хочуть забезпечити, щоб існуючий енергетичний вакуум не використовувався таким чином, що може заважати їх здатності досягти своїх стратегічних та політичних цілей державою.

Основною стратегією забезпечення інформаційної та кібербезпеки в міжнародній сфері є орієнтування на співпрацю з зовнішніми партнерами і зміцнення договірно-правової бази для глобального регулювання даної сфери, також в той же час варто не забувати про посилення внутрішнього регулювання та орієнтації на власні ресурси і рішення. Необхідно сконцентрувати увагу на два основні напрямки роботи: зниження ризиків військово-політичного використання ІКТ та формування основ міжнародно-правового режиму відповідальної поведінки держав в кіберпросторі.

Держави повинні забезпечити, щоб їх закони та практика усували притулок для тих, хто злочинно зловживають інформаційними технологіями. Співпраця між правоохоронними органами в розслідуванні та судовому переслідуванні міжнародних випадків злочинного використання інформаційних технологій повинні бути узгоджені між усіма зацікавленими державами. Співробітники правоохоронних органів повинні бути навчені і оснащені для вирішення злочинного використання інформаційних технологій.

Це включає в себе розробку національного законодавства для усунення злочинного використання технологій, вдосконалення правоохоронних можливостей для співпраці між країнами в розслідуванні та судовому переслідуванні міжнародних випадків злочинного використання інформаційних технологій, поліпшення обміну інформацією, підвищення безпеки даних і

комп'ютерних систем, підготовка співробітників правоохоронних органів, які безпосередньо стосуються проблем, пов'язаних з кіберзлочинністю та, створення режимів взаємної допомоги і підвищенням обізнаності громадськості щодо загрози кіберзлочинності.

РОЗДІЛ 3. ДЕРЖАВНА ПОЛІТИКА ЩОДО ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

3.1. Імплементація міжнародних стандартів щодо інформаційної безпеки

Протягом останніх років Україна, як і більшість країн світу, робить певні кроки в розбудові інформаційного суспільства, забезпечення інформаційної і кібербезпеки, а також у боротьбі з кіберзлочинністю.

Розглянемо основні елементи, інформаційної безпеки що сформувалися а саме:

1. Міжнародні стандарти у галузі інформаційної безпеки;
2. Інститути, що створюються військово-політичними організаціями (на прикладі НАТО);
3. Міжнародно-регіональні інститути та структури, які створюються інтеграційними об'єднаннями (на прикладі, ЄС);

Основними міжнародними стандартами в сфері інформаційної безпеки, що прийняті ISO, є ISO/IEC серії 27000.

Стандарти серії 27000:

- ISO / IEC 27000 до: 2014 Information technology. Security techniques. Information security management systems. Overview and vocabulary – Визначення та основні принципи.
- ISO / IEC 27001 до: 2013 Information technology. Security techniques. Information security management systems. Requirements – Інформаційні технології. Методи забезпечення безпеки. Системи управління інформаційною безпекою. Вимоги.
- ISO / IEC 27002 до: 2013 Information technology. Security techniques. Code of practice for information security management – Інформаційні технології. Методи забезпечення безпеки. Практичні правила управління інформаційною безпекою.

– ISO / IEC 27003: 2010 Information Technology. Security Techniques. Information Security Management Systems Implementation Guidance – Керівництво по впровадженню системи управління інформаційною безпекою.
– ISO / IEC 27004: 2009 Information technology. Security techniques. Information security management. Measurement – Вимірювання ефективності системи управління інформаційною безпекою.
– ISO / IEC 27005: 2011 Information technology. Security techniques. Information security risk management – Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки.
– ISO / IEC 27032 до: 2012 Information technology. Security techniques.
– Guidelines for cybersecurity – Керівництво по забезпеченню кібербезпеки та інші [1]. Містить керівні вказівки щодо поліпшення стану кібербезпеки, висвітлюючи унікальні аспекти цієї діяльності та її залежності від інших областей безпеки, зокрема: інформаційна безпека, мережева безпека, безпека в Інтернеті та критична інфраструктура захисту.Він охоплює практику базової безпеки для зацікавлених сторін у кіберпросторі.

Цей міжнародний стандарт передбачає:

– огляд кібербезпеки;
– пояснення зв'язку між кібербезпекою та іншими видами безпеки;
– визначення зацікавлених сторін та опис їх ролі в кібербезпеці;
– керівництво для вирішення загальних проблем кібербезпеки та структуру, яка дозволить зацікавленим сторонам співпрацювати у вирішенні проблем кібербезпеки.

Перераховане вище є міжнародними стандартами в сфері інформаційної безпеки та кібербезпеки.

Наразі в Україні як єдиний (крім банківського сектору) державний стандарт технічного захисту інформації діє серія нормативних документів,

центральним з яких є НД ТЗІ 2.5–004–99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу». Стандарт розроблений на основі Канадських критеріїв безпеки комп'ютерних систем (Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)), а також з урахуванням прийнятих в 2005 р. міжнародних «Загальних критеріїв» (Common Criteria for Information Technology Security Evaluation (ISO 15408)). На відміну від найпоширенішої у світі серії ISO/IEC27000, яка сфокусована на менеджменті інформаційної безпеки, критерієм захищеності інформації в НД ТЗІ 2.5–004–99 є відповідність архітектури та параметрів програмно-апаратних засобів об'єкта чіткого регламенту – комплексній системі захисту інформації (КСЗІ). Сама ідея, внутрішня структура і модель впровадження КСЗІ здебільшого не відповідає вимогам сучасного ні інформаційного ні кіберзахисту, особливо в недержавному секторі.

Нині у світі існує ціла низка відкритих для використання міжнародних стандартів в сфері інформаційної та кібербезпеки, але насамперед варто згадати про два їх різновиди, оскільки саме вони задають нині у світі певну концептуально-технологічну рамку і широко застосовуються в багатьох країнах, а до того ж у них враховані найсучасніші тренди розвитку і відсутні вади, властиві українському НД ТЗІ 2.5–004–99. По-перше, це серія міжнародних стандартів ISO/IEC27000, розроблена Міжнародною організацією з стандартизації (ISO) спільно з Міжнародною електротехнічною комісією (IEC), яка постійно доповнюється новими документами. Серія, по суті, являє собою модель (фреймворк) для розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та поліпшення системи менеджменту інформаційної безпеки як на загальному рівні (27001), так і в окремих секторах та галузях, – таких як фінанси, транспорт, енергетика, охорона здоров'я, оператори зв'язку, хмарні обчислення, інфраструктурні проекти, аудит і сертифікація тощо. Впровадження системи управління інформаційною безпекою (СУІБ) відповідно до ISO/IEC27000 дозволяє оптимізувати процес захисту інформаційних ресурсів і управління ризиками для цих ресурсів.

У нашій країні статус державного стандарту отримала перша версія ISO/IEC27001 (найновішою є ISO/IEC27001:2013), проте де-факто імплементований він лише в банківській сфері – у вигляді вимог СОУ Н НБУ 65.1 СУІБ 1.0: 2010 211 (згідно із Законом «Про основні засади забезпечення кібербезпеки України» Національний банк України є одним з суб'єктів національної системи кібербезпеки) [6].

Практичне застосування ISO/IEC27001 в інших галузях української економіки та бізнесу поки залишається відкритим через нормативно-правову неврегульованість. Одним із найбільш авторитетних і відомих у світі є також National Institute of Standarts and Technology Cybersecurity Framework (NIST CSF) – розроблений американським Інститутом стандартів і технологій для організацій приватного сектору США комплекс методологій та рекомендацій щодо зниження IT-ризиків, запобігання, моніторингу і реагування на кібератаки. Фреймворк є відкритим, призначений виключно для добровільного використання і достатньо «гнучкий». Треба відзначити, що нормальною світовою практикою є розробка і застосування у разі необхідності альтернативних або призначених для тих чи інших секторів недержавного сектору стандартів та фреймворків з кібербезпеки. Серед іншого, це дозволяє уникати надмірної регуляторної монополізації, недоброчесної конкуренції й корупції, що нині особливо актуальне для України.

Отже саме ці стандарти рекомендують запровадити в українському ПЕК експерти київського відділення ISACA. Так, саме згідно з NERC CIP (у комплексі зі стандартами NIST 800-SERIES, IEC62443 та ISO 27000) побудований та сертифікований захист критичної IT-інфраструктури в ТОВ ДТЕК Енерго. У «Типовому положенні про інформаційну безпеку підприємств ПЕК», розміщеному на офіційному веб-порталі міністерства, є положення щодо «реалізації вимог міжнародних стандартів з інформаційної безпеки ISO 27000-series, ISA 099-series та IEC 62443». Останні два – спеціалізовані відкриті стандарти, оптимізовані в тому числі для застосування на об'єктах критичної інфраструктури приватної форми власності.

Таким чином, можна говорити про те, що в українському ПЕК уже зараз триває формування єдиного пакета галузевих стандартів з інформаційної безпеки. На отримання міжнародної сертифікації у сфері інформаційної безпеки в Україні орієнтовані також й інші приватні гравці. Наприклад, компанія De Novo – найбільший в Україні провайдер хмарових сервісів, яка має сертифікат відповідності вимогам українським стандартам КСЗІ для свого сервісу G-Cloud (хмара для органів державної влади), водночас впровадила у середині 2017 р. систему управління інформаційною безпекою (СУІБ) і отримала сертифікат відповідності згідно з міжнародним стандартом ISO 27001 220 [6]. Отже в Україні діють вище перечислені стандарти в IT сфері. На даному етапі інформаційна безпека тільки розвивається у західному напрямі. Є рекомендації щодо запровадження стандартів, це допоможе більш розшити сферу та внести нові корективи до старих стандартів та значно оживити розвиток інформаційної безпеки.

Наступним елементом є документи, країн, що лідирують у сфері ІКТ, наприклад США (National Information Infrastructure Protection Act, International strategy for cyberspace) та Індії (National Cyber Security Policy). Для України великий інтерес викликає досвід і стратегії лідерів ЄС (Франції, Великої Британії, Нідерландів), постсоціалістичних країн Європи (Естонії, Словаччини, Чехії, Литви та ін.), Канади, Японії тощо. Урахування цих стратегій дозволяє координувати національну політику України та визначити пріоритети співробітництва з окремими країнами ЄС та НАТО.

Відчутний поштовх до активізації зусиль у напрямку інформаційної безпеки дало ухвалення організацією НАТО програмного документа під назвою «Рамки для співробітництва у питаннях кібернетичного захисту між НАТО та державами партнерами. У документі наголошується, що головний елемент політики НАТО у сфері кіберзахисту полягає в тому, що держави – члени Альянсу несуть пряму відповідальність за захист власних національних комунікацій та інформаційних систем. Альянс, у свою чергу, повинен бути здатний надати підтримку своїм партнерам, які зазнали кібератак

міжнаціонального значення. Цим документом передбачено, зокрема, що головні цілі співпраці НАТО з державами-партнерами у сфері кіберзахисту полягають у підвищенні здатності НАТО та держав-партнерів у сфері захисту критичних комунікаційних та інформаційних інфраструктур проти кібератак, наданні допомоги у відновленні нормального функціонування відповідної інфраструктури після кібератак, а також у створенні основ для вжиття заходів із підтримки потерпілих від кібератак. Відповідно до головних положень згаданого документа країни-партнери закликаються до невідкладної гармонізації національного законодавства у сфері кібернетичної безпеки з відповідними міжнародними нормами, такими як Конвенція Ради Європи з питань кіберзлочинності, із неодмінним дотриманням таких головних принципів.

1. Співпраця між НАТО та країною-партнером має бути взаємовигідною в такому сенсі: Альянс може надати країні-партнерові інформацію та підтримку у сфері кібербезпеки, якщо ця країна неухильно виконує умови взаємодії.

2. НАТО може надати країні-партнерові як експертну допомогу, так і свої технічні можливості для захисту від кібернетичних атак.

3. Країни-партнери можуть звертатися з пропозиціями щодо співпраці у сфері кіберзахисту та отримання підтримки з боку НАТО, якщо зазнають кібератак національного масштабу.

4. Альянс і партнери мають уникати дублювання зусиль, що докладаються в рамках інших міжнародних організацій, залучених до захисту ІС від кібератак.

5. Наявність угоди про безпеку між НАТО та країною-партнером має визначати обсяги допомоги та інформаційного обміну. Проте інформацію стосовно захисту критичної інфраструктури національних комунікаційних та інформаційних систем буде позначено та передано належним чином лише в разі потреби ознайомлення з нею [3].

Документ, про який ідеться, визначає також сфери співробітництва НАТО з державами-партнерами у сфері кіберзахисту, а саме: узагальнений обмін інформацією щодо відповідної політики та доктрин; обговорення технічних засобів захисту комунікаційної та інформаційної інфраструктури (може бути передбачено на більш змістовному рівні співробітництва). Загальна кількість Цілей партнерства в рамках ППОС, схвалених для України, дорівнює 96, з них на Збройні сили України покладено 70; на МВС України – 8; на МЗС України – 6; на СБУ – 11; на Мінфін України – 1 [3]. Отже співробітництво України та НАТО має великі перспективи та можливості у майбутньому. Країни-партнери НАТО можуть висувати пропозиції із питань кібербезпеки та інформаційної безпеки у форматі «28+n» та також щорічні національні програми слугують інструментами налагодження співпраці між державами-партнерами в питаннях інформаційного захисту та кібербезпеки з підлаштуванням до обставин та урахуванням індивідуальних потреб кожної держави.

Великим кроком с сфері інформаційної безпеки та кібербезпеки стало підписання Радою Європи Конвенції про кіберзлочинність 23 листопада 2001 року у Будапешті. Ця Конвенція була ратифікована Україною у травні 2005 року. МВС України у травні 2017 р. імплементувало положення Конвенції про кіберзлочинність у частині забезпечення строків збереження комп'ютерних даних, збирання і вилучення доказів в електронній формі в кримінальних справах про вчинення комп'ютерних злочинів та терористичних актів з використанням комп'ютерних систем і мереж. У перспективі Національної поліції імплементація всіх норм Конвенції до українського законодавства. Найперші зміни будуть стосуватися обов'язків та правил для постачальників контенту. Покладення обов’язків на провайдерів Інтернет-зв’язку із зберігання та логування незаконних процесів, які відбуваються у мережі. Передбачається, що зберігання такої інформації відбуватиметься за запитом правоохоронних органів та триватиме до 90 діб. Планується закривати доступ до конкретно взятої інформації. Подібна система існує в США та багатьох країнах Європи, серед яких Німеччина, Великобританія, Італія, Швейцарія. Процедура

блокування як тимчасова або часткова, так і постійна повинна існувати [10]. В Європейській конвенції дуже багато корисних статей, які потрібно імплементувати до нашого законодавства.

Як зазначає доктор юридичних наук, старший науковий співробітник, проректор Національної академії внутрішніх справ з науково-методичної роботи Орлов Ю.Ю. чинне законодавство України свідчить, що за більшість злочинів, зазначених у Конвенції, у нашій країні передбачено кримінальну відповідальність. Так, розділ XVI Особливої частини КК України містить низку статей, що передбачають кримінальну відповідальність за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: ст. 361 (несанкціоноване втручання в роботу електронно-обчислювальних машин автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку); ст. 361(1) (створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут); ст. 361(2) (несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації); ст. 362 (несанкціоновані дії з інформацією, яку опрацьовують в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігають на носіях такої інформації, вчинені особою, яка має право доступу до неї); ст. 363 (порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яку в них опрацьовують); автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку) [29].

На виконання вимог Конвенції до розділу XVI Особливої частини КК України Законом України від 5 червня 2003 р. № 908-IV внесено відповідні зміни. Водночас перелік кіберзлочинів не вичерпується діяннями, визначеними

в розділі XVI Особливої частини КК України [20]. Певні злочини, що існували задовго до створення комп'ютерів, також можуть бути вчинені із застосуванням інформаційних технологій. Використання комп'ютерів спрощує вчинення злочину або уможливлює його вчинення в нових формах. Отже, ці злочини можна розглядати як такі, що підпадають під дію Конвенції. Зокрема, ідеться про такі злочинні діяння: різні види підроблення грошей, цінних паперів, платіжних карток, знаків поштової оплати, марок акцизного збору, контрольних марок, номерів вузлів та агрегатів транспортних засобів, документів на отримання наркотиків, інших документів тощо (ст. 199, 200, 215, 216, 224, 290, 318, 358, 366 КК України) [20]; шахрайство з різними предметами (ст. 190, 192, 222, 262, 308, 312, 313, 357, 410 КК України) [20]; увезення, виготовлення, збут і розповсюдження порнографічних предметів (ст. 301 КК України) [29].

Злочини проти конфіденційності, цілісності й доступності комп'ютерних даних і систем:

- 2 ст. Конвенції про кіберзлочинність – Протизаконний доступ за Українським Кримінальним кодексом це статті – 361, 363.
- 3 ст. Конвенції – Протизаконне перехоплення – 362, 363 ст. ККУ.
- 4 ст. Конвенції – Вплив на дані – 361, 362, 3631 ККУ.
- 5 ст. Конвенції – Вплив на функціонування системи– 361, 3611, 362, 363, 3631 ККУ.
- 6 ст. Конвенції – Протизаконне використання пристроїв і комп'ютерних програм – 3611, 362, 363 ККУ.

Злочини, пов'язані з використанням комп'ютерних засобів:

- 7ст. Конвенції – Підроблення з використанням комп'ютерних технологій– 199, 200, 215, 216, 224, 290, 318, 358, 366 ККУ.
- 8 ст. Конвенції – Шахрайство з використанням комп'ютерних технологій – 190, 192, 222, 262, 308, 312, 313, 357, 410 ККУ.
- 9 ст. Конвенції –Злочини, пов'язані з дитячою порнографією – 301 ст. ККУ.

Злочини, пов’язані з порушенням авторського права та суміжних прав:

– 10 ст. Конвенції–Злочини, пов’язані з порушенням авторського права та суміжних прав – 176 ККУ [20].

Також слід зауважити що не всі положення конвенції були застосовані до українського кримінального законодавства. Щодо придбання шкідливих комп'ютерних програм та пристроїв які були зроблені, продаж комп’ютерних паролів, кодів доступу чи інших видів продажу інформації для учинення комп'ютерних злочинів ККУ не передбачає відповідальності. Тобто відповідальність за ці злочини в Україні не встановлено.

Отже потрібно звернути увагу щодо подолання проблем імплементації в Україні стандартів ЄС і НАТО в сфері інформаційної та кібербезпеки а саме : недотримання чинного законодавства; низький рівень обізнаності і культури населення і підприємницького сектору; економія ресурсів на запровадження міжнародних стандартів і розвиток інфраструктури; низька якість підготовки фахівців у сфері безпеки; низький рівень технічного оснащення тощо. Міжнародна співпраця у галузі інформаційної безпеки сприяє розвитку даної сфери. Імплементація конвенцій, стандартів інших країн підіймає Україну на більш вищий рівень розвитку та сприяє більш тісній взаємоспівпраці з більш розвиненими країнами світу.

3.2. Проведення державної політики України в сфері інформаційної безпеки

Нормативно-правову базу забезпечення інформаційної та кібербезпеки становлять наступні документи:

- Конвенція Ради Європи про кіберзлочинність, ратифікована Законом України від 07.09.2005 року № 2824-IV;
- Закони України «Про інформацію», «Про основи національної безпеки України», «Про Державну службу спеціального зв’язку та захисту інформації України», «Про телекомунікації», «Про захист інформації в

інформаційно-телекомунікаційних системах», «Про доступ до публічної інформації», «Про оборону України», «Про засади внутрішньої і зовнішньої політики», «Про об'єкти підвищеної небезпеки»;

– Укази Президента України, зокрема про Доктрину інформаційної безпеки, Стратегію національної безпеки України та Воєнну доктрину України;
– окремі положення Кримінального кодексу України, окремі постанови Кабінету Міністрів та рішення РНБОУ.

При цьому, ключову роль у забезпеченні інформаційної безпеки та кібербезпеки відіграють:

– Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», який регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та ІТ-системах;
– запропонований Міністерством внутрішніх справ (МВС) законопроект «Про внесення змін до Закону України «Про основи національної безпеки України» щодо Кібербезпеки України», яким має бути запроваджено низку термінів, пов'язаних із кібербезпекою [23]. Така нормативна база в сфері інформаційної та кібербезпеки була розроблена та впроваджена в Україні.

Питанню національної безпеки України в законодавчій практиці вперше було надано увагу в Декларації про державний суверенітет України від 16 липня 1990 року. Питання національної безпеки, з самого початку, має безпосередній зв'язок з державною політикою та певними політичними процесами, що відбуваються в державі. В Конституції України містяться норми, якими визначаються основні принципи регулювання сфери інформаційної безпеки. По-перше, це норма ч. 1. ст. 17 Конституції України, яка визначає статус відповідного напряму державної діяльності, встановлюючи,

що захист інформаційної безпеки є однією з найважливіших функцій держави, справою всього Українського народу. По-друге, це норми ст. 31 Конституції України, якими визначаються ключові права людини у сфері інформації, забезпечення яких гарантує її інформаційну безпеку [18].

Тривалий час у вітчизняному законодавстві не було визначення інформаційної безпеки. Зокрема, в Законі «Про основи національної безпеки України» вживається лише загальний термін «національна безпека» (ст. 1), яка визначена як «захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам». А питання інформаційної безпеки розглядається в цьому Законі як певні аспекти національних інтересів та національної безпеки в інформаційній сфері. Цим же Законом виділено три об'єкти національної та, відповідно, інформаційної безпеки (ст. 3), до яких належать:

– людина і громадянин – їхні конституційні права і свободи;
– суспільство – його духовні, морально-етичні, культурні, історичні, інтелектуальні та матеріальні цінності, інформаційне і навколишнє природне середовище і природні ресурси;
– держава – її конституційний лад, суверенітет, територіальна цілісність і недоторканність [9].

У законодавстві України визначено також багато аспектів інформаційної безпеки з питань інформатизації та розвитку інформаційного суспільства. Так, поняття інформаційної безпеки міститься в Законі України «Про Концепцію національної програми інформатизації». Згідно п. 3 розділу VI Концепції, «Інформаційна безпека є невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки». Проте цей Закон дещо інакше, ніж Закон «Про основи національної безпеки України», визначає

класифікацію об’єктів інформаційної безпеки. Так, уже в п. 3 розділу VI визначається об’єктами інформаційної безпеки названо:

- інформаційні ресурси;
- канали інформаційного обміну і телекомунікації;
- механізми забезпечення функціонування телекомунікаційних систем і мереж;
- інші елементи інформаційної інфраструктури країни [9].

25 лютого 2017 року Президентом України Петром Порошенком було затверджено та введено в дію Доктрину інформаційної безпеки – 47/2017, яка попередньо була ухвалена Радою національної безпеки та оборони 29 грудня 2016 року. У змісті документу зазначається про національні інтереси України в інформаційній сфері, пріоритети державної політиків інформаційній сфері і механізм реалізації доктрини, актуальні загрози національним інтересам та національній безпеці. Основні положення даної доктрини: захист українського суспільства від «агресивного інформаційного впливу Російської Федерації; розвиток публічної дипломатії, в тому числі культурної та цифрової; захист права на вільний доступ до інформації; створення механізмів захисту від пропаганди; видалення інформації з українського сегменту інтернету; квотування національного аудіовізуального контенту та багато іншого. Бачення розвитку й функціонування свого інформаційного простору та визначення того, що Російська Федерація є супротивником, що веде системну інформаційну війну – основний виклад держави в даній доктрині. У документі зазначаються пропозиції, щодо реагування на агресію та інформаційне забезпечення громадян. Доктрина вказує на саморегулювання медіа та зазначає про несення ними соціальної відповідальності [9]. Ця доктрина є ще одним кроком до розвитку сфери інформаційної безпеки.

Підписання Радою Європи Конвенції про кіберзлочинність (23 листопада 2001 р., Будапешт), що була ратифікована Україною 2005 р., – стало вагомим етапом у створенні міжнародно-правових засад захисту інформаційної безпеки.

Дана Конвенції (міжнародно-правовий акт) визначає систему правил, що стосуються ідентифікації видів з використанням інформаційних та телекомунікаційних технологій, які мають бути реалізовані в національних законодавствах країн–сторін даної конвенції [19].

Затвердженням, Указом Президента України (від 15 березня 2016 р. № 96/2016), національної Стратегії кібербезпеки – Україна розпочала процес імплементації даної конвенції. 5 жовтня 2017 р. – ухвалено Верховною Радою, 7 листопада 2017 р. – підписано Президентом України Закон України «Про основні засади забезпечення кібербезпеки України». Саме ці дії дали початок основі національного галузевого законодавства і визначили ключові вектори його подальшого розвитку відповідно до європейських демократичних практик. Законом «Про основні засади забезпечення кібербезпеки України» встановлено, що порядок та методика здійснення аудиту кібербезпеки повинна здійснюватися на основі міжнародних стандартів, проте в його прикінцевих та перехідних положеннях немає жодної згадки про чинний Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», згідно зі статтею 7 якого «державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю». Більшість об'єктів критичної інформаційної інфраструктури, значна кількість яких перебуває в недержавному секторі (наприклад, транспортній системі, телеком-індустрії, в енергетиці, фармацевтиці тощо) потрапляють під дію цієї норми. Поряд із цим і сама Комплексна система захисту інформації (КСЗІ), базована на українському стандарті КСЗІ НД ТЗІ 2.5–004–99, і вимога її обов’язкового застосування на об’єктах НКІІ здебільшого піддається гострій критиці у вітчизняних експертних та бізнесових колах. [6]. Також Кабінет міністрів України розробляє Стратегію кібербезпеки на кожен рік, 2018 рік не є виключенням.

Україна розробила стратегію національної безпеки до 2020 року. Згідно якої пріоритетними напрямками політики інформаційної безпеки України є:

1. Протидія диверсійній пропаганді та спеціальних інформаційних операціях іноземних держав проти України, запобігання спробам маніпулювати громадськістю – прикладом є цільова інформаційна війна проти України з боку російського телебачення та Російської Федерації.

Інші засоби пропаганди представляють собою життєво важливу загрозу для національних інтересів України як на своїй території, так і за її межами. Створення спотвореної картини світу Російські ЗМІ, включаючи Інтернет, руйнують будь-які перспективи добросусідських відносин між українським та російським народами, що підтримують етнічні, расові, релігійні та соціальні відносини.

Російські спецслужби продовжують вести небезпечні інформаційні операції проти України. Гострі загрози системних кібер-атак на критичну інформаційну інфраструктуру залишається актуальною, що може загрожувати людським життям та на шляху до державних послуг та створення фінансово-економічних проблем національного масштабу .

2. Створення системи кібербезпеки, включаючи координацію зусиль у цьому боротьба з кібертероризмом, захист від кібер-атак на критичну інфраструктура, зокрема у військовій, енергетичній, транспортній, телекомунікаційній та інфраструктурній сферах, банківські сфери.

3. Захист державних інформаційних ресурсів, системи електронного уряду, та захист криптографічної інформації з урахуванням НАТО та ЄС, найкращі практики держав-членів.

4. Реформування системи захисту державних таємниць та іншого обмеженого доступу інформації відповідно до стандартів ЄС та НАТО.

5. Підвищення обізнаності громадськості за допомогою відповідних освітніх програм [6].

Ще одним пріоритетом є реалізація міжнародної практики кібербезпеки та інформаційної безпеки, зокрема використовуючи національний контактний пункт 24/7 для боротьби з ІТ-злочинами "Великої сімки" за консультативною та фінансовою підтримкою, наданою Україні НАТО і ЄС. [6]. Міжнародна

співпраця щодо інформаційної безпеки грає важливу роль та її потрібно налагоджувати.

В Україні триває робота над створенням потужного центру з кібербезпеки на базі ДК «Укроборонпром». Крім представників Ради національної безпеки і оборони України, Міністерства оборони, Служби безпеки України, Державної служба спеціального зв'язку та захисту інформації України, Департаменту кіберполіції, фахівців НАТО, консультантів турецької державної компанії HAVELSAN та спеціалістів НТУУ «КПІ», у проекті беруть участь громадська неприбуткова організація «Українська академія кібербезпеки» і українська команда «білих» хакерів DCUA (одна з найсильніших у світі). Проект державного концерну «Укроборонпром» Cyber Guard був реалізований у партнерстві з приватними компаніями для захисту від кібератак приватних і державних установ України. З кінця 2015 р. в Україні, крім державного CERT-UA, діє офіційно акредитований міжнародною мережею FIRST приватний центр реагування та боротьби з кіберінцидентами (computer emergency response team, або CERT). Ідеться про вітчизняну компанію CyS-Centrum, яка спеціалізується на моніторингу й нейтралізації ІБ-загроз з використанням апаратно-програмних рішень власної розробки, а також на консалтингу у сфері інформаційної безпеки. Ще у квітні 2015 р. МВС України та корпорація «Майкрософт» підписали Меморандум про взаєморозуміння, який засвідчив взаємну зацікавленість у співпраці у сфері захисту даних, інформаційної та кібербезпеки. У листопаді 2017 р. подібний же меморандум, спрямований на організацію взаємодії в побудові комплексних рішень технічного забезпечення відомчої діяльності у масштабах держави, застосування інновацій у сфері держуправління, а також оптимізації наявного ресурсу, був підписаний представниками Національної поліції України та компанії «Майкрософт Україна» [6].

Особливо високу динаміку розвитку демонструє Департамент кіберполіції Національної поліції України. Кіберполіцію було засновано 5 жовтня 2015 року, як структурний підрозділ Національної поліції. Метою

створення Кіберполіції в Україні було реформування та розвиток підрозділів МВС України, що забезпечило підготовку та функціонування висококваліфікованих фахівців в експертних, оперативних та слідчих підрозділах поліції, задіяних у протидії кіберзлочинності, та здатних застосовувати на високому професійному рівні новітні технології в оперативно-службовій діяльності [15].

Основними завдання Кіберполіції є:

1. Реалізація державної політики у сфері протидії кіберзлочинності.
2. Завчасне інформування населення про появу новітніх кіберзлочинів.
3. Впровадження програмних засобів для систематизації та аналізу інформації про кіберінциденти, кіберзагрози та кіберзлочини.
4. Реагування на запити закордонних партнерів, що надходитимуть каналами Національної цілодобової мережі контактних пунктів.
5. Участь у підвищенні кваліфікації працівників поліції щодо застосування комп'ютерних технологій у протидії злочинності.
6. Участь у міжнародних операціях та співпраця в режимі реального часу. Забезпечення діяльності мережі контактних пунктів між 90 країнами світу.
7. Протидія кіберзлочинам [15].

Протидія кіберзлочинам у сфері інформаційної безпеки:

- соціальна інженерія – технологія управління людьми в Інтернет просторі;
- шкідливе програмне забезпечення – створення та розповсюдження вірусів і шкідливого програмного забезпечення;
- протиправний контент – контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості і насильства;
- рефайлінг – незаконна підміна телефонного трафіку [15].

Отже кіберполіція є досить новою установою для України, вона знаходиться в стадії розвитку та показує свою ефективність для громадян.

Крім того, за підрахунками спеціалістів кіберполіції, збільшити ефективність реагування на кіберзагрози в декілька разів дозволило розміщення онлайн-форми зворотного зв'язку на її сайті. У вересні 2017 р. за сприяння Української асоціації операторів зв'язку «Телас» було підписано меморандум про співпрацю між Департаментом кіберполіції й дата-оператором lifecell, за умовами якого останній на безоплатній основі передав Департаменту систему власної розробки для екстреного інформування в умовах надзвичайних ситуацій Emergency Notifi cation System (ENS). Серед іншого, система дає змогу локалізувати кіберзагрозу й уникнути її розповсюдження за допомогою оперативного інформування про небезпеки завчасно визначених груп отримувачів через голосові виклики, SMS та електронні листи. За повідомленнями керівництва, ENS вже успішно пройшла тестування й її абонентами можуть стати як державні, так і приватні компанії, включаючи об'єкти критичної інфраструктури [6].

Якщо розглянути інформаційну безпеку у державних установах, як приклад Управління патрульної поліції у м. Києві ДПП, то система захисту дуже слабка. Більшість інформації зберігається у Google таблицях. Тобто при якихось кібератаках доступ отримати до інформації не складе великих проблем. Також використовують систему Армор яка є більш захищена, але деякі данні все ж зберігаються в Google таблицях.

Протягом останніх чотирьох років спостерігалося помітне зростання ролі волонтерських та громадських структур, які допомагали державі в різних аспектах національної безпеки. Ця допомога набула особливого значення в перші роки конфлікту на сході України із російсько-терористичними силами. Не стала винятком і кіберсфера. Проукраїнські хактивісти (зокрема, «Українські кібервійська», «Кіберсотня», «FalconsFlame», «Trinity», «RUH8» та інші) здійснювали:

– злами комп'ютерних систем – як терористів, так і їх російських кураторів;

- отримували доступ до поштових скриньок осіб, які задіяні в організації та реалізації російської агресії проти України;
- відслідковували аканти в соціальних мережах та мережі Інтернет, через які терористичні угруповання вели свою агітацію та збирали кошти;
- блокували окремі електронні гаманці фінансистів терористів;
- допомагали у ідентифікації осіб, які беруть участь у збройному протистоянні на сході України проти сил АТО та багато іншого.

Вочевидь для класифікації їх діяльності найбільш доцільно використовувати концепцію «кольорових капелюхів» (hats) 242, що вже стала звичною при характеристиці дій хакерських (чи просто IT-експертних) угруповань. «Білі капелюхи» (White hat) зазвичай є повністю легальними IT-фахівцями, що здійснюють свою діяльність законно і частіше за все – на комерційній основі. Основна їх мета – вдосконалення систем кібербезпеки тих чи інших структур (державних чи приватних), у т. ч. через пошук недоліків коду тих інформаційних систем, які використовують ці структури. Важливим є те, що ці дії вони застосовують на запит самої організації та за чіткою попередньою домовленістю з нею. Іншим полюсом є «чорні капелюхи» (Black hat), які більшою мірою є традиційними кіберзлочинцями, що здійснюють свою діяльність заради особистого зиску, використовуючи будь-які методи зламу. Водночас послугами таких груп дедалі частіше користуються військові та розвідувальні структури задля досягнення своїх військово-політичних цілей, але мінімізуючи при цьому юридичні наслідки від такого втручання (неможливість визнання відповідальності держав за такі атаки). В таких випадках «чорні капелюхи» виступають як своєрідні «проксі-групи», аналогічні за своєю суттю до різноманітних форм найманців, які здійснюють свою діяльність проти України з територій «ДНР/ЛНР». Водночас українські хактивісти швидше підпадають під третю класифікаційну групу – «сірих капелюхів» (Grey hat). До них відносяться хакери чи фахівці з комп'ютерної безпеки, які почасти порушують законодавство чи типові етичні

норми, але не здійснюють деструктивного впливу на зламану систему, що є типовим для «чорних капелюхів». Така характеристика проукраїнських хакерських груп меншою мірою стосується їх діяльності проти інформаційних ресурсів «ДНР» та «ЛНР», а також російських інформаційних ресурсів, щодо яких вони діють саме як «чорні капелюхи».

Останнім часом їх безпосередня активність дедалі частіше спрямовується на внутрішні інформаційні системи (передусім – державні органи та об'єкти критичної інфраструктури), щодо яких вони проводять несанкціоновані пентести, скачуючи при цьому окремі документи (які не мають грифів обмеження доступу) для підтвердження наявності уразливості. Незважаючи на те, що ці дії здійснюються ними в інтересах забезпечення більшої кібербезпеки держави в умовах агресії (принаймні така мета ними публічно декларується), але відповідно до чинного українського законодавства, частіше за все вони його порушують. Показовим у цьому сенсі був випадок із українським програмістом О. Моховим, який у 2013 р. помітив уразливість у системі «Приват-24» та, здійснивши декілька тестів уразливості, звернувся до Служби безпеки ПриватБанку. Однак фактично експлуатацію цієї уразливості можна було кваліфікувати як порушення законодавства (про що і заявила тоді прес-служба банку 245). Надалі ситуацію урегулювали, однак при цьому принципова проблема не зникла [6]. Отже розвиток інформаційної безпеки та кібербезпеки почався з дня Незалежності України. Та більш ефективний розвиток цих сфер прийшовся на теперішній час. На це вплинула Євроінтеграція та агресія зі сторони Російської Федерації. Звісно, сферу інформаційної безпеки потрібно розвиватися бо технології з кожним днем все більше розвиваються, та їх потрібно контролювати. Світ інформаційної безпеки змінився настільки, що будь-яка політика, написана більше двох років тому, майже не має значення, і будь-яка політика, написана сьогодні, швидше за все, матиме дуже короткий термін зберігання. Вжиття заходів для поліпшення політики інформаційної безпеки є необхідністю, а не розкішшю, у сьогоднішніх загрозливих умовах.

3.3. Шляхи вдосконалення державної політики України щодо інформаційної безпеки

Після проведення аналізу законодавства України та забезпечення державної політики в сфері інформаційної безпеки, можна побачити необхідність у здійсненні шляхів по вдосконаленню не тільки інформаційного простору, а й стійкої організаційно-інформаційної мережі та системи, об'єднаної в державну інформаційно-комунікативну інфраструктуру.

В законодавстві України є такі прогалини:

1. Було створено багато нормативно-правових актів в сфері інформаційної безпеки, але жоден з них не регулює конкретну сферу інформаційної безпеки.
2. Незважаючи на наявність цілої низки чинних нормативно-правових документів щодо проблем забезпечення безпеки інформаційного простору держави, вони не охоплюють всього спектру сучасних загроз для держави.
3. В чинній нормативно-правовій базі відсутні визначення (відповідно і не реалізовані особливі форми захисту, реагування та відповідальності) ключових елементів державної інфраструктури саме від кібератак.
4. Термінологічне поле сфери кібербезпеки держави все ще залишається фрагментарним, що унеможливлює формування дієвих нормативно-правових документів із протидії кіберзагрозам.
5. Відсутні усталені визначення ключових термінів («інформаційна безпека», «інформаційний простір», «інформаційні злочини») що можуть ефективно застосовуватись в практиці правоохоронної діяльності.
6. Єдина загальнодержавна система протидії інформаційній злочинності та кіберзлочинності із відповідним нормативним забезпеченням все ще знаходиться в процесі розробки і потребує ще чимало доопрацювань.

Отже, можна сказати, що вітчизняні реалії інформаційної сфери свідчать про низку важливих проблем, які заважають створенню ефективної системи протидії загрозам у інформаційному просторі. До таких проблем належать передусім: термінологічна невизначеність, відсутність належної координації діяльності відповідних відомств, залежність України від програмних і технічних продуктів іноземного виробництва, складнощі з кадровим наповненням відповідних структурних підрозділів [24]. Основною складовою національної безпеки має бути забезпечення інформаційної безпеки.

Потрібно звернути увагу на подолання таких проблем імплементації в Україні стандартів ЄС і НАТО у галузі інформаційної безпеки: низький рівень обізнаності і культури населення і підприємницького сектору; низька якість підготовки фахівців у сфері безпеки; економія ресурсів на запровадження міжнародних стандартів і розвиток інфраструктури; недотримання чинного законодавства; низький рівень технічного оснащення тощо. Враховуючи це, якомога скоріше має бути розроблений комплексний план заходів. Першочерговими повинні стати: регулярні навчальні та інформаційні програми; розробка систем захисту конфіденційної інформації у нових сферах використання Інтернету, власних методологій криптографії; обґрунтування стратегії інвестування у галузь інформаційної безпеки, зокрема технічні засоби, кіберпродукти, створення служб інформаційної безпеки. У військовій сфері поштовхом стала Річна національна програма співробітництва Україна–НАТО, за результатами якої у наступних роках необхідно розширити партнерство у сфері інформаційної безпеки [6].

Агресія Росії, складна ситуація на Сході України зробила свій вклад у сферу інформаційної та кібербезпеки. Також потрібно зробити акцент на розвиток міжнародних відносин в інформаційній сфері.

Вкрай важливим є постійний та системний обмін даними щодо актуальних інформаційних загроз та кіберзагроз і можливостей боротьби з ними. Для цього оптимальним було б створення та підтримка на основі міжнародного співробітництва національної системи обміну даними про

інформаційні та кіберінциденти та їх реєстр. Це дозволило б підрозділам з ІТ-безпеки компаній та установ перевіряти маркери компрометації, відслідковувати, кому ще розсилалися аналогічні зразки шкідливого програмного забезпечення, обмінюватися індикаторами атак, убезпечуючи таким чином свої об’єкти від ІТ злочинців. В Україні поки не існує такої системи, однак необхідно наголосити, що її створення є складною проблемою у більшості країн світу, причому в зв’язку з позицією саме недержавних (передусім бізнесових) акторів [6].

Безпека інформації повинна включати в себе захист її конфіденційності (інформація повинна бути доступна тільки для тих, хто має право користуватися нею), захист інформації від несанкціонованої модифікації (цілісність), а також захист систем від відмов надання послуг і від несанкціонованого доступу.

У цьому контексті також такі критерії повинні бути прийняті до уваги для розвитку Інформаційної безпеки в Україні:

- Гармонізація національного законодавства з метою забезпечення інформаційної безпеки.
- Створення нормативної бази, що визначає критичну інформаційну інфраструктуру та забезпечує інформаційну безпеку.
- Оновлення правової бази забезпечення кібербезпеки інформаційних систем.
- Вдосконалення механізмів співпраці з постачальниками критично важливих інформаційних систем.
- Розробка механізмів виконання зобов'язань, визначених законодавством.
- Продовження виконання зобов'язань, взятих внаслідок ратифікації Конвенції Ради Європи «Про кіберзлочинність».

- Розробка та уточнення планів резервування та процедур для відповідних дій, у надзвичайних ситуаціях, військових та інші види кризових ситуацій.
- Створення єдиної інтерактивної бази даних про інформційні та кіберінциденти [31].
- Організація обміну інформацією про кібератаки на об’єкти критичної інфраструктури [31].
- Подальше впровадження норм міжнародних стандартів, стандартів ЄС та НАТО у сфері електронних комунікацій, захисту інформації, інформаційної безпеки та кібербезпеки [31].
- Імплементації Директиви (ЄС) 2016/1148 Європейського Парламенту та Ради ЄС від 6 липня 2016 р. щодо заходів з підвищення загального рівня безпеки мереж та інформаційних систем в ЄС [31].
- Забезпечення внутрішньодержавної та зовнішньої інформаційної політики розширення та оновлення вітчизняного інформаційного простору новим модернізованим програмним забезпеченням.
- Орієнтованість на законодавство в інформаційній сфері на більш розвинені держави.
- Міжнародна співпраці в даній галузі.
- Створення єдиної системи захисту інформації.
- Кодифікація створених нормативно-правових актів.
- Створення Інформаційного кодексу України в якому б поєднувалися інформаційна безпека та кібербезпека та були б зазначені шляхи регулювання та забезпечення інформаційної безпеки та відповідальність за скоєні злочини ІТ сфері.
- Організації, що використовують технології мають нести відповідальність за належне використання своїми співробітників і, отже, повинні розробляти політику безпеки для досягнення цієї мети, а також заходи і процедури, що забезпечують їх контроль.

– Провайдери комп'ютерних мереж і послуг мають завжди нести відповідальність за забезпечення безпеки систем, у яких вони працюють. Вони також повинні нести відповідальність за інформування користувачів про свою політику безпеки і будь-якої зміни такої політики.

Однією з характерних особливостей сучасного етапу світового науково-технічного прогресу є глобальна інформаційна революція – швидкий розвиток і повсюдне застосування найостанніших інформаційних технологій і глобальних телекомунікаційних засобів. Які охоплюють усі сфери життєдіяльності держав, інформаційна революція відкриває нові можливості для розвитку міжнародного співробітництва та створення глобальної інформаційної галузі, в якій стає надзвичайно цінною частиною багатства країни і її стратегічних ресурсів інформація.

У той же час, стає ясно, що, поряд з позитивними аспектами цього процесу, також існує реальна загроза, що розвиток подій в інформаційному полі можуть бути використані з метою, несумісних із завданнями забезпечення міжнародної стабільності і безпеки, з дотриманням принципів суверенної рівності держав, мирного врегулювання суперечок і конфліктів, незастосування сили, невтручання у внутрішні справи і поваги прав і свобод людини.

Використання самих останніх інформаційних технологій для створення військового потенціалу країн змінює глобальний і регіональний баланс сил і призводить до виникнення напруженості між традиційними і виникаючими центрами сили і впливу.

Принципово нова область протистояння на міжнародній арені в процесі становлення, і існує небезпека, що наукові та технологічні розробки в області інформації та комунікації можуть привести до ескалації гонки озброєнь. У такій ситуації, як національна безпека окремих держав і в цілому система міжнародної колективної безпеки на регіональному і глобальному рівнях порушені. Створення «інформаційної зброї», використання якої, в залежності

від рівня суспільства інформаційних технологій і уразливості своїх життєво важливих структур, може мати руйнівні наслідки, які можна порівняти з ефектом зброї масового знищення. Очевидно, що така зброя може бути використана терористичними, екстремістських або злочинними групами, а також окремими правопорушниками.

Таким чином, універсальність, скритність або знеособленість інформаційної зброї, можливість його широкого використання через національні кордони і її економіка і загальна ефективність роблять його надзвичайно небезпечним засобом здійснення впливу, і сучасне міжнародне право не має практично ніяких засобів регулювання розвитку і застосування такої зброї.

Дуже важливо, що спільний розгляд ситуації в області інформаційної безпеки повинна бути продовжена з метою виявлення всіх існуючих позицій і поглядів, і прийняти їх до уваги в загальних зусиллях по просуванню концепції інформаційної безпеки.

Як визначаються загальні підходи і тенденції, повинна початися робота по розробці міжнародних принципів (наприклад, режим, кодекс поведінки для держав) з метою зміцнення міжнародної інформаційної безпеки. Перш за все, ці принципи могли б прийняти форму багатосторонньої декларації, вони згодом будуть включені в багатосторонній міжнародно-правовий документ.

У той же час міжнародне співтовариство повинне розглянути і прийняти вищезазначені принципи в пакеті, тобто, маючи на увазі загрози військового, терористичного або кримінального характеру і з метою застосування цих принципів як до військової і цивільної сфери.

Також існує необхідність в створенні міжнародно-правової бази:

– Визначення характерних особливостей і класифікації інформаційних воєн.

- Визначення характерних особливостей і класифікації інформаційної зброї, а також методи і засоби, які можуть бути розцінені як інформаційна зброя.
- Обмеження трафіку для інформаційної зброї, та заборона розробки, поширення або використання особливо небезпечних видів інформаційної зброї.
- Запобігання загрози інформаційних воєн.
- Заборона використання інформаційних технологій і засобів у ворожих цілях і, зокрема, щодо узгоджених категорій об'єктів.
- Створення умов для справедливого і безпечного міжнародного інформаційного обміну, на основі балансу інтересів особистості, суспільства і держави.
- Запобігання загрози використання інформаційних технологій і засобів в терористичних або інших злочинних цілях.
- Запобігання загрози використання інформаційних технологій і засобів впливу на суспільну свідомість з метою дестабілізації суспільства і держави.
- Розробка процедури взаємного сповіщення і запобігання несанкціонованого використання інформації.
- Створення механізму для врегулювання конфліктних ситуацій в сфері інформаційної безпеки.
- Створення міжнародної системи сертифікації інформаційних технологій і засобів (в тому числі програмного і апаратного забезпечення) з метою забезпечення їх інформаційної безпеки.
- Розробка системи міжнародного співробітництва між правоохоронними органами з метою запобігання злочинам в інформаційній сфері.
- Створення механізму контролю за дотриманням умов міжнародного режиму інформаційної безпеки.

Для забезпечення інформаційної безпеки особлива увага приділяється зміцненню кібербезпеки.

На технічному рівні особливо важливо створити кібер-дослідну лабораторію, діяльність якої буде пов'язана з розробкою різних інноваційних рішень що стосується питань кібербезпеки. Крім того, лабораторія забезпечить сучасні знання для відповідних служб України, що також має життєво важливе значення для національної безпеки, беручи до уваги той факт, що сучасні технології прогресують швидкими темпами, а органи безпеки постійно потребують розвитку навичок, що стосуються технологічного прогресу. Також потрібно зробити внесок у підтримку та подальший розвиток кіберполіції.

Таким чином, завдяки впровадженню розглянутих пропозицій вдосконалення та модернізації нормативно-правової бази України у сфері інформаційної безпеки, буде сформована цілісна система регулювання інформаційної безпеки України.

Висновки до розділу 3

Отже в Україні діє державний стандарт технічного захисту інформації серії НД ТЗІ 2.5–004–99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу». До українського законодавства було імплементовано Європейський стандарт 27001:2013 р. На даний час триває формування єдиного пакета галузевих стандартів з інформаційної безпеки. Також на розвиток інформаційної безпеки впливає співробітництво з НАТО та ЄС.

В Україні було прийнято декілька нормативно-правових актів у сфері інформаційної безпеки та кібербезпеки. Було ратифіковано деякі положення Європейської конвенції з кіберзлочинності. МВС України має на меті ратифікувати як можна більше положень даної конвенції.

Наша економіка дедалі більше залежить від даних та всесвітньої інформаційної інфраструктури, яка не тільки збирає та передає ці дані, але

також контролює важливі системи, включаючи фінансові мережі платежів, транспортної інфраструктури, комунальні послуги (наприклад, інтелектуальну мережу), точність у часі і виробничі ланцюги, а також структури управління військовими та цивільними операціями. Інформаційна безпека – це швидко зростаюча сфера права, яка відповідає потребам забезпечувати ці дані та комп'ютерну інфраструктуру від хакерських та інших форм несанкціонованого доступу, вірусів, терористичних нападів, крадіжок, неправильного використання та випадкового знищення чи зміни.

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

На підставі зробленого дослідження, можна зробити натупні висновки:

1. виявлено та охарактеризовано становлення та розвиток інформаційного простору. Становлення інформаційного простору розпочалося ще у XX столітті. Міжнародний інформаційний простір – це сума складних інформаційних технологій, які є основою і визначальним компонентом промислово-економічного комплексу транснаціональних спільнот, які впливають на формування світоглядних процесів у суспільстві. Головними періодами становлення інформаційного простору є: 1940-1960 рр. – пов'язані з винаходом і впровадженням в практичну діяльність електронно-обчислювальних машин (комп'ютерів); 1970-1980 рр. – поява перших персональних комп'ютерів, було створено «Інтернет» та почався розвиток інформаційної безпеки; 1990-2000 рр. – Інтернет став загальнодоступним для звичайних користувачів, з'явився знаменитий Веб-браузер NCSA Mosaic. Всесвітня павутина ставала дедалі популярнішою;

2. уточнено поняття інформаційної безпеки та кібербезпеки: Інформаційна безпека – це процес захисту даних від несанкціонованого доступу, використання, розголошення, знищення, модифікації або порушення.

Інформаційна безпека призначена для захисту конфіденційності, цілісності та наявності даних комп'ютерної системи від тих, хто мають шкідливі наміри. Важливість інформаційної безпеки можна виокремити в так звану тріаду інформаційної безпеки або систему інформаційної безпеки:

- несанкціоноване вивільнення інформації (конфіденційність);
- неавторизована модифікація інформації (цілісність);
- несанкціонована відмова в користуванні (доступність).

Кібербезпека – це інформаційні технології, пов'язані з безпекою комп'ютерних систем та інформації. Кібербезпека охоплює загрози комп'ютерної апаратури, програмного забезпечення та даних, включаючи крадіжки, хакерство, віруси тощо;

3. обґрунтувано різницю між кібербезпекою та інформаційною безпекою: проаналізувавши поняття кібербезпеки та інформаційної безпеки стає зрозумілим що кібербезпека – це інформаційні технології, пов'язані з безпекою комп'ютерних систем та інформації (обладнання та програм), тоді як інформаційна безпека – це практика захисту інформації від несанкціонованого доступу, використання, розкриття, порушення, модифікації, перегляду, перевірки, запису або знищення зазвичай організації чи компаній у тому числі в IT системах. Кібербезпека є частиною Інформаційної безпеки будь-якої організації. Об’єктами інформаційної безпеки є – інформаційні бази, інформаційні потоки, штатні співробітники. Об’єктами кібербезпеки є – органи та канали управління, канали інтерактивної взаємодії, системи моніторингу та збору даних.

Термін «інформаційна безпека» вживається в широкому сенсі. У вузькому сенсі доречно застосовувати термін «безпека інформації», що має на увазі просто комплекс заходів щодо захисту інформації. Термін кібербезпека слід розуміти як забезпечення «безпеки інформації»;

4. проаналізовано міжнародно-правові акти в сфері інформаційної безпеки та кібербезпеки. У сфері інформаційної безпеки було розроблено різні нормативні акти для регулювання даної сфери як на міжнародному рівні так і на національному. Такі як Окінавська хартія,Будапештська конвенція про кіберзлочинність, Конституція Міжнародного союзу електрозв'язку, Угода про співпрацю в галузі інформаційної безпеки в Шанхайській організації співробітництва та Конвенція про кібербезпеку Африканського Союз.

Окінавська хартія визначає вільний обмін інформацією та знаннями однією з демократичних цінностей людства, Будапештська конвенція 2001 року про кіберзлочинність є правоохоронним договором, спрямована на визначення, покарання та тим самим стримування злочинів, пов'язаних з інформаційною безпекою та кібербезпекою, Конституція 1992 року Міжнародного союзу електрозв'язку, Угода про співпрацю в галузі інформаційної безпеки в Шанхайській організації співробітництва 2009 року та Конвенція 2014 року про

кібербезпеку Африканського Союзу, хоча ці міжнародні угоди є важливими, вони регулюють лише невелику частину інформаційної безпеки та кібербезпеки, що пов'язано з діяльністю (наприклад, кримінальні правопорушення, вчинені за допомогою комп'ютерних систем чи операції, що перешкоджають існуючим телекомунікаційним мережам), або мають дуже обмежений членський склад (шість держав у випадку домовленості Шанхайської організації співробітництва та їх відсутність в конвенції Африканського Союзу);

5. виявлено особливості організаційно-правового механізму міжнародного співробітництва держав у сфері забезпечення інформаційної безпеки на міжнародному рівні. Співробітництво зумовлено такими міжнародними організаціями: ЮНЕСКО в рамках свого мандата сприяє політиці в галузі створення інформаційного простору на міжнародному рівні, ENISA допомагає країнам ЄС бути краще оснащеним та підготовленим до запобігання, виявлення та реагування на проблеми інформаційної безпеки та також БРІКС у сфері інформаційної безпеки країни БРІКС дотримуються стратегій і програм регіональних організацій, до яких вони належать і які демонструють різні підходи до розуміння глобальних інформаційних загроз і практики протидії викликам високих технологій, ООН, ОЕСР Міжнародний союз електрозв’язку, ІНТЕРПОЛ. Вони вирішують більш глобальні питання, що стосуються забезпечення кібербезпеки.

В кожній країні по різному проходить регулювання інформаційної безпеки. Більш розвинені в цій сфері країни: Китай, США, Росія та ЄС. Наприклад на початку цього року Китай випустив остаточну версію національного стандарту захисту персональних даних, інформаційні технології GB/T 35273-2017 – Специфікація захисту персональної інформації (Специфікація). Специфікація набрала чинності з 1 травня 2018 року. Специфікація не є законом чи нормативним актом, яка вимагає обов'язкового дотримання. Однак, цілком імовірно, що китайські державні установи покладаються на стандарт, щоб визначити, чи відповідають компанії правилам

захисту даних Китаю. Сучасна політика інформаційної безпеки Бразилії пов’язана з концепціями інформаційного протиборства США і пріоритетами співробітництва у форматі «інформаційної парадигми», що передбачає інформаційно-технологічні переваги держави, здатні зберегти досягнуту в докризовий період стабільність і забезпечити посткризовий розвиток, зробити прогнозованими перебіг соціальних конфліктів, запобігти суперечностям у суспільстві. Також майже у кожній країні розроблено Державну стратегію з кібербезпеки яка включає в себе як кібер безпеку так і інформаційну безпеку. Також є країни в яких інформаційна безпека потребує більших зусиль для розвитку. Такою країною є і Україна;

6. з’ясовано сутність кіберзлочинності та кібертероризму як загроз інформаційній безпеці у міжнародному праві. В інформаційній безпеці розрізняють два види загрози – це кіберзлочинність та кібертероризм. кібертероризм – це використання комп'ютерів та інформації, зокрема через Інтернет, для заподіяння фізичної, реальної шкоди або суттєвого порушення інфраструктури. Кіберзлочинність – це використання комп'ютера як інструменту до незаконного доступу для здійснення фальсифікації, незаконного обороту інтелектуальної власності, крадіжки ідентичності або порушення конфіденційності;

7. проаналізовано стан державної політики у сфері інформаційної безпеки в Україні. Україна імплементувала до національного законодавства деякі положення Європейської конвенції з кіберзлочинності. Вони були ратифіковані Законом України від 7.09.2005 року № 2824-IV та до деяких статей Кримінального кодексу України. В пріоритеті МВС є ратифікація як можна більше статей з даної конвенції. Також на законодавство України у цій галузі вплинуло співробітництво з НАТО та ЄС. В Україні діє державний стандарт технічного захисту інформації серії НД ТЗІ 2.5–004–99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу». Також статус державного стандарту має серія Європейських стандартів ISO/IEC27001:2013. Створено орган який забезпечує реалізацію

державної політики у сфері боротьби з кіберзлочинністю, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність. Цим органом є Кіберполіція Національної поліції України. Поки що як стає зрозумілим триває формування єдиного пакета галузевих стандартів з інформаційної безпеки.

В Україні розроблені такі нормативно-правові акти в сфері інформаційної та кібербезпеки: Закони України «Про інформацію», «Про основи національної безпеки України», «Про Державну службу спеціального зв'язку та захисту інформації України», «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про доступ до публічної інформації», «Про оборону України», «Про засади внутрішньої і зовнішньої політики», «Про об'єкти підвищеної небезпеки»; Укази Президента України, зокрема про Доктрину інформаційної безпеки, Стратегію національної безпеки України та Воєнну доктрину України і інші. Значним поштовхом для розвитку інформаційної безпеки в Україні стали терористичні дії с боку Російської Федерації. Інформаційна пропаганда, інформаційні війни дали поштовх для захисту інформаційного та кіберпростору держави від пропаганди. Тобто як можна бачити інформаційна безпека в Україні лише набирає обертів для розвитку, запозичуючи досвід більш розвинених країн у цій сфері та упроваджуючи нові положення;

8. розроблено пропозиції з вдосконалення міжнародно-правового регулювання співробітництва держав у сфері забезпечення інформаційної безпеки шляхом створення єдиної міжнародної системи. Повинна розпочатися робота по розробці міжнародних принципів (наприклад, режим, кодекс поведінки для держав) з метою зміцнення міжнародної інформаційної безпеки. Перш за все, ці принципи могли б прийняти форму багатосторонньої декларації, вони згодом будуть включені в багатосторонній міжнародно-правовий документ. У той же час міжнародне співтовариство повинне розглянути і прийняти вищезазначені принципи в пакеті, тобто, маючи на увазі

загрози військового, терористичного або кримінального характеру і з метою застосування цих принципів як до військової так і цивільної сфери;

9. розроблено рекомендації та пропозиції з вдосконалення державної політики у сфері інформаційної безпеки. Отже такі критерії повинні бути прийняті до уваги для розвитку інформаційної безпеки в Україні:

- гармонізація національного законодавства з метою забезпечення інформаційної безпеки;
- створення нормативної бази, що визначає критичну інформаційну інфраструктуру та забезпечує інформаційну безпеку та кібербезпеку;
- оновлення правової бази забезпечення кібербезпеки інформаційних систем;
- вдосконалення механізмів співпраці з постачальниками критично важливих інформаційних систем;
- розробка механізмів виконання зобов'язань, визначених законодавством;
- продовження виконання зобов'язань, взятих внаслідок ратифікації Конвенція Ради Європи «Про кіберзлочинність»;
- розробка та уточнення планів резервування та процедур для відповідних дій у надзвичайних ситуаціях, військових та інших видах кризових ситуацій;
- посилення можливостей у сфері інформаційної та кібербезпеки;
- міжнародна співпраця в даній галузі;
- створення Інформаційного кодексу України в якому б були зазначені шляхи регулювання та забезпечення інформаційної безпеки та відповідальність за скоєні злочини ІТ сфері;
- для забезпечення інформаційної безпеки особлива увага приділяється зміцненню кібербезпеки;
- на технічному рівні особливо важливо створити кібер-дослідну лабораторію, діяльність якої буде пов'язана з розробкою різних

інноваційних рішень що стосується питань кібербезпеки. Крім того, лабораторія забезпечить сучасні знання для відповідних служб України, що також має життєво важливе значення для національної безпеки, беручи до уваги той факт, що сучасні технології прогресують швидкими темпами, а органи безпеки постійно потребують розвитку навичок, що стосуються технологічного прогресу. Також потрібно зробити внесок у підтримку та подальший розвиток кіберполіції.

Таким чином, завдяки впровадженню розглянутих пропозицій вдосконалення та модернізації нормативно-правової бази України у сфері інформаційної безпеки, буде сформована цілісна система регулювання інформаційної безпеки України. Повна інформаційна безпека не може бути досягнута – це безперервний процес. Це потребує стратегії, засобів, технологій, організації та людей. Уряд в державі має оптимізувати ресурси (особливо людський капітал) та залучати іноземні інвестиції, одночасно вирішувати інституційні та правові прогалини у своєму національному підході до кібербезпеки з метою зменшення його вразливості. До цього часу Україна залишається вразливою.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бакалинский А.О, Безштанько В.М. Семейство стандартов ISO/IEC 27000 как источник для создания национального стандарта по кибербезопасности// НТУУ «КПИ» [Електронний ресурс]. — Режим доступу : http://www.niss.gov.ua/public/File/2014_table/0311_prez2.pdf
2. Баранов О.А. Про тлумачення та визначення поняття [Електронний ресурс]. — Режим доступу : http://ippi.org.ua/sites/default/files/14boavpk.pdf
3. Бурячок В. Л Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект [Електронний ресурс]. — Режим доступу : http://www.dut.edu.ua/uploads/p_303_79299367.pdf
4. Вікіпедія,WikiLeaks [Електронний ресурс]. — Режим доступу : https://uk.wikipedia.org/wiki/WikiLeaks
5. Голіна В.В., Головкін Б.М. Поняття та кримінологічна характеристика кіберзлочинності [Електронний ресурс]. — Режим доступу : http://libnet.com/content/9684_Ponyattya_ta_kriminologichna_harakteristika_kiberzlochinnosti.html
6. Дубова Д. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України [Електронний ресурс]. — Режим доступу : http://www.niss.gov.ua/content/articles/files/AD_Dubov_206x301_pp1-84_press-b44d7.pdf
7. Двадцять фактів російського вторгнення в Україну [Електронний ресурс]. — Режим доступу : http://mfa.gov.ua/mediafiles/sites/china/files/20___.pdf
8. Діордіца І.В. Сучасний кібертероризм: Аспекти правового регулювання [Електронний ресурс]. — Режим доступу : http://goal int.org/suchasnij kiberterorizm aspekti pravovogo regulyuvannya/
9. Жуган Вікторія, Доктрина інформаційної безпеки України [Електронний ресурс]. — Режим доступу : https://www.radiosvoboda.org/a/28336852.html

10. Імплементація норм міжнародної конвенції про кібербезпеку [Електронний ресурс]. — Режим доступу : http://ukrainepravo.com/news/ukraine/v-ukrayinske-zakonodavstvo-normy-mizhnarodnoyi-konventsiyi-pro-kiberbezpeku/
11. Інформаційна безпека [Електронний ресурс]. — Режим доступу : https://uk.wikipedia.org/wiki/Інформаційна_безпека
12. Інформаційний тероризм [Електронний ресурс]. — Режим доступу : https://uk.wikipedia.org/wiki/Інформаційний_тероризм#cite_note-1
13. Інформаційні злочини [Електронний ресурс]. — Режим доступу : http://www.nidiot.de/uk/Інформаційні_злочини
14. Історія становлення інтернету та розвитку веб-технологій [Електронний ресурс]. — Режим доступу : https://infopedia.su/9x5b4c.html
15. Кіберполіція [Електронний ресурс]. — Режим доступу : https://uk.wikipedia.org/wiki/Кіберполіція_(Україна)#Історія
16. Кібертероризм [Електронний ресурс]. — Режим доступу : http://studopedia.com.ua/1_67343_kIberterorizm.html
17. Комп'ютерна безпека [Електронний ресурс]. — Режим доступу : https://uk.wikipedia.org/wiki/Комп%27ютерна_безпека
18. Конституція України [Електронний ресурс]. — Режим доступу : https://www.president.gov.ua/documents/constitution
19. Кормич Б. А. Інформаційне право [Електронний ресурс]. — Режим доступу : http://dspace.onua.edu.ua/bitstream/handle/11300/7911/Kormych_Inf_pr.pdf?sequence=1)
20. Кримінальний кодекс України [Електронний ресурс]. — Режим доступу : http://zakon.rada.gov.ua/laws/show/2341-14
21. Ліпкан В.А. Національна безпека України [Електронний ресурс]. — Режим доступу : http://politics.ellib.org.ua/pages-8280.html
22. Макаренко Є.А. Суперечність співробітництва країн БРІКС у сфері інформаційної безпеки : тенденції і перспективи [Електронний ресурс]. — Режим доступу : http://vmv.kymu.edu.ua/v/p05/ar356371.pdf

23. Малик Я. Інформаційна безпека : Стан та перспективи розвитку [Електронний ресурс]. — Режим доступу : http://www.lvivacademy.com/vidavnitstvo_1/edu_44/fail/ch_1/3.pdf
24. Малишев М.А. Проблеми реалізації положень Конвенції про Кіберзлочинність в Україні [Електронний ресурс]. — Режим доступу : http://conf.inf.od.ua/doklady-konferentsii/spisok-dokladov-iii-konferentsii/81-malishev-m-a
25. Міжнародна інформаційна безпека [Електронний ресурс]. — Режим доступу : https://stud.com.ua/59267/pravo/mizhnarodna_informatsiyna_bezpeka
26. Міжнародна співпраця і законодавство в сфері інформаційної безпеки [Електронний ресурс]. — Режим доступу : http://ni.biz.ua/20-5/26308.html
27. Міжнародно-правові засади інформаційної безпеки [Електронний ресурс]. — Режим доступу : http://studies.in.ua/inform-pravo-shporu/2532-mzhnarodno-pravov-zasadi-nformacynoyi-bezpeki.html
28. Операційні системи мейнфреймів [Електронний ресурс]. — Режим доступу : http://wiki.tneu.edu.ua/index.php?title=Операційні_системи_мейнфреймів
29. Орлов Юрій Юрійович, Реалізація Вимог Міжнародної Конвенції про Кіберзлочинність у законодавстві України [Електронний ресурс]. — Режим доступу : http://www.pravoznavec.com.ua/period/article/43919/O.
30. Поняття та зміст інформаційної безпеки [Електронний ресурс]. — Режим доступу : http://pidruchniki.com/16850303/politologiya/ponyattya_zmist_informatsiynoyi_bezpeki
31. Про затвердження плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України// Кабінет Міністрів України Розпорядження від 11 липня 2018 р. № 481-р Київ [Електронний ресурс]. — Режим доступу : http://zakon.rada.gov.ua/laws/show/481-2018-p
32. Пропозиції до політики щодо реформування сфери кібербезпеки в Україні [Електронний ресурс]. — Режим доступу : http://parlament.org.ua/wp-content/uploads/2017/12/au_White-book-on-cybersecurity-draft_5.pdf

33. Пропозиції до політики щодо реформування сфери кібербезпеки в Україні Матеріал для обговорення [Електронний ресурс]. — Режим доступу : https://docplayer.net/73151177-Propoziciyi-do-politiki-shchodo-reformuvannya-sferi-kiberbezpeki-v-ukrayini-material-dlya-obgovorennya.html
34. Пфо О.М. Основні поняття і класифікація кіберзлочинності [Електронний ресурс]. — Режим доступу : http://dspace.kntu.kr.ua/jspui/bitstream/123456789/5119/1/AUConferenceCyberSecurity_November2016_p33.pdf
35. Становлення світового інформаційного простору [Електронний ресурс]. — Режим доступу : http://studall.org/all2-79388.html
36. Юдін О.К., Богуш М.В. Інформаційна безпека держави [Електронний ресурс]. — Режим доступу : https://studfiles.net/preview/5376129/page:99/