Міністерство освіти і науки України
Київський Національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ПОЯСНЮВАЛЬНА ЗАПИСКА
Дипломної роботи

магістра
(назва освітньо-кваліфікаційного рівня)

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

спеціальність *125 Кібербезпека*
(код і назва спеціальності)

освітній рівень ***магістр***
(назва освітнього рівня)

кваліфікація
(код і назва кваліфікації)

на тему: *Система реагування на загрози кібербезпеки*

Виконавець: студент *2* **курсу, групи** ***КБм-21***

Палагейченко Данило Сергійович
(підпис) (прізвище ім'я по-батькові)

	Прізвище, ініціали	Оцінка	Підпис
Науковий керівник	*Бучик С. С.*		
Рецензент	*Сайко В. Г.*		
Нормоконтроль			

Київ
2021

Міністерство освіти і науки України
Київський Національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри
кібербезпеки та захисту інформації
_____ Лукова-Чуйко Н.В.
«_____»_____20___року

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

студенту *КБм-21* (група) *Палагейченко Данило Сергійович* (прізвище ім'я по-батькові)

Тема дипломного роботи *Система реагування на загрози кібербезпеки*

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол №_____ від _____

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень *Процес створення системи реагування на загрози кібербезпеки*

Предмет досліджень *Елементи інформаційно-аналітичної системи реагування на загрози кібербезпеки*

Мета *Удосконалити існуючу систему реагування на загрози кібербезпеки*

Вихідні дані для проведення роботи *Існуюча система реагування на загрози кібербезпеки в Україні, сучасне законодавство України в сфері кібербезпеки, міжнародні договори України в сфері інформаційної Безпеки*

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна *удосконалення реалізації системи забезпечення та реагування на загрози кібербезпеки за рахунок дієвого організаційно нормативного алгоритму там впровадження систем обміну інформаціє про каберзагрози*

Практична цінність *покращення сучасної системи реагування за загрози кібербезпеки*

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Отримання завдання	20.09.2020 – 19.10.2020
Збір матеріалів для дослідження	22.10.2020 – 14.01.2021
Розробка 1 розділу	15.01.2021 – 25.03.2021
Розробка 2 розділу	26.03.2021 – 02.04.2021
Розробка 3 розділу	03.04.2021 – 25.04.2021
Оформлення атестаційної роботи	26.04.2021 – 02.05.2021

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект *Зниження збитків через кіберзагрози*

Соціальний ефект *Покращення технологій забезпечення захисту інформації на національному рівні*

7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ _____
(підпис) (прізвище, ініціали)

Завдання прийняв до виконання _____ _____
(підпис) (прізвище, ініціали)

Дата видачі завдання: _____

Термін подання дипломної роботи до ЕК _____

РЕФЕРАТ

Пояснювальна записка: 93 с., 7 рис., 5 табл., 1 додаток, 39 джерел.

Об’єкт дослідження – процес створення системи реагування на загрози кібербезпеки.

Мета роботи – удосконалити існуючу систему реагування на загрози кібербезпеки.

Методи дослідження – методи аналізу, синтезу, порівняння.

У роботі досліджено сучасні системи реагування на кіберзагрози. Проведено аналіз систем реагування на кіберзагрози які реалізовані в зарубіжних країнах. Запропоновано алгоритми реагування на кіберзагрози. Розроблено комплекс рішень по вдосконаленню сучасної системи реагування на кіберзагрози.

Наукова новизна: удосконалення реалізації системи забезпечення та реагування на загрози кібербезпеки за рахунок дієвого організаційно нормативного алгоритму там впровадження систем обміну інформаціє про каберзагрози.

Актуальність теми: Кібератаки є серйозною загрозою національній безпеці та безпеки інфраструктури практично кожної окремої організації. Традиційно кіберзагрози є досі латентні та складні в їх оперативному виявлення а отже і в реагуванні на них. Тому система реагування на кіберінциденти є дуже актуальною, так як допомагає вчасно виявити та локалізувати наслідки кіберзагрози.

Ключові слова: безпека інформації, інформаційна безпека, та кібербезпека, система забезпечення суб’єктів реагування на кіберзагрози

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ІБ	–	Інформаційна система;
СЗІ	–	Система захисту інформації;
ПЗ	–	Програмне забезпечення
АСУ	–	Автоматизована система управління
ПК	–	Персональний комп’ютер
СБУ	–	Служба безпеки України
МОУ	–	Міністерство оборони України
НПУ	–	Національна поліція України
НБУ	–	Національний банк України
СЗР	–	Служби зовнішньої розвідки
ДССЗЗІУ	–	Державна служба спеціального зв’язку та захисту інформації України
РНБО	–	Ради національної безпеки і оборони України
НКЦК	–	Національний координаційний центр кібербезпеки
APT	–	Advanced Persistent Threat
DNS	–	Domain Name System
HTTP	–	HyperText Transfer Protocol
CPU	–	Central processing unit
SSL	–	Secure Sockets Layer
TLS	–	Transport layer security
OS	–	Operating system
SMB	–	Server Message Block
IPS	–	Intrusion Prevention System
REST	–	Representational State Transfer
API	–	Application programming interface
EPP –	–	Extensible Provisioning Protocol

MISP – Malware Information Sharing Platform

CISA – Агентство з питань кібербезпеки та безпеки інфраструктури США

NCPS – Національна система захисту кібербезпеки США

US-CERT – Команда підготовки США до комп'ютерних надзвичайних ситуацій

NCSD – Національне Управління кібербезпеки США

ЄС – Європейський Союз

ENISA – Агентство Європейського Союзу з питань мережевої та інформаційної безпеки

EFMS – Європейський форум для держав-членів

ЕСЗ – Комісією Європейського Центру з боротьби з кіберзлочинністю

ВСТУП

Актуальність теми: розвиток інформаційних технологій є надзвичайно важливою складовою сучасного суспільства. Зараз важко знайти сферу, у якій не застосовуються електронні носії. Відповідно й законодавство у цій сфері має відповідати сучасним вимогам суспільства. Україна, в умовах інтеграційних процесів, вже здійснила чимало кроків у впровадженні ефективної моделі захисту інформаційної безпеки держави. Це дає змогу в майбутньому віднайти нові переваги розвитку та гармонізації у багатьох галузях цієї сфери дослідження.

Стрімкий розвиток обсягу інформації, її оновлення та структурна складність є тими чинниками, що виявляють необхідність у використанні інтегрованих систем обміну інформацією. Адже, до початку 2014 року кількість користувачів Інтернет в Україні була 280 тисяч, а вже на сьогодні вона становить 21 600 000. Система регулювання кібератак має відповідати викликам суспільства та вносити відповідні зміни у свою діяльність, тому що Інтернет – це можливість активної комунікації для суспільства.

Зараз у нашій державі відбувається стрімка адаптація усіх сфер життя до світових інновацій, зокрема й активного використання електронних інформаційних систем задля полегшення роботи з діловодством, обміну даними у різних професійних галуззях та у приватному житті громадян. Зокрема, вже у 2021 році стали реальністю наступні дії: прирівнення цифрових паспортів до паперових і пластикових; автоматична реєстрація бізнесу; створення електронного лікарняного; ведення податкових онлайн послуг; зміна місця реєстрації онлайн. Проте, саме в карантинних умовах ми потребуємо найбільшої захищеності даних, адже практично усі сфери життя тільки за 2020-2021 роки, в період обмеженням умов пересування, стали максимально діджиталізованими.

В таких умовах особливого значення набуває пошук нових можливостей забезпечення безпеки держави з огляду на формування нового поля протиборства – кіберпростору. На сьогоднішній день кіберпростір, через певну новизну, все ще не

повністю нормативно врегульований на міжнародному рівні, тому спецоперації, що здійснюються в ньому військовими чи розвідувальними підрозділами, не підпадають під визначення „акту війни". Крім того, це призводить до трансформації державної політики більшості провідних держав в питанні контролю за власним інформаційним (кібер) простором та посиленні яскраво виражених обмежувальних тенденцій. Україна потребує створення адекватної системи безпеки у світі, що трансформується, де виклики національній безпеці все частіше набувають рис, відмінних від традиційних загроз. Активність з боку провідних держав світу у кіберпросторі, глибинні зміни відношення до внутрішньої інформаційної політики та формування потужних транснаціональних злочинних груп, що спеціалізуються на злочинах в кіберпросторі все це обумовлює необхідність виробленні рекомендацій щодо коротко – та довгострокових пріоритетів трансформації вітчизняного безпекового сектору з урахуванням вищезазначених трендів.

Мета і задачі дослідження:

Метою роботи є удосконалити існуючу систему реагування на загрози кібербезпеки.

Мета обумовлена вирішенням наступних задач:

- обґрунтувати поняття «загроза кібербезпеки» та визначити його особливості в умовах сьогодення;
- на підставі реалізованої практики іноземних держав, що успішно користуються перевагами реагування на кіберзагрози, систематизувати основні цілі їх впровадження на національному рівні;
- визначити основні аспекти та вимоги, що ставляться при виявленні та реагуванні на кіберінциденти;
- комплексно дослідити поняття «система суб'єктів забезпечення реагування на кіберзагрози», зокрема проблемні питання у реалізації цієї системи та шляхи їх вирішення.

Об'єктом дослідження є процес створення системи реагування на загрози кібербезпеки.

Методи дослідження: бзисом дослідницької методології визначена сукупність методів сучасної теорії пізнання, заснованих на філософії діалектичного розвитку загальнолюдських цінностей, із використанням таких принципів наукового мислення, як індукція та дедукція, аналіз і систематизація, порівняння та спостереження. У дослідженні використовувались універсальні загальнонаукові методи та спеціальні методи; метод системного аналізу правових норм, використовувався зокрема в процесі порівняння загальних та спеціальних норм, що регулюють питання із процесів діяльності системи суб'єктів забезпечення реагування на кіберзагрози, а саме шляхи координуванн, створення, функціонування та реалізації відповідної національної системи (1.1., 1.2., 1.3., 2.1); комперативний метод, що дозволив дослідити особливості впровадження системи реагування на кіберзагрози на міжнародному рівні, тобто у країнах Західної Європи та США (розділ 3); порівняльно-правовий метод, застосовувався в процесі порівняння міжнародно-правових, конституційних, галузевих норм, завдяки якому стало можливим внесення конкретних пропозицій щодо вдосконалення українського законодавства у цій сфері (розділ 3); статичний метод, його використання забезпечило обґрунтування теоретичних положень роботи з статистичною інформацією; історико-правовий метод, що дав змогу розглянути етапи становлення в нашій державі елементів забезпечення системи реагування на кіберзагрози, а також діяльність суб'єтів системи у цій сфері (підрозділ 1.2., 1.3); соціологічний метод, використовувався для забезпечення зібрання відповідних даних з аналізу, пов'язаних зі статистичними показниками (підрозділ 1.2). Звернення до зазначених методів обумовлене специфікою і характером магістерської роботи. Усі методи використовувались в роботі у взаємодії і взаємозалежності , що забезпечило переконливість, достовірність, всебічність та об'єктивність стосовно результатів дослідження.

Таким чином варто приділити особливу увагу структурі магістерської роботи. Робота складається з 3 розділів. У першому розділі «Основні засади забезпечення кібербезпеки та система реагування на кіберінциденти», розкриваються поняття «кіберзагрози» (види та особливості), а також «система забезпечення реагування на

кіберінциденти» (структура системи, координація повноважень суб'єктів та її недосконаліть); розкривається питання нормативного врегулювання даної сфери відносин. За своїм змістом перший розділ є вступним. Другий розділ «Удосконалення вітчизняної системи виявлення та реагування на кіберзагрози пропозиції», складається з трьох підрозділів. Саме в ньому піднімаються актуальні проблеми та шляхи їх вирішення. Розробляються вирішення наступних питань: системи обміну інформацією; нормативно-організаційних заходів координування суб'єктів забезпечення кіберпезпеки, міжнародної співпраці в сфері обміну інформації щодо кіберінидентів. У третьому розділі «Пропозиції щодо покращення української системи реагування на кіберзагрози та перспективи її ефективності на основі іноземного досвіду», описується та порівнюється система забезпечення реагування на кіберзагрози у передових країнах світу – тобто систематизується досвід застосування на практиці цього поняття. Розділ складається з двох підрозділів. Усі розділи між собою пов'язані.

Нормативну основу роботи склали норми Конституції та законів України, Укази Президента України та постанови КМУ (зокрема особливу увагу варто приділити саме Указам Президента), міжнародно-правові акти, згода на обов'язковість яких надана Верховною Радою, документи Ради Європи.

Теоретичним фундаментом магістерської роботи стали праці і дослідження науковців даної сфери розгляду. Так, Г. А. Піскорська та Н. Л. Яковенко, І. В. Діордіц, І. В. Арістова, І. Р. Березовська, О. П. Дзьобаня, Р. А. Калюжний та інші. Ці дослідження здебільшого зосереджені на сфері правового регулювання та формування системи інформаційної безпеки України. З урахуванням відносної сучасності теми роботи, важливе значення мали праці (наукові статті) студентів вишів, аспірантів тощо.

Наукова новизна визначається тим, що дана робота є однією з перших вітчизняних досліджень організаційно-правових основ впровадження та особливостей реалізації системи суб'єктів забезпечення реагування на кіберзагрози. На підставі проведеного дослідження обґрунтовано низку нових теоретичних та

практичних положень, що конкретизують наукову новизну отриманих результатів. Зокрема:

- доведено, що необхідна координація та структуризація повноважень суб’єктів забезпечення;
- визначено передумови для активної реалізації взаємодії між вищевказаними суб’єктами.
- Удосконалено:
- Теоретичні підходи щодо здійснення ефективної системи реагувань на кіберзагрози;
- Обґрунтування наукової позиції стосовно порівняння західно-європейського та українського методу у сфері протидії кіберзагрозам;

В умовах стрімкого розвитку впровадження новітніх технологій у всі суспільні сфери, актуальною є оцінка його дієвості. Відповідно стає потрібним проведення досліджень з питань реалізації системи реагування на кіберзагрози, здійснити які можливо тільки урахувавши практичні здобутки як України, так і інших передових держав у цій сфері.

РОЗДІЛ 1
ОСНОВНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ТА СИСТЕМА РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ

1.1 Особливості поняття «загроза кібербезпеки»

Формування й ефективна реалізація кібербезпекової політики, в рамках якої розробляється комплекс заходів щодо прогнозування та протидії кіберзагрозам, є необхідною умовою розвитку суспільства. В умовах глобалізації інформаційних процесів, їх інтеграції в різні сфери суспільного життя, керівництво провідних держав світу приділяє посилену увагу створенню й удосконаленню ефективних систем захисту критичної інфраструктури від зовнішніх і внутрішніх загроз кібернетичного характеру.

Важливості питань інформаційної безпеки нашої країни і формуванню механізму міжнародної кібербезпеки приділяли увагу численні науковці. Так, Г. А. Піскорська та Н. Л. Яковенко у своїй роботі [1] дійшли висновку, що забезпечення міжнародної безпеки в інформаційній сфері та у світовому кіберпросторі вимагає не лише зусиль окремих країн світу, а й розроблення та реалізації максимально ефективних міжнародних інструментів. І. В. Діордіца [2] пропонує для розроблення дієвого механізму протидії кіберзагрозам в Україні взяти за приклад наявну практику зарубіжних країн і міжнародної спільноти та привести її у відповідність до українських реалій. Аналіз останніх досліджень і публікацій свідчить про те, що певні аспекти вітчизняних проблем інформаційної безпеки досліджувались у наукових працях І. В. Арістова, І. Р. Березовської, О. П. Дзьобаня, Р. А. Калюжного, Б. А. Кормича, В. А. Ліпкана, А. І. Марущака, В. С. Цимбалюка, О. К. Юдіна та інших. Проте ці дослідження здебільшого зосереджені на сфері правового регулювання та формування системи інформаційної безпеки України.

Нині побудова дієвої системи кібернетичної безпеки України в умовах гібридної війни вимагає чіткого аналізу вже реалізованих заходів у сфері захисту

комп'ютерних і телекомунікаційних мереж від кібератак та визначення потрібних для реалізації заходів щодо створення умов для безпечного функціонування кіберпростору задля випереджального реагування на динамічні зміни, що відбуваються у кіберпросторі.

У багатьох провідних країнах світу вже сформовані загальнодержавні системи кібернетичної безпеки як найбільш оптимальні організаційні структури, що здатні в короткий проміжок часу акумулювати сили та засоби компетентних органів державної влади для протидії кіберзагрозам. В Україні також відбувається процес формування системи кібернетичної безпеки. Як складник такої системи варто розглядати єдину загальнодержавну систему протидії кіберзлочинності, пропозиції щодо створення якої ще у 2011 році доручалося розробити Кабінету Міністрів України за участю Служби безпеки України. На загал інституційний ландшафт кібербезпеки можна позначити через організаційно-структурні й нормативно-правові зміни. До структурних змін належить створення Міністерства інформаційної політики України, у складі Національної поліції – кіберполіції, Національного координаційного центру кібербезпеки, Ради з питань комунікацій – консультативно-дорадчого органу Кабінету Міністрів України, Об'єднаного інформаційно-аналітичного центру «Єдина Країна» тощо.

Кіберзагрози в сучасному суспільстві набирають значного масштабу. Відтепер успішна атака хакерів може знеструмити область або країну, призвести до пограбування банку чи знищити успішну організацію. Наприклад, за різними оцінками, за 2015 рік із рахунків підприємств України зникло близько 100 млн грн. [2].

Найсвіжіша статистика свідчить, що кіберзлочинці націлені на малий бізнес, щоб отримати несанкціонований доступ до даних, які вони можуть продавати в DarkNet. Хакерські атаки з використанням знань соціальної інженерії зосереджені на слабких місцях у системах, мережах, програмному забезпеченні, щоб отримати доступ до необхідних джерел інформації.

Кібератаки стають безперечною загрозою сьогодення. Звіт 2019 Data Breach Investigation Report [3] виділив декілька тенденцій:

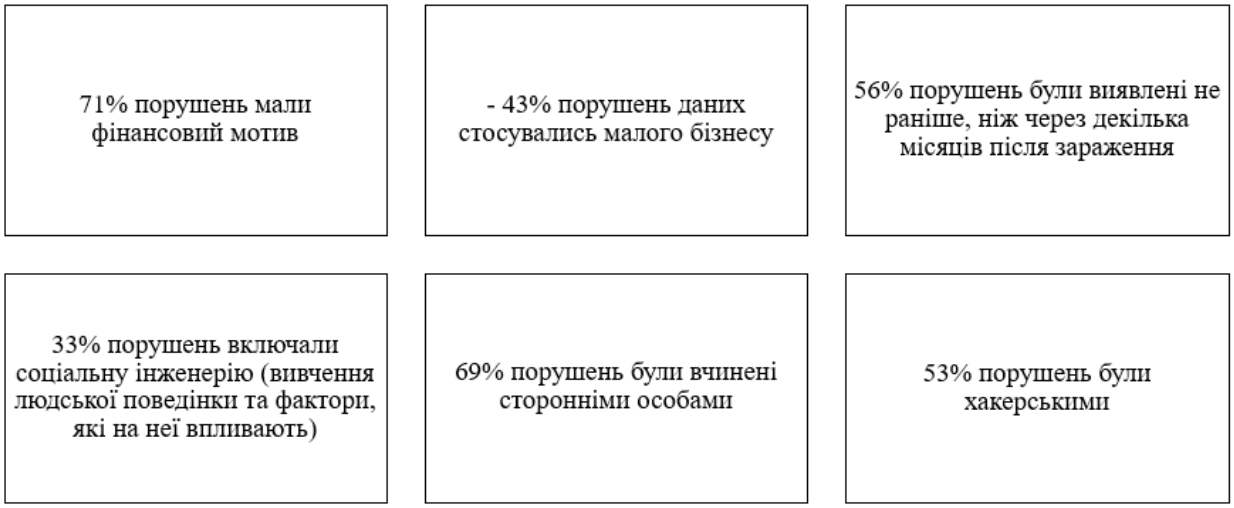

Рисунок 1.1 – Відсоткове співвідношення кіберзлочинів

В останні роки численні гучні кібератаки призвели до викриття конфіденційних даних [4]. Наприклад, порушення 2017 року Equifax мало вплив на особисті дані приблизно 143 мільйонів споживачів, включаючи дати народження, адреси та номери соціального страхування. У 2018 році Marriott International повідомила, що хакери отримали доступ до його серверів і викрали дані приблизно 500 мільйонів клієнтів. В обох випадках загроза кібербезпеці була спровокована тим, що організація не впровадила, не протестувала та не перевірила технічні засоби захисту, такі як шифрування, автентифікація тощо. Кіберзловмисники можуть використовувати конфіденційні дані особи чи компанії для викрадення інформації або отримання доступу до їх фінансових рахунків.

На противагу цьому, законодавство України регулює поняття «кіберзагроза». Так у п.6, ст. 1 ЗУ «Про основні засади забезпечення кібербезпеки України» [5] вказано, що кіберзагроза – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об’єктів.

На основі прецедентних проявів кіберзагроз, можна виокремити, що вищевказані можливі негативні явища і чинники, мають на меті порушити доступність, повноту, цілісність, достовірність, автентичність режиму доступу до інформації, яка циркулює у різних проявах галузей інформаційної інфраструктури суспільства. Зокрема, у наш час ця загроза викликана прогалинами в регулюванні та відстеженні потенційних проблем у безпеці країни. При цьому кіберзагроза є явищем міжнаціональним, адже від її проявів поки ще немає чітких випрацюваних роками чинників протидії, зважаючи на її швидкість розповсюдження та дестабілізацію в суспільстві. Кіберзагрози також стосуються кібератаки, метою якої є отримання несанкціонованого доступу, пошкодження або викрадення активів інформаційних технологій, комп'ютерної мережі, інтелектуальної власності або будь-якої іншої форми конфіденційних даних. Кіберзагрози можуть надходити зсередини організації довіреними користувачами або з віддалених місць невідомими особами.

У цілому, загроза кібербезпеки – це зловмисна дія, яка має на меті пошкодити дані, викрасти дані або змінити цифрове життя. Кіберзагрози включають комп'ютерні віруси, знешкодження даних , атаки на відмову в обслуговуванні. Варто виділити дії зловмисника, що вказують на загрозу кібербезпеці, вони можуть бути наступними: читання файлів інших користувачів; перенаправляння запитів, зроблених до веб-сервера, на власний веб-сервер; модифікування бази даних; віддалений запуск команди на сервері.

Кіберзагрози походять від різноманітних факторів, місць, людей та контексту. Зокрема, за цими ознаками можна виділити наступних суб'єктів здійснення кіберзагроз:

1) Ворожі держави: національні програми кібервійн забезпечують кіберзагрози, що виникають, починаючи від пропаганди, псування веб-сайтів, шпигунства, порушення роботи ключової інфраструктури до загибелі людей. Програми, що фінансуються урядом, стають все більш досконалими і представляють найбільші загрози в порівнянні з іншими суб'єктами загроз. Їх можливості можуть завдати широкого, довгострокового збитку національній безпеці багатьох країн.

2) Терористичні групи: терористичні групи все частіше використовують кібератаки для нанесення шкоди національним інтересам. Цілком ймовірно, що терористичні угрупування представлятимуть значні кіберзагрози, оскільки до їхніх лав приєднуються більш технічно-компетентні покоління.

3) Корпоративні шпигуни та організована злочинність: вони становлять ризик через свою здатність вести промислове шпигунство з метою викрадення комерційної таємниці або масштабних крадіжок грошей. Як правило, ці суб'єкти зацікавлені в діяльності, заснованій на прибутку, а також на порушенні здатності бізнесу отримувати прибуток, атакуючи ключову інфраструктуру конкурентів, викрадаючи комерційну таємницю або отримуючи доступ та матеріали для шантажу.

4) Хактивісти: більшість хактивістських груп заклопотані поширенням пропаганди, а не пошкодженням інфраструктури або порушенням роботи служб. Їх метою є підтримка політичного порядку.

5) Особи, що мають індивідуальний інтерес: саме вони є основним джерелом кіберзлочинів. інсайдерам часто не потрібен високий ступінь комп'ютерних знань для викриття конфіденційних даних, оскільки вони можуть бути уповноважені на доступ до даних. Інсайдерські загрози також включають сторонні постачальники та співробітники, які можуть випадково ввести шкідливе програмне забезпечення в системи.

6) Хакери: зловмисники можуть скористатися експлойтом нульового дня, щоб отримати несанкціонований доступ до даних. Раніше це вимагало високого рівня майстерності. Сьогодні автоматизовані сценарії атак та протоколи можна завантажувати з Інтернету, роблячи складні атаки простими.

7) Стихійні лиха: стихійні лиха представляють кіберзагрозу, оскільки вони можуть порушити ключову інфраструктуру так само, як це може зробити кібератака.

8) Випадкові дії уповноважених користувачів: уповноважений користувач може забути правильно налаштувати безпеку на носії інформації, спричиняючи можливий витік даних. Деякі з найбільших порушень даних були спричинені поганою конфігурацією, а не хакерами або незадоволеними інсайдерами.

9) Шкідливе програмне забезпечення для мобільних додатків: мобільні пристрої вразливі до атак шкідливого програмного забезпечення, як і інше обчислювальне обладнання. Зловмисники можуть вбудовувати шкідливе програмне забезпечення у завантажувані програми, мобільні веб-сайти або фішинг-листи та текстові повідомлення. Після злому мобільний пристрій може надати зловмиснику доступ до особистої інформації, даних про місцезнаходження, фінансових рахунків тощо.

Отож, аналізуючи види потенційних загроз кібербезпеки можна виділити елементи кібербезпеки:

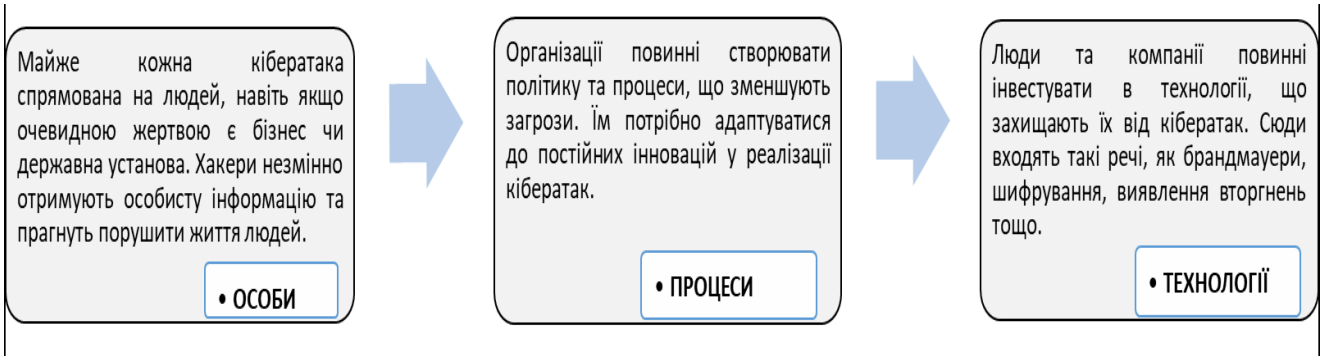

Рисунок 1.2 – Основні елементи кібербезпеки

Також, поміж переваг використання інноваційних технологій, трапляються і суттєві недоліки систем передачі інформації. Так, у ході досліджень стало відомо, що порушення захисту комп'ютерних програм, за даними сайту ComputerSecurityInstitute (Сан-Франциско, штат Каліфорнія, США) може здійснюватись з таких підстав: несанкціонований доступ – 2%, укорінення вірусів – 3%, технічні відмови апаратури мережі – 20%, цілеспрямовані дії персоналу – 20%, помилки персоналу (у зв'язку з недостатньою кваліфікацією) – 55% [6].

Кіберзагрози ніколи не бувають статичними. Щороку створюються мільйони.

У зв'язку з розвитком загроз кібербезпеки, та виходячи з їх суб'єктів, необхідно виділити основні завдання для відповідних органів та структур у цій сфері:

– Захищати суверенітет кіберпростору

– Захищати національну безпеку
– Захищати інформаційну інфраструктуру
– Створити «безпечну» інтернет-культуру
– Боротись з кіберзлочинністю, шпигунством та тероризмом
– Посилити правову базу кібербезпеки
– Підвищити можливості захисту кіберпростору
– Покращити міжнародне співробітництво

З огляду діяльність, що здійснюється у віртуальному просторі, легко зливається з фізичним світом. Кібер-зловмисники можуть порушити такі важливі інфраструктури, як фінансові системи та системи управління повітряним рухом, створюючи наслідки, що схожі на теракти; розкриття державної та військової таємниці; вербування злочинців та інших осіб для здійснення фізичної терористичної діяльності. З огляду на зростаючі загрози, кібер-готовність систем безпеки постійно випробовується. Хоча системи безпеки все дорожчі, запуск кібератак є відносно економічним.

Основоположними факторами в боротьбі із кібергазгрозами мають бути наступні елементи дії:

запобігти – здійснення доступу до даних та підключення до технологій ведеться виключно відповідним персоналом організації;

виявити – віднаходження несправності та її виправлення має реалізуватись якнайшвидше, навіть якщо вказівки на злочинні дії несуттєві;

обмежити – покращувати та оновлювати систему виявлення загроз, навіть коли на її утримання потрібні великі фінансові затрати;

відновити – через злагоджену систему підготовки до кіберзагроз відновлення інформації реалізується ефективніше та із мінімальними затратами часу.

Збиток, заподіяний кіберзловмисниками, може бути не легко впізнаним, а в деяких випадках може залишитися непоміченим. Відстежити кібератаку непросто, оскільки Інтернет не має географічних кордонів і не має юрисдикцій. Не існує міжнародних законів / угод, які могли б допомогти у відстеженні кібератак.

Із Рішення Ради РНБО «Про Стратегію кібербезпеки України», загрози кібербезпеці актуалізуються через дію таких чинників, зокрема, як:

невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам;

недостатній рівень захищеності критичної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, від кіберзагроз;

безсистемність заходів кіберзахисту критичної інфраструктури;

недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інфраструктури та державних електронних інформаційних ресурсів;

недостатня ефективність суб'єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру;

недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки.

Системи виявлення мережевих вторгнень і виявлення ознак кібератак на інформаційні системи вже давно застосовуються як один з необхідних рубежів оборони інформаційних систем на міжнародному рівні. Розробниками систем захисту інформації та консультантами в цій галузі активно застосовуються такі поняття, як захист по периметру, стаціонарна і динамічний захист, стали з'являтися власні терміни, наприклад, проактивні засоби захисту.

1.2. Характеристика українського законодавства у сфері кібербезпеки та прогалини її застосування

З метою проведення коректних та ефективних заходів щодо відвернення кіберзагроз і ліквідації їх негативних наслідків, передусім необхідною є їх легітимація – вироблення та закріплення законодавчої дефініції задля уникнення порізненості під час застосування цієї категорії, а також колізії з іншими нормативними актами, визначення їх змісту, уніфікованості правозастосовної практики.

Україна зарекомендувала себе, як одна з передових держав на європейському рівні, яка здатна протистояти викликами інформаційно-технологічного прогресу, впроваджуючи низку спеціальних законодавчих та підзаконних актів задля покращеного регулювання цієї сфери. Здійснення та реалізація усіх нормативних актів потребує співпраці із сьогочасним суспільством.

Україна за часи незалежності набула власний досвід у сфері правового врегулювання та забезпечення питань пов’язаних з кібербезпекою та активно імплементувала міжнародний досвід, таким чином в сучасному законодавстві набули визначень ряд ключових понять та цілей які безпосередньо пов’язані с забезпеченням кібербезпеки в державі.

Так в сучасному законодавстві України набули визначення такі важливі поняття, як:

– кіберзагроза;
– кібератака;
– кіберзлочин;
– інформаційна безпека, тощо;

Розглянемо систему основних нормативних актів, що виділяють при визначенні кібербезпеки, врегулюють питання пов’язані з виникненням загроз кібербезпеки, кібератакам та кіберзагроз.

Таблиця 1.1 – Нормативне забезпечення що врегульовують питання кібербезпеки в Україні

Нормативне регулювання кіберзагроз в Україні			
Конституція України	**Закони України**	**Укази Президента**	**Ратифіковані міжнародні акти**
Ст.3 «Людина, її життя і здоров'я, честь і гідність, недоторканність і безпека…», Ст.17 «Захист суверенітету і територіальної цілісності України...», Ст.31 «Кожному гарантується таємниця листування…», Ст.32 «Не допускається збирання, зберігання, використання…», Ст.34 «Кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію…»	«Про інформацію», «Про національну безпеку України», «Про Національну програму інформатизації», «Про захист персональних даних», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основні засади забезпечення кібербезпеки», «Про електронний цифровий підпис», «Про електронні довірчі послуги»	Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України", Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України», Про Національний координаційний центр кібербезпеки	Конвенція про захист прав та основоположних свобод, Конвенція про захист осіб у зв'язку автоматизованою обробкою персональних даних, Конвенція про кіберзлочинність

Поняття інформаційні технології можна пов'язати із забезпеченням та реалізацією такого принципу як доступність. Адже за змістом ст. 1 Конституції, Україна є правовою державою, яка заснована на визнанні та реальному

забезпеченні прав та свобод людини і громадянина, дотриманні верховенства права, взаємній відповідальності людини та держави [7].

Відповідно до ст. 3 Конституції України: «Людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю. Права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави. Держава відповідає перед людиною за свою діяльність. Утвердження і забезпечення прав і свобод людини є головним обов'язком держави» [7]. Дане положення є одним з найбільш визначальних в українській системі права. Однією із складових найвищої соціальної цінності в цій нормі визначається саме безпека людини.

Відповідно до ч. 1 ст. 17 Конституції України: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу» [7]. У даному нормативному документі законодавець прямо вказав на важливість інформаційної безпеки саме держави, поставивши її в один ряд з економічною безпекою. Тобто можна констатувати, що сфера інформаційної безпеки визнається надзвичайно важливою не тільки щодо приватних осіб, але і щодо цілої держави.

Рада Європи заклала правове підґрунтя для визнання країнами учасницями потреби в імплементуванні у своє законодавство норм, що регулюють не тільки основоположні права та свободи громадян, а й таку сферу діяльності як правове забезпечення інформаційних технологій. Тому, Рада Європи не тільки здійснює діяльність, яка спрямована на вирішення порушених прав та свобод, а й виконує роботу по укомплектуванні єдиної правозастосовної практики для держав – учасниць організації. Її мета буде досягнута під час реалізації зусиль при розгляді питань, що мають загальний інтерес у кіберпросторі. Забезпечення дієвості верховенства права є однією з актуальних та нагальних потреб юридичної науки, саме тому вона повинна мати не лише теоретичний, а й практичний характер застосування. Адже, Україна, як учасниця Ради Європи, має певні обов'язки, зокрема й визнавати принцип верховенства права. У статті 6 Договору про

Європейський Союз наголошується, що основоположними принципами Союзу є демократія, панування прав людини та засадничих свобод, зокрема й верховенство права [8].

Наступним міжнародним актом, який необхідно проаналізувати є Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних. Даний нормативний акт був прийнятий у 1981 році і ратифікований Україною в 2010 році. Незважаючи на те, що цей нормативний акт було прийнято досить давно, він не втрачає своєї актуальності та закріплює в собі надважливі положення в сфері інформаційної безпеки. Відповідно до статті 2, термін "персональні дані" означає будь-яку інформацію, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною (далі – суб'єкт даних). Термін "автоматизована обробка" включає такі операції, що здійснюються повністю або частково за допомогою автоматизованих засобів: зберігання даних, виконання логічних та (або) арифметичних операцій із цими даними, їхню зміну, знищення, вибірку або поширення» [9].

Конвенція про Кіберзлочинність підрозділяє злочини в кіберпросторі на 4 групи. У першу групу злочинів, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних даних і систем входять: незаконний доступ (ст. 2), незаконне перехоплення (ст. 3), дія на комп'ютерні дані (ст. 4) або на системи (ст. 5). Також до цієї групи злочинів входить протизаконне використання спеціальних технічних пристроїв (ст. 6).

Відповідно, основоположною історичною передумовою для системи реагування на загрози кібербезпеки, одразу після отримання Україною незалежності, стало прийняття таких нормативних актів як: Закон України «Про інформацію» у 1992 році та Закон України «Про Національну програму інформатизації» у 1998 році. Відповідно до ст. 3 Закону України «Про інформацію» [10], одним з основних напрямків державної інформаційної політики визначались створення умов для формування в Україні інформаційного суспільства, забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень, а також створення інформаційних систем і мереж інформації, розвиток електронного

урядування та постійне оновлення забезпечення та зберігання національних інформаційних ресурсів.

В 1994 році був прийнятий ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах» [11]. Цей закон зокрема надає легальні визначення для таких понять як «інформаційна система» та «інформаційно-телекомунікаційна система. Відповідно до ст. 1: «інформаційна (автоматизована) система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;» «інформаційно-телекомунікаційна система – сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле». Також потрібно зазначити, що цим законом безпосередньо було закріплено обов'язок власника системи захищати дані, які в ній обробляються.

Ще одним надважливим законом в цій сфері є ЗУ «Про захист персональних даних» [12], що був прийнятий у 2010 році. Даний закон регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних. Також цим нормативним актом встановлено, що саме необхідно розуміти під персональними даними.

Протягом довгого періоду часу в Україні діяв закон «Про основи національної безпеки» [13], який був прийнятий у 2003 році. 9 травня 2018 року зазначений закон втратив чинність, а набув чинності ЗУ «Про національну безпеку України» [14]. Фактично, прийняттям цього закону законодавець підкреслив надважливе значення інформаційної безпеки в аспекті захисту інформаційного середовища та закріпив фундаментальні аспекти регулювання цієї сфери. Варто зазначити про наявність у ньому таких визначень «кібербезпека» та «кіберзахист».

Важливе значення для захисту інформації в електронному вигляді має Закон "Про електронний цифровий підпис" у 2003 році, адже це було підставою для здійснення гармонізації українського законодавства до європейського. Цей Закон додав у наше законодавство такі поняття як «електронний підпис» та «електронний

цифровий підпис». Після цього здійснилось активне введення цієї легітимної можливості засвідчення документів. І хоча підпис не був захищений криптографічно, проте став досить вживаним та набув широке адміністративне прийняття. 7 листопада 2018 в Україні введений в дію новий Закон «Про електронні довірчі послуги» [15]. Може здатись, що новий Закон був прийнятий лише в силу змін Європейського законодавства в цій сфері, адже попередній Закон «Про електронний цифровий підпис» мав схожість у характері сфери регулювання. Проте наявні й нові аспекти у його застосуванні, зокрема вони пов'язані з тим, що поширення електронного підпису набуває широкого застосування у різних сферах суспільного життя, а тому ризик по захисту та безпеці інформації є надзвичайно актуальним питанням. До прикладу, торговельна діяльність стає все більш залежною від Інтернету, тому спостерігається дистанційне спілкування між її суб'єктами. Виникає цілком очікувана необхідність у застосуванні нових методів для ідентифікації особи. Перевагами використання саме електронного підпису є зокрема те, що він дає змогу повністю оцифрувати бізнес-процеси.

Чи не найважливішим регулятивним актом у даній сфері є закон «Про основні засади забезпечення кібербезпеки України» від 09.05.2018 р. Він визначає основні об'єкти кіберзахисту, які створюють критичну інфраструктуру країни, нормативно закріплює понятійний апарат у сфері кібербезпеки на найвищому рівні, регламентує принципи забезпечення кібербезпеки та національну систему кібербезпеки, окреслює державно-приватну взаємодію у сфері кібербезпеки та встановлює відповідальність за порушення законодавства у цій сфері і контроль за законністю заходів щодо забезпечення кібербезпеки України.

Велике значення серед нормативних актів цієї сфери має також постанова КМУ «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» від 19.06.2019р., у якій описано що таке система інформаційної безпеки. На жаль це питання стосується саме об'єктів інфраструктури, проте в подальшому це поняття може стати фундаментом для створення повноцінного комплексного визначення для роз'яснення системи кіберзагроз.

Надважливу роль в забезпеченні інформаційної безпеки держави відіграє Рада національної безпеки та оборони. Одразу слід згадати про указ Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». Встановлено, що Доктрина інформаційної безпеки України (далі - Доктрина) визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері. Метою Доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни. Доктрина базується на принципах додержання прав і свобод людини і громадянина, поваги до гідності особи, захисту її законних інтересів, а також законних інтересів суспільства та держави, забезпечення суверенітету і територіальної цілісності України. Зазначений нормативний акт є помітним кроком вперед в діяльності держави щодо протидії російській інформаційній агресії. І якщо порівняти його зміст із попередньою Доктриною інформаційної безпеки України від 2009 року, то різниця справді відчутна [16]. Головним досягненням є спроба визначити та гармонізувати повноваження органів влади, силових структур щодо їхньої діяльності із захисту інтересів суспільства і держави в інформаційній сфері, національного інформаційного простору.

Потрібно констатувати, що яким би чітким не було законодавство, порушення в цій сфері є досить розповсюдженими, в тому числі кримінальні правопорушення. Розвиток сучасних інформаційних технологій, удосконалення виробництва і розширення сфери застосування новітніх інформаційно-комунікаційних технологій дали можливість зародженню специфічного, складного виду злочинних діянь, де комп'ютерна техніка та електронна інформація є об'єктом протиправного посягання, або ж – знаряддям вчинення злочину. Поряд з позитивними здобутками інформатизація супроводжується побічним – негативним явищем криміногенного характеру, до якого відносять злочини у сфері електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж або ж «комп'ютерну злочинність». За останні 10-15 років поняття «комп'ютерна злочинність» трансформувалось у термін

«кіберзлочинність» – поняття, яке охоплює власне комп'ютерну злочинність та інші протиправні діяння, де комп'ютер є знаряддям або способом вчинення злочину проти власності, авторських прав, громадської безпеки, моралі тощо. Відтак, кіберзлочин можна розуміти будь-який злочин, який може вчинятися за допомогою комп'ютерної системи або мережі, в рамках комп'ютерної системи або мережі чи проти інформації в комп'ютерній системі або мережі. В принципі, таке визначення охоплює будь-який злочин, який може бути скоєно в електронному середовищі.

З метою посилення стійкості критичної національної інфраструктури з кібербезпеки український Уряд регулярно бере участь у міжнародному співробітництві з реагування на кіберінциденти, маючи доступ до передового міжнародного досвіду та сучасних алгоритмів реагування на кіберінциденти. Саме розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, участь у заходах зі зміцнення довіри у кіберпросторі, які проводяться під егідою ОБСЄ, та поглиблення співпраці України з ЄС та НАТО посилюють спроможності України у сфері кібербезпеки у відповідності до національних інтересів.

Незважаючи на те, що за останні роки відбулася велика кількість позитивних перетворень у сфері інформаційної безпеки, наявна досить велика кількість проблемних моментів, які потребують дослідження. Треба констатувати, що певна частина законодавства на даний момент не відповідає реаліям та не враховує сучасних тенденцій, які насправді і повинні визначати політику держави у цій сфері. Відповідно до наведеної статистики, кількість злочинів у сфері використання електронно обчислювальних машин за останні роки значно зросла. У 2017 році було вчинено в 4 рази більше кіберзлочинів, ніж в 2015. Але це лише офіційна статистика. Варто зазначити, що подібні злочини відрізняються високою латентністю, тобто більшість таких злочинів навіть не обліковуються органами досудового розслідування. Проблеми у сфері притягнення особи до відповідальності за кіберзлочини можна умовно поділити на проблеми які безпосередньо витікають з недосконалості законодавства та проблеми більш практичні, які пов'язані з неефективною роботою органів досудового розслідування, судів та експертних установ. Розглядаючи проблеми законодавства, перш за все слід вказати, що деякі

кримінально-правові норми просто неможливо застосувати на практиці, тобто можливості притягнути особу до кримінальної відповідальності за ними фактично немає.

Серед наявних проблем найбільш гострою та актуальною є притягнення осіб до кримінальної відповідальності за вчинення так званих «кіберзлочинів». Для того щоб зрозуміти наскільки поширеними нині є кіберзлочини, необхідно звернутися до офіційної статистики Генеральної прокуратури щодо зареєстрованих кримінальних проваджень за останні три роки та проаналізувати її. У 2015 році органами досудового розслідування було зареєстровано 598 кримінальних проваджень, які були кваліфіковані за статтями 16 розділу Особливої частини ККУ. З них лише у 263 провадженнях була вручена підозра і тільки 128 обвинувальних актів було передано до суду [17]. Відповідно до даних, що містяться у Єдиному державному реєстрі судових рішень, з цих 128 справ вироки винесені лише по 36 з них. Всі ці 36 вироків є обвинувальними [18].

Усі ці факти в сукупності утворили дуже сприятливу ситуацію для розвитку кіберзлочинності. Також необхідно наголосити на тому факті, що працівники органів досудового розслідування дуже часто не мають достатньої кваліфікації для проведення ефективного розслідування таких злочинів. Для того, щоб провести досудове розслідування по таким справам, працівники поліції мають володіти спеціальними знаннями, тобто чітко розуміти алгоритм процесу доказування по таких справах та усвідомлювати специфіку відповідних злочинів. Нажаль, на сьогоднішній день можна констатувати, що більшість слідчих не володіють необхідною кваліфікацією.

Кіберзагрози неможливо обмежити якоюсь однією сферою, це вимагає від усіх зацікавлених сторін всебічної обізнаності з факторами ризику, умінь і навиків для їхнього вирішення та відповідних заходів для запобігання кібератак ще до їх початку.

Адже, інформаційні технології змінюють структуру відносин у суспільстві. І хоча зрозуміло, що законодавчу основу запобіганню кібератакам Україна має, проте

реалізувати цей потенціал вдасться лише гармонійним поєднанням організаційно-політичних чинників.

1.3 Національна система реагування на кіберзагрози та її проблематика

Система забезпечення інформаційної безпеки України (далі – СЗІБ) створюється і розвивається відповідно до Конституції України та інших нормативно-правових актів, що регулюють суспільні відносини в інформаційній сфері. Основу даної системи складають органи, сили та засоби забезпечення інформаційної безпеки, які вживають систему адміністративно-правових, інформаційно-аналітичних, організаційно-управлінських, та інших заходів, спрямованих на забезпечення стійкого функціонування системи державного управління.

Національна система кібербезпеки має насамперед забезпечити взаємодію з питань кібербезпеки державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських об’єднань, а також підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об’єктів критичної інформаційної інфраструктури [19]

Головне призначення цієї системи полягає у досягненні цілей національної безпеки в інформаційній сфері, а отже основною функцією даної системи є забезпечення збалансованого існування інтересів особи, суспільства і держави в інформаційній сфері.

Законодавець виділяє наступні основні складові системи кібербезпеки, що в першу чергу здійснюють реагування на загрози у кіберпросторі:

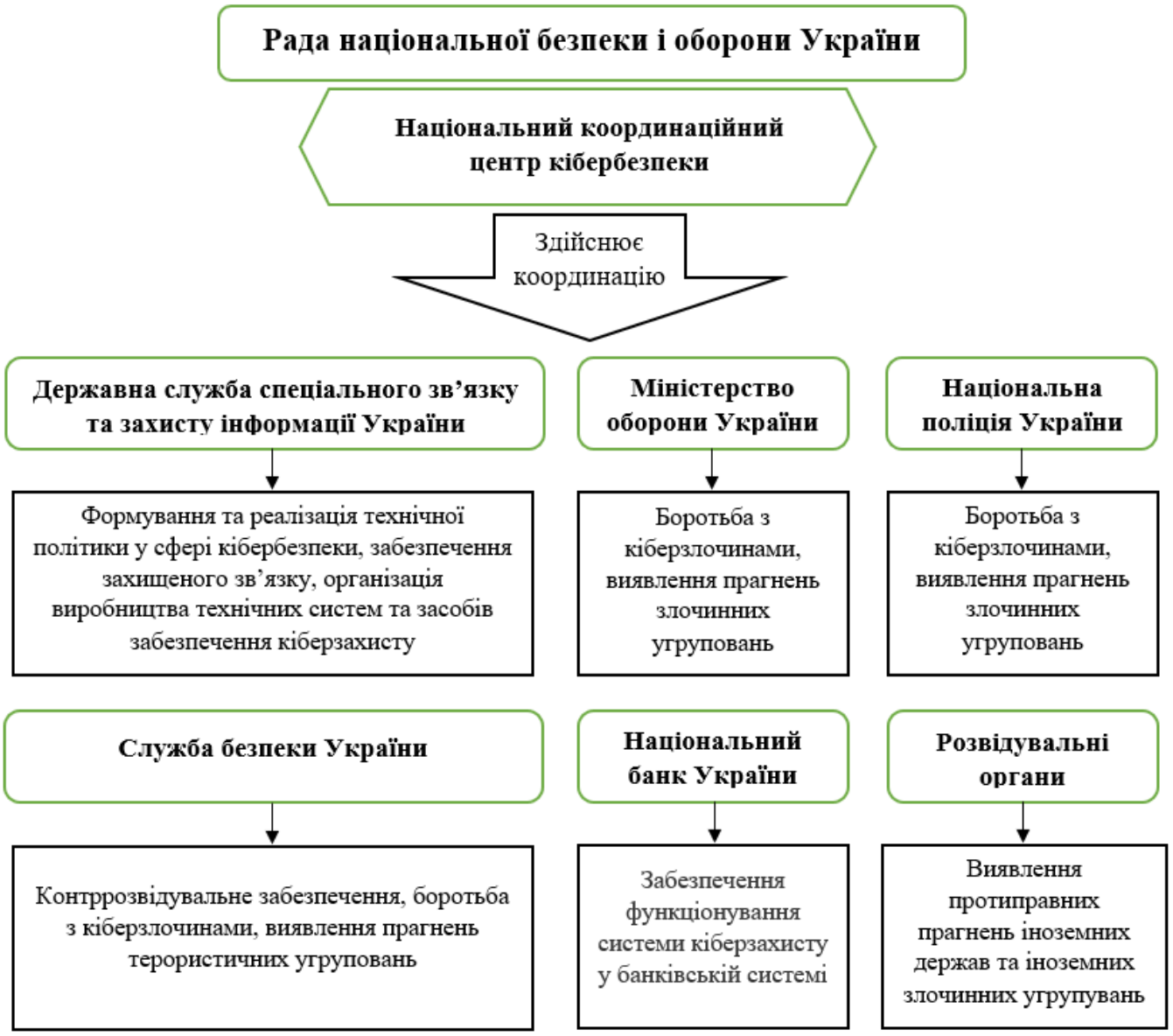

Рисунок 1.3 – Система забезпечення кібербезпеки

Основними завданнями такої системи є:

- виявлення і прогнозування дестабілізуючих факторів і інформацій них загроз життєво важливим інтересам особистості, суспільства та держави;
- здійснення комплексу оперативних і довготривалих заходів з їхнього попередження і усунення;
- створення і підтримання в готовності сил та засобів забезпечення інформаційної безпеки.

Для того, щоб зрозуміти специфіку роботи вказаних структур, необхідно розглянути детальніше їх завдання, функції та особливості.

Варто розпочати аналіз з чи не найважливішої структури, а саме з Ради національної безпеки і оборони України (далі – РНБО), адже відповідно до Конституції України, саме вона в встановленому законом порядку має здійснювати координацію та контроль діяльності суб'єктів сектору безпеки і оборони, які покликані забезпечувати кібербезпеку України.

Завданням РНБО є формування державної політики та координація суб'єктів забезпечення кібербезпеки.

Функціями Ради національної безпеки і оборони України [20] є:

1) внесення пропозицій Президентові України щодо реалізації засад внутрішньої і зовнішньої політики у сфері національної безпеки і оборони;

2) координація та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки і оборони у мирний час;

3) координація та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки і оборони в умовах воєнного або надзвичайного стану та при виникненні кризових ситуацій, що загрожують національній безпеці України.

У відповідності до специфіки завдань та функцій РНБО, було створено Національний координаційний центр кібербезпеки (далі – НКЦК), що в свою чергу керується Указом Президента «Про Національний координаційний центр кібербезпеки». Отож, саме до НКЦК мають надходити дані, пов'язані з можливими протиправними діями, що посягають на кібербезпеку держави, а центр в свою чергу має приймати як превентивних мір захисту на них, так і боротись із вже існуючими кіберінидентами. У силу своїх завдань, повноважень та функцій НКЦК має здійснювати аналіз стану кібербезпеки в державі, координацію суб'єктів системи кіберзагроз, прогнозування/виявлення потенційних кіберінцидентів тощо. Проте, на практиці виникає ряд невирішених питань імплементації передбачених у нормативних актах положень, зокрема щодо відсутності:

1) дієвої комунікації з суб'єктами системи забезпечення реагування на кібезагрози;

2) системної координації та алгоритму дій у виявленні кіберінидентів;

3) єдиного каналу поширення / передачі інформації між суб'єктами.

Також надзвичайно важливим суб'єктом забезпечення кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України (далі – ДССЗЗІУ), що відповідає за формування та реалізацію політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, захисту критичної інформаційної інфраструктури та контроль у цій сфері. Відповідно до компетенції служба також здійснює координацію діяльності інших суб'єктів кібербезпеки.

Завданням ДССЗЗІУ є формування та реалізація технічної політики у сфері кібербезпеки, забезпечення захищеного зв'язку, організація виробництва технічних систем та засобів забезпечення кіберзахисту.

Спеціалізовані структури ДССЗЗІУ щодо кіберзахисту є чи не найпершими у цій сфері. Їх мета – виділити їх досвід у виявленні потенційних кіберзагроз. Кіберпідсистема служби пройшла довгий шлях реформування за останнє двадцятиліття, наразі створено Державний центр кіберзахисту ДССЗЗІУ. Варто виділити останні напрацювання пов'язані з організаційно-технічною моделлю кіберзахисту, що є складовою національної системи кібербезпеки.

Служба безпеки України (далі – СБУ) – покликана попереджати, виявляти, припиняти та розкривати злочини проти миру і безпеки, що вчиняються в кіберпросторі.

Завданням СБУ у сфері забезпечення кібербезпеки є контррозвідувальне забезпечення, боротьба з кіберзлочинами, виявлення прагнень терористичних угруповань тощо.

Структурним підрозділом, що займається профільною кваліфікаціє реагування та виявлення кіберзагроз є створений у 2018 році Ситуаційний центр забезпечення кібернетичної безпеки (далі – Центр). Його створення відбулось на основі Угоди про реалізацію Трастового фонду Україна – НАТО з питань кібербезпеки – у цих цілях було отримано спеціальне технічне обладнання та програмне забезпечення. Метою

Центру є протидія кіберрозвідкам іноземних держав; боротьба з кібертероризмом і кібершпигунством; контррозвідка та оперативно-розшукові заходи.

Міністерство оборони України (далі – МОУ) та Генеральний штаб Збройних Сил України покликані здійснювати заходи з підготовки держави до відбиття воєнної агресії в кіберпросторі, співпрацювати з НАТО задля сумісного захисту від кіберзагроз.

Завданням МОУ є створення сил активного кіберзахисту.

Однією із найважливіших підструктур даного суб'єкта є Головне управління зв'язку та інформаційних систем Генерального штабу Збройних Сил України (далі – Управління). Призначенням Управління є проведення єдиної державної технічної політики в сфері зв'язку та інформатизації, захисту інформаційних ресурсів в інформаційно-телекомунікаційних системах Збройних Сил України, а також їх організація зв'язку.

На Національну поліцію України (далі – НПУ), як на суб'єкта системи забезпечення кіберзагроз, було делеговано здійснення захисту прав і свобод громадянина. Його мета: запобігати, виявляти, припиняти та розкривати кіберзлочини; підвищувати проінформованість громадян у кіберпросторі.

Завданням НПУ є боротьба із кіберзлочинами та виявлення прагнень злочинних угрупувань.

Не так давно в Україні був створений Департамент Кіберполіції Національної поліції України. Основними завданнями цього Департаменту є участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку та сприяння у порядку, передбаченому чинним законодавством, іншим підрозділам Національної поліції у попередженні, виявленні та припиненні кримінальних правопорушень. Безумовно, створення окремого департаменту, який має сприяти розкриттю кіберзлочинів є вірним кроком. Проте необхідно зазначити, що результати роботи Департаменту кіберполіції поки що залишають бажати кращого. Фактично проблеми, які існували

до створення Департаменту кіберполіції нікуди не зникли, а деякі навіть набули ще більшої серйозності. Тому треба констатувати, що лише докорінні та систематичні зміни до чинного законодавства зможуть вплинути на досягнення позитивного результату у сфері боротьби з кіберзлочинністю.

Національний банк України (далі – НБУ) відповідає за формування вимог щодо кіберзахисту критичної інформаційної інфраструктури саме банківської сфери.

Завданням НБУ у сфері захисту від кіберзагроз є здійснення заходів з контролю виконання банками забезпечення кіберзахисту та інформаційної безпеки.

З метою організації процесу контролю за здійсненням реагування на потенційні кіберзагрози, було ініційовано створення Центр кіберзахисту НБУ (далі – Центр), у складі якого функціонує команда реагування на кіберінциденти в банківській системі (CSIRT-NBU). Основними елементами діяльності Центру стали: реалізування кіберстійкості у банківській системі України до сучасних загроз, що у майбутньому дасть змогу ефективніше реагувати та протистояти актуальним кіберзагрозам. Діяльність Центру має сприяти стабільності банківської системи України. Робота Центру пов'язана з недопущенням кіберінцидентів у банківській справі усієї держави, адже як показала практика, у 2017 році від банківської кібератаки постраждала третина усіх банків в Україні. Тоді не постраждав тільки Нацбанк, у зв'язку з ефективною нейтралізацією кіберзагрози фахівцями команди реагування на кіберінциденти Національного банку.

На розвідувальні органи покладена функція пов'язана з здійсненням розвідувальної діяльності щодо загроз національній безпеці України у кіберпросторі.

Розглянемо як приклад діяльність Служби зовнішньої розвідки (далі – СЗР). СЗР покликана виявляти протиправні прагнення іноземних держав та іноземних злочинних угрупувань.

Робота СЗР наразі пов'язана з відслідкуванням можливих кібезагроз зі сторони Російської Федерації. Тому в умовах інтеграції до нормативних актів Європейського Союзу, стратегія СЗР покликана розробити та ввести в дію наступні елементи кіберзахисту:

– створити мережі оперативних моніторингових центрів на випередження можливим кібератакам;
– розробити систему зв’язку нового покоління;
– зміцнити, модернізувати та адаптувати до новітніх кібернетичних викликів ключові стандартів безпеки в мережі Інтернет тощо.

Органи (служби) інформаційної безпеки можуть створюватися (на законодавчих засадах) і в недержавних структурах для захисту своїх потреб в забезпеченні необхідною інформацією. Дані органи на основі укладення відповідних угод можуть бути приєднані до єдиної державної системи інформаційної безпеки.

У підсумку детального розгляду усіх суб’єктів забезпечення реагування на загрози у кіберпросторі, можна виділити нагальні проблеми системи, зокрема:

1) відсутність національної бази індикаторів щодо події кіберзагроз, а також загальнодержавної системи швидкого реагування на загрози кібербезпеки. Наразі немає чітких розроблених індикаторів, що сповіщали б про кіберзагрози та передавали відповідну інформацію до координаційного центру, у зв’язку з цією проблемою, стає неможливим оперативне отримання інформації про кіберзагози (атаки).

2) відсутність чіткого алгоритму реагування та протидій кіберзагрозі\кіберінцеденту. Не розробленість чіткої системи визначених дій реагування на кіберзагрози сповільнює процес реагування на них. Це в своє чергу провокує інший недолік, такий як відсутність єдиного підходу до системи протидії кіберзагрозам.

3) проблематика кваліфікацій співробітників органів що є суб’єктами забезпечення кібербезпеки. Практично кожен суб’єкт даної сфери розгляду має власну підконтрольну структуру, що спеціалізується на кіберзагрозах, проте на практиці стає зрозуміло, що кожна служба має свою сферу реагування, а тому дещо іншу специфіку у роботі із потенційними загрозами. Особливості протидії кіберзагрозам є відокремленими від інших систем реагування на протиправні дії. Реагування на загрози кіберпезпеки має бути детально розглянутим науковцями з виділенням особливостей методики та її роз’яснення працівникам. Адже,

нормативна база у сфері є, проте немає чіткого розуміння її застосування на практиці.

4) відсутність ефективної міжнародної співпраці. Міжнародна спільнота, зокрема країни Євросоюзу та США на шляху розвитку кіберпростору вже мали суттєві кіберінциденти, а тому виробили алгоритм дії на них. Україна намагається інтегрувати як і міжнародні законодавчі ініціативи так і передове технічне забезпечення, яке б допомогло ефективно реагувати на кіберзагрози. Проте, недосконаліть наявного людського потенціалу, зокрема невелика кількість якісних професійних кадрів у структурах, не дає змогу реалізувати усі можливості системи забезпечення у реагуванні на кіберзагрози.

5) відсутність єдиного електронного документообігу між всіма органами кібербезпеки. Електронний документообіг – це створення відповідної інформаційної бази на носіях передачі інформації, задля реалізації умов для користування цією системою відповідного управлінського апарату у процесі здійснення своїх функцій. Основними засадами функціонування електронного документообігу є: реєстрація документу відбувається одноразово; при роботі з актом гарантується його безперервність руху; база документів повинна бути єдиною – це робить дублювання документів неможливим; пошукова система є ефективно організованою. Усі ці ознаки дають змогу при мінімальному володінні пошукової інформації знайти будь-який конкретний документ у системі. Наразі, в Україні кожна служба має свій документообіг, проте доступ до цих документів, а тому його захист кваліфікованими фахівцями стає некоординований.

6) відсутність інформування населяння про актуальні кіберзагрози та відповідні методи захисту від них. Передові країни використовують різні методи інформування населення: передача актуальних потенційних загроз через новини по телебаченню, радіо, смс повідомлення, навіть соціальні мережі. Проте, в Україні наразі немає дієвої системи сповіщення населення про можливі кіберзагрози, від політичної дезінформації населення до маніпуляцій із персональними даними громадян. Подібні сповіщення в Україні є хаотичними, з використанням різноманітних соціальних мереж. Хоча, до прикладу, не у всіх пенсіонерів є

сторінки в соціальних мережах та навіть доступ до Інтернету є не у всього дієздатного населення країни.

7) Недостатньо кваліфікований персонал. У зв'язку з постійною зміною видів та особливостей кіберзагроз, реагування на їх виявлення та в подальшому на їх протидію, має здійснюватись відповідним підготовленим персоналом. Адже, технологій змінюються, а тому потрібно змінювати підходи до реагування. Змінити ситуацію з недостатньою кваліфікованістю можна проведенням відповідних інструктажів, курсів із залученням іноземних спеціалістів та обміном досвіду у сфері кіберзахисту.

8) Недосконалість національної нормативно-технічної бази. Відсутність системної бази електронного обміну інформації між різними структурами, а також єдиного підходу до реагування на кіберзагрози провокує впровадження заходів кіберзахисту у суб'єктів забезпечення кіберзахисту на власний розсуд.

9) Відсутні офіційні канали для комунікації між підприємствами. Кожна служба має власну систему ведення інформації (документації, наказів, розпоряджень тощо). Для того, щоб отримати доступ до документів певної служби необхідно проти шлях бюрократії, а тому виникає безглузда трата часу – навіть координаційному органу важко отримати інформацію від суб'єкта забезпечення реагування оперативно.

10) Невизначена роль та місце суб'єктів, що безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки. Безсистемність дії суб'єктів, невизначеність конкретних цілей та завдань у їх нормативних документах сприяє неможливості правильного та чіткого делегування повноважень координаційним центром. А тому виникає така проблема як реагування на кіберзагрози, які не є в межах компетенції служб.

11) Не приділена увага державним колегіальним органам, підпорядкованим Президенту України, які охоплюють своєю регуляторною діяльністю певні галузі економіки, громадським організаціям, тощо.

12) Неефективність засвоєння уроків за результатами реагування на кіберінциденти. Ця проблема наразі є надзвичайно важливою, адже кіберінциденти

в Україні відбуваються часто, проте суб'єкти реагування практично ніколи після подолання проблеми не пишуть звітів з ефективного реагування на кібербезпеки. Тобто, не аналізують проведені дії, щоб в майбутньому вкиористати набутий досвід у вигляді плану реагування на кіберінциденти, тому це залишається однією з найменш реалізованих функцій суб'єктів забезпечення реагування.

Відсутність практики чіткого документування результатів внутрішніх перевірок може вкрай ускладнити процес удосконалення власної системи кібербезпеки (в тому числі через відсутність чіткого переліку проблем, які потребують вирішення, а відтак і контролю за їх вирішенням) [21].

Отже, тривалий час у інноваційно-інформаційному розвитку країни виникали різного роду трактування поняття «кіберпезпека» та «кіберзлочин». Ці поняття будуть і надалі змінюватись, відповідно до потреб суспільства. Сучасний розвиток у сфері інформаційних технологій стимулює підвищення використання такої технології, яка б дозволяла безпечно автоматизувати процедури у різних галузях держави. Таким чином, законодавче і підзаконне регулювання кібербезпеки у значенні ефективного реагування на кіберзагрози, має велике значення для започаткування відповідного підґрунтя стосовно розвитку у цій сфері. І хоча у даній сфері була прийнята велика кількість нормативних актів, а в структурах суб'єктів забезпечення реагування на кіберзагрози були створені відповідні центри їх протидії – відсутність чіткого алгоритму реагування та безсистемний підхід до вирішення кіберінцидентів є основоположними прогалинами у боротьбі з кіберзлочинністю.

Висновок до розділу 1

Загрози кібрпезпеки, в умовах інтеграційних процесів для України, набувають все більшого значення у різних сферах життя суспільства.

Україна зарекомендувала себе, як одна з передових держав на європейському континенті, яка здатна протистояти викликами інформаційно-технологічного прогресу, впроваджуючи низку спеціальних законодавчих та підзаконних актів

задля покращеного регулювання цієї сфери. Здійснення та реалізація усіх нормативних актів потребує співпраці із сьогочасним суспільством.

Національна система кібербезпеки має насамперед забезпечити взаємодію з питань кібербезпеки державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських об'єднань, а також підприємств, установ та організацій у сфері електронних комунікацій, захисту інформації.

Детальніше розглядаючи систему забезпечення суб'єктів реагування на кіберзагрози стає зрозумілим, що варто конкретно описати повноваження та завдання кожного суб'єкта, у тому числі координаційного центру, виділивши сферу реагування.

Нормативна база у сфері кібербезпеки є надзвичайно наближеною до законодавства передових держав світу у боротьбі з кіберінцидентами, проте її проблематика застосування на практиці не дозволяє виробити чіткий алгоритм у протидії злочинам. Потрібно констатувати, що яким би довершеним не було законодавство, порушення в цій сфері, у тому числі кримінальні є досить розповсюдженими.

РОЗДІЛ 2
УДОСКОНАЛЕННЯ ВІТЧИЗНЯНОЇ СИСТЕМИ ВИЯВЛЕННЯ

2.1 Розробка дієвої системи обміну інформацією щодо виявлення кіберзагроз

Інформаційні та комунікаційні технології стрімко розвиваються, посилюючи свій вплив на всі ключові сфери діяльності громадянина, організацій і держави. Мережа Інтернет та інші складові елементи кіберпростору затвердилися в якості системо-утворюючого фактора економічного розвитку і модернізації. У зв'язку з цим потрібна цілеспрямована і системна державна політика розвитку національного сектора застосування інформаційних технологій.

Суб'єкти системи забезпечення кібернетичної безпеки перебувають у тісній взаємодії між собою, але при цьому кожен із них спеціалізується на вирішенні конкретних завдань відповідно до своєї предметної компетентності та в межах повноважень, визначених законодавством. Незважаючи на це, загрози кібербезпеці актуалізуються через дію таких чинників, як недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки.

Таким чином, основним призначенням системи забезпечення кібербезпеки є сприяння у досягненні цілей кібернетичної безпеки, а тому основною функцією даної системи можна визначити забезпечення збалансованого існування інтересів особи, суспільства і держави шляхом здійснення перевірок, діагностування; виявлення та ідентифікації, запобігання та припинення, мінімізації та нейтралізації дії внутрішніх і зовнішніх загроз і небезпек у кібернетичній сфері. Дані реакції на загрози повинні бути адекватними за характером та масштабами, а також рівнем можливого і бажаного стану забезпечення кібернетичної безпеки [22].

Ефективність функціонування системи забезпечення кібербезпеки насамперед залежить від досконалості системи обміну інформацією та досвідом державних та громадських органів, а також неурядових організацій.

При встановленні операційних рамок для обміну інформацією, пов'язаною з протидією кіберзагрозам, плани реалізації повинні враховувати три основних питання:

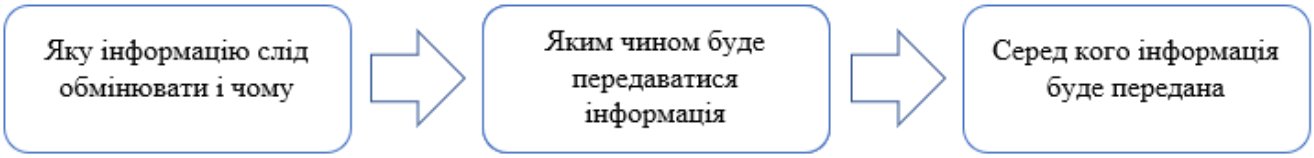

Рисунок 2.1 – Основні питання обміну інформацією

Інформацією можна обмінюватися на стратегічному, технічному або тактичному рівні. З іншої сторони, інформація може бути пов'язаною або непов'язаної з інцидентом. Це може також прийняти форму обміну інформацією в режимі реального часу в контексті неминучої або триваючої загрози, коли очікується, що сторона, яка отримує інформацію щодо кіберзагрози зробить негайні дії.

Обмін інформацією між урядовими установами (суб'єктами реагування на кіберінциденти) та координаційним центром повинен проходити в обох напрямках і охоплювати, зокрема:

Загрози: наприклад, правоохоронні органи і розвідувальні служби повинні передавати інформацію про нові типи загроз координаційному центру. Ця інформація гарантує, що працівники центру проведуть оцінку ризиків і вживатимуть необхідних заходів щодо їх реагування. З іншого боку, працівники координаційного центру повинні повідомляти про результати оцінки ризиків та заходи щодо пом'якшення, прийняті відповідними державними структурами, щоб забезпечити кращу модуляцію планів по реагуванню. У цьому контексті прикладом злагодженої роботи є повідомлення-реагування Інтерполу. Адже, «фіолетові і помаранчеві повідомлення» Інтерполу мають особливе значення для поширення термінової інформації серед світової спільноти правоохоронних органів і громадськості. У той час як фіолетові повідомлення допомагають шукати або

надавати інформацію про modus operandi (метод роботи), об'єкти, пристрої і методи приховування, які використовуються злочинцями, помаранчеві повідомлення використовуються для попередження про подію, людину, об'єкт або процес, що представляє серйозну і неминучу загрозу для державної безпеки;

Підозрілі дії: працівникам координаційного центру може бути рекомендовано повідомляти про так звані «Слабкі сигнали», тобто про незвичайні ситуації, які самі по собі недостатні для спрацьовування тривоги, але виявляють загрозу, що насувається при розгляді в контексті аналогічних подій або коли виникає підозра через інформацію, що надходить з інших джерел;

Дані про інциденти: досвід минулих інцидентів загроз (включаючи те, що було зроблено та не зроблено для їх усунення), вони можуть дати важливу інформацію про способи запобігання повторення такої ж ситуації, що в свою чергу, забезпечує основу для більш ефективного управління ризиками та діями з відновлення.

Стратегія Японії в області кібербезпеки спрямована на подолання коливань бізнесу, тому приватні структури діляться інформацією з державними органами. Відповідно до цієї стратегії, щоб зробити обмін інформацією більш активним, важливо встановити чіткі правила щодо надання даних до координаційних центрів, з метою підтвердження довіри до державних структур та обмеживши псування репутації своїх підприємств, задля умови надання інформації з обмеженим доступом координаційному центру і доступу до особливостей діяльності підприємства, так, щоб не відбулось «втрати або збитку» від надання інформації.

В контексті кіберзагроз обмін інформацією може включати інформацію щодо:

– уразливостей (наприклад, недоліки програмного забезпечення, що використовується);
– інформування про інцидент, а також про спроби порушення інформаційної безпеки;
– обмін досвідом протидії загрозам, у тому числі надання відомостей про перспективне реагування на кіберзагрози.

Необхідність створення дієвих механізмів обміну інформацією в першу чергу стосується суб'єктів реагування на кіберзагрози. Адже у кожного суб'єкта наявна

власна система протидії кіберзагрозам, випрацювана на основі досвіду служби. У свою чергу, незважаючи на види кіберзагроз та на різноманіття суб'єктів їх здійснення, реагування у службах відбувається одноманітно. Проте, обмін досвідом та інформацією про методології оцінки ризиків мають вирішальне значення в реагуванні на кіберініденти. Тому, досвідчена служба (суб'єкт забезпечення реагування) з багаторічним практичним досвідом в області кіберзахисту може з користю передати свої знання службам, які менш знайомі з застосованою нормативно-правовою базою та стратегіями реагування на загрози.

Наразі ми спостерігаємо стрімке реформування суб'єктів забезпечення реагування на кіберзагрози, щодо створення у структурах нових департаментів, управлінь, центрів з боротьби кіберзлочинності. Проте, варто зауважити, що нові працівники цих підструктур не зовсім обізнані в методології виявлення та реагування на кіберзагрози. Важливим фактором в обміні інформації є те, що кожна служба розробляє свою систему реагування, а тому не хоче розповсюджувати матеріали з її розробки.

Ефективність обміну інформацією серед суб'єктів забезпечення реагування на кіберзагрози залежить від двох основних чинників:

- Можливості координаційного центру створювати довіру серед зацікавлених сторін. Створення довіри між суб'єктами щодо обміну інформацією може зайняти багато часу і вимагає активної прихильності всіх зацікавлених сторін. Однак після встановлення довіри потоки інформації значно зростуть як в якісному, так і в кількісному відношенні.
- Забезпечення адекватних рівнів захисту конфіденційної інформації, обмін якою заохочується або буде дозволятись відповідно до розробки нормативних актів щодо обміну інформацією. Створення довірливого середовища для обміну інформацією залежить від встановлення чітких правових і операційних рамок для захисту конфіденційної інформації, у контексті спільно використовуваних даних. При розробці таких рамок головна мета полягає в сприянні поширенню інформації для цілей оперативного реагування на кіберзагрози – повинна завжди враховувати

необхідність дотримання застосовних документів, що стосуються прав на недоторканність приватного життя і захисту даних.

Не вся інформація, пов'язана з реагуванням на кіберзагрози, повинна розглядатися конфіденційно. Так само і не вся інформація, яка вважається «конфіденційною» заслуговує однакової міри захисту. Обмеження на поширення даної інформації, можуть приймати різні форми і бути більш або менш суворими в залежності від конкретних обставин і цілей певного типу обміну інформацією. Наприклад, в Новій Зеландії установлено базовий принцип, згідно з яким кіберінциденти повинні розглядатися на найнижчому рівні конфіденційності в якості способу раннього і ефективного поширення критично важливої інформації серед всіх респондентів-реагування на кіберзагрози, які відповідають за зниження їх впливу на суспільство. Часто передові держави використовують ряд методів і рішень для захисту поширення конфіденційної інформації.

Як правило, вони зосереджені навколо:

1) процедур допуску та благонадійності;
2) системи колірного кодування;
3) електронних інструментів.

Всі три часто доповнюють один одного. За цією системою координаційний центр міг би надати допуск до відповідної інформації для ключових суб'єктів забезпечення реагування на кіберзагрози, яким необхідний доступ до певної конфіденційної інформації. Вказані елементи засновані на принципі, згідно з яким той, хто надає інформацію, визначає ступінь її поширення.

Обмін інформацією може здійснюватись не тільки в межах діяльності суб'єктів забезпечення реагування на кіберзагрози, але і в системі обміну інформацією між державними службами реагування та підприємствами приватної сфери. До прикладу, створена Урядом Австралії в 2003 році, довірена мережа обміну інформацією (TISN) є основним механізмом взаємодії в країні з ініціативами по обміну інформацією між бізнесом і урядом з підвищенням стійкості кібербезпеки у державі. TISN забезпечує безпечне середовище, в якому працівники координаційного центру в семи галузевих групах регулярно зустрічаються для

обміну інформацією та співпраці всередині і між секторами для вирішення проблем безпеки і безперервності бізнесу. Галузеві групи TISN включають банківську справу і фінанси, зв'язок, енергетику, продукти харчування і продовольство, охорону здоров'я, транспорт і водопостачання. Крім того, існують спеціалізовані форуми (між-секторальні групи за інтересами), які допомагають у тимчасовому вивченні комплексних питань, і експертно-консультативна група по стійкості, яка приділяє велику увагу організаційної стійкості.

Побудова дієвої системи забезпечення кібернетичної безпеки вимагає від державних органів України чіткого визначення державної політики у цій сфері та випереджального реагування на динамічні зміни, що відбуваються у світі у сфері забезпечення кібернетичної безпеки. При цьому вибір конкретних засобів і шляхів забезпечення кібернетичної безпеки України зумовлюється необхідністю своєчасного вжиття заходів, адекватних характеру і масштабам реальних та потенційних кібернетичних загроз життєво-важливим інтересам людини і громадянина, суспільства і держави.

Організаційне забезпечення системи кібербезпеки також можна розглядати як цілеспрямовану діяльність суб'єкта забезпечення кібербезпеки, пов'язану:

– зі створенням і впорядкуванням (розвитком) організаційних структур, найбільш доцільних для забезпечення безпеки у кіберпросторі;
– з упорядкуванням (налагодженням) процесу управління у сфері забезпечення безпеки у кіберпросторі, забезпеченням найліпших умов для прийняття та реалізації відповідних управлінських рішень.

Отож, варто здійснити трансформацію на державному рівні з наступних питань сфери забезпечення протидії кіберзагрозам:

1) покращити, встановити або зміцнити національні, регіональні та міжнародні партнерські відносини із зацікавленими сторонами, як державними, так і приватними, згідно з обставинами, метою обміну інформацією та досвідом і тим самим запобіганню терористичних нападів на інфраструктуру держави;

2) забезпечити системний захист від кіберзагроз, пом'якшення їх наслідків, розслідування, реагування на них і відновлення нормальної діяльності після

заподіяної ними шкоди, в тому числі шляхом проведення спільних навчальних заходів; та застосування або створення відповідних мереж зв'язку між суб'єктами забезпечення протидії кіберзагрозам [23].

Отож, на основі розглянутих елементів дієвої системи обміну інформацією щодо виявлення кіберзагроз, можна виділити наступні пропозиції з покращення відповідної системи:

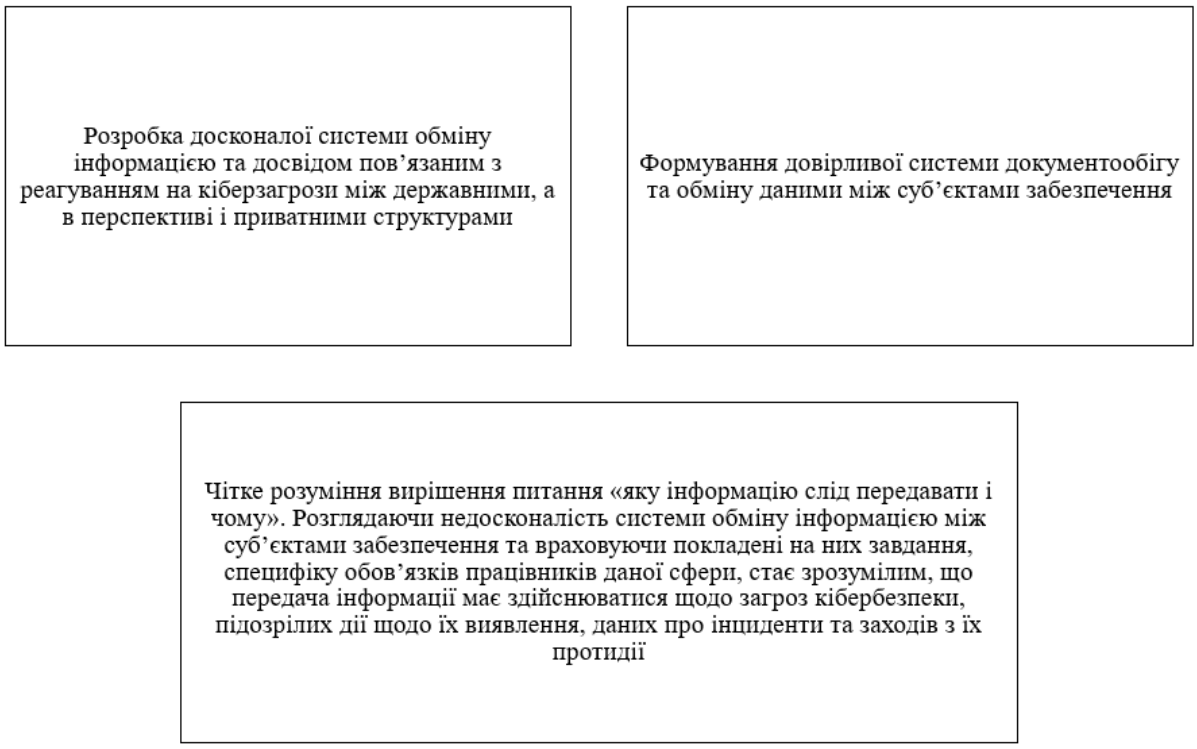

Рисунок 2.2 – Основні пропозицій з покращення відповідної системи

Отже, потрібно впровадити систему обміну інформації про кіберзагрози на національному рівні. Технічно такі системи існують, наприклад «Open Source Threat Intelligence Platform» (далі – MISP), це програмне забезпечення з відкритим програмним кодом, за допомогою якого, можливо збирати, передавати та обробляти інформацію про кіберзагрози, кіберінциденти та шляхи виявлення кіберзагроз і захисту від них. Але, програмне забезпечення не вирішить питання дієвого обміну інформації про кіберзагрози без якісного нормативно-організаційного забезпечення, тому потрібно розробити та прийняти комплекс нормативних документів які яке

повинно вирішити питання пов’язані з організацією роботи з системою обміну інформацією про кіберзагрози. В нормативних документах повинні знайти своє відображення наступні аспекти:

- закріпити статус єдиної інформаційної системи щодо обміну інформацією про кіберінциденти;
- порядок підключення суб’єктів кібербезпеки до системи;
- визначити основних суб'єктів забезпечення кібербезпеки як постійних та обов’язкових учасників системою обміну інформацією про кіберзагрози.
- зобов'язати всіх суб'єктів забезпечення кібербезпеки вносити всі данні в систему щодо кіберінцидентів які сталі їм відомі;

В якості відповідального за чітку роботу системи обміну інформацією про кіберзагрози та підтримку її в належному стані пропонується призначити НКЦК як основний робочій орган РНБО який здійсню координацію між всіма суб’єктами забезпечення кібербезпеки.

В подальшому, потрібно впровадити алгоритм внесення інформацій до системи, який повинні містити процедуру внесення інформацій, класифікацію кіберінцидентів та строки внесенні інформацій, для цього проаналізувавши міжнародну практику пропонується наступне:

- Внесення інформації про кіберзагроз та кіберінцидентів, суб’єктом забезпечення кібербезпеки до єдиної інформаційної системи обміну інформацією про кіберзагрози повинно відбуватися невідкладно або не пізніше ніж 24 години з моменту як суб’єкту забезпечення кібербезпеки стало відомо про загрозу або кіберінцидент;
- Класифікувати інформацію яка вноситься до системи обміну інформацією про кіберзагрози за наступними критеріями: загрози, підозріла активність та данні про інцидент кібербезпеки.

Для того, щоб дані яка потрапляють до системи обміну інформацією про кіберзагрози, вчасно оброблялась, потрібно якимось чином на неї реагувати. В враховуючи специфіку даних про кіберзагрози, їх латентність та велику складність в їх виявлення та реагуванні на ней, потрібно прийняти доволі гнучкі але ефективні

шляхи реагування на інформацію про кіберзагрози. Для цього потрібно ввести рівень небезпеки даних про кіберзагроз як це зроблено в багатьох країна світу. Пропонується наступна шкала:

– низькій рівень небезпеки;
– середній рівень небезпеки;
– високий рівень небезпеки;

Відповідно до рівня небезпеки потрібно встановити строки реагування на них, наприклад, для високого рівня небезпеки – до одного тижня, середній рівень – до одного місяця та низький рівень – до шести місяців. Ці строки пропонується вести за-для реагування на сам перед на най небезпечні кіберзагрози, чим виконується превентивна функція реагування на кіберзагрози та попередження наслідків спричинених кіберзагрозою.

НКЦК не зважаючи на свій колегіальних характер, повинен виступити в ролі розподільника та розподілити який суб'єкт буде аналізувати ту чи іншу інформацію про кіберзагрози, з урахуванням специфіки кожного суб'єкту забезпечення кібербезпеки.

Суб'єкти забезпечення кібербезпеки працюють, не взаємодіючи один з одним. Проте, якщо налагодити систему обміну даних пов'язаних з напрацьованим досвідом протидії кіберзагрозам, стане можливим: формування і застосування цілісного понятійного апарату; удосконалення стандартів інформаційної безпеки і управління кіберризиками; формування системи бар'єрів реалізації кіберінцидентів; вдосконалення координації діяльності і керованості підрозділів, відповідальних за забезпечення кібербезпеки; підвищення стійкості і вдосконалення функціонування механізмів реагування на кіберзагрози тощо.

2.2 Практичне впровадження нормативно-організаційних заходів координування суб'єктів забезпечення кіберпезпеки

Різні державні органи, у сфері забезпечення реагування на кіберзагрози, встановлюють безліч внутрішніх ідентифікаторів, правил і стандартів з питань

безпеки в різних секторах. Ефективні заходи з управління кризами і реагування на них вимагають здатності кількох державних структур (на місцевому, муніципальному, регіональному і національному рівнях) виконувати свою діяльність оперативно. Проте, наявність чіткого розмежування (делегування) субординації завдань та системність до підходу їх розподілення є ключовими елементами дієвості системи забезпечення реагування.

Усе ще триває робота над розбудовою НКЦК. Відповідно викликів сучасності, головним завданням якого визначено: координування, прогнозування і виявлення потенційних та реальних кіберзагроз, а також забезпечення РНБО України аналітичними матеріалами. Проте, в умовах сьогодення необхідна актуальна розробка чіткого координування між суб'єктами забезпечення реагування на кіберінциденти.

Інституційні рамки при здійсненні реагування на кіберзагрози повинні (як мінімум) охоплювати наступні аспекти:

- визначити агентство, яке відіграє загальну координуючу роль в реалізації національної стратегії з реагування на кіберзагрози. В Україні такою структурою є РНБО з відповідним підрозділом НКЦК. РНБО надана законодавча ініціатива по регулюванню питання координації суб'єктів реагування на кіберзагрози.
- розподіл обов'язків конкретних секторів. У державі діє система розподілу повноважень та реагувань, відповідно до якої кожна служба, що є суб'єктом реагування на кіберзагрози, розробила власну підструктуру з протидії кіберзагроз у відповідності до функцій, досвіду і предметної компетенції служби;
- визначити обсяг і форми взаємодії між суб'єктами реагування на кіберзагрози. Наразі не розроблена чітка система обміну документообігом, досвідом та у загальному не конкретизована форма взаємодії між суб'єктами. Проте, саме завдяки ефективній взаємодії між відповідними державними структурами, буде досягнута мета з розробки дієвого механізму і зібрання найкращих практик реагування на кіберзагрози для

підвищення рівнів запобігання, пом'якшення, готовності, реагування та відновлення.

Тобто, елементи дієвого реагування на кіберзагрози у державі наявні, проте усе ще не вдається досягнути довершеності у формах взаємодії між законодавчо-визначеними суб'єктами системи реагування на кіберзагрози.

Широка міжвідомча координація є ключовою передумовою для реалізації адекватних рівнів реагування на кіберзагрози. Стратегії різних служб з протидії кіберінцидентам повинні «зв'язати точки» між різними національними агентствами, відповідальними за захист інформації.

Координація повинна бути досягнута з зацікавленими сторонами, такими як суб'єкти забезпечення реагування на кіберзлочини, регіональними органами та іншими регуляторами, які співпрацюють на стратегічному, тактичному та оперативному рівнях.

Однак, досягнення мети злагодженої взаємодії між усіма державними суб'єктами цієї сфери наразі є не досконалою. Використання різної термінології і професійної мови суб'єктами, які беруть участь в діях щодо запобігання / захисту / реагування, а також відсутність уніфікованих процедур і каналів зв'язку можуть серйозно вплинути на якість всієї роботи суб'єктів. Адже, у деяких випадках державні органи мають тенденцію слідувати «різним повістками дня» щодо захисту інформації та дотримуються власних розроблених положень реагування на кіберінциденти, тоді як інші віддають безперечну законодавчому елементу реагування.

З метою досягнення системності у вирішенні конкретних завдань, що виникають при реагуванні на кіберзагрози, необхідно дотримуватись наступного: наділяти керівників відповідних інформаційних підрозділів (у державних службах) повноваженнями щодо ефективнішого використання технологій при виконанні завдань задля усунення дублюючих процесів та підвищувати рівень інвестицій в інформаційні технології.

Основними передумовами для системного координаційного реагування при прийнятті рішень щодо потенційних кіберзагроз є:

1) Чіткий розподіл ролей і обов'язків, наслідком чого є те, що рішення повинні прийматися на найнижчому відповідному рівні, а координація – на найвищому. Можна стверджувати, що «тісна інтеграція координаційних операторів в антикризове управління вимагає виконання особистісних нормативних вимог. Взаємне розуміння ролей, обов'язків, здібностей і можливостей – це тривалий процес, що вимагає інвестицій з точки зору часу, людського співробітництва, навчання термінології суб'єктів тощо.

2) Розуміння наслідків руйнування системного координування суб'єктів забезпечення реагування на кіберзагрози, включаючи його каскадні ефекти. Варто відзначити, що міжнародному рівні виділяється саме реагування координаційного центру на одиничне порушення і його потенційні наслідки. Тобто, у випадку спричинення негативних наслідків у багатьох галузях суспільства, відбувається чітке розмежування реагування повноважень суб'єктів. До прикладу, якщо кібератака відбувається у декількох галузевих напрямах, реагування має бути оперативним відповідно до чіткого розмежування компетенцій.

3) Діяльність координаторів повинна бути з цілодобовою доступністю до реагування на кіберінциденти.

4) Створення адекватних систем управління інформацією для підтримки ефективного збору, аналізу та поширення даних для прийняття єдиних централізованих рішень, у тому числі для надання інформації населенню.

Ефективність процесу консолідації у сфері забезпечення реагування та протидії кіберзагрозам великою мірою залежить від активної позиції держави в цьому питанні. Для здійснення «соціального поштовху» у бік посилення консолідації органами державної влади мають бути розроблені та реалізовані практичні заходи.

На основі передумов, стає необхідністю виділення цілей системи взаємодії між суб'єктами реагування на кіберзагрози:

– аналіз загроз, вразливостей;

– оцінка загроз та безперервний процес інформування суб'єктів системи забезпечення щодо ризиків (ведення активного діалогу, пов'язаного з результатами аналізу, оцінками, цілями захисту та варіантів дій);
– аналіз існуючих нормативних актів і (де це може бути застосовано) визначення додаткових заходів.

Організація взаємодії повинна бути розроблена таким чином, щоб мінімізувати ситуації, коли приймаються суперечливі інструкції. У зв'язку з досягненням вищевказаних завдань необхідними є проведення між-організаційних тренінгів задля досягнення загального розуміння застосовних процесів і методологій; визначення ролі і відповідальності в мірах захисту інформації тощо.

Таблиця 2.1

Основні види тренінгів з кібербезпеки

Перелік найбільш поширених видів навчань і їх основних застосувань		
Семінар: загальне роз'яснення по керівництву існуючих стратегій, планів, процедур	Тренувальне навчання: проводити навчання на новому обладнанні, перевіряти процедури або поточну практику і підтримувати поточні здібності	Штабне навчання: обговорення гіпотетичної, змодельованої кіберзагрози (корисні для полегшення концептуального розуміння, визначення сильних та слабких сторін підрозділу)

Важливо відзначити, що деякі з вищезгаданих навчань, особливо ті, в яких буде задіяна велика кількість учасників і які засновані на складних імітаціях кіберзагроз в реальному часі, вимагають ретельного планування – місяців, якщо не років, підготовки. Адже, ключовою концепцією міжвідомчої координації є «функціональна сумісність». Сумісність може бути операційною / функціональною або технічною.

(1) Операційна / функціональна можливість взаємодії – це здатність ефективно працювати разом. Зокрема, це здатність різних юрисдикцій або напрямків надавати та приймати інформацію, пов'язану з кіберінцидентами скоординованим чином. З практичної точки зору експлуатаційна сумісність означає, що працівники з різних юрисдикцій або служб виступають в якості команди під загальною структурою координування і управління.

(2) Технічна можливість взаємодії – це здатність спілкуватися і обмінюватися інформацією, а також інтегрувати обладнання і технічні можливості. У тому числі це можливість систем забезпечувати динамічний інтерактивний обмін інформацією та даними між елементами командування, управління і зв'язку для планування, координації, інтеграції та виконання операцій реагування.

У контексті міжвідомчої координації можливість покладатися на сумісні процеси видається особливо важливою для зв'язку в надзвичайних ситуаціях. Професійні відмінності між суб'єктами забезпечення реагування на кіберзагрози можуть перешкоджати досягненню оптимальних рівнів співробітництва. Певні відмінності в реагуванні можуть бути виявлені щодо діяльності цивільних і військових – ролі і обов'язки в цивільній сфері часто бувають менш чіткими, ніж у військовій.

Отож, у міру закономірного розвитку суспільства, правила і процедури при реагуванні на кіберзагрози можуть бути відсутніми або такими, що втратили свою актуальність, а лінії юрисдикції можуть розглядатися як додаткові або конкуруючі.

Метою роботи НКЦК наразі має стати залучення технологічного та інженерного потенціалу до співпраці з координаційним центром, використати існуючу в Україні інсталяційну базу на об'єктах критичної інфраструктури, поглибити співпрацю із суб'єктами кібербезпеки та приватними компаніями.

Отже, поява в Україні НКЦК була зумовлена саме необхідністю вирішення питання ефективної координації всіх суб'єктів, які діють в сфері кіберзахисту. Наскільки ефективний та дієвий цей механізм покаже час.

Таким чином, для досягнення національних і регіональних цілей у сфері кібербезпеки необхідний розвиток міцної співпраці в регіоні та ефективний і швидкий обмін інформацією.

2.3 Покращення міжнародної співпраці в сфері обміну інформації щодо кіберзагроз

Розбудова національної системи кібербезпеки, здатної забезпечити належну протидію кіберзагрозам національної безпеки, є нагальним завданням, що постало сьогодні перед Україною. У цьому контексті, з урахуванням транснаціонального та транскордонного характеру, кіберзагрози набувають особливого значення у міжнародному співробітництві розвитку цієї сфери. Україна як європейська держава здійснює відкриту зовнішню політику і прагне рівноправного взаємовигідного співробітництва з усіма зацікавленими партнерами виходячи насамперед із пріоритетів гарантування безпеки, суверенітету та захисту територіальної цілісності.

Варто розглянути детальніше злочинних суб'єктів сфери дослідження – ними можуть виступати: міжнародні злочинні групи хакерів, підготовлені кіберзлочинці, спецслужби іноземних держав, терористичні та екстремістські угруповання тощо. Наразі інформаційний простір є вразливим до зовнішніх кіберзагроз, особливо зі сторони агресора – Російської Федерації.

Саме тому доцільно виділити загальні складові, що потребують особливого захисту у межах забезпечення протидії кіберінцидентів:

- кібернетичні ресурси
- кібернетична інфраструктура
- кібернетичні технології

На основі міжнародного досвіду можна стверджувати, що національна безпека не може існувати без реалізації заходів щодо формування виваженої державної інформаційної політики, у тому числі й інтеграції світових систем колективної

безпеки. Система забезпечення кібербезпеки має відповідати критеріям Організації Північноатлантичного договору (далі – НАТО), особливо в умовах, коли Україна інтегрує законодавчі акти Європейського Союзу (з метою подальшого членства у ньому). Важливе значення у перейманні передової законодавчої ініціативи має й факт наявності агресивної політики країни-сусіда.

Міжнародна інтеграція в сфері кібербезпеки передбачена й українським законодавством, а саме ст. 14 ЗУ «Про основні засади забезпечення кібербезпеки України». Так, Україна відповідно до укладених нею міжнародних договорів здійснює співробітництво у сфері кібербезпеки з іноземними державами, їх правоохоронними органами і спеціальними службами, а також з міжнародними організаціями, які здійснюють боротьбу з міжнародною кіберзлочинністю [14].

Адже, кожна країна бажає підвищити обізнаність у сфері кіберзахисту і знайти найшвидші та найдієвіші шляхи протидії кіберзагрозам. У зв'язку з цим за останні декілька років зросла роль усвідомлення того, що кіберінциденти не припиняються на державних кордонах, а тому необхідне укладення ряду міжнародних угод з партнерства у цій сфері.

Зважаючи на загальну міжнародну інтеграцію законодавчого рівня, варто виділити що, кожна держава індивідуально визначає сфери, які вона відносить до кібернетичної безпеки, тому перелік об'єктів і суб'єктів кіберзагроз, розробляється у відповідності до стратегічних цілей і завдань, які стоять перед державою на національному і міжнародному рівнях, у тому числі з практичних можливостей реалізації національних інтересів.

Важливе значення для міжнародного «спілкування» у сфері кібербезпеки є створенням наступних умов:

– підвищення прозорості, співпраці та стабільності між державами в кіберпросторі за допомогою заходів з підтвердження довіри;
– розробка прийнятних норм поведінки держави в кіберпросторі та уточнення, як у цій галузі застосовується міжнародне право;
– поглиблення міжнародної співпраці;

– нарощування національного / міжнародного потенціалу для вирішення кіберпроблем.

Першочергову увагу захисту кібербезпеки приділяє Організація Об'єднаних націй (далі – ООН). Починаючи з 1996 року саме вона ініціювала інтерес громадськості до формування нормативної бази та організаційних механізмів щодо розбудови системи протидії кіберзлочинам. Саме завдяки відповідним Резолюціям ООН країни змогли зміцнити стратегію захисту від кібернетичних, психологічних та медійних загроз. Так, у процесі інтеграції міжнародних норм Україна змогла спочатку прийняти Доктрину інформаційної безпеки, а надалі й Стратегію кібербезпеки на національному рівні.

Проте, зрушення відбулись не лише в нормативному просторі кібербезпеки, а й в науковому. Адже ООН часто проводить різноманітні зустрічі, семінари конференції у цій сфері (до прикладу, проведення всесвітньої зустрічі з питань інформаційного суспільства). Отож, як показує аналіз, проведення даних конференцій у Тунісі, Швейцарії породжує не тільки інтерес до відповідної сфери відносин, а й провокує подальший розвиток та набуття кваліфікованих кадрів у боротьбі з кіберзлочинністю.

Кібербезпека, як частина національної безпеки є стратегічним завданням діяльності НАТО. Адже, чи не усі політичні і військові конфлікти розпочинаються з кіберпростору. Варто розглянути детальніше заходи кібербезпеки формату НАТО, які започаткували надання: рекомендацій щодо координації суб'єктів кібербезпеки; допомоги окремим країнам-членам НАТО у боротьбі з кіберінцидентами. Вирішальне значення в набуті досвіду на міжнародному рівні мали наукові дослідження НАТО. Адже, центр НАТО з кібербезпеки реалізував підготовку з проведення операцій у кіберпросторі. Вирішальне значення для України у сфері протидії кіберзагрозам має Трастовий фонд допомоги Альянсу та Комплексний пакет допомоги НАТО. Саме ця міжнародна співпраця допомогла Україні розробити власні групи протидії кіберзагрозам, вдосконалити законодавство у цій сфері тощо. Завдяки допомозі НАТО – українським державним структурам вдалось отримати передове обладнання та програмне забезпечення. А у 2015 році у рамках

Трастового фонду, Естонія провела та організувала ряд навчальних курсів щодо підготовки працівників на стратегічному та оперативному рівнях [24].

На противагу європейської моделі сприяння розвитку захисту інформаційних технологій суттєвим міжнародним партнером із забезпечення передового технічного обладнання наразі є Сполучені Штати Америки. До прикладу, саме США за останні декілька років були чи не найбільшими інвесторами України щодо забезпечення найсучаснішого обладнання у координаційному центрі та структурах МЗС.

Отже, світова спільнота розуміє, що Україна, перебуваючи у безпосередній близькості до агресора – Російської Федерації, потребує як забезпечення обладнанням працівників сфери кіберзахисту так і їх належної підготовки та навчання.

Наразі наявні суттєві зрушення в міжнародній співпраці між вітчизняними суб'єктами забезпечення реагування на кіберінцидентами. До прикладу, на основі співпраці міжнародного рівня з працівниками координаційного центру стає можливою побудова таких компонентів як: національна сенсорна інфраструктура та інфраструктура моніторингу, центрів очистки трафіку та протидії DDoS-атакам, варіантів запуску масштабної системи оцінки вразливостей, побудова системи НКЦК з розслідування загроз та інцидентів, цифрової криміналістики та аналізу шкідливого коду, масштабування платформи обміну інформацією про кіберзагрози (MISP тощо), платформи координації та автоматизації процесів реагування на інциденти, національної хмарної платформи сервісів кібербезпеки, впровадження національного безпечного DNS, систем захисту від шкідливого коду на кінцевому обладнанні (EDR), системи захисту електронної пошти державних службовців, системи захисту веб-сервісів тощо [25].

Проте, хоча й за наявності суттєвих позитивних зрушень щодо кіберзахисту, Україна все ж має і недоліки роботи системи суб'єктів забезпечення реагування на кіберінциденти. Мова йде про останні міжнародні дослідження стану кібербезпеки в світі, де Україна серед 160 аналізованих країн посіла 25 місце. Негативними показниками у аналізі були саме: освіта у сфері кіберзахисту та електронна ідентифікація (яка наразі є практично не дієвою) [26].

Аналізуючи тенденції розвитку щодо міжнародної співпраці в сфері обміну досвідом у боротьбі з кіберзлочинами, стає зрозумілим, що нашій державі потрібно зосереджувати розвиток системи реагування на кіберінциденти в наступних напрямках:

1) завершити створення чіткої робочої системи координації;

2) використати досвід та практики ЄС і НАТО та США у створенні національної системи сертифікації з кібербезпеки, широкомасштабного плану-відповіді на кіберінциденти і кризи;

3) поглиблювати державно-приватне партнерство і посилювати дослідження у цій сфері;

4) нарощувати навчальні зв'язки України у сфері кібербезпеки за сприяння Трастового фонду НАТО;

5) розробити та реалізувати план реагування інциденти в кіберпросторі;

6) розробити механізм розподілення ризиків через використання захищених хмарних сервісів задля мінімізації можливих втрат у разі кібернападу на інформаційні бази органів державної влади;

7) розробити систему навчань та мотивацій для працівників кібербезпеки та кібероборони.

У сучасних реаліях перед політичним керівництвом нашої держави постає важливе та відповідальне завдання: запозичуючи передовий зарубіжний досвід спільними зусиллями активізувати реалізацію дієвих заходів щодо боротьби з міжнародною кіберзлочинністю, кібертероризмом. Завдання передбачає насамперед побудову ефективної моделі національної системи кібербезпеки, її інтеграцію до ЄС та НАТО, дієвого захисту національних та комерційних інформаційно-комунікаційних ресурсів та їх критичної інфраструктури, затвердження офіційної акредитації з боку НАТО національного центру кіберзахисту та протидії кіберзагрозам, з метою розвитку конструктивної співпраці із Альянсом у цій галузі, блокування будь-яких посягань на національну інформаційну сферу, створення оптимальної моделі надійного захисту вітчизняного кіберпростору, формування засад для розробки методів і принципів здійснення «електронної оборони» [27].

Отже, Україна у відповідності до укладених міжнародних угод реалізує співробітництво у сфері кібербезпеки з іноземними державами (їх державними службами, збройними формуваннями, правоохоронними органами тощо). Особлива увага наразі приділяється розвитку законодавства у сфері кібербезпеки; кіберінцидентам; якісному наданні освіти; забезпеченні захисту послуг, у тому числі електронних; електронній ідентифікації та довірчим послугам; захисту персональних даних; заходам з реагування на кібератаки та кіберінциденти; боротьбі із кіберзлочинністю тощо.

Висновок до розділу 2

Суб'єкти системи забезпечення кібернетичної безпеки перебувають у тісній взаємодії між собою, але при цьому кожен із них спеціалізується на вирішенні конкретних завдань відповідно до своєї предметної компетентності та в межах повноважень, визначених законодавством. Незважаючи на це, загрози кібербезпеці актуалізуються через дію таких чинників, як недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки.

Розробка дієвої стратегії обміну інформації, пов'язаної з виявленням кіберзагроз має включати в себе наступні елементи:

1) заповнення прогалин в регулюванні забезпечення кібербезпеки;

2) систематизування дії всіх суб'єктів забезпечення кібербезпеки з метою підвищення її рівня;

3) формулювання моделі загроз кібербезпеки.

Актуальними та своєчасними як з позиції фундаментальної теорії, так і практичної складової залишаються подальші наукові розробки й дослідження проблем формування базових концептів виваженої державної інформаційної політики в сучасних умовах, поглиблення міжнародного співробітництва та конструктивної співпраці з НАТО та ЄС з метою запозичення передового досвіду забезпечення кібербезпеки, результативності функціонування інституцій, які опікуються питаннями кіберзахисту [27].

Аналізуючи тенденції розвитку щодо міжнародної співпраці в сфері обміну досвідом у боротьбі з кіберзлочинами, стає зрозумілим, що нашій державі потрібно зосереджувати розвиток системи реагування на кіберінциденти в наступних напрямках:

- завершити створення чіткої робочої системи координації;
- використати досвід та практики ЄС і НАТО та США у створенні національної системи сертифікації з кібербезпеки, широкомасштабного плану-відповіді на кіберінциденти і кризи;
- розробити та реалізувати план реагування інциденти в кіберпросторі;
- розробити систему навчань та мотивацій для працівників кібербезпеки та кібероборони.

Побудова дієвої системи забезпечення кібернетичної безпеки вимагає від державних органів України чіткого визначення державної політики у цій сфері та випереджального реагування на динамічні зміни, що відбуваються у світі у сфері забезпечення кібернетичної безпеки. При цьому вибір конкретних засобів і шляхів забезпечення кібернетичної безпеки України зумовлюється необхідністю своєчасного вжиття заходів, адекватних характеру і масштабам реальних та потенційних кібернетичних загроз життєво-важливим інтересам людини і громадянина, суспільства і держави.

РОЗДІЛ 3
ПРОПОЗИЦІЇ ЩОДО ПОКРАЩЕННЯ УКРАЇНСЬКОЇ СИСТЕМИ РЕАГУВАННЯ НА КІБЕРЗАГРОЗИ ТА ПЕРСПЕКТИВИ ЇЇ ЕФЕКТИВНОСТІ НА ОСНОВІ ІНОЗЕМНОГО ДОСВІДУ

3.1 Модель Країн Європейського Союзу щодо системи виявлення кіберзагроз та можливості її імплементації в Україні

Досвід країн пов'язаний з кібербезпекою може значно відрізнятися в залежності від конкретних інституційних, соціальних і економічних структур, в яких мають значення їх різні професійні особливості. Прагнучи «уніфікувати» глибоко вкорінену поведінку, кожна країна може бажає підвищити обізнаність про проблеми у цій сфері і знайти шляхи їх подолання (наприклад, шляхом відкритого і регулярного обговорення цих питань на спільних тренінгах, щоб гарантувати, що вони в кінцевому підсумку не ставлять під загрозу триваючі зусилля, пов'язані з витратами часу і ресурсів, з огляду на зусилля по досягненню стійкості до кібератак).

Зрушення щодо забезпечення 27-ми країн-членів ЄС у сфері розробки спільної стратегії, що стосується кіберзахисту, почалися ще на початку 20 століття. У період 1991-1999 рр., що передував Маастрихтському договору, характер європейського політичного співробітництва було переформульовано із запровадженням Спільної Політики безпеки. Спільна політика безпеки та оборони є життєво-важливим компонентом у службах безпеки ЄС, і вона має свою власну мету: поступове формування загальної оборонної політики Європейського Союзу. Оборонна кіберполітика не могла існувати без законодавчого підґрунтя, яким стала у ЄС перша стратегія безпеки в 2003 році «Безпечна Європа в кращому світі". Таким чином, Стратегія кібербезпеки ЄС поширювалась на оборонні внутрішні сфери держав – правосуддя і внутрішні справи.

Чотири основні цілі міжнародної політики ЄС щодо кіберпростору:

1) свобода та відкритість, де стратегія окреслює бачення та принципи застосування основних цінностей та прав ЄС у кіберпросторі.

2) закони та норми ЄС, адже основні засади забезпечння повинні застосовуватися як у кіберпросторі, так і у фізичному світі.

3) розбудова потенціалу кібербезпеки залучатиме ЄС до міжнародних партнерів та організації.

4) метою має бути сприяння міжнародному співробітництву в ЄС.

Стратегія у подальшому зазнавала чимало змін, проте її прийняття стало рушійним кроком у забезпеченні протидії кіберзагрозам у ЄС. Звичайно, українська Стратегія не є цілковитим відображенням європейської версії, проте, важко не погодитись, що схожість мети та структури нормативних актів очевидна.

Серед регіональної співпраці у галузі кібербезпеки варто відзначити зусилля, докладені Радою Європи та прийняття Конвенції про кіберзлочинність та її додаткового Протоколу. Ця Конвенція є першим і поки що єдиним багатостороннім правовим документом з кіберзлочинності, і це забезпечує основу для встановлення договірних відносин між державами, що її прийняли.

Положення Стратегії щодо електронних комунікацій діяли з 2009 року та встановлювали певні обов'язки щодо постачальників послуг електронного зв'язку. До травня 2011 року ці вимоги повинні були бути накладеними на національному рівні в усіх держав-членах ЄС. Нормативна база щодо захисту даних вимагає від всіх суб'єктів, які контролюють дані (такі як банки та лікарні) встановлення заходів, що дозволяють захистити особисті дані. Крім того, про порушення персональних даних повідомляється національний наглядовий орган влади, задля створення більш контрольованої ситуації.

Варто розглянути основні інститути забезпечення кібербезпеки, адже саме вони та договори ЄС мали сильний вплив на розвиток та процес вироблення та впровадження політики кібербезпеки в ЄС.

Європейська комісія провідна організація у створенні політики кібербезпеки в Європейському Союзі. Комісія – інституційний орган, який представляє інтереси ЄС спільними діями та здійснення наднаціональних повноважень, особливо на території

ЄС. Найважливіший аспект повноважень Комісії, щодо розвитку реагування на загрози кібербезпеки – це її роль «Охоронця договорів», а також повноваження забезпечувати виконання законодавства ЄС. Якщо Комісія вважає, що національний уряд не застосовує правильно законодавство ЄС – вона має повноваження спочатку надіслати офіційний лист із проханням до держави-члена виправити проблему; після чого, в крайньому випадку, Комісія може направити це питання до Європейського суду. Європейський суд, отримавши запит від Комісії, може накладати штрафи, а його рішення є остаточними та обов'язковими для всіх держав-членів. Роль Комісії як виконавця законодавства ЄС надзвичайно важлива у світлі кіберініціативи в галузі безпеки. Основними проблемами, про які повідомляється в директивах щодо боротьби з кіберзлочинністю є існуючі прогалини у впровадженні та застосуванні, особливо з точки зору, рівня національного та координаційного (у випадку інцидентів, що охоплюють кордони).

Союз своїми договорами, законодавством та директивами, а також створеними органами та установами в рамках співпраці у галузі кібербезпеки започаткував: спеціальний підрозділ Європолу – Агентство (Комісія) Європейського Союзу з питань мережевої та інформаційної безпеки (далі – ENISA) та Європейський форум для держав-членів (далі – EFMS).

Отож, ЄС має два основних форуми для співпраці та обміну інформацією щодо кібербезпеки, ENISA та EFMS.

EFMS була створена в 2009 році як рішення політичної ініціативи щодо захисту критичної інформаційної інфраструктури, також вона розглядає питання безпеки та стратегії боротьби з кіберзлочинністю, забезпечуючи платформу для представників національних державних органів для представлення та перегляду питань державної політики.

EFMS не бере участі у технічних та експлуатаційних питаннях, але в цих неофіційних дискусіях може скоріше доповнювати та надавати подальшу підтримку офіційним процесам прийняття рішень. Є обмеження щодо діяльності EFMS, адже, держави-члени, як правило, не діляться важливою інформацією про інциденти, ризики та загрози, що виникають у країнах. Оскільки EFMS є лише форумом для

членів ЄС, а форум діє виключно в межах спілкування та співпраці у сфері кібербезпеки – вимога до держав-членів має мінімальні можливості.

У 2004 р. Європейське Співтовариство заснувало Європейське агентство мережевої та інформаційної безпеки (ENISA), що спрямоване на створення високого рівня мережевої та інформаційної безпеки у ЄС. ENISA надає підтримку та поради Комісії та державам-членам ЄС, з метою покращення загального рівня кібербезпеки. Однак ENISA не має інституційних повноважень і не може втрутитися, щоб вирішити проблеми конкретних країн щодо кіберзагроз. Це незалежна установа, створена для консультативної ролі. Зовнішня оцінка ENISA у 2007 році дійшла висновку, що завдання форуму полягає в його здатності забезпечити незалежну платформу для оцінки проблем та запропонувати їх рішення.

Прикладом суб'єкта знешкодження кіберзагроз на європейському рівні, є й створення Комісією Європейського Центру з боротьби з кіберзлочинністю (далі – ЕСЗ) у складі Європолу (у січні 2013 року). Як координатора в ЄС, його завдання: керувати зростаючою кількістю незаконної діяльності в регіоні. Центр стверджує, що кіберзлочинність є суспільно значимою проблемою, в недавньому звіті вказується, що збитки становлять близько 290 млрд. євро щороку у всьому світі. Конвенція Ради Європи про кіберзлочинність є основою для створення обов'язкового міжнародного партнерства, яке визначає засади, що мають бути прийняті регіональними національними законодавчими органами. Центр призначений для збору експертних знань з питань кіберзлочинності по всій Європі в порядку підтримки аналітичного та оперативного розвитку потенціалу в державах-членах. Центр було створено для боротьби з трьома основними напрямами кіберзлочинності:

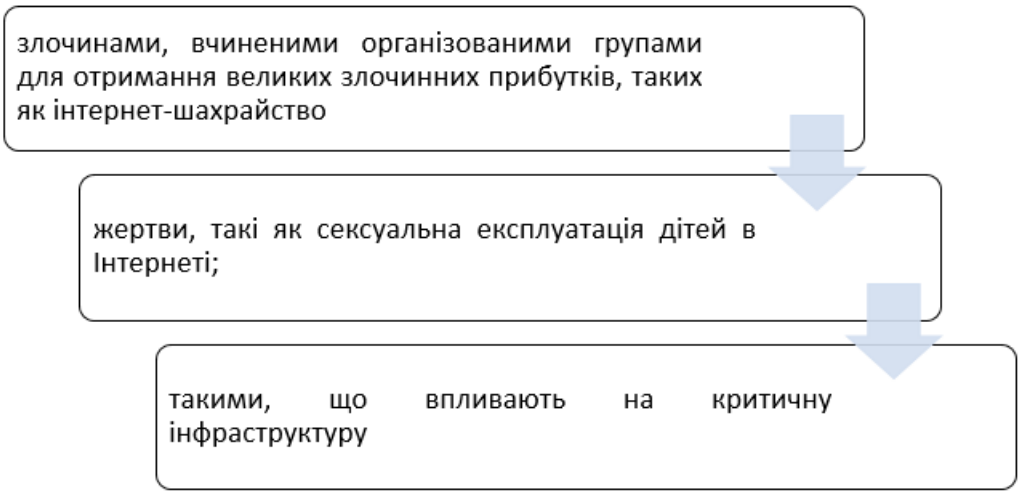

Рисунок 3.1 – Три основні напрямами кіберзлочинності

Ці три установи забезпечують платформу для співпраці у галузі кібербезпеки, щоб покращити обмін інформацією про ризики та загрози – хоча це не передбачає обов'язковості в забезпеченні співпраці та обміну інформацією. Жодна з цих установ не має юридичної компетенції передбачати дії та санкції проти держав-членів, коли вони не бажають співпрацювати.

Хоча обмін інформацією необхідний, його рівень на таких інституціях як ENISA та EC3 на неналежному рівні, оскільки деяким державам-членам не вистачає «кіберстійкості» у внутрішній безпеці. ENISA дає можливість для тісного співробітництва, при цьому Європол підтримує боротьбу з кіберзлочинністю. Зрештою, Європол є саме тим ключовим агентством, яке координує зусилля правоохоронних органів у боротьбі з кіберзлочинністю.

Проте, хоча у ЄС встановлена чітка система нормативних актів у боротьбі з кіберзлочинністю – відповідальність за конкретну кіберзагрозу у відповідній державі несуть внутрішні інституції та органи, до компетенції яких належить як повідомляти координційний центр ЄС про загрозу кібербезпеки так і віднаходити ефективне реагування із забезпеченням стабільного кіберпростору. Кількість підконтрольних держав, наявність однієї економічної зони та єдиного центру реагування потребують ще більшого рівня відповідальності інституцій та

збільшення уваги до реагування на кіберзагрози. У зв'язку з цим виникають наступні проблеми у забезпеченні кіберзахисту країнами-членами ЄС, зокрема:

Таблиця 3.1 – Основні проблеми у забезпеченні кіберзахисту країнами ЄС

Порушення внутрішнього ринку	**Поодинокі інциденти**	**Економічний взаємозв'язок**	**Зловмисне програмне забезпечення та зловмисні атаки**
• спричинені інцидентами в країнах ЄС, це кіберінциденти, що походять з тієї чи іншої країни. Вони не утримується внутрішніми інституціями належним чином - швидко поширюються на інші країни і тим самим підривають функціонування внутрішнього ринку ЄС, що впливає на електронну комерцію та вільний потік капіталу та товарів у ЄС.	• Інциденти, які вирішити можна лише за допомогою співпраці держав ЄС. Ці випадки найчастіше є наслідком людських помилок або зловмисних атак. Людський фактор є надзвичайно важливим, оскільки самі ж люди нехтують правилами безпеки у кіберпросторі. Такі інциденти спричинені недбалістю чи відволіканням уваги, наприклад, особами, які використовують заражені флешки, відкривають небажані електронні листи, розкривають паролі.	• Коли кібератаки впливають на економічних суб'єктів, вони швидко поширюється через економічну систему, що впливає на приватні, державні організації. Державні адміністрації, підприємства та споживачі залежать безпосередньо від використання персональної інформації (Інтернет-послуги). Враховуючи критичну роль мереж і інформаційних систем, можливість нападу або збою системи поширилася б на всі сфери суспільства.	• Шкідливе програмне забезпечення може мутувати, коли воно поширюється, і зловмисники можуть генерувати майже унікальну версію шкідливого програмного забезпечення для кожної потенційної жертви. Лише частка виявлених випадків розкриваються. Відсутність інформації про інциденти заважає здатності реагувати та вживати відповідних заходів на їх реагування.

Проблематика вирішення питання з координацією інституалізації у країнах ЄС полягає також у тому, що учасники державного сектору, які мають справу з кіберінцидентами в ЄС, розширились і тепер включають різноманітні міністерства, відомства та національні регуляторні органи. Ряд існуючих органів, кожен з яких має різні повноваження, ускладнює координаційним інституціям ЄС визначення правильного внутрішнього органу до звернення. Адже, зважаючи на велику кількість структур у кожній державі ЄС, важко визначити її координаційний центр. У випадку визначення координаційного органу нелегко отримати від нього повідомлення про загрозу, яка може мати відношення на рівні міжнаціональному. У цьому випадку потрібно звернути увагу на зміцненні прав людини, захисту даних та

підвищення рівня довіри до цифрового середовища у всіх країнах-членах ЄС. Потрібно також посилити довіру серед правоохоронних органів влади для сприяння обміну даними між ними та співпраці у боротьбі проти кіберзлочинності, забезпечуючи при цьому високий рівень захисту персональних даних осіб у ЄС.

У підсумку розгляду системи кібербезпеки ЄС варто вказати, що існування розробленої системи законодавчих ініціатив, а саме Директив, законів тощо – не є підставою вважати, що усі держави-члени ЄС дотримуються вказаних положень, у тому числі передають дані у випадку серйозних загроз кібербезпеці усього ЄС. Проблематикою також є і недовіра країн-учасниць до інститутів ЄС з захисту кібербезпеки. Тому, кожна держава, у відповідності до розуміння положень керівних органів ЄС, намагається створити органи та установи реагування на кіберзагрози у відповідності до власних міркувань. Система реагування на кіберзагрози у Європейському Союзі не є ідеальною, проте вона є динамічною та розробленою. Враховуючи світовий фактор зміни та динамічності кіберінцидентів Європейський Союз задіює усі необхідні механізми для розробки законодавчого реагування на кіберзагрози. У зв'язку з цим можна виділити спільні особливості для української моделі забезпечення реагування на кіберзагрози у порівнянні з моделлю Європейського Союзу:

– Наявність розроблених нормативних актів.
– Схожість щодо існуючих нормативних актів у сфері кібербезпеки є надзвичайною – як в Україні, так і в Європейському Союзі.

Адже, маючи локальну економічну близькість та у відповідності до інтеграційних процесів, враховуючи бажання України стати учасницею ЄС, стає зрозумілим, що, українські торгівельні процеси неможливо не адаптувати до системи економічного обігу товарів ЄС. Проте, важливо зазначити, що усі передові нормативні ініціативи впроваджуються спочатку саме передовими державами ЄС – до України вони надходять тільки через десятиліття. Якщо в нормативному плані усе простіше: Україною з легкістю приймаються більшість конвенцій, директив та відповідних законів, то на практиці їх імплементація усе ще не відрегульована. До прикладу, закон, пов'язаний з веденням електронного підпису вже пройшов декілька

ітерацій в Україні – розроблено чіткий план його введення, відкриті відповідні адміністративні центри з його надання, проте фактично він не набув широкого застосування в Україні, навіть у період пандемії у 2020 році. На противагу, передові держави Європейського Союзу, у відповідності до своїх нормативних актів у цій сфері, одразу знайшли шляхи реалізації ідеї застосування електронного підпису. Тепер Данія, Швеція, Велика Британія тощо використовують його у судових процедурах, економічних діях та навіть у медицині. У контексті використання електронних підписів варто звернутись саме до Європейського законодавства, адже, воно передбачає схожі норми, проте із різним застосуванням. У той час як різні рівні електронних підписів можуть бути доречними в певних контекстах, тільки кваліфіковані електронні підписи є офіційно визнаними, та мають еквівалентну юридичну силу рукописних підписів по всьому ЄС.

Факт того, що Україна з прийняттям відповідних нормативних актів у цій сфері керується саме європейським законодавством є безспірним. Проте цей чинник є здебільшого позитивним. Адже досвід Європейських країн у застосуванні електронного документообігу є надзвичайно більшим ніж в України. Також фактор прогресивності та досвіду таких передових інформаційно – технічних держав як Фінляндії, Естонії, Німеччини, Нідерландів є надзвичайно важливим для запровадження поняття електронного підпису саме в Україні. А також, варто очікувати, що так, як Закон «Про електронні довірчі послуги» у змісті має досить багато схожих положень із Європейським аналогом, то й їх трактування буде відповідно за європейською практикою [28].

Створення великої кількості державних галузевих органів, пов’язаних із забезпеченням кібербезпеки. Якщо розглядати модель ЄС, то стає зрозумілим, що маючи розвинену систему нормативних актів, у відповідності, були створені координуючі органи, що описані вище. Проте, враховуючи характерні особливості кожної держави та бажання вирішувати питання кібербезпеки на національному рівні у елементах децентралізації від ЄС, виникає проблема із неефективністю звернень органів країнами-членами ЄС. Зрозуміти прояв недовіри неважко, адже кожна держава опікується захистом даних своїх громадян. Проте, саме завдяки

цьому, приймаючи законодавчі акти ЄС, кожна відповідна держава намагається створити власні умови для забезпечення реагування на кіберінциденти. До прикладу, лідером у використанні безпаперового діловодства у Європі стала Фінляндія. Передумовами для переходу країни на електронний документообіг стало те, що дільниці правоохоронних органів, у територіальному розумінні, знаходяться відносно далеко один від одного. Велику роль мав факт світового лідерства країни у впровадженні інформаційних технологій у суспільне життя громадян. Саме тому з 2003 року спеціальна інформаційна платформа правоохоронних органів обслуговує більшість судів у державі. Координатором із діяльності електронного документообігу є Міністерство Юстиції Фінляндії. Перевагою такого швидкого впровадження технологій в роботу стало те, що зараз майже все діловодство здійснюється у електронному вигляді, тому й сканувати документи не потрібно.

У Бельгії Федеральною службою інформаційних технологій та комунікацій «FedIct» у межах організації суттєвих інноваційних проектів у державних структурах, було запроваджено електронні системи: Tax-on-web, Police-on-web, e-Justice. Реалізація електронного обміну документами відбулась ще в 2005 році, саме вона дає змогу наразі здійснювати обмін документами між трьома вищезазначеними системами [29].

Проте, бути цифровим суспільством означає мати схильність до кіберзагроз. Завдяки значним інвестиціям в інфраструктуру кібербезпеки, Естонія тепер має великий досвід у цій галузі, ставши одним з найбільш визнаних і цінних міжнародних експертів з кібербезпеки. Після досвіду Естонії в хвилі кібератак весною 2007 року було розроблено технологію блокчейну, щоб забезпечити цілісність даних, що зберігаються в державних архівах, і захистити їх від внутрішніх загроз. Естонія стала своєрідним «Центром передового досвіду кіберзахисту НАТО» і Європейського агентства інформаційних технологій, адже під час здійснення кібератаки постраждали такі важливі інформаційні державні системи як: сайт Парламенту Естонії, портали міністерств, банківських установ та засобів масової інформації. У зв'язку з цим була створена захищена «центральна інформаційна система – e-File», що надає огляд всіх етапів кримінальних,

адміністративних та цивільних процедур, судових рішень і процесуальних дій, що відкриті для громадськості. Розробка e-File була здійснена урядом Естонії в 2005 році, визнавши необхідність ламати інформаційні бар'єри, які функціонували незалежно один від одного. E-File був впроваджений Центром реєстраторів і інформаційних систем. Як інтегрована система, e-File забезпечує одночасний обмін інформацією між інформаційними системами різних структур: поліцією, прокуратурою, судами, в'язницями, наглядом за умовно-достроковим звільненням, судовими приставами, системою юридичної допомоги, податковим та митним управлінням, державним центром обслуговування акцій, юристами і громадянами. E-File економить час і гроші, так як дані вводяться тільки один раз і зв'язок між сторонами є електронним [30].

Проблема великої кількості установ з кіберзахисту у різних сферах держави є найбільшим викликом сьогодення. Не усім країнам Європейського Союзу вдалось подолати протиріччя різних інституції в небажанні вести партнерство навіть з організації єдиної бази документообігу. Проте, ЄС на стадії, коли обмін досвідом та інформацією між державними органами на достатньо-високому рівні, а тому співпрацю між установами налагоджено. Проте, в Україні дотепер існує проблематика з реагуванням координаційного центру на кіберзагрози, у тому числі з причини недовіри інших державних органів цієї сфери. Адже, саме небажання обмінюватись досвідом, даними та знаннями є найважливішою прогалиною у захисті кіберпростору в Україні.

Чи не найважливішою проблемою як в Україні, так і в державах-членах ЄС є саме не розробка детального плану, що б передбачав протоколи з комунікації та скоординованих дії у кризових ситуаціях. Більшість порушень безпеки йдуть непомітно і не повідомляється через небажання державних установ ділитися інформацією зі страху репутаційної шкоди або відповідальності.

Отож, кількість кібератак та кіберзлочинність зростає в Європі. Ця тенденція має підвищуватись і в майбутньому, враховуючи, що до 2024 року, як очікується, 22,3 мільярда пристроїв у всьому світі будуть підключені до Інтернету. У світлі цих викликів суб'єкти забезпечення кібербезпек ЄС працюють у різних напрямках, щоб:

підвищити кіберстійкість; боротися з кіберзлочинністю; посилити кібердипломатію; посилити кіберзахист; стимулювати дослідження та інновації у цій сфері; захистити критичну інфраструктуру. Рада Європи у свою чергу закликає до посилення стійкості та протидії гібридним загрозам, включаючи дезінформацію [31].

Посилена реакція на кібербезпеку для побудови відкритого та безпечного кіберпростору може створити більшу довіру серед громадян до цифрових інструментів та послуг. Адже, мережеві та інформаційні системи життєво-важливі для полегшення руху товарів, послуг та навіть людей у ЄС. Це означає, що порушення в одній державі-члені може вплинути у сукупності на ЄС. Для створення безпроблемного функціонування внутрішнього ринку існує потреба в стійких та стабільних мережевих та інформаційних системах.

Варто підкреслити, що Україна у тій чи іншій мірі має усі прогалини, що наявні в сфері кіберзахисту Європейського Союзу, та на противагу, усі країни ЄС колись мали такі ж прогалини в імплементації нормативних ініціатив, які наразі має Україна. Модель Європейського Союзу не є ідеальною, враховуючи різний розвиток конкретної держави-учасниці у інформаційно-електронному полі. Проте, на прикладі Фінляндії, Бельгії та Естонії стає зрозумілим, що в України є приклад відповідної системи обміну досвідом та інформацією, яким потрібно скористатись.

3.2 Досвід США в побудові системи виявлення кіберзагроз та його практичне застосування в Україні

За останні кілька років зросло усвідомлення того, що взаємозалежності кіберзахисту не припиняються на державних кордонах, це і сприяло укладенню ряду міжнародних угод і партнерств. Зважаючи на економічну вагу і наявність дуже складних інфраструктурних мереж, варто розглянути досвід США в побудові системи виявлення кіберзагроз.

Особливої важливості питання захисту кіберпростору у США набуло саме після теракту 11 вересня 2001 році. Тоді на практично усі сфери, національної

безпеки США, почало виділятись грунтовне фінансування, а нормативна база у цих сферах зазнала чимало змін. В 2001р. президент Д. Буш, вказав основні загрози національній безпеці США. На другому місті після тероризму стала саме інформаційна війна і вже за нею – розповсюдження зброї масового ураження, засобів його доставки.

Законодавство США у сфері забезпечення інформаційної безпеки складається з основоположних державних законів, федеральних законів та законів штатів, а також державних стратегій та програмних документів у цій сфері. Саме це є передумовою для створення правової основи формування єдиної державної політики в галузі захисту інформації щодо забезпечення інтересів національної безпеки.

Насамперед, варто розглянути основоположні закони США у цій сфері та їх програмні документи [32].

Таблиця 3.2 – Закони США, що регулюють кібербезпеку

Закони США, що регулюють кібербезпеку							
Закон «Про захист дітей у XXI ст.» (Protecting Children in the 21st Century Act)	Закон «Про електронні транзакції» (Uniform Electronic Transactions Act)	Закон «Про інформаційну безпеку» (Federal Information Security Management Act)	Закон «Про недоторканість особистого життя» (Privacy Act)	Закон «Про дослідження та розвиток кібербезпеки» (Cyber Security Research and Development Act)	Закон «Про національну безпеку» (Homeland Security Act)	Закон «Про електронні підписи» (Electronic Signatures in Global and National Commerce Act)	Закон «Про захист дітей в Інтернеті» (Children's Internet Protection Act)

Таблиця 3.3 – Програмні документи США, що регулюють кібербезпеку

Програмні документи США, що регулюють кібербезпеку				
Міжнародна стратегія для кіберпростору «Процвітання, безпека, відкритість умережевому світі» 2011	Кіберстратегія Міністерства оборони від квітня 2015	Міжвідомчий план дій з кібербезпеки систем управління	План дій з посилення кібербезпеки найважливіших об'єктів інфраструктури 2014	План дій з забезпечення кібербезпеки систем енергопостачання

У всьому світі США були в першості розробки політики та стратегії кібербезпеки. Вже у 2003 році уряд видав першу національну стратегію кібербезпеки.

Стратегія захисту кіберпростору 2003 року встановила три стратегічні цілі національної безпеки кіберпростору: запобігання кібератакам на національні критичні інфраструктури; зменшення національної вразливості до кібернападів; мінімізування шкоди та часу на відновлення від кібератак. Варто виділити 5 національних пріоритетів, що були визначені для досягнення цих цілей: забезпечення федеральних комп'ютерних систем та мереж; розвиток системи реагування; створення програми зменшення загроз та вразливостей; ініціювання усвідомлення та навчальної програми з кібербезпеки; розвиток системи міжнародного співробітництва. Проте, до 2010 року у США не було єдиного координаційного інституту кібербезпеки: у кожній сфері суспільства, що мала відношення до кіберзагроз діяли відповідні нормативні акти.

У огляді національної безпеки 2010 р. було визначено, що захист кіберпростіру є одним з п'яти пріоритетних місій національної безпеки. З метою забезпечення національної безпеки, Департамент планування національної безпеки для безпечного кібер-майбутнього у 2011 року надав план дій, який окреслив дві сфери: захист критичної інформаційної інфраструктури та зміцнення кібер-екосистеми. Наступний чотирирічний огляд національної безпеки 2014 року визначив пріоритет інвестицій, які б підтримали національні інтереси та місії, включаючи кіберзахист, та описав ті кіберзагрози, які становлять ризик національних інтересів [33].

Чинна Стратегія Національної Безпеки, прийнята на початку 2015 року, визнає зростаючу небезпеку, яка завдає руйнівних збитків зі сторони кібератак, і повідомляє про намір США зміцнити кібербезпеку критично важливої інфраструктури, збільшити інвестиції в кібернетичні можливості тощо. Як показує досвід, незважаючи на прогресивність США у сфері кіберзахисту, випадки кіберінцидентів мають надзвичайно великий спектр руйнівних наслідків. Так, коли в травні 2021 року хакерами було захоплено мережу, що обслуговувала нафто-газо

проводи у США – було потрачено багато часу, сил та кошт для відновлення роботи на підприємстві, а в деяких штатах навіть було запроваджено надзвичайну ситуацію.

Оновлена стратегія кібербезпеки врахувує російську загрозу та називає Росію і Китай головною загрозою національним інтересам США (у попередній редакції стратегії від 2011 р. російська загроза в кіберпросторі зовсім не згадувалася). Проте, оновлена версія не є абсолютно новим документом, хоча і вдвічі по обсягам збільшена (в порівнянні з документом від 2011р.).

Також, з метою реалізації безпеки у кіберпросторі у світі, у 2011 році Білий дім оприлюднив Міжнародну стратегію кіберпростору, яка відображає підхід США до взаємодії з міжнародними партнерами та інформування про національні пріоритети. Загальна мета Стратегії як полягає в наступному: США працюватимуть на міжнародному рівні задля сприяння відкритості, сумісності, безпеці та надійності інформаційно-комунікаційної інфраструктури, що підтримує міжнародну торгівлю, зміцнює міжнародну безпеку та сприяє свободі слова та інноваціям у сфері [34].

Розглянемо краще суб'єктів реагування на кіберзагрози у США та їх основні інструменти реагування:

Рисунок 3.2 – Основні суб'єкти реагування на загрози кібербезпеки США

Координатор органів виконавчої влади з питань кібербезпеки, який виступає в якості помічника Президента. Функції з контролю та координації імплементації національної стратегії кібербезпеки, політики та згаданих планів дій органами виконавчої влади виконують Міністерство національної безпеки та Міністерство Оборони.

Національне Управління кібербезпеки США (далі – NCSD) створено в 2003 р. NCSD має співпрацювати з приватним сектором, урядом, військовими та зацікавленими сторонами для проведення оцінок ризиків та пом'якшення вразливості та загроз активам та діяльності інформаційних технологій. NCSD також забезпечує аналіз кіберзагроз та вразливостей, раннє попередження та допомогу у реагуванні на інциденти для представників державного та приватного сектору.

Для захисту кіберінфраструктури NCSD визначила дві загальні цілі: створення та підтримка ефективної національної системи реагування на кіберпростір та впровадження програми управління кіберризиками для захисту критичної інфраструктури.

NCSD фінансується за рахунок наступних трьох програм, проектів та заходів, прийнятих Конгресом: Команда підготовки США до комп'ютерних надзвичайних ситуацій (далі – US-CERT), Стратегічні ініціативи та інформаційно-пропагандистські програми:

US-CERT використовує технічні компетенції у федеральних мережах та центрах аналізу загроз для розвитку знань та практики управління знаннями. US-CERT забезпечує єдиного підзвітного координатора для підтримки федеральних зацікавлених сторін у процесі прийняття ключових оперативних рішень та рішень щодо реалізації та захисту цивільних мереж Федеральної виконавчої влади. Це робиться за допомогою цілісного підходу, що дозволяє федеральним зацікавленим сторонам вирішувати проблеми кібербезпеки таким чином, щоб максимізувати цінність, мінімізуючи ризики, пов'язані з інвестиціями в технологію та безпеку. Крім того, US-CERT аналізує загрози та вразливості, поширює інформацію про попередження про кіберзагрози та координує роботу з партнерами та замовниками

для досягнення спільної ситуаційної обізнаності, пов'язаної з кіберінфраструктурою країни. Фонди US-CERT також підтримують розробку Національної система захисту кібербезпеки (NCPS) EINSTEIN.

Національний центр кібербезпеки є складовою частиною бюджету US-CERT. Його функції, у відповідності до повноважень, наданих президентом: інтеграція місій, співпраця та координація, обізнаність про ситуацію та реагування на кіберінциденти, аналіз та звітування, управління знаннями, розробка та управління технологіями, кожна з яких підтримується розробкою програм та можливостей центру.

Стратегічні ініціативи дозволяють NCSD створити механізми для федеральних партнерів застосовувати стандартизовані інструменти та послуги із зниженою вартістю, відкриваючи шлях до середовища співпраці, яке дозволяє обмінюватися найкращими практиками та загальними проблемами та недоліками безпеки.

Інформаційно-пропагандистська діяльність сприяє можливостям залучення інвестицій в кібербезпеку державних та приватних партнерів у галузі. Ця інституція заохочує поінформованість про кібербезпеку серед широких кіл громадськості та серед ключових спільнот, підтримує відносини з урядовими фахівцями з кібербезпеки для обміну інформацією про ініціативи з кібербезпеки та розвиває партнерські відносини для сприяння співпраці з питань кібербезпеки. Інформаційно-просвітницька робота та програми дозволяють врядування та допомогу у визначенні напряму політики та встановлюють вимоги до ресурсів.

Варто звернути увагу на Національну систему захисту кібербезпеки, адже саме ця система є уявленням роботи усіх суб'єктів забезпечення реагування кіберзагрози. У зв'язку з великою кількістю адміністративних одиниць у США було надзвичайно важко дійти до створення єдиної такої системи.

Національна система захисту кібербезпеки (далі – NCPS) – це інтегрована система, що надає цілий ряд можливостей, таких як виявлення вторгнень, аналітика, обмін інформацією та запобігання вторгненню. Ці можливості забезпечують технологічну основу, яка дозволяє Агентству з питань кібербезпеки та безпеки

інфраструктури (далі – CISA) захищати інформаційну інфраструктуру агентств Федеральної цивільної виконавчої влади від передових кіберзагроз.

CISA – це автономне федеральне агентство США, оперативний компонент під наглядом Департаменту національної безпеки, створене у 2018 році за ініціативи президента Трампа. Роль CISA полягає у вдосконаленні кібербезпеки на всіх рівнях управління, координації програм кібербезпеки із штатами США та вдосконаленні урядового захисту кібербезпеки від приватних та національних державних хакерів. NCPS виконує обов'язки CISA [35].

Можливості NCPS охоплюють чотири широкі технологічні галузі.

1) Виявлення вторгнень: можливість виявлення вторгнень NCPS, що надається через EINSTEIN 1 та EINSTEIN 2, є пасивною сенсорною сіткою на основі підписів, яка контролює мережевий трафік на предмет зловмисної діяльності до та з підрозділів та установ. Ця можливість дозволяє ідентифікувати потенційну шкідливу діяльність та трафік, що надходить або виходить із федеральних мереж, використовуючи технологію виявлення вторгнень на основі підписів.

2) Аналітика: NCPS Analytics надає аналітикам кібербезпеки CISA можливість збирати та аналізувати інформацію про кібердіяльність у багатьох сферах безпеки та інформувати державні органи, партнерів приватного сектору, власників інфраструктури та операторів, а також громадськість про поточні та потенційні загрози та вразливості в галузі кібербезпеки. Можливість Analytics включає рішення щодо захисту інформації та управління подіями (SIEM) для NCPS. Рішення SIEM спрощує кібер-аналіз шляхом: агрегування подібних подій, зменшуючи тим самим дублювання; співвіднесення пов'язаних подій, які в іншому випадку можуть залишитися непоміченими; і забезпечуючи можливості візуалізації, тим самим полегшуючи бачення стосунків. Функція Analytics також включає інструменти захоплення пакетів, лабораторію аналізу шкідливого програмного забезпечення, засоби візуалізації потоку.

3) Обмін інформацією: функції обміну інформацією NCPS створюють гнучкий набір можливостей, реалізованих на різних рівнях класифікації, що дозволяють швидко обмінюватися інформацією про кіберзагрози та кіберінциденти

між аналітиками кібербезпеки CISA та їх партнерами з кібербезпеки. Метою можливості обміну інформацією є: (1) запобігання інцидентам кібербезпеки через покращений обмін інформацією про загрози; (2) скоротити час реагування на інциденти завдяки вдосконаленим можливостям координації та співпраці; (3) підвищення ефективності завдяки більш автоматизованому обміну інформацією за допомогою розкриття можливостей аналізу. Обмін інформацією забезпечує безпечне середовище для обміну інформацією про кібербезпеку з широким спектром операцій з безпеки та центрами обміну інформацією у федеральних, штатних, місцевих, приватних та міжнародних кордонах.

4) Запобігання проникненню: до можливостей запобігання вторгненню NCPS відноситься EINSTEIN 3 (діє з 2012 р.), забезпечуючи активні захисні можливості мережі та можливість запобігання та обмеження зловмисних дій від проникнення у федеральні мережі та системи. Завданням можливості запобігання вторгненню NCPS є виявлення та характеристика зловмисного мережевого трафіку для покращення аналізу кібербезпеки, ситуаційної обізнаності та реагування на безпеку [35].

Якщо розглядати США у полі розвитку кібербезпеки, то безспірно вона досягла суттєвих успіхів в розвитку та запровадженні електронного підпису при засвідченні правдивості документа. Електронні підписи являють собою одну з найбільших можливостей для прискорення переходу до використання цифрових бізнес-рішень. У 2000 році уряд США прийняв Акт ESIGN (Електронні підписи в глобальній і національній торгівлі), щоб полегшити прийняття електронних підписів, відкриваючи нову еру раціоналізації документів. На додаток до закону ESIGN Комісія по уніфікованому праву розробила UETA (Закон про однакові електронні операції) в 1999 році, щоб забезпечити правову основу для використання електронних підписів в кожному штаті. UETA була прийнята в 47 штатах, окрузі Колумбія, Пуерто-Ріко і Віргінських островах США. Хоча Іллінойс, Нью-Йорк і Вашингтон не прийняли UETA, вони впровадили аналогічні закони, що підтверджують електронні підписи. Ці закони надають електронним підписам такий же правовий статус, що і для традиційних підписів та печаток з мокрим чорнилом в

США. Це дає змогу: в електронному вигляді представляти угоди як доказ в суді; запобігати відмові в дійсності або можливості застосування документа з електронним підписом виключно тому, що він знаходиться в електронній формі.

Отож, на основі проведеного аналізу діяльності США як в нормативному так і в практичному полі стає зрозуміло, що переваги шляху розвитку США у даній сфері є безспірними й одними з найпередовіших у світі. У зв'язку з численими актами терактів США, у історичному контексті, розвинулось підгрунття для реалізації дієвої системи захисту не тільки від кібератак, а і для усіх сфер безпеки країни. Зважаючи на стрімкий розвиток кібербезпеки починаючи з 2003 року, США досягла найвищих показників захисту кібербезпеки у світі. Проте, зважаючи на стрімкі навчання та розвиток цієї сфері – зміна відбулась не тільки в позитивному руслі. Адже, саме США є тією країною, що змушена постійно реагувати на чисельні кібертакаки.

За останні 35 років у США сформувалася чітка система забезпечення інформаційної безпеки, яка характеризується поступовими тенденціями та, разом з тим, кардинальними заходами. Тож американський досвід державної політики в сфері інформаційної безпеки являється важливим для української зовнішньої та внутрішньої політики.

Отож, зараз США стала передовою державою у реалізації дієвої системи кіберзахисту. Держава намагається ділитись набутим досвідом як в законодавчому так і в практичному плані (забезпечуючи Україну передовими технологіями та здійснюючи навчання працівників у сфері кіберзахисту).

Треба все ж зазначити, що хоча Україна є одним з лідерів у світі з підготовки висококваліфікованих ІТ-спеціалістів і одним з основних постачальників «мізків» відповідного напряму за кордон, слід констатувати існуючу залежність України від американського програмного продукту, що можна спостерігати в комп'ютерних засобах майже кожної державної установи та окремих громадян. Отже, для забезпечення національної безпеки України необхідно спрямувати зусилля на створення власних конкурентноздатних ІТ-технологій, та повернення наших фахівців «додому» [36].

У свою чергу США мають величезний досвід у сфері впровадження інформаційних технологій в діяльність держави з усіх напрямів. Особливо важливим, в умовах військового захисту Україною своїх територій у відповідь на збройну агресію іноземної держави, є американський досвід використання інформаційних технологій для створення систем зв'язку та військового управління, а також високоточного озброєння.

Надзвичайно цінним для українських спеціалістів має бути саме аналіз дієвих американських систем, таких як CISA, US-CERT тощо. Зважаючи на чітку розробку та сферу розподілу повноважень у цих системах – українським працівникам сфери кібербезпеки є що запозичити. Інформаційну безпеку можна без перебільшення назвати одним з перспективних напрямів взаємовигідного співробітництва між Україною та США.

Висновок до розділу 3

Одним з найбільш яскравих проявів глобалізації є інтернаціоналізація ланцюжків обміну інформацією у сфері кіберзахисту. Особливо актуальною ця тема є в розумінні створення єдиного міжнаціонального підходу до оперативного виявлення та знешкодження потенційних кіберзагроз. Адже, даного роду загрози є питанням не однієї конкретної держави, а кіберпростір та його загрози не мають чітких державних кордонів. Тому, у разі кризи кібербезпеки можливо, що надзвичайна ситуація, яка розгортається в одній країні, може бути вирішена тільки в іншій країні, у якій, в свою чергу, не порушена кібербезпека безпосередньо. У зв'язку з цим виникає потреба в розробці як потенційний сценаріїв кіберзагрозам, так і їх протидії, які б ілюстрували необхідність міцного включення міжнародного співробітництва в стратегії країн у цій сфері.

ЄС створив установи для реагування на кіберзлочини, кожна з яких має свій мандат і має надавати інституційну відповідь. Однак, компетенція органів кіберзахисту починається з міжнародних домовленостей та договорів, які й надають

установам держав ЄС, реалізовувати рамки та повноваження щодо реагування на кіберзлочини. Проте, якщо розглядати, на конкретних прикладах, систему реагування на кіберінциденти у різних державах ЄС, стає зрозумілим, що зважаючи на єдині запозичнені стандарти ЄС, кожна держава віднайшла свій шлях розвитку у цій сфері.

У свою чергу США мають величезний досвід у сфері впровадження інформаційних технологій в діяльність держави з усіх напрямів. Особливо важливим, в умовах військового захисту Україною своїх територій у відповідь на збройну агресію іноземної держави, є американський досвід використання інформаційних технологій для створення систем зв'язку та військового управління, а також високоточного озброєння. Варто вказати про слушне запозичення, яке потрібно було б використати в шляху покращення кібербезпеки в Україні, а саме – посилення відповідальності за комп'ютерні злочини й зобов'язання інтернет-провайдерів надавати інформацію про клієнтів за вимогою правоохоронних органів.

Стандарти кібербезпеки мали велике значення в сучасному бізнесі, керованому технологіями. Щоб максимізувати свій прибуток, корпорації використовують технології, керуючи більшістю своїх операцій через Інтернет. Оскільки існує велика кількість ризиків, пов'язаних з операціями в мережі Інтернет, такі операції повинні бути захищені вичерпними та розширеними нормативними актами. Усі існуючі норми щодо кібербезпеки охоплюють різні аспекти господарських операцій і часто різняться залежно від регіону або країни, в якій працює бізнес. Через відмінності в суспільстві, інфраструктурі та цінностях країни один всеосяжний стандарт кібербезпеки не є оптимальним для зменшення ризиків. Хоча стандарти США забезпечують основу для діяльності, Європейський Союз створив більш пристосований регламент для підприємств, що працюють спеціально в межах ЄС.

Отож, поле кібербезпеки не розмежовується кордонами, у зв'язку з цим варто виділити основоположні світові проблеми даної сфери захисту. Серед основних загроз національним кіберпросторам стратегії більшості країн визначають:

- Кібершпигунство та військові дії, які здійснюються за підтримки або з відома держави. Усі технологічно розвинені держави та корпорації стають об’єктом кібершпигнуства, яке має на меті заволодіння державними або промисловими таємницями, персональними даними або іншою цінною інформацією.
- Використання Інтернету у терористичних цілях. Терористичні угрупування використовують Інтернет з метою пропаганди, збору коштів і вербування громадян.
- Кіберзлочинність: викрадення персональних даних та відмивання коштів, отриманих незаконним шляхом. Зловмисники продають інформацію про номери банківських карток, паролі від комп’ютерних серверів та шкідливе ПЗ. Відповідно, національні законодавства країн, як правило, регулюють питання:
    - Захисту персональних даних (Нідерланди, Естонія, Швеція, Фінляндія, Іспанія);
    - Захисту електронної комерції та безпеки електронних транзакцій та платіжних інструментів (США, Польща, Естонія, Італія);
    - Захисту дітей (США);
    - Захисту важливих об’єктів інфраструктури та інформаційних систем (Франція).

Поточні рівні міжнародного співробітництва по кіберзахисту істотно розрізняються в залежності від потреб і їх сприйняття країною. Вони можуть бути більш-менш широким за обсягом в залежності від конкретного типу діючих домовленостей, близькості країн і рівнів економічної інтеграції.

При розгляді планів нових або посилених транскордонних партнерств, країнам слід розглянути ряд особливостей: зусилля з міжнародного співробітництва зазвичай зосереджені на обміні інформацією, регулюванні криз та спільних навчаннях.

ВИСНОВКИ

Вплив глобалізації на кіберпростір, що проявляється в розповсюдженні кіберзлочинності, кібертероризму та експансії інформації, потребує надійного захисту, а забезпечення кібербезпеки України стає невід'ємною складовою та фактором національної безпеки. Доведено, що встановлення сформованої системи інформаційної безпеки держави в умовах глобалізації та розвитку інформаційних технологій та телекомунікаційних систем вимагає з'ясування системних основ та основних принципів системи забезпечення кібербезпеки як найважливішої складової інформаційної безпеки України.

В умовах глобалізації, інтелектуалізації злочинності, охоплення інформатизацією всіх суспільних відносин, міжнародна спільнота усвідомлює необхідність удосконалення чинних та розробки уніфікованих нормативно-правових актів у сфері регулювання як державної так і міжнародної інформаційної безпеки.

Методологічною основою вирішення цього питання є системний підхід, що дозволяє враховувати не лише певні типи інформаційних загроз, а й багатофункціональність та багатовимірність предметного поля інформаційної безпеки при розумінні інформаційної безпеки як системного явища. Доведено, що на основі виявлення об'єктів, що потребують захисту, розгалуження функцій та секторів відповідальності державних та приватних структур, доцільно розмежовувати предметні галузі інформації та кібербезпеки. Визначення інформаційної безпеки в широкому розумінні цього поняття, як сфери національної безпеки, що характеризується всебічною (правовою, економічною, технологічною та організаційною) безпекою встановленого функціонування інформаційного простору, захистом інформації, інформаційно-технологічних та сформульовано інтереси безпеки держави та суспільства, інформацію та права і свободи людини – має найважливіше значення у подоланні прогалин системи реагування суб'єктів на кіберзагрози.

Суб'єкти системи забезпечення кібернетичної безпеки перебувають у тісній взаємодії між собою, але при цьому кожен із них спеціалізується на вирішенні конкретних завдань відповідно до своєї предметної компетентності та в межах повноважень, визначених законодавством. Незважаючи на це, загрози кібербезпеці актуалізуються через дію таких чинників, як недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки.

Розробка дієвої стратегії обміну інформації, пов'язаної з виявленням кіберзагроз має включати в себе наступні елементи:

1) заповнення прогалин в регулюванні забезпечення кібербезпеки;

2) систематизування дії всіх суб'єктів забезпечення кібербезпеки з метою підвищення її рівня;

3) формулювання моделі загроз кібербезпеки.

Посилена реакція на кібербезпеку для побудови відкритого та безпечного кіберпростору може створити більшу довіру серед громадян до цифрових інструментів та послуг.

Варто підкреслити, що Україна у тій чи іншій мірі має усі прогалини, що наявні в сфері кіберзахисту Європейського Союзу, та на противагу, усі країни ЄС колись мали такі ж прогалини в імплементації нормативних ініціатив, які наразі має Україна. Модель Європейського Союзу не є ідеальною, враховуючи різний розвиток конкретної держави-учасниці у інформаційно-електронному полі. Проте, на прикладі Фінляндії, Бельгії та Естонії стає зрозумілим, що в України є приклад відповідної системи обміну досвідом та інформацією, яким потрібно скористатись.

Треба все ж зазначити, що хоча Україна є одним з лідерів у світі з підготовки висококваліфікованих ІТ-спеціалістів і одним з основних постачальників «мізків» відповідного напряму за кордон, слід констатувати існуючу залежність України від американського програмного продукту, що можна спостерігати в комп'ютерних засобах майже кожної державної установи та окремих громадян. Отже, для забезпечення національної безпеки України необхідно спрямувати зусилля на створення власних конкурентноздатних ІТ-технологій, та повернення наших фахівців «додому».

У свою чергу США мають величезний досвід у сфері впровадження інформаційних технологій в діяльність держави з усіх напрямів. Особливо важливим, в умовах військового захисту Україною своїх територій у відповідь на збройну агресію іноземної держави, є американський досвід використання інформаційних технологій для створення систем зв'язку та військового управління, а також високоточного озброєння.

Варто, вказати і на роль систем та програм, що використовуються суб'єктами реагування на кіберзагрози. Адже, саме це є найважливішим аспектом, у сфері розробки систем, на шляху розвитку українського кіберпростору. Надзвичайно цінним для українських спеціалістів має бути саме аналіз дієвих американських систем, таких як CISA, US-CERT тощо. Адже, зважаючи на чітку розробку та сферу розподілу повноважень у цих системах – українським працівникам сфери кібербезпеки є що запозичити.

Аналізуючи тенденції розвитку щодо міжнародної співпраці в сфері обміну досвідом у боротьбі з кіберзлочинами, стає зрозумілим, що нашій державі потрібно зосереджувати розвиток системи реагування на кіберінциденти в наступних напрямках:

1) завершити створення чіткої робочої системи координації;

2) використати досвід та практики ЄС і НАТО та США у створенні національної системи сертифікації з кібербезпеки, широкомасштабного плану-відповіді на кіберінциденти і кризи;

3) поглиблювати державно-приватне партнерство і посилювати дослідження у цій сфері;

4) нарощувати навчальні зв'язки України у сфері кібербезпеки за сприяння Трастового фонду НАТО;

5) розробити та реалізувати план реагування інциденти в кіберпросторі;

6) розробити механізм розподілення ризиків через використання захищених хмарних сервісів задля мінімізації можливих втрат у разі кібернападу на інформаційні бази органів державної влади;

7) розробити систему навчань та мотивацій для працівників кібербезпеки та кібероборони.

У зв’язку з розвитком загроз кібербезпеки, та виходячи з їх суб’єктів, необхідно виділити основні завдання для відповідних органів та структур у цій сфері:

– Захищати суверенітет кіберпростору
– Захищати національну безпеку
– Захищати інформаційну інфраструктуру
– Створити «безпечну» інтернет-культуру
– Боротись з кіберзлочинністю, шпигунством та тероризмом
– Посилити правову базу кібербезпеки
– Підвищити можливості захисту кіберпростору
– Покращити міжнародне співробітництво

З огляду діяльність, що здійснюється у віртуальному просторі, легко зливається з фізичним світом. Кіберзловмисники можуть порушити такі важливі інфраструктури, як фінансові системи та системи управління повітряним рухом, створюючи наслідки, що схожі на теракти; розкриття державної та військової таємниці; вербування злочинців та інших осіб для здійснення фізичної терористичної діяльності. З огляду на зростаючі загрози, кіберготовність систем безпеки постійно випробовується. Хоча системи безпеки все дорожчі, запуск кібератак є відносно економічним.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Піскорська Г. А. Сучасні виклики і загрози в кіберпросторі: формування механізму міжнародної інформаційної безпеки / Г. А. Піскорська, Н. Л. Яковенко // Міжнародні відносини. Серія «Політичні науки». – 2018. – № 18–19 [Електронний ресурс]. – Режим доступу : http://journals. iir. kiev.ua/index.php/pol_n/article/view/3389.

2. Діордіца І. Поняття і зміст кіберзагроз на сучасному етапі / І. Діордіца // Адміністративне право і процес. – 2017. – № 4. – С. 99–107. http://pgp-journal.kiev.ua/archive/2017/4/22.pdf

3. Стаття «Комплаєнс та кібербезпека. Загроза існує!» від 28.08.2020 [Електронний ресурс] – Режим доступу: https://yur-gazeta.com/dumka-eksperta/komplaens-ta-kiberbezpeka-zagroza-isnue-vona-realna.html

4. Стаття «7 Types of Cyber Security Threats» від 21.02.2020 [Електронний ресурс] – Режим доступу: https://onlinedegrees.und.edu/blog/types-of-cyber-security-threats/

5. Закон України «Про основні засади забезпечення кібербезпеки України» [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: http://zakon0.rada.gov.ua/laws/show/2163-19

6. Стаття «До Єдиного дня інформування населення» від 13.10.2016 [Електронний ресурс] – Режим доступу: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiBkPanlcfwAhW9g_0HHareB4gQFjAAegQIAxAD&url=http%3A%2F%2Fkr.gov.ua%2Fua%2Fosxfile%2Fpg%2F201117468312558_s_1o%2F1440876074.doc&usg=AOvVaw2sL3RGmE9kbcq_6EGA1DFG

7. Конституції України [Електронний ресурс]. – 1996. – Режим доступу до ресурсу: http://zakon3.rada.gov.ua/laws/show/254к/96-вр.

8. Договір про Європейський Союз, в редакції від 13.12.2007// [Електронний ресурс] // – Режим доступу: https://zakon.rada.gov.ua /laws/show/994_029

9. Конвенція «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» [Електронний ресурс]. – 2010. – Режим доступу до ресурсу: http://zakon0.rada.gov.ua/laws/show/994_326

10. Закон України «Про інформацію» [Електронний ресурс]. – 1992 – Режим доступу до ресурсу: http://zakon3.rada.gov.ua/laws/show/2657-12

11. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [Електронний ресурс]. – 1994. – Режим доступу до ресурсу: http://zakon5.rada.gov.ua/laws/show/80/94-вр

12. Закон України «Про захист персональних даних» [Електронний ресурс]. – 2010. – Режим доступу до ресурсу: http://zakon0.rada.gov.ua/laws/show/2297-17

13. Закон України «Про основні засади забезпечення кібербезпеки України» [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: http://zakon0.rada.gov.ua/laws/show/2163-19

14. Закон України «Про національну безпеку України» [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2469-19#Text

15. Закон України «Про електронні довірчі послуги» [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: http://zakon5.rada.gov.ua/laws/show/2155-19

16. Закон України «Про Доктрину інформаційної безпеки України» [Електронний ресурс]. – 2009. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/514/2009#Text

17. Статистика Генеральної прокуратури [Електронний ресурс]. – 2016 – 2018. – Режим доступу до ресурсу: https://www.gp.gov.ua/ua/stat.html

18. Єдиний державний реєстр судових рішень [Електронний ресурс]. – 2016 – 2018. – Режим доступу до ресурсу: http://reyestr.court.gov.ua

19. Указ Президента України №96/2016 Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/96/2016#Text

20. Закон України «Про Раду національної безпеки і оборони України» [Електронний ресурс]. – 1998. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text

21. Стаття «Оцінка стану комунікації, кординації та взаємодії між суб'єктами національної системи кібербезпеки» від 01.02.2021 [Електронний ресурс] // – Режим доступу: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/analityka.pdf

22. Стаття «Система забезпечення кібербезпеки:сутність та призначення» від 01.07.2017 [Електронний ресурс] – Режим доступу: http://www.pgp-journal.kiev.ua/archive/2017/7/24.pdf

23. Стаття Computer Security Institute «Причини порушення захисту в комп'ютерних програмах» від 13.05.2019 [Електронний ресурс] – Режим доступу: https://www.csoonline.com/article/2116316/computer-security-institute.html

24. Стаття «Співробітництво Україна – ЄС – НАТО з протидії гібридним загрозам у кіберсфері» від 06.02.2019 [Електронний ресурс] – Режим доступу: https://www.kas.de/documents/270026/4625039/UA+Ukraine+-+EU+-+NATO+cooperation+to+counter+hybrid+threats+in+cyber+sphere.pdf/c970b17f-d9db-aba3-7990-bb4441a3e041?version=1.0&t=1554283399244

25. Стаття «Національний координаційний центр кібербезпеки посилює співпрацю із міжнародними виробниками кібер-технологій» від 07.08.2020 [Електронний ресурс] – Режим доступу: https://www.rnbo.gov.ua/ua/Diialnist/4658.html

26. Стаття «Україна посіла 25 місце у міжнародному рейтингу з кібербезпеки» від 10.12.2020 [Електронний ресурс] – Режим доступу: https://www.kmu.gov.ua/news/ukrayina-posila-25-misce-u-mizhnarodnomu-rejtingu-z-kiberbezpeki]

27. Забара І. М. Міжнародна інформаційна безпека: сучасні концепції в міжнародному праві [Електронний ресурс] / І. М. Забара // Теорія і практика правознавства. – 2013. – Вип. № 2. – Режим доступу : http://nbuv.gov.ua/j-pdf/tipp_2013_2_77.pdf

28. Стаття «Електронна ідентифікація захистить персональні дані українців» від 21.05.2018 [Електронний ресурс] – Режим доступу: http://uz.ligazakon.ua/ua/magazine_article/EA011023

29. Офіційний веб-портал сукупності нормативних актів ради Європи // [Електронний ресурс] – Режим доступу: https://www.coe.int/en/web/conventions/full-list

30. Стаття «Слідувати цифрі закону» від 21.05.2018 [Електронний ресурс] – Режим доступу: http://yur-gazeta.com/publications/events/sliduvati-cifri-zakonu.html

31. Стаття «Кібербезпека: вразливі моменти» від 14.05.2019 [Електронний ресурс] – Режим доступу: https://yur-gazeta.com/publications/practice/inshe/kiberbezpeka-vrazlivi-momenti.html

32. Стаття «Законодавство та стратегії у сфері кібербезпеки країн європейського союзу сша, канади та інших» від 11.08.2019 [Електронний ресурс] – Режим доступу: http://euinfocenter.rada.gov.ua/uploads/documents/28982.pdf

33. Стаття «National Cyber Security Division» від 24.04.2021 [Електронний ресурс] – Режим доступу: https://en.wikipedia.org/wiki/National_Cyber_Security_Division

34. International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World [Електронний ресурс]. – Washington, 2011. Режим доступу: https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

35. National cybersecurity protection system [Електронний ресурс] – Режим доступу: https://www.cisa.gov/national-cybersecurity-protection-system-ncps#:~:text=The%20National%20Cybersecurity%20Protection%20System,information%20sharing%2C%20and%20intrusion%20prevention.

36. Стаття «Інформаційна безпека США: законодавче регулювання та перспективи співпраці для України» від 15.09.2017 [Електронний ресурс] – Режим доступу: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2988:informatsij

na-bezpeka-ssha-zakonodavche-regulyuvannya-ta-perspektivi-spivpratsi-dlya-ukrajini&catid=8&Itemid=350