Національний університет водного господарства та природокористування
Навчально-науковий інститут економіки та менеджменту
Кафедра менеджменту та публічного врядування

Пояснювальна записка
до кваліфікаційної магістерської роботи

магістр
(рівень вищої освіти)

на тему:

УДОСКОНАЛЕННЯ ДЕРЖАВНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В УКРАЇНІ

Виконав: студент 6 курсу, групи ПУА 61-м спеціальності 281 «Публічне управління та адміністрування»
Рясний Микола Володимирович

Керівник: к.політ.наук., доцент кафедри менеджменту та публічного врядування
Шинкарук Антон Любомирович

Рецензент: к.п.н., доцент кафедри менеджменту та публічного врядування
Мартинюк Галина Федорівна

Рівне – 2023

Форма № Н-9.01

Національний університет водного господарства
та природокористування
(повне найменування вищого навчального закладу)

Навчально-науковий інститут економіки та менеджменту
Кафедра менеджменту та публічного врядування
Рівень вищої освіти магістр
Спеціальність 281 «Публічне управління та адміністрування»
(шифр і назва)

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
менеджменту та публічного
врядування
_____ (Л.Х. Тихончук)
“__”_____ 2023 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
Рясному Миколі Володимировичу
(прізвище, ім’я, по батькові)

1. **Тема роботи:** Удосконалення державного управління інформаційною безпекою в Україні.
Керівник роботи: к.політ.наук, доцент Шинкарук А.Л.
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від “ 9 ” листопада _2023 року С №-1323
2. Строк подання студентом роботи «10» грудня» 2023 року
3. Вихідні дані до роботи: нормативно-правові акти, розпорядження органів виконавчої влади та місцевого самоврядування, статистичні дані Державної служби статистики, підручники, посібники, монографії, періодичні видання.
4. **Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)** 1. Теоретичні аспекти державного управління інформаційною безпекою в Україні 2. Аналіз державного управління інформаційною безпекою в Україні 3. Шляхи удосконалення державного управління інформаційною безпекою в Україні
5. Перелік графічного матеріалу (з точним зазначенням обов’язкових креслень) 1.Мета, завдання, предмет та об’єкт дослідження. 2. Складові державного управління інформаційною безпекою. 3.Історія створення держспецзв’язку. 4. Зарубіжний досвід державного управління інформаційною безпекою. 5. Кількість показників зібраних та опрацьованих даних по інформаційні безпеці. 6. Типи подій в інформаційній безпеці 7. Динаміка видатків на «Адміністрація Державної служби спеціального зв`язку та захисту інформації України» за 2019-2023 рік. 8. Видатки за напрямком «Головне управління урядового фельд’єгерського зв’язку Державної служби спеціального

зв'язку та захисту інформації України» за 2019-2023 роки. 9. *Правила інформаційної безпеки під час війни*. 10. *Пріоритети формування політики кібербезпеки в Україні*. 11. Стратегія покращення державного управління інформаційною безпекою в Україні

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Розділ 1	Шинкарук А.Л., доцент	11.11.2023	
Розділ 2	Шинкарук А.Л., доцент	18.11.2023	
Розділ 3	Шинкарук А.Л., доцент	02.12.2023	

7. Дата видачі завдання « 11» листопада 2023 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів	Примітка
1.	Вступ Розділ 1. Теоретичний розділ	11.11.23- 17.11.23	
2.	Розділ 2. Аналітичний розділ	18.11.23- 01.12.23	
3.	Розділ 3. Проектування, обґрунтування, оптимальні рішення, їх впровадження	02.12.23- 08.12.23	
4.	Перевірка випускної кваліфікаційної роботи на наявність текстових збігів, оформлення презентації, документів та підготовка до захисту	09.12.23- 15.12.23	

Студент

_____ М.В.Рясний
(підпис) (прізвище та ініціали)

Керівник магістерської роботи

_____ А.Л. Шинкарук
(підпис) (прізвище та ініціали)

UNICHECK
by Turnitin

Имя пользователя:
Микола Володимирович Рясний

ID проверки:
1016039205

Дата проверки:
28.12.2023 06:24:27 EET

Тип проверки:
Doc vs Library

Дата отчета:
28.12.2023 06:27:45 EET

ID пользователя:
12281

Название файла: **Riasnyi M. Udoskonalennia derzhavnoho upravlinnia informatsiinoiu bezpekoiu v Ukraini.docx**

Количество страниц: **96** Количество слов: **19694** Количество символов: **165243** Размер файла: **961.28 KB** ID файла: **1015732843**

9.09%
Совпадения

Наибольшее совпадение: **1.59%** с источником из Библиотеки (ID файла: **1000062887**)

Поиск совпадений с Интернетом не производился

9.09% Источники из Библиотеки | **980** ..... Страница 98

1.43% Цитат

Цитаты | **2** ..... Страница 99

Исключение списка библиографических ссылок выключено

0% Исключений

Нет исключенных источников

Модификации

Обнаружены модификации текста. Подробная информация доступна в онлайн-отчете.

Замененные символы | **7**

АКТ

перевірки випускної кваліфікаційної роботи на наявність текстових збігів

Відповідно до даних сервісу Unicheck файл «Riasnyi M. Udoskonalennia derzhavnoho upravlinnia informatsiinoiu bezpekoiu v Ukrainidocx»,

автор: Рясний Микола Володимирович.

містить 90,91 % авторського тексту.

28.12.2023 _____

(підпис)

ЗМІСТ

ВСТУП

Актуальність теми. У сучасному інформаційному суспільстві, якому притаманний високий рівень технологічного розвитку, тема удосконалення державного управління інформаційною безпекою в Україні набуває особливої актуальності. Різкі зміни в сфері технологій, зокрема цифрові трансформації, а також постійне зростання загроз кібербезпеці, роблять необхідним глибокий аналіз та оптимізацію системи управління інформаційною безпекою на державному рівні. Сьогодення характеризується зростанням кількості та складності кіберзагроз, що ставить під загрозу важливі інформаційні ресурси держави. Ворожі дії в кіберпросторі можуть призвести до важливих політичних, економічних та соціальних наслідків для країни. Прискорений розвиток цифрових технологій та їх широке впровадження в усі сфери суспільства ставлять під сумнів традиційні методи забезпечення безпеки інформації. Потрібна переоцінка та адаптація систем управління інформаційною безпекою для ефективного функціонування в нових умовах цифрової реальності. Забезпечення інформаційної безпеки стає невід'ємною складовою загальної національної безпеки. Завданнями державного управління є не лише захист важливих інформаційних ресурсів, а й забезпечення стійкості суспільства до можливих кіберзагроз. Умови глобалізації вимагають від держави активної участі в міжнародних процесах з обміну досвідом та спільного розв'язання проблем кібербезпеки. Ефективне управління інформаційною безпекою стає ключовим фактором для підтримання позитивних міжнародних відносин.

Отже, дослідження теми удосконалення державного управління інформаційною безпекою в Україні визначається необхідністю адаптації до сучасних реалій, забезпечення національної безпеки та підвищення рівня стійкості держави до сучасних кіберзагроз. Це дослідження відкриє нові перспективи для розвитку системи управління інформаційною безпекою,

забезпечуючи сталість та ефективність державних структур в умовах високотехнологічного суспільства.

Науковий внесок у цьому напрямі належить таким вітчизняним дослідникам, як Я. Базилюк, О. Власенко, О. Білорус, О. Бодрук, Ю. Битяк, Л. Бучило, Д. Видрін, В. Глушков, А. Гончаренко, В. Горбулін, В. Гурковський, О. Делінський, В. Ємельянов, В. Картавцев, А. Качинський, З. Коваль. О. Копан, Б. Кормич, В. Косевцов, Г. Костенко, В. Ковальський, М. Левицька, О. Логінов, О. Литвак, Н. Нижник, О. Олійник, Г. Перепелиця, К. Павлюк, В. Петрик, Г. Пономаренко, Г. Почепцов, О. Пулим, С. Расторгуєв, А. Стрельцов, Л. Харченко, О. Хилько, М. Цюрупа, З. Чуйко, й інші.

Мета дипломної роботи – дослідження та розробка практичних рекомендацій щодо вдосконалення державного управління інформаційною безпекою в Україні.

Для досягнення мети визначено такі *завдання*:

– розкрити сутність державного управління інформаційною безпекою;

– навести організаційно-правовий механізм державного управління інформаційною безпекою;

– розглянути зарубіжний досвід державного управління інформацію безпекою країни;

– провести аналіз кібератак в Україні в період війни;

– оцінити фінансовий механізм державного управління інформаційною безпекою в Україні;

– розглянути інформаційну безпеку в Україні умовах воєнного стану;

– навести напрямки покращення державного управління інформаційної безпекою в Україні;

– навести пріоритети формування політики кібербезпеки в Україні;

– описати стратегію державного управління інформаційною безпекою в Україні.

Об'єктом дипломної роботи є процес вдосконалення державного управління інформаційною безпекою в Україні.

Предметом дослідження є теоретико-методологічні основи та практичні аспекти вдосконалення державного управління інформаційною безпекою в Україні.

Методи дослідження. Для досягнення поставленої в кваліфікаційній роботі мети були використані загальнонаукові та спеціальні методи наукового дослідження: аналізу та синтезу, систематизації, компаративний, класифікації, термінологічний, проблемно-орієнтовний.

Інформаційну базу дослідження становлять: закони України, укази Президента України, постанови Кабінету Міністрів України; довідкові та інструктивні матеріали; наукові праці різних жанрів інших авторів; періодичні видання; інформаційні матеріали, розміщені в мережі Інтернет.

Практичне значення результатів дослідження: полягає у розробці та науковому обґрунтуванні рекомендацій щодо удосконалення державного управління інформаційною безпекою в Україні.

Структура роботи. Дипломна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел.

РОЗДІЛ 1
ТЕОРЕТИЧНІ АСПЕКТИ ДЕРЖАВНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В УКРАЇНІ

1.1. Сутність державного управління інформаційною безпекою

Державне управління інформаційною безпекою є важливою складовою сучасного державного управління і має на меті забезпечення захисту інформаційних ресурсів, систем та інфраструктури від можливих загроз, втрат, пошкоджень або несанкціонованого доступу [23, с.80]. Основною сутністю державного управління інформаційною безпекою є створення ефективного та комплексного механізму захисту інформації від різних видів загроз, які можуть виникнути як зовнішні, так і внутрішні. На рис.1.1. представлено складові державного управління інформаційною безпекою.

Рис.1.1. Складові державного управління інформаційною безпекою [15, с.77]

Державне управління інформаційною безпекою вимагає системного підходу, врахування всіх можливих аспектів та постійного вдосконалення стратегій і заходів для забезпечення ефективного захисту національної інформаційної інфраструктури.

1. Аналіз та оцінка загроз у сфері інформаційної безпеки є ключовим етапом для ефективного захисту інформаційних ресурсів. Ретельний аналіз потенційних загроз передбачає вивчення різноманітних сценаріїв, які можуть викликати порушення безпеки інформації. Це включає в себе вивчення технічних, організаційних та соціальних аспектів можливих загроз, таких як кібератаки, витоки даних, внутрішні порушення безпеки тощо [3, с.44].

Після ретельного аналізу виникає необхідність оцінки рівня ризику. Цей процес включає в себе визначення потенційних наслідків загроз, ймовірності їх виникнення та важливості для інформаційної безпеки. Оцінка ризику дозволяє виділити пріоритетні напрямки захисту та розробити стратегії управління ризиками.

Визначення прийнятних стратегій управління ризиками полягає в розробці і впровадженні конкретних заходів для зменшення або прийняття ризику. Це може включати в себе застосування технічних засобів захисту, вдосконалення політик безпеки, навчання персоналу з питань безпеки, а також впровадження систем моніторингу та виявлення інцидентів.

Такий інтегрований підхід до аналізу та оцінки загроз дозволяє державам, організаціям і підприємствам визначити найбільш критичні точки збоїв у системі безпеки та розробити ефективні стратегії для їх запобігання та подолання.

2. Створення політики інформаційної безпеки є важливим кроком для забезпечення ефективного захисту інформаційних ресурсів у державних органах та інших організаціях. Цей комплексний процес включає в себе кілька ключових етапів [17, с.30].

На етапі розробки політики визначаються основні принципи та цілі, адаптовані до стратегічних завдань держави чи організації. Окрім цього,

встановлюються вимоги до захисту конфіденційної, цілісної та доступної інформації.

Стандарти та процедури безпеки визначають конкретні вимоги та технічні аспекти захисту інформації. Розробляються процедури управління доступом, моніторингу та виявлення інцидентів, а також стратегії реагування на кіберзагрози та інші аспекти безпеки.

Залучення співробітників включає проведення навчань та тренінгів, щоб забезпечити розуміння важливості та виконання політики інформаційної безпеки. Працівники також залучаються до виконання стандартів та процедур безпеки [20, с.22].

На етапі аудиту та внутрішнього контролю розробляються механізми для перевірки дотримання політики інформаційної безпеки, а також визначаються відповідальні особи за моніторинг та аналіз безпекових показників.

Інтеграція з IT-інфраструктурою передбачає забезпечення сумісності політики інформаційної безпеки з існуючою IT-інфраструктурою та впровадження технічних рішень для забезпечення безпеки мережі, даних та програмного забезпечення.

Оновлення та вдосконалення включають регулярне оновлення політики відповідно до змін у загрозах та технологічному середовищі, а також постійне вдосконалення стратегій забезпечення інформаційної безпеки на основі аналізу інцидентів та найкращих практик. Такий підхід дозволяє створити ефективну систему захисту інформаційних ресурсів, об’єднуючи правові, технічні та організаційні аспекти.

3. Захист інфраструктури та ресурсів становить критичний елемент стратегії інформаційної безпеки, передбачаючи розробку та впровадження комплексу заходів для забезпечення стійкості перед різноманітними загрозами. Цей процес включає два ключові аспекти.

На першому етапі розробляються технічні рішення для захисту інфраструктури від кіберзагроз, включаючи віруси, хакерські атаки та інші форми зловживань. Використовуються криптографічні методи для захисту

конфіденційної інформації та забезпечення цілісності даних під час їх передачі та зберігання. Запроваджується система контролю доступу для обмеження прав доступу лише авторизованим користувачам [27, с.90].

На другому етапі розробляються політики та процедури безпеки для забезпечення ефективного функціонування інформаційних технологій відповідно до визначених стандартів. Мережі захищаються від несанкціонованого доступу та атак, використовуючи заходи, що запобігають перехопленню та зміні інформації в транзиті. Безпека баз даних забезпечується за допомогою відповідних заходів шифрування, аудиту та контролю доступу, що гарантують цілісність та конфіденційність інформації.

Ці заходи орієнтовані на створення комплексної системи безпеки, яка враховує технічні, організаційні та процесуальні аспекти. Захист інфраструктури та ресурсів є необхідним для запобігання витоку чутливої інформації, забезпечення стійкості систем та ефективного функціонування інформаційних технологій у сучасному цифровому середовищі.

4 Своєчасна реакція та ефективне відновлення після кібератак чи інших порушень безпеки є важливим етапом стратегії інформаційної безпеки. Цей процес включає в себе два ключові аспекти:

Розробка планів реагування на інциденти і відновлення:

- створення детальних планів, які визначають кроки та процедури для ефективної реакції в разі кібератак, витоку інформації чи інших порушень безпеки;
- визначення відповідальних осіб та команд для керування реакцією на інциденти та відновленням;
- врахування можливих сценаріїв інцидентів для ефективного впорядкування ситуації та запобігання подальшим загрозам [6, с.90].

Підготовка персоналу до ефективної реакції у випадку інцидентів:

- проведення навчань та тренінгів для персоналу з використання планів реагування та відновлення;

– встановлення чітких ролей та відповідальностей для працівників під час інцидентів;

– проведення симуляцій та практичних вправ для перевірки ефективності планів та забезпечення готовності персоналу до дій в екстрених ситуаціях [19, с.45].

Своєчасна реакція та ефективне відновлення після інцидентів є критичними для мінімізації збитків, відновлення нормального функціонування та підвищення стійкості системи до подібних загроз у майбутньому. Готовність персоналу та вивчення найкращих практик грають важливу роль у забезпеченні успішної реакції на інциденти та швидкому відновленні роботи після їх виникнення.

5. Залучення та співпраця в інформаційній безпеці є важливою стратегічною складовою, що передбачає взаємодію з різними рівнями влади, громадськістю, приватним сектором та міжнародними партнерами для обміну інформацією та спільної боротьби з загрозами [9, с.102]. Цей процес включає в себе кілька важливих аспектів:

Взаємодія з різними рівнями влади:

– встановлення механізмів обміну інформацією та співпраці з усіма рівнями державного управління для швидкого реагування на загрози;

– співпраця з правоохоронними органами, розвідувальними службами та іншими державними структурами для об’єднання зусиль у сфері кібербезпеки [7, с.45].

Громадськість:

– залучення громадськості до питань інформаційної безпеки через кампанії засвідомленості та навчання;

– сприяння обміну інформацією та зворотньому зв’язку з громадськістю щодо виявлення можливих загроз та інцидентів [2, с.55].

Приватний сектор:

– встановлення партнерств та співпраця з підприємствами для обміну інформацією про нові загрози та вразливості;

– сприяння розвитку стандартів та практик інформаційної безпеки у приватному секторі [8, с.34].

Міжнародні партнери:

– участь у міжнародних ініціативах та форумах з метою обміну досвідом та координації заходів у глобальному масштабі;

– співпраця з міжнародними організаціями та партнерами для розробки та впровадження спільних стратегій забезпечення кібербезпеки [11, с.78].

Залучення та співпраця створюють ефективний механізм відповіді на загрози, оскільки об’єднують різні суб’єкти та рівні для спільного реагування на сучасні виклики в галузі інформаційної безпеки. Взаємодія з різними стейкхолдерами дозволяє створити комплексну та динамічну систему захисту інформації в умовах постійно зростаючих кіберзагроз.

6. Законодавче забезпечення в інформаційній безпеці передбачає розробку та удосконалення відповідного законодавства для ефективного забезпечення безпеки інформаційних ресурсів. Цей процес включає в себе два основних напрямки:

1) розробка та удосконалення відповідного законодавства щодо інформаційної безпеки:

– розробка нових законів та правових актів, які враховують сучасні виклики та технологічні тенденції в галузі інформаційної безпеки;

– удосконалення існуючого законодавства для адаптації до швидко змінюючогося характеру кіберзагроз та забезпечення відповідності новим вимогам [46].

2) забезпечення додержання нормативно-правових вимог у сфері інформаційної безпеки:

– створення механізмів для моніторингу та контролю за дотриманням законодавчих норм у галузі інформаційної безпеки;

– розробка ефективних систем санкцій та відповідальності для тих, хто порушує встановлені норми і стандарти [46].

Законодавче забезпечення створює правовий фундамент для регулювання та захисту інформаційної сфери, а також забезпечує нормативно-правовий контекст для розвитку та впровадження стратегій інформаційної безпеки. Постійне удосконалення законодавства дозволяє адаптувати правові норми до нових викликів та змін у кіберпросторі, забезпечуючи ефективний захист інформаційних ресурсів у сучасному цифровому середовищі.

Державне управління інформаційною безпекою вимагає системного підходу, врахування всіх можливих аспектів та постійного вдосконалення стратегій і заходів для забезпечення ефективного захисту національної інформаційної інфраструктури. Цей комплексний підхід передбачає не лише розробку та впровадження ефективних технічних рішень, але й формування відповідної політики, стандартів, процедур, аудиту та навчання персоналу. Такий підхід дозволяє адаптуватися до постійно змінюючогося ландшафту кіберзагроз, виявляти та вирішувати потенційні ризики, а також взаємодіяти з іншими рівнями влади, громадськістю та приватним сектором для створення міцної системи інформаційної безпеки нації.

1.2. Організаційно-правовий механізм державного управління інформаційною безпекою

Державна служба спеціального зв’язку та захисту інформації України грає ключову роль у забезпеченні безпеки та ефективності державних комунікаційних систем. Організація виконує ряд стратегічних завдань, спрямованих на забезпечення захисту інформації та кібербезпеки.

Державної служби спеціального зв’язку та захисту інформації України в виступає важливим ланцюгом у забезпеченні національної безпеки, особливо в умовах сучасних кіберзагроз та гібридних конфліктів. Забезпечення ефективного функціонування інформаційних систем та захисту від кіберзагроз є важливою складовою безпеки країни в цифрову епоху.

Держспецзв’язку створено на виконання прийнятого 23 лютого 2006 року Закону України «Про Державну службу спеціального зв’язку та захисту інформації України» на базі ліквідованого Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби Безпеки України.

На рис.1.2. представлено історія створення Держспецзв’язку.

Рис.1.2. Історія створення Держспецзв’язку [30]

На початку 1998 року Указом Президента України від 11 лютого 1998 року № 110 »Про заходи щодо вдосконалення криптографічного захисту інформації в телекомунікаційних і інформаційних системах» на Головне управління урядового зв’язку СБУ (ГУУЗ СБУ) покладено завдання вирішення усього комплексу завдань, пов’язаних зі створенням такої системи в Україні. Указом Президента України від 22 травня 1998 року № 505 на ГУУЗ СБУ покладено завдання з реалізації державної політики в цій сфері. З метою концентрації зусиль у сфері захисту інформації за рішенням Президента України в серпні 1998 року на базі ГУУЗ СБУ із залученням фахівців

Головного управління технічного захисту інформації Держкомсекретів був створений Департамент спеціальних телекомунікаційних систем та захисту інформації СБУ (ДСТСЗІ СБУ), який став головною структурою в державі з питань криптографічного та технічного захисту інформації.

Державна служба спеціального зв'язку та захисту інформації України має таку загальну структуру:

– «центральний орган виконавчої влади, що забезпечує формування та реалізацію державної політики у сферах організації спеціального зв'язку, захисту інформації;

– територіальні органи центрального органу виконавчої влади, що забезпечує формування та реалізацію державної політики у сферах організації спеціального зв'язку, захисту інформації;

– територіальні підрозділи;

– Головне управління та підрозділи урядового фельд'єгерського зв'язку;

– навчальні, охорони здоров'я, санаторно-курортні та інші заклади, науково-дослідні, науково-виробничі та інші установи і організації» [15].

Керівним органом системи Держспецзв'язку є Адміністрація Держспецзв'язку, яка діє відповідно до Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України. До складу Адміністрації входять 17 департаментів та відділів, які виконують покладені на службу завдання.

До сфери управління Адміністрації Держспецзв'язку входять державні підприємства, установи та організації, діяльність яких пов'язана із забезпеченням виконанням завдань, покладених на Службу.

Адміністрація Держспецзв'язку.

Департаменти Адміністрації Держспецзв'язку.

Департамент захисту інформації Адміністрації Держспецзв'язку.

Департамент кіберзахисту Адміністрації Держспецзв'язку.

Департамент державного контролю у сфері захисту інформації Адміністрації Держспецзв’язку.

Департамент розвитку електронних комунікацій Адміністрації Держспецзв’язку.

Департамент європейської інтеграції та міжнародного співробітництва Адміністрації Держспецзв’язку.

Режимно-секретне управління Адміністрації Держспецзв’язку.

Відділ інформаційних комунікацій Адміністрації Держспецзв’язку.

Департамент планування застосування органів і підрозділів та спеціального зв’язку Адміністрації Держспецзв’язку.

Інші департаменти та відділи.

Територіальні органи.

Головне управління урядового зв’язку. Забезпечує урядовим зв’язком вищих посадових осіб держави в місцях їх постійного та тимчасового перебування на території України та за її межами. Забезпечують функціонування мереж та комплексів державної системи урядового зв’язку.

Управління Держспецзв’язку в областях. Забезпечує урядовим зв’язком державні органи в областях, реалізують державну політику у сферах криптографічного та технічного захисту інформації, впровадження сервісів кіберзахисту.

Територіальні підрозділи Забезпечують урядовим зв’язком органи військового управління сил оборони та сектору безпеки на польових пунктах управління.

2 територіальний вузол урядового зв’язку

3 територіальний вузол урядового зв’язку

4 територіальний вузол урядового зв’язку

8 територіальний вузол урядового зв’язку

10 територіальний вузол урядового зв’язку

Заклади та установи, підприємства, що входять до сфери управління Держспецзв’язку

Центральним органом виконавчої влади, який відповідає за формування та реалізацію державної політики у сферах організації спеціального зв'язку, захисту інформації в Україні, є Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ). Однак, для забезпечення виконання її завдань і функцій, до сфери управління цього центрального органу входять державні підприємства, установи та організації.

Ці державні установи можуть бути підпорядковані ДССЗЗІ і діяти у сферах, що пов'язані з організацією спеціального зв'язку, криптографією, захистом конфіденційної інформації, кібербезпекою та іншими аспектами сфери інформаційної безпеки. Їхні завдання можуть включати розробку та впровадження технічних рішень для захисту інформації, управління криптографічними системами, а також забезпечення безпеки і ефективного функціонування комунікаційних систем та інших інформаційних технологій.

Управління цими підприємствами та установами відбувається в рамках державної політики, яка визначається Державною службою спеціального зв'язку та захисту інформації України та має на меті забезпечення високого рівня інформаційної безпеки та захисту конфіденційної інформації в країні.

Голова Державної служби спеціального зв'язку та захисту інформації України виступає як вищий керівник центрального органу виконавчої влади, що відповідає за формування та реалізацію державної політики у сферах організації спеціального зв'язку та захисту інформації. Відмічається, що ця посада передбачає не лише відповідальність за виконання завдань служби, але й особисту відповідальність перед державою за ці завдання.

Важливим аспектом є процедура призначення та звільнення з посади Голови, яка здійснюється на рішення Кабінету Міністрів України за поданням Прем'єр-міністра країни. Це підкреслює важливість ролі, яку відіграє Голова у реалізації стратегічних завдань у сферах зв'язку та захисту інформації.

22 жовтня 2021 року Президент України Володимир Зеленський затвердив Концепцію реформування Держспецзв'язку (Указ Президента України № 544/2021 «Про рішення Ради національної безпеки і оборони

України від 22 жовтня 2021 року «Про Концепцію реформування Державної служби спеціального зв'язку та захисту інформації України»«). До 2025 року Державна служба спеціального зв'язку та захисту інформації України буде реформована.

Реформа Держспецзв'язку це посилення інституційних спроможностей. Унаслідок реформування Служба стане більш ефективною та прозорою. Будуть розв'язані питання соціального забезпечення військовослужбовців. Відбудеться демілітаризація Служби виконання деяких військових функцій буде передане цивільним співробітникам.

Основні засади реформування:

Урядовий зв'язок. Система урядового зв'язку буде повністю інтегрована до Національної телекомунікаційної мережі, осучаснені та модернізовані системи зв'язку. Фельд'єгерський зв'язок стане оперативнішим і більш захищеним.

Кібербезпека. Сучасна система кіберзахисту буде розгорнута на об'єктах критичної інформаційної інфраструктури, посилено захист державних інформаційних ресурсів, буде розширено сучасну нормативно-правову базу у сфері кіберзахисту.

Захист інформації. Буде розроблено та імплементовано нові сучасні стандарти технічного і криптографічного захисту інформації, протидії технічним розвідкам.

Ефективність. Відбудеться реформування структури Служби, посилення демократичного цивільного контролю. Робота у Держспецзв'язку буде престижною і забезпечуватиме гідний соціальний рівень. Підвищимо якість освіти з кібербезпеки, рівень фахівців із захисту інформації.

Міжнародна співпраця. Внаслідок реформи Держспецзв'язку розширить співпрацю з НАТО з метою впровадження стандартів Альянсу у повсякденну діяльність та задля наближення набуття Україною членства у Альянсі. Служба стане акредитаційним центром із питань безпеки національних комунікаційно-

інформаційних систем, у яких обробляється інформація НАТО з обмеженим доступом

«Основні завдання Державної служби спеціального зв'язку та захисту інформації України:

1. Основними завданнями Державної служби спеціального зв'язку та захисту інформації України є:

1) формування та реалізація державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах (далі - інформаційно-комунікаційні системи) і на об'єктах інформаційної діяльності, а також у сферах використання державних інформаційних ресурсів в частині захисту інформації, протидії технічним розвідкам, функціонування, безпеки та розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, активної протидії агресії у кіберпросторі;

2) участь у формуванні та реалізації державної політики у сферах електронного документообігу (в частині захисту інформації державних органів та органів місцевого самоврядування), електронної ідентифікації (з використанням електронних довірчих послуг, захисту критичної інформаційної інфраструктури), електронних довірчих послуг, захисту критичної інформаційної інфраструктури (у частині встановлення вимог з безпеки та захисту інформації під час надання та використання електронних довірчих послуг, захисту критичної інформаційної інфраструктури, контролю за дотриманням вимог законодавства у сфері електронних довірчих послуг, захисту критичної інформаційної інфраструктури);

3) забезпечення в установленому порядку та в межах компетенції діяльності суб'єктів, які безпосередньо здійснюють боротьбу з тероризмом.

4.) реалізація державної політики щодо захисту критичної технологічної інформації, кіберзахисту об’єктів критичної інформаційної інфраструктури, здійснення державного контролю в цих сферах;

5) визначення вимог до захисту критичної технологічної інформації, формування загальних вимог до кіберзахисту об’єктів критичної інфраструктури, ведення переліку об’єктів критичної інформаційної інфраструктури, здійснення заходів щодо його оновлення та актуалізації;

6) виконання інших завдань, передбачених законодавством у сфері забезпечення кібербезпеки та кіберзахисту» [15].

На рис.1.3. представлено функції Держспецзв’язку.

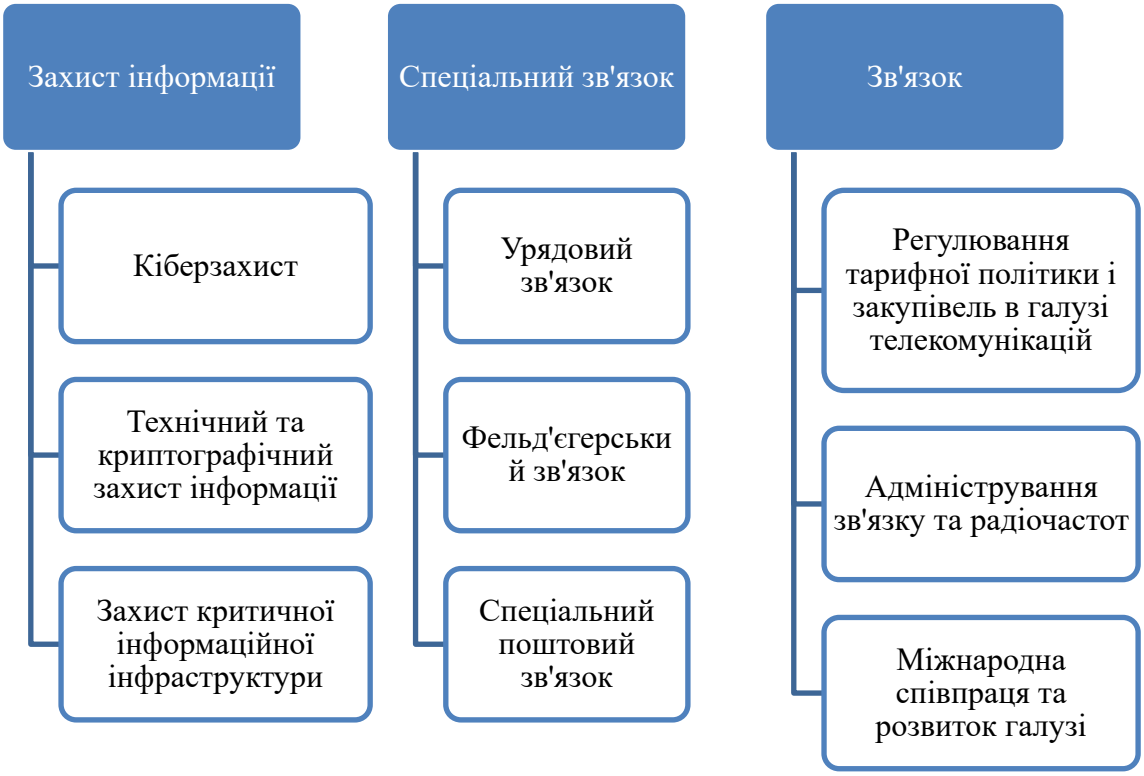

Рис.1.3. Загальні функції Держспецзв’язку [30]

Принципи функціонування Державної служби спеціального зв’язку та захисту інформації України базуються на фундаментальних цінностях та нормах. Ця діяльність визначається принципами верховенства права, гарантії прав і свобод громадян, забезпечення безперервності, законності, єдності

державної політики, відкритості для демократичного цивільного контролю, прозорості та відсутності партійної впливовості. У своїй діяльності Державна служба дотримується принципу єдиноначальності, що визначає однозначність та консистентність в управлінні та прийнятті рішень.

Важливим аспектом діяльності Держспецзв'язку є співпраця з іншими суб'єктами кібербезпеки, щоб створити єдиний і вперше ефективний механізм захисту від кіберзагроз. Це включає в себе обмін інформацією про потенційні загрози, впровадження спільних стратегій та розвиток новітніх технологічних рішень для кіберзахисту.

Загалом, Держспецзв'язку виступає в ролі стратегічного лідера в області кібербезпеки, спрямовуючи зусилля національних ресурсів на захист інформаційних активів країни від сучасних кіберзагроз.

Державна служба спеціального зв'язку та захисту інформації України відіграє визначальну роль у розвитку та ефективному функціонуванні державної системи урядового зв'язку. Зобов'язанням агентства є забезпечення безперебійного та продуктивного обміну інформацією між ключовими посадовими особами країни, зокрема Президентом України, Головою Верховної Ради України, Прем'єр-міністром України та іншими вищими чиновниками державних і місцевих органів.

Держспецзв'язку взяло на себе відповідальність за модернізацію урядового зв'язку в 2020 році, щоб надати сучасний, надійний та безпечний спеціальний зв'язок. Ця ініціатива включає розширення функціональних можливостей Національної телекомунікаційної мережі (НТМ). Передбачається, що це дозволить інтегрувати і уніфікувати системи спеціального зв'язку та захищених електронних комунікацій різних державних органів у єдиному безпековому контурі, використовуючи передові цифрові технології.

Зокрема, Держспецзв'язку здійснює нагляд за дотриманням законодавства у сфері захисту інформації в приміщеннях абонентів урядового зв'язку, щоб забезпечити високий рівень конфіденційності та безпеки обміну

інформацією на найвищому рівні в умовах звичайних та надзвичайних ситуацій.

Урядовий фельд'єгерський зв'язок, управління та підрозділи Держспецзв'язку є важливими ланками в системі організації та забезпечення урядового фельд'єгерського зв'язку в Україні. Задачами цих структур є забезпечення безперебійної та конфіденційної обробки кореспонденції різного рівня секретності та її ефективної доставки між вищими державними посадовцями, державними органами, органами місцевого самоврядування та іншими юридичними особами, які мають важливий статус відповідно до законодавства.

Головним органом, який керує системою урядового фельд'єгерського зв'язку, є Головне управління урядового фельд'єгерського зв'язку Держспецзв'язку. Це управління відповідає за координацію та ефективне функціонування підрозділів урядового фельд'єгерського зв'язку у регіонах України, зокрема в обласних центрах.

Очільник системи урядового фельд'єгерського зв'язку Держспецзв'язку несе відповідальність за впровадження нових технологій та систем автоматизації контролю за проходженням кореспонденції. Зазначено, що прототип такої системи буде запущено в 2022 році, а повноцінне функціонування передбачено вже наступного року. Це реформування сприятиме надійній, оперативній та безпеці доставці кореспонденції, що містить державну таємницю, службову інформацію, офіційну листування та дипломатичну пошту від вищих посадових осіб України до різних адресатів в межах країни та за кордоном.

Спеціальний поштовий зв'язок. Держспецзв'язку здійснює формування та реалізацію державної політики в галузі поштового зв'язку спеціального призначення.

Постанова Кабінету Міністрів України від 23 грудня 2020 року №1295 «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки» визначає принципи та засади

роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. Ці заходи здійснюються відносно об’єктів кіберзахисту, які визначені у частині другій статті 4 Закону України «Про основні засади забезпечення кібербезпеки України».

У постанові встановлені основні принципи функціонування системи виявлення вразливостей та реагування на кіберінциденти, а також визначені завдання, повноваження та відповідальність суб’єктів, які здійснюють ці заходи. Це створює правовий фреймворк для ефективної роботи системи кібербезпеки, спрямованої на запобігання та реагування на кіберзагрози в Україні.

1. Закони України:

1. Закон України «Про інформацію» від 02.10.1992 № 2657-XII

Закон є важливим правовим документом, який визначає ключові принципи обігу інформації в Україні. Його основна мета полягає у встановленні засад прозорості та відкритості інформаційних процесів, а також визначенні прав та обов’язків осіб у цій сфері. Закон регулює створення, збирання, зберігання, використання, поширення, охорону та захист інформації.

Цей документ встановлює правовий статус інформації та визначає її режим, враховуючи її важливу роль у суспільстві та державі. Закон також визначає правила обігу конфіденційної та обмеженої інформації, забезпечуючи баланс між вільним доступом до інформації та необхідністю захисту конфіденційності та безпеки. Його положення є важливим фундаментом для правової системи, що регулює інформаційні відносини в Україні.

2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР

Цей закон є важливим правовим актом, спрямованим на забезпечення ефективного захисту інформації в інформаційно-телекомунікаційних системах (ІТС). Визначаючи правові та організаційні засади, закон регулює відносини в сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах.

Основна мета цього закону - гарантувати конфіденційність та цілісність інформації, знаходячись у телекомунікаційному та інформаційному просторі. Закон визначає правила захисту інформації та інформаційних технологій, організаційні принципи проведення заходів з захисту, а також встановлює відповідальність за порушення цих правил. Його норми сприяють створенню надійного інформаційного середовища, необхідного для сталого розвитку та безпеки інформаційного суспільства.

3. Закон України «Про державну таємницю» від 21.01.1994 № 3855-XIIЗакон України «Про державну таємницю» визначає фундаментальні принципи та регулює важливі аспекти управління державною таємницею в Україні. Цей правовий акт встановлює чіткі механізми класифікації інформації, визначає порядок її зберігання, розголошення та використання. Закон також регламентує обіг документів, які мають статус державної таємниці, встановлюючи стандарти безпеки та вимоги до їхнього захисту.

Основна мета закону – забезпечення національної безпеки шляхом ефективного управління конфіденційною інформацією та контролю за її обігом. Він визначає правові принципи розсекречування матеріальних носіїв державної таємниці, що стають невід’ємною частиною системи забезпечення державної безпеки.

4. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI

Закон визначає обов’язки та відповідальність суб’єктів обробки персональних даних, встановлює права громадян на контроль та захист своїх відомостей. Його область застосування охоплює всі аспекти обробки, незалежно від застосування автоматизованих чи неавтоматизованих засобів, а також включає обробку інформації в різних сферах життя, від публічних служб до комерційних структур.

Загальний принцип закону полягає в створенні ефективного механізму, спрямованого на гармонізацію інтересів суб’єктів даних і тих, хто їх обробляє,

забезпечуючи високий стандарт захисту особистої приватності та конфіденційності в епоху стрімкого розвитку цифрових технологій.

5. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII

Зазначений закон встановлює нормативні та організаційні засади для забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі. Він визначає основні цілі, напрями та принципи державної політики у сфері кібербезпеки. Згідно з цим законом, визначені повноваження державних органів, підприємств, установ, організацій, осіб та громадян у сфері кібербезпеки. Також закріплені основні принципи координації діяльності цих суб'єктів з метою забезпечення кібербезпеки в країні. Цей закон виступає основоположним документом, що регулює відносини в галузі кібербезпеки в Україні, забезпечуючи необхідний правовий фундамент для ефективної боротьби з кіберзагрозами та захисту інформаційних ресурсів країни.

2. Постанови КМУ:

Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373

Постанова Кабінету міністрів України «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію» від 19 жовтня 2016 р. № 736[1] [Архівовано 22 березня 2022 у zakon.rada.gov.ua]

3. Нормативні документи в галузі технічного захисту інформації та державні стандарти України (ДСТУ) стосовно створення і функціонування КСЗІ:

НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі [Архівовано 10 січня 2020 у Wayback Machine.]

Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96 [Архівовано 18 вересня 2020 у Wayback Machine.]

НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі [Архівовано 10 січня 2020 у Wayback Machine.]

НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу [Архівовано 20 березня 2022 у Wayback Machine.]

НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу [Архівовано 20 березня 2022 у Wayback Machine.]

НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2 [Архівовано 20 березня 2022 у Wayback Machine.]

НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу [Архівовано 23 січня 2020 у Wayback Machine.]

НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі [Архівовано 20 березня 2022 у Wayback Machine.]

НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу [Архівовано 3 лютого 2020 у Wayback Machine.]

Автоматизированные системы. Требования к содержанию документов РД 50-34.698 [Архівовано 2 червня 2019 у Wayback Machine.]

Техническое задание на создание автоматизированной системы. ГОСТ 34.602-89 [Архівовано 10 вересня 2016 у Wayback Machine.]

НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу [Архівовано 20 березня 2022 у Wayback Machine.]

1.3. Зарубіжний досвід державного управління інформацію безпекою країни

Зарубіжний досвід державного управління інформаційною безпекою включає різноманітні підходи та стратегії, які можуть бути використані для підвищення рівня безпеки інформації в Україні. В табл.1.1. представлено зарубіжний досвід державного управління інформацію безпекою країни.

Таблиця 1.1

Зарубіжний досвід державного управління інформаційною безпекою

№	Країна	Досвід
1.	Естонія	Естонія славиться своєю успішною електронною системою управління, включаючи електронне голосування, електронну ідентифікацію та електронний доступ до громадянських послуг. Країна приділяє велику увагу кібербезпеці, включаючи навчання громадян щодо кіберзагроз та ефективний механізм реагування на кібератаки.
2.	Ізраїль	Ізраїль є однією з країн, де інновації в галузі кібербезпеки знаходяться на високому рівні. Країна активно розвиває та впроваджує передові технології в галузі кіберзахисту, а також здійснює співпрацю між урядовими структурами, приватним сектором та академічною галуззю.
3.	США	Сполучені Штати відомі своєю активною роботою в галузі кібербезпеки. У США створено Національну стратегію кібербезпеки, яка охоплює різноманітні аспекти, включаючи кіберзахист критично важливої інфраструктури та протидію кіберзагрозам.
4.	Сінгапур	Сінгапур визначається своєю високотехнологічною економікою і активними заходами з підвищення кібербезпеки. Країна вкладає зусилля в розвиток кадрового потенціалу в галузі кібербезпеки та впровадження передових технологій для захисту критично важливої інфраструктури.

Джерело: складено автором згідно [48]

Естонія визначається своєю передовою інформаційною інфраструктурою та успішними практиками в галузі кібербезпеки. Нижче розглядаються деталізовані аспекти, які дозволяють Естонії славитися своєю ефективною системою управління інформаційною безпекою:

1. Електронна система управління: Естонія впровадила інноваційну електронну систему управління, яка охоплює різні сфери, включаючи електронне голосування та електронний доступ до громадянських послуг. Громадяни можуть взаємодіяти з урядовими органами, використовуючи

цифрові інструменти, що полегшує та прискорює різні аспекти взаємодії з владою.

2. Електронна ідентифікація: Велика увага приділяється системі електронної ідентифікації, яка дозволяє громадянам легко та безпечно ідентифікувати себе в цифровому просторі. Це важливий компонент для забезпечення безпеки та конфіденційності при використанні електронних сервісів та зменшення ризиків шахрайства та зловживань.

3. Кібербезпека та навчання громадян: Естонія активно інвестує у кібербезпеку, забезпечуючи високий рівень захисту від кіберзагроз. Крім того, проводяться ініціативи з навчання громадян щодо кібербезпеки, зокрема надання інформації про потенційні загрози та заходи безпеки для індивідів та підприємств.

4. Ефективний механізм реагування на кібератаки: Естонія розвинула ефективний механізм реагування на кібератаки. Швидка і координована реакція владних структур дозволяє мінімізувати можливі збитки та відновлювати нормальне функціонування систем.

5. Співпраця з приватним сектором та міжнародними партнерами: Естонія активно співпрацює з приватним сектором та міжнародними партнерами для обміну інформацією, виявлення нових загроз та вдосконалення стратегій кібербезпеки. Ця взаємодія сприяє створенню комплексної та ефективної системи захисту [51].

Узагальнюючи, успішний досвід Естонії в галузі інформаційної безпеки демонструє, як інновації, ефективне управління та співпраця з громадянами і міжнародними структурами можуть взаємодіяти для забезпечення високого рівня кібербезпеки в цифровому суспільстві.

Ізраїль служить прикладом країни, де кібербезпека поєднується з високим рівнем інновацій та ефективного управління. Країна визначається своєю активною роботою в галузі розвитку та впровадження передових технологій кіберзахисту, а також тісною співпрацею між різними секторами суспільства.

Ізраїль вирізняється наступними ключовими аспектами:

1. Інновації в кібербезпеці: Країна володіє динамічним екосистемою стартапів у сфері кібербезпеки, що сприяє появі новаторських рішень. Ізраїльські компанії активно працюють над вдосконаленням технологій виявлення, захисту та реагування на кіберзагрози.

2. Співпраця з урядовими структурами: Уряд Ізраїлю активно співпрацює з кібербезпечними підрозділами та агентствами для розробки та впровадження стратегічних заходів щодо захисту країни в кіберпросторі. Ця співпраця забезпечує комплексний та координований підхід до кібербезпеки.

3. Партнерство з приватним сектором: приватний сектор в Ізраїлі відіграє ключову роль у розвитку та впровадженні інновацій в галузі кібербезпеки. Співпраця між урядовими органами та приватними компаніями сприяє обміну експертизою та швидкому впровадженню нових технологій.

4. Академічна галузь та навчання: Ізраїль вкладає значні ресурси в академічні програми та навчання в галузі кібербезпеки. Університети та дослідницькі інститути сприяють розвитку та поглибленню знань у цій критичній галузі.

5. Міжнародна співпраця: Ізраїль активно співпрацює з іншими країнами та міжнародними організаціями в галузі кібербезпеки. Ця взаємодія сприяє обміну інформацією та розробці міжнародних стандартів безпеки [54].

Узагальнюючи, Ізраїль визначається як країна, що не лише володіє передовими технологіями в галузі кібербезпеки, але і вдало об’єднує зусилля урядових, приватних та академічних структур для створення ефективної та інтегрованої системи кіберзахисту.

Сполучені Штати відомі своєю активною роботою в галузі кібербезпеки. У США створено Національну стратегію кібербезпеки, яка охоплює різноманітні аспекти, включаючи кіберзахист критично важливої інфраструктури та протидію кіберзагрозам.

Сполучені Штати дійсно приділяють велику увагу кібербезпеці та мають широкий спектр заходів для захисту від кіберзагроз. Національна стратегія

кібербезпеки США орієнтована на захист критично важливих систем та забезпечення стійкості країни в кіберпросторі [52].

Однією з ключових структур, що відповідає за координацію заходів у галузі кібербезпеки в США, є Національний центр кібербезпеки та зв'язку (NCCIC), який є частиною Кіберкоманди Сполучених Штатів та Департаменту безпеки США.

США також активно співпрацює з приватним сектором, адже багато критично важливих інфраструктурних об'єктів належать приватним компаніям. Заходи включають в себе регулярні аудити та перевірки на кібербезпеку, обмін інформацією про загрози та поглиблену співпрацю для виявлення та протидії кібератакам.

Крім того, США приділяють увагу міжнародному співробітництву в галузі кібербезпеки і активно працюють з іншими країнами для розробки міжнародних стандартів та спільних заходів для боротьби з кіберзагрозами.

Додатково варто відзначити, що Сполучені Штати також вкладають зусилля у підготовку та розвиток кадрів у галузі кібербезпеки. Здобуття та удосконалення навичок фахівців у цій області визначається як один із пріоритетів, оскільки ефективний захист від кіберзагроз вимагає висококваліфікованих спеціалістів [34].

Крім того, США активно впроваджують стратегії кібердетеренції, що передбачає вживання заходів для запобігання кібератак та відповіді на них у випадку їхнього виникнення. Це включає в себе не лише технічні заходи, але й правові та політичні аспекти, в тому числі міжнародні спроби встановлення норм та правил для кіберпростору.

Нарешті, США активно сприяють створенню та підтримці міжнародних механізмів обміну інформацією про кіберзагрози та події, які мають потенційно серйозний вплив на кібербезпеку світового співтовариства.

Сінгапур визначається своєю високотехнологічною економікою і активними заходами з підвищення кібербезпеки. Країна вкладає зусилля в

розвиток кадрового потенціалу в галузі кібербезпеки та впровадження передових технологій для захисту критично важливої інфраструктури [39].

Досягнення Сінгапуру в галузі кібербезпеки також включають активну участь у міжнародних форумах та ініціативах, спрямованих на зміцнення глобальної кібербезпеки. Країна активно приєднується до міжнародних дискусій з питань розробки стандартів безпеки в кіберпросторі та регулювання цієї сфери.

Сінгапур також визначається своєю готовністю реагувати на кіберзагрози і розробляє цілісні стратегії відповіді на можливі інциденти. Це включає в себе не лише технічні аспекти, але і аспекти управління кризовими ситуаціями та співпрацю з приватним сектором для виявлення та нейтралізації загроз.

Крім того, Сінгапур вдосконалює свою законодавчу базу в галузі кібербезпеки, враховуючи швидкі зміни технологій та ризики, пов’язані з кіберзлочинністю. Це допомагає створити ефективну правову платформу для розслідування та притягнення до відповідальності осіб, які порушують кібербезпеку [22].

Загалом, Сінгапур продовжує вдосконалювати свої підходи до кібербезпеки, враховуючи постійні зміни в кіберзагрозах та викликах, які виникають у цьому динамічному сегменті.

Ці приклади підкреслюють важливість інтеграції технологічних інновацій, ефективних стратегій та міжсекторальної співпраці для забезпечення ефективного управління інформаційною безпекою держави.

Висновки до розділу 1

Державне управління інформаційною безпекою в сучасному світі визначається як невід’ємна частина державного управління, орієнтована на забезпечення високого рівня захисту інформаційних ресурсів та інфраструктури від можливих загроз. Це складний процес, який постійно змінюється та постійно і передбачає аналіз та оцінку різноманітних загроз, від розробки стратегій інформаційної безпеки до реалізації заходів з превентивного

реагування та відновлення. Ключовими аспектами державного управління інформаційною безпекою є створення ефективної політики захисту, оперативна відповідь на інциденти та взаємодія з різними зацікавленими сторонами. Системний підхід включає в себе регулярний аналіз інформаційних загроз, розробку стратегій управління ризиками та вдосконалення механізмів виявлення та реагування на інциденти. Залучення та співпраця з різними суб'єктами, включаючи державні органи, приватний сектор та громадянське суспільство, вирішує завдання створення єдиної системи захисту від інформаційних загроз. У цьому контексті, законодавче забезпечення грає ключову роль у визначенні правового статусу та взаємодії учасників процесу, забезпечуючи ефективне функціонування системи інформаційної безпеки. Важливо також враховувати швидкі зміни технологій та їх вплив на загрози, що вимагає постійного вдосконалення стратегій та технічних засобів захисту національної інформаційної інфраструктури.

Організаційно-правовий механізм державного управління інформаційною безпекою в Україні, зокрема через діяльність Державної служби спеціального зв'язку та захисту інформації України, відіграє визначальну роль у забезпеченні безпеки та ефективності державних комунікаційних систем. Організація виконує ряд стратегічних завдань, спрямованих на гарантування захисту інформації та кібербезпеки, що є критичними аспектами національної безпеки, особливо в умовах сучасних кіберзагроз та гібридних конфліктів. Враховуючи важливість інформаційної безпеки, основні законодавчі акти, такі як Закони України «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про державну таємницю», «Про захист персональних даних», і «Про основні засади забезпечення кібербезпеки України», становлять фундаментальний правовий каркас для регулювання цієї сфери. Державна служба спеціального зв'язку та захисту інформації України виступає ключовим ланцюгом у системі національної безпеки, забезпечуючи ефективне функціонування інформаційних систем та захист від кіберзагроз. Важливим аспектом є також наявність постанов КМУ, нормативних документів

та державних стандартів, які регулюють технічний захист інформації та функціонування КСЗІ. У контексті постійно зростаючих загроз та швидкого технологічного розвитку, організаційно-правовий механізм вказаної служби потребує постійного вдосконалення, а також врахування міжнародних стандартів та передового досвіду для забезпечення оптимального рівня інформаційної безпеки в Україні.

Зарубіжний досвід державного управління інформаційною безпекою в особі таких країн, як Естонія, Ізраїль, США та Сінгапур, становить цінний джерело навчання для України у вдосконаленні власної системи кібербезпеки. Естонія, завдяки передовій інформаційній інфраструктурі та ефективним практикам у галузі кібербезпеки, може послужити прикладом для впровадження систем електронної ідентифікації та ефективного реагування на кібератаки. Ізраїль, з своєю активною роботою у сфері інновацій та ефективного управління, демонструє, як високий рівень кібербезпеки може поєднуватися з інноваційним підходом та успішною співпрацею між різними секторами суспільства. США визначаються своєю систематичною роботою у галузі кібербезпеки, включаючи захист критично важливої інфраструктури та протидію кіберзагрозам через національну стратегію. Сінгапур, з високотехнологічною економікою та активними заходами в плані кібербезпеки, надає важливі уроки з розвитку кадрового потенціалу та впровадження передових технологій. Цей досвід дозволяє визначити ключові аспекти, які можуть бути використані для оптимізації стратегій управління інформаційною безпекою в Україні. Враховуючи високий рівень захисту інформації в зазначених країнах, Україна може взяти на увагу інноваційні методи та ефективні практики для забезпечення стійкості своєї інформаційної інфраструктури та ефективного впровадження заходів кібербезпеки. Такий підхід допоможе країні досягти найвищого рівня захисту в цифровому середовищі, а також сприятиме розвитку власного потенціалу в галузі кібербезпеки та інновацій.

РОЗДІЛ 2
АНАЛІЗ ДЕРЖАВНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В УКРАЇНІ

2.1. Аналіз кібератак в Україні в період війни

Оперативний центр реагування на кіберінциденти Державного центру кіберзахисту державної служби спеціального зв'язку та захисту інформації України є ключовим структурним вузлом в системі кібербезпеки країни.

Підсистема оперативного центру реагування на кіберінциденти є центральною складовою системи виявлення вразливостей і реагування на кіберінциденти та кібератаки і забезпечує:

1) централізоване управління усіма підсистемами системи виявлення вразливостей і реагування на кіберінциденти та кібератаки;

2) централізований збір та накопичення інформації про мережеві події інформаційної безпеки;

3) проведення моніторингу та обробки в режимі реального часу кіберзагроз та кіберінцидентів;

4) надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів та кібератак.

Підсистема оперативного центру реагування на кіберінциденти виявляє шкідливу активність, а також системні і мережеві аномалії на об'єктах кіберзахисту шляхом аналізу даних, отриманих з мережевих пристроїв (активні сенсори, міжмережеві екрани, сканери вразливостей), робочих та серверних станцій, систем авторизації, внутрішніх і зовнішніх джерел даних про кіберзагрози.

Проведення моніторингу, виявлення і протидії кіберзагрозам на об'єктах кіберзахисту, активне реагування на мережеві атаки забезпечують сенсори, які встановлюються на об'єктах кіберзахисту.

Система виявлення вразливостей і реагування на кіберінциденти та кібератаки з метою інформаційного обміну щодо кіберінцидентів, виявлення і припинення кібератак взаємодіє з центрами з управління кібербезпекою, галузевими центрами з управління кібербезпекою, іншими системами об’єктів критичної інформаційної інфраструктури, підприємств, установ та організацій незалежно від форми власності.

Нормативно-правова база:

1. Закон України «Про основні засади забезпечення кібербезпеки України»;

2. Указ Президента Указ Президента України від 26 серпня 2021 року № 447 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»«;

3. Постанова Кабінету Міністрів України від 23 грудня 2020 року № 1295 «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки».

4. Наказ Адміністрації Держспецзв’язку від 24 червня 2022 року № 284 «Про затвердження Порядку передачі комплектів обладнання підсистеми збору телеметрії інформаційно-комунікаційних систем (активні сенсори) системи виявлення вразливостей і реагування на кіберінциденти та кібератаки до об’єктів кіберзахисту».

Функції оперативного центру включають в себе:

1. Моніторинг і виявлення: проведення цілодобового моніторингу кіберпростору. Виявлення потенційних загроз та атак на інформаційні системи.

2. Аналіз та класифікація: аналіз та класифікація виявлених кіберзагроз за різними параметрами. Визначення потенційних наслідків інцидентів.

3. Реагування та відновлення: реалізація оперативних заходів щодо припинення кібератак та зменшення можливих збитків. Відновлення роботи інформаційних систем після інцидентів.

4. Співпраця та комунікації: взаємодія з іншими структурами забезпечення кібербезпеки. Надання рекомендацій та інформування зацікавлених сторін.

5. Попередження та освіта: здійснення превентивних заходів для уникнення можливих загроз. Проведення освітніх заходів для підвищення рівня кібербезпеки в общині.

Оперативний Центр Реагування відіграє критичну роль у забезпеченні кібербезпеки та захисті інформаційно-комунікаційних ресурсів України в умовах постійно змінюючогося кіберзагрозами ландшафту.

Система виявлення вразливостей і реагування на кіберінциденти та кібератаки представляє собою комплекс програмних та програмно-апаратних рішень, спрямованих на забезпечення постійного моніторингу, аналізу та передачі телеметричної інформації про події в кіберпросторі. Ці заходи спрямовані на виявлення та ефективне управління кіберзагрозами, які можуть виникнути або вже виникають на об’єктах кіберзахисту, здатні впливати негативно на їх стійке функціонування.

Ця система включає в себе ряд технологічних рішень, які працюють у взаємодії для надання повного спектру захисту. Серед них можуть бути інтелектуальні системи моніторингу мережі, аналізатори вразливостей, системи ідентифікації та відновлення, антивірусні та антишпигунські програми, системи реагування на інциденти, а також інші компоненти, спрямовані на посилення безпеки об’єктів інформаційно-комунікаційних систем.

Ця сукупність інструментів і технологій дозволяє оперативно виявляти, класифікувати та вирішувати кіберінциденти та кібератаки, що допомагає забезпечити надійний рівень кібербезпеки та управління ризиками в сучасному цифровому середовищі.

Підсистема Оперативного Центру Реагування на Кіберінциденти виступає ключовою компонентою в складі Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. Її завданням є централізоване керування всіма підсистемами системи, забезпечення централізованого збору та накопичення

інформації про мережеві події інформаційної безпеки, а також проведення моніторингу та оброблення в режимі реального часу кіберзагроз та кіберінцидентів.

Основні функції підсистеми оперативного центру реагування на кіберінциденти включають:

1. Централізоване управління: координація та управління всіма підсистемами системи виявлення вразливостей і реагування. Забезпечення єдиної стратегії реагування на кіберзагрози.

2. Збір та накопичення інформації: централізований збір даних про мережеві події та інциденти в інформаційній безпеці. Накопичення інформації для подальшого аналізу та створення звітів.

3. Моніторинг та оброблення в реальному часі: проведення моніторингу в режимі реального часу кіберзагроз та кіберінцидентів. Швидке реагування на виявлені загрози та вжиття заходів для їх ліквідації.

Підсистема оперативного центру реагування на кіберінциденти виявляє шкідливу активність та системні аномалії, аналізуючи дані з мережевих пристроїв, робочих та серверних станцій, систем авторизації та інших джерел даних про кіберзагрози. Це дозволяє оперативно визначати та вирішувати потенційні кіберінциденти для забезпечення безпеки об’єктів кіберзахисту.

Протягом першого кварталу 2023 року було проведено розширений аналіз за допомогою інструментів Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, що призвело до наступних результатів:

1. Оброблено 9 мільярдів подій, які були отримані в результаті моніторингу, аналізу та передачі телеметричної інформації про кіберінциденти та кібератаки.

2. Виявлено 7 мільйонів підозрілих подій інформаційної безпеки на етапі первинного аналізу.

3. Опрацьовано 34 тисячі критичних подій інформаційної безпеки, які були визначені як потенційні кіберінциденти через фільтрацію підозрілих подій і подальший вторинний аналіз.

4. Зареєстровано та оброблено безпосередньо аналітиками безпеки 202 кіберінциденти, які виявились найбільш значущими та вимагаючими негайного реагування.

Отримані результати свідчать про високий рівень ефективності та швидкості виявлення, аналізу та реагування на потенційні загрози кібербезпеки в розглядуваний період.

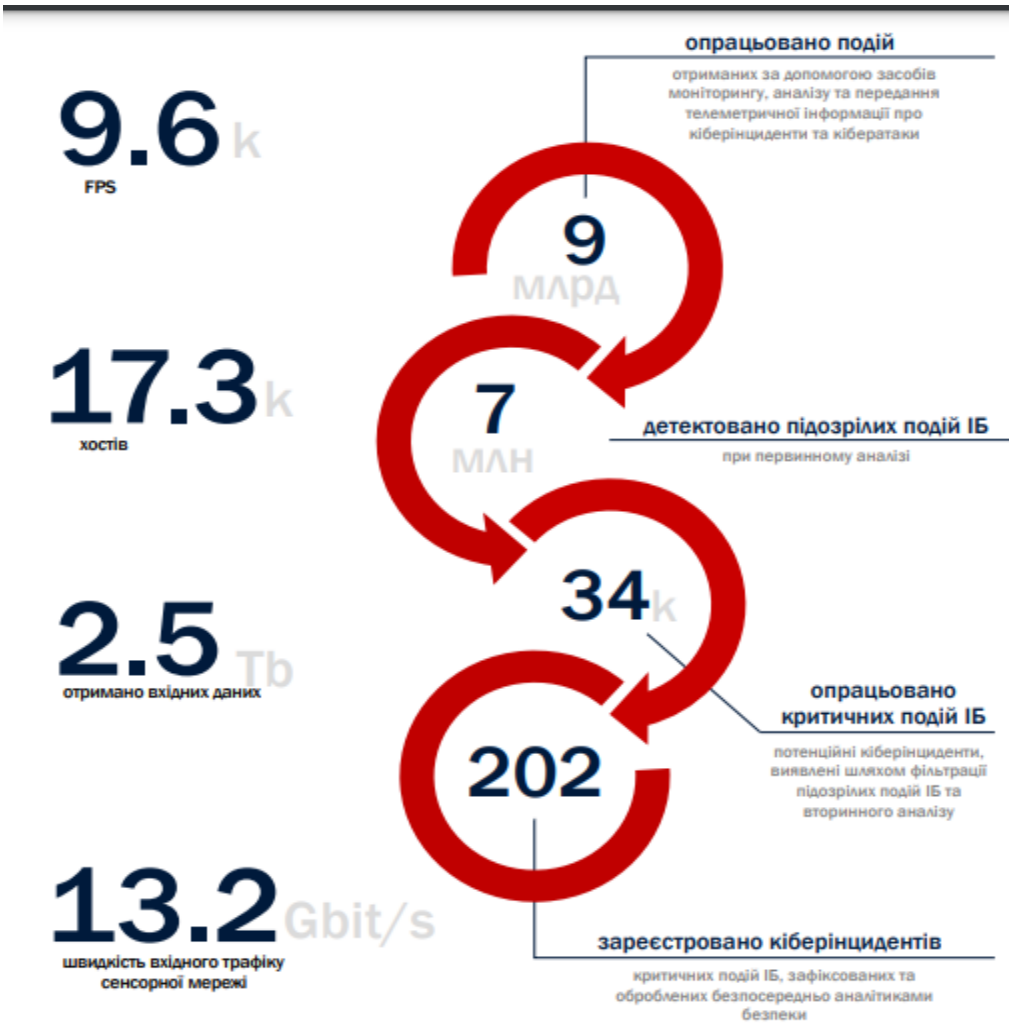

Рис.2.1. Кількість показників зібраних та опрацьованих даних

Джерело: звіт оперативного центру реагування на кіберінценденти [15]

За засобами моніторингу, аналізу та передачі телеметричної інформації про кіберінциденти та кібератаки було оброблено вражаючу кількість — 9 мільйонів подій, що відображає великий обсяг даних, підданих детальному вивченню. Під час першочергового аналізу вдалося виявити 7 мільйонів

підозрілих подій в галузі інформаційної безпеки (ІБ), що свідчить про високий рівень схильності до кіберзагроз.

Зареєстровано 202 кіберінциденти, які є критичними з точки зору подій ІБ. Ці кіберінциденти були екстрено визначені та оброблені професійними аналітиками забезпечення безпеки, підкреслюючи їх важливість та загрозливий характер.

Додатково, 34 тисячі потенційних кіберінцидентів пройшли детальну фільтрацію та вторинний аналіз, визначаючи їх як критичні події ІБ. Цей етап важливий для подальшого уточнення та покращення виявлення кіберзагроз, забезпечуючи високу ефективність у виявленні та реагуванні на потенційні загрози в кіберпросторі.

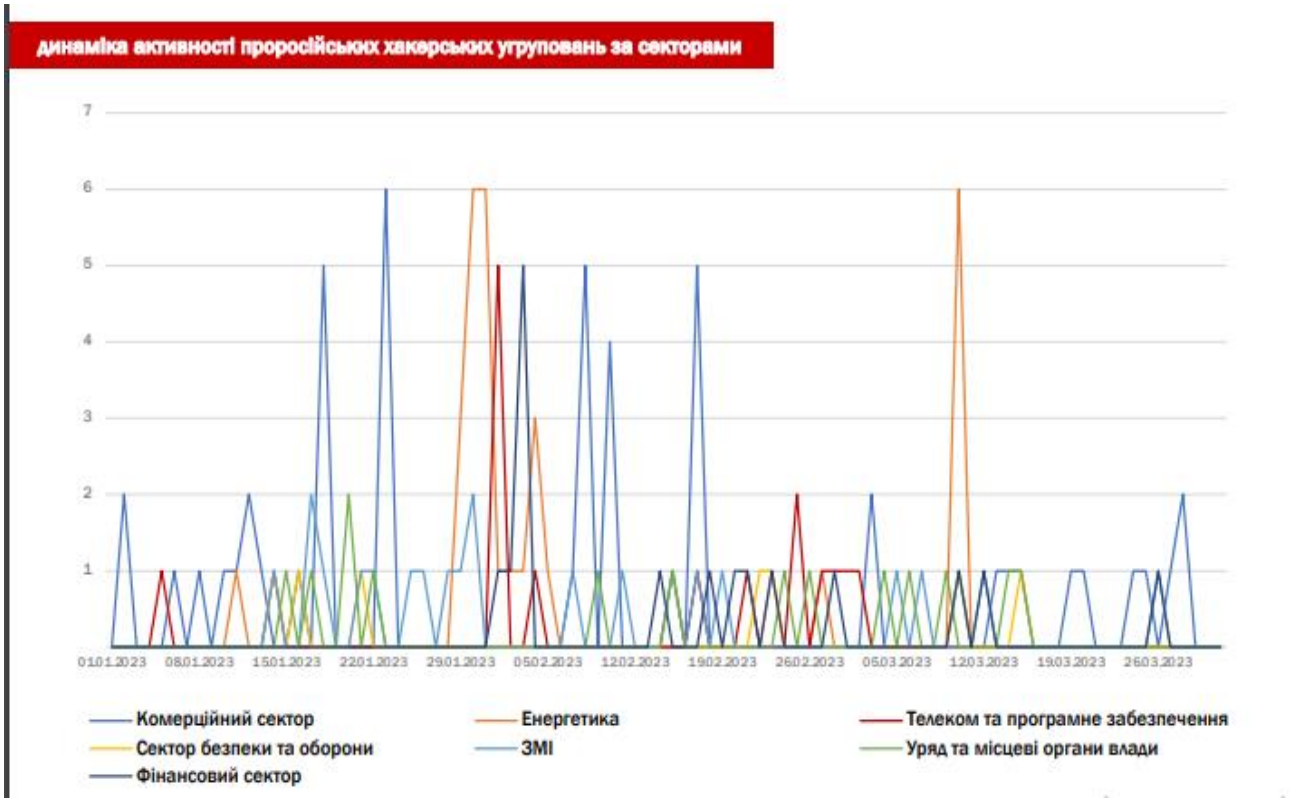

Рис.2.2. Динаміка активності проросійських хакерських угруповань за секторами [15]

У початку 2023 року відзначається помітне зменшення кількості кібератак, організованих проросійськими угрупованнями хактивістів, у порівнянні з IV кварталом 2022 року. Зниження є вражаючим, варіюючи від 1.5

до 2.9 разів у різних секторах, зокрема комерційному, фінансовому, урядовому та місцевому секторах влади, а також в секторі безпеки та оборони.

Це свідчить про ефективність вжитих заходів та удосконалених систем кіберзахисту, які були впроваджені протягом минулого періоду. Співвідношення зусиль між кіберзагрозами та захистом виявляється в користь захисних заходів, що сприяє стабільності в роботі ключових галузей.

BARAT, Emotet, Cobalt Strike та Meris визначаються як найбільш вживані C2 інфраструктури, які регулярно стають джерелом спроб мережевих вторгнень та порушень політик безпеки в організаціях. Ці шкідливі програми виявляються завдяки високотехнологічній Підсистемі збору телеметрії Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки.

BARAT відомий своєю здатністю обходити захист та залишатися непоміченим, використовуючи різні техніки введення. Emotet, у свою чергу, володіє високим ступенем складності та може встановлювати додатковий шкідливий код на заражених системах. Cobalt Strike використовується для проведення цільованих атак та може слугувати засобом для створення backdoors. Meris є сучасним троянцем, що активно використовується для кібершпигунства та викрадення конфіденційної інформації.

Щодо сімейств ШПЗ, що підпадають під категорію «02 Шкідливий програмний код», можна відзначити Snake Keylogger, який служить для ведення логування натискань клавіш і збору паролів; Agent Tesla, який відомий своєю функціональністю, включаючи відстеження клавіатури та збір паролів; LokiBot, який здатний виконувати широкий спектр функцій, включаючи витягування інформації з браузерів; PurpleFox, який використовується для експлуатації вразливостей і встановлення інших зловредних програм; та Formbook, який визначається своєю здатністю крадіжки облікових даних.

Ці зазначені деталі дозволяють більш повно і докладно уявити про різноманітні аспекти кіберзагроз, які виявляються та аналізуються в рамках системи виявлення та реагування на кіберінциденти.

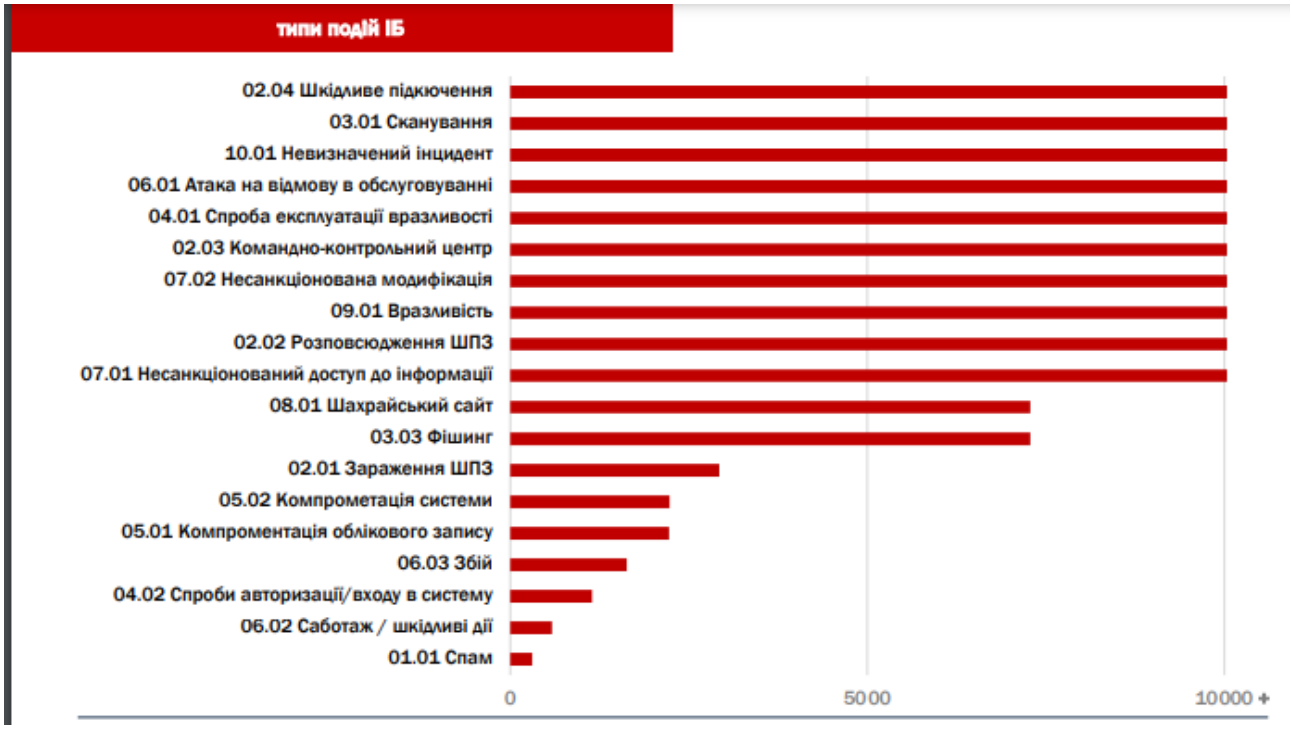

Рис.2.3. Типи подій в інформаційній безпеці

Джерело: звіт оперативного центру реагування на кіберінценденти [15]

Значною мірою сповільнення атак спостерігається в секторах, які раніше були особливо цільовими для хакерських груп. Зараз комерційні структури, фінансові установи, урядові та місцеві органи влади, а також сектор безпеки та оборони мають можливість працювати в більш безпечному і стійкому інтернет-середовищі.

Наприкінці 2022 року та на початку 2023 року залишається на тому ж рівні інтенсивність кібератак на сектори енергетики та ЗМІ. Це може свідчити про те, що ці галузі залишаються високопріоритетними об’єктами для кіберзагроз, та вимагають подальших заходів у забезпеченні кібербезпеки.

На рис.2.4. представлено динаміка активності проросійських хакерських угруповань станом на І квартал 2023 року.

Рис.2.4. Динаміка активності проросійських хакерських угруповань станом на I квартал 2023 року

Джерело: звіт оперативного центру реагування на кіберінценденти [15]

XakNet, NoName057(16), RussianHackersTeam, RaHDit та Free Civillian представляють собою найактивніші проросійські угруповання хактивістів на сучасній кіберарені. Протягом I кварталу 2023 року ці групи взяли на себе відповідальність за 90% від загальної кількості зафіксованих кібератак, що організовані подібними угрупованнями протягом цього звітного періоду.

XakNet відомий своєю високоорганізованою та спритною командою хакерів, які використовують різноманітні техніки для проведення кібератак на об’єкти з інтересами, що співпадають із проросійською агендою. NoName057(16) славиться своєю анонімністю та ефективністю у сфері хакерської діяльності, часто використовуючи різні методи атак.

RussianHackersTeam володіє розгалуженою структурою та великими ресурсами, що дозволяє їй втілювати складні та масштабні кібератаки на різні об’єкти. RaHDit відомий своєю агресивною кібердіяльністю, яка орієнтована на виклик іншим країнам та організаціям. Free Civillian виступає проти визначених політичних та соціальних поглядів, використовуючи кібератаки як інструмент для вираження своїх переконань.

Ці угруповання активно впливають на кіберпростір, завдяки своїм високотехнологічним здібностям та глибокій аналітиці. Заходи по забезпеченню кібербезпеки повинні бути направлені на ефективне виявлення, відповідь та захист від атак, що організовані цими угрупованнями, з метою запобігання потенційним серйозним наслідкам для цільових систем та організацій.

На діаграмі 2.5. наведено інфраструктуру управління та контролю (C2), що була залучена до потенційно шкідливої мережевої активності або порушень політик безпеки організацій. Ці потенційні загрози були виявлені у вихідному мережевому трафіку за допомогою Підсистеми збору телеметрії Системи виявлення вразливостей та реагування на кіберінциденти/кібератаки.

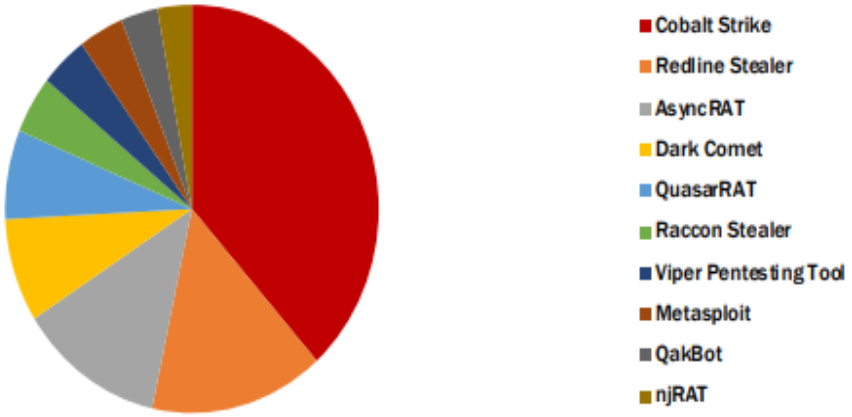

Рис.2.5. C2 детектування в подіях ІБ, пов’язаних із вихідним трафіком

Джерело: звіт оперативного центру реагування на кіберінценденти [15]

З першого кварталу 2023 року докладено про понад 80 000 випадків мережевих вторгнень та 600 вихідних з’єднань із унікальними серверами командно-контрольного управління (C2). Ці дані отримані від платформи Recorded Future та ідентифіковані як такі, що належать до зазначених категорій.

За допомогою методів проактивного сканування та систематичного збору даних, зазначена платформа веде моніторинг за процесами створення та модифікації інфраструктури, яку використовують інструменти пост-експлуатації, кастомні зловмисні програми та трояни дистанційного доступу з

відкритим кодом з метою осушествлення кібератак та подальшої експлуатації компрометованих систем.

Ці дані свідчать про високий рівень активності кіберзлочинців, які застосовують різноманітні техніки та інструменти для реалізації мережевих атак та забезпечення подальшої експлуатації уражених систем.

Враховуючи динамічний характер кіберзагроз та постійне розвиток методів атак, надзвичайно важливо постійно вдосконалювати системи кіберзахисту та застосовувати ефективні заходи для виявлення та реагування на ризики, пов’язані із мережевим простором. Ці заходи є неодмінною частиною стратегії забезпечення інформаційної безпеки та запобігання кібератак.

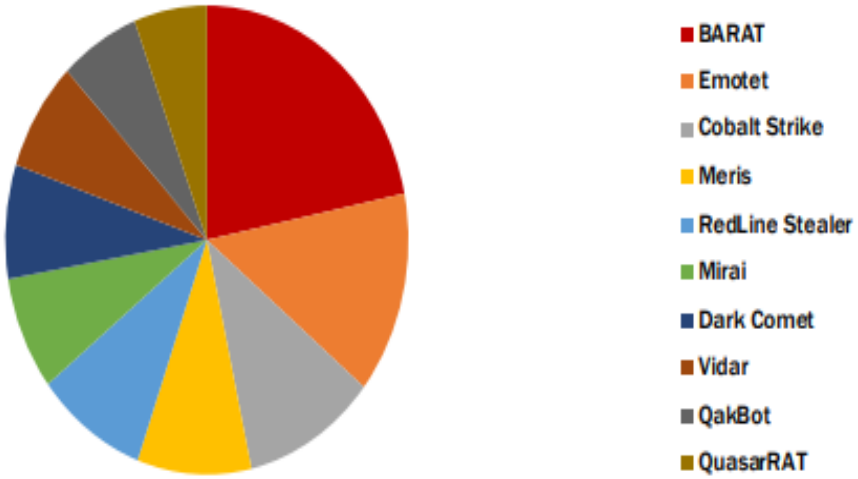

Рис.2.6. C2 детектування в подіях ІБ, пов’язаних із вхідним трафіком

Джерело: звіт оперативного центру реагування на кіберінценденти [15]

У першому кварталі 2023 року серед серверів, які мають відношення до потенційно шкідливої мережевої активності та порушень політик безпеки організацій, варто відзначити домінування кількох видів серверів. Зокрема, до категорії OST (Operational Security Tools) входять такі сервери, як Cobalt Strike та Metasploit, які відзначаються своєю високою функціональністю та здатністю емулювати атаки для оцінки вразливостей систем безпеки.

Сервери типу RAT (Remote Access Trojan), зокрема BARAT, AsyncRAT, QuasarRAT та njRAT, відіграють значущу роль у сценаріях віддаленого

доступу, які можуть використовуватися для незаконного керування комп’ютерами або мережами, а також для здійснення атак і збору конфіденційної інформації.

Серед сімейств ботнетів, які виявилися активними у зазначений період, варто виділити Emotet, Mirai та Meris. Emotet відомий своєю здатністю поширювати інші види шкідливого коду, Mirai спрямований на зараження Інтернету речей (IoT), а Meris визначається своєю ефективністю у реалізації кібератак.

Аналіз та вивчення цих типів серверів стає важливою частиною кіберзахисту, оскільки дозволяє розуміти характер та методики потенційних кіберзагроз, а також розробляти стратегії захисту та виявлення атак для забезпечення безпеки мереж та інформаційних ресурсів.

2.2. Фінансовий механізм державного управління інформаційною безпекою в Україні

Фінансовий механізм державного управління інформаційною безпекою в Україні визначається розподілом видатків з державного бюджету на ключові напрями, спрямовані на забезпечення ефективності та надійності системи інформаційної безпеки. Серед основних напрямків фінансування можна виділити наступні:

1. Адміністрація Державної служби спеціального зв’язку та захисту інформації України: забезпечення необхідних фінансових ресурсів для оплати праці та функціонування адміністративного апарату.

2. Забезпечення функціонування державної системи спеціального зв’язку та захисту інформації: видатки на технічне обслуговування, ремонт та оновлення засобів зв’язку та захисту інформації. забезпечення програмних та апаратних засобів для забезпечення безпеки інформаційних систем.

3. Розвиток і модернізація державної системи спеціального зв’язку та захисту інформації: фінансування проектів інноваційного розвитку та впровадження новітніх технологій у сфері інформаційної безпеки.

4. Підготовка, перепідготовка та підвищення кваліфікації кадрів у сфері зв’язку закладами вищої освіти: фінансування освітніх програм та тренінгів для підготовки кваліфікованих фахівців у галузі інформаційної безпеки.

5. Будівництво (придбання) житла для військовослужбовців Державної служби спеціального зв’язку та захисту інформації України: забезпечення соціальної та житлової інфраструктури для персоналу, залученого до забезпечення інформаційної безпеки.

6. Головне управління урядового фельд’єгерського зв’язку Державної служби спеціального зв’язку та захисту інформації України: фінансування діяльності та розвитку управління, включаючи координацію підрозділів урядового фельд’єгерського зв’язку.

7. Доставка дипломатичної кореспонденції за кордон і в Україну, доставка спеціальної службової кореспонденції органам державної влади: фінансування логістичної інфраструктури для забезпечення безпечної та конфіденційної передачі кореспонденції.

Фінансовий механізм забезпечує відповідні ресурси для здійснення цих напрямків та забезпечує стабільність та ефективність системи інформаційної безпеки в Україні.

На рис.2.7. представлено видатки на інформаційну безпеку України за 2018-2023 роки.

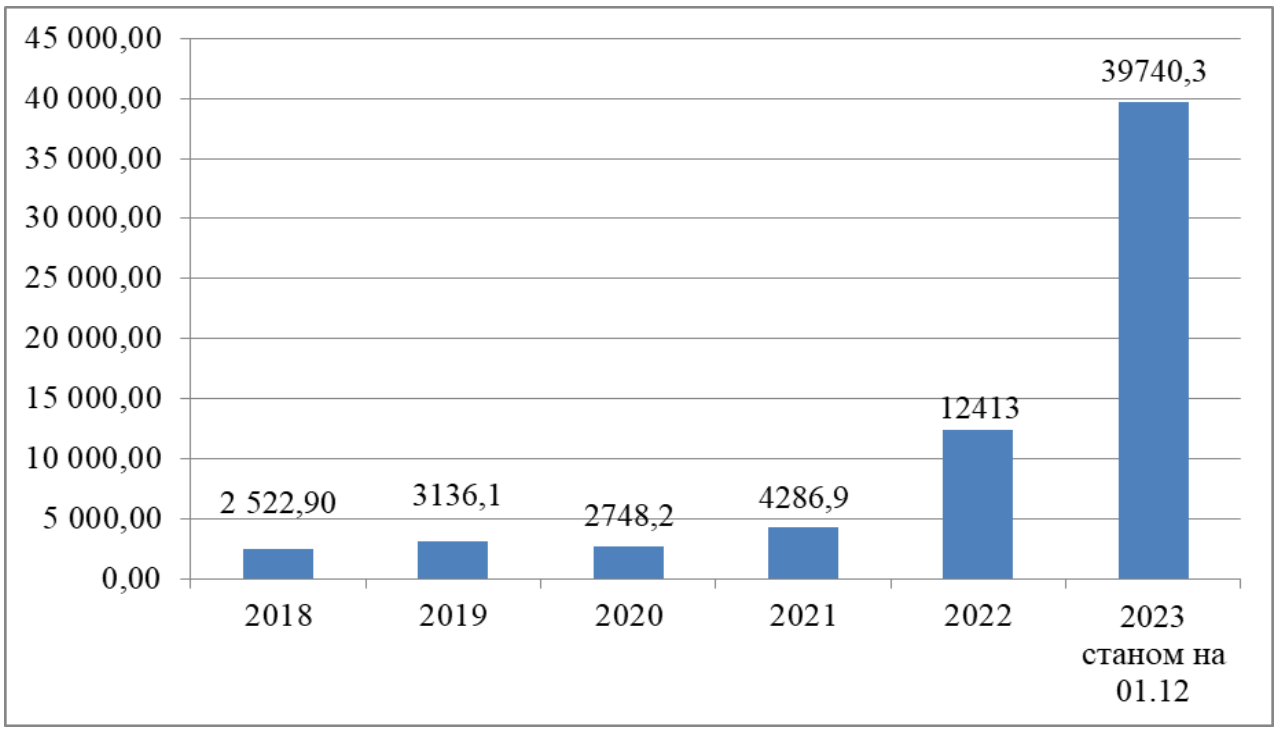

Рис.2.7. Видатки державного бюджету на інформаційну безпеку в Україні, млн.грн.

Джерело: складено автором згідно даних openbudget.gov.ua

Зростання видатків на інформаційну безпеку в Україні вказує на серйозні виклики та високий пріоритет, який приділяє держава захисту інформаційних ресурсів у сучасних умовах, особливо під час воєнного конфлікту. Різке збільшення видатків в 2023 році в порівнянні з попередніми роками свідчить про рішучий курс на підвищення ефективності та масштабів заходів з інформаційного захисту в умовах військових дій.

Аналіз років 2022 та 2023 років вказує на те, що держава витрачає значно більше ресурсів для забезпечення інформаційної безпеки в умовах війни. Це може включати в себе розвиток та модернізацію технічних та програмних засобів, підвищення кваліфікації персоналу, а також підвищення загального рівня захищеності інформаційних систем.

Збільшення видатків може бути також пов’язане із запровадженням нових заходів та стратегій інформаційної безпеки, в тому числі з посиленням заходів щодо захисту важливих інформаційних об’єктів та критичної інфраструктури.

Зростання видатків може бути спрямовано на підвищення реагування на кіберзагрози та забезпечення високого рівня стійкості інформаційних систем у воєнний період.

Важливо відзначити, що це збільшення видатків свідчить про серйозне ставлення держави до захисту інформаційної безпеки в умовах війни та свідчить про готовність вживати всі необхідні заходи для забезпечення кібернетичної безпеки країни в таких складних умовах.

В табл.2.1 представлено видатки в напрямку інформаційної безпеки в Україні за напрямками.

Таблиця 2.1

Видатки в напрямку інформаційної безпеки в Україні за напрямками

Назва	Роки				
	2019	2020	2021	2022	2023 станом на 01.12
Адміністрація Державної служби спеціального зв`язку та захисту інформації України	2922,8	2526,1	4050,4	11816,5	39162,2
Забезпечення функціонування державної системи спеціального зв'язку та захисту інформації	2093,3	1991,9	2639,6	7816,4	7225,6
Розвиток і модернізація державної системи спеціального зв'язку та захисту інформації	707,4	376,2	1245,3	3124,6	986,7
Підготовка, перепідготовка та підвищення кваліфікації кадрів у сфері зв'язку закладами вищої освіти	102,8	112,9	132,4	286,6	192
Будівництво (придбання) житла для військовослужбовців Державної служби спеціального зв'язку та захисту інформації України	19,1	45,1	33,1	47,5	15,9
Здійснення заходів із забезпечення спеціальною технікою та обладнанням	0	0	0	0	30742
Головне управління урядового фельд'єгерського зв'язку Державної служби спеціального зв'язку та захисту інформації України	213,2	222,1	236,4	596,4	578
Доставка дипломатичної кореспонденції за кордон і в Україну	7,5	2,1	5,6	5,8	10,1
Доставка спеціальної службової кореспонденції органам державної влади	205,7	220	230,8	590,6	567,9
Разом	3136	2748,2	4286,8	12412,9	39740,2

Джерело: складено автором згідно даних openbudget.gov.ua

Зазначені суми видатків державного бюджету на інформаційну безпеку в Україні свідчать про розподіл коштів на два ключових напрямки:

1. Адміністрація Державної служби спеціального зв’язку та захисту інформації України: сума видатків на цей напрямок станом на 01.12.2023 року складає 39162,2 млн.грн. Це свідчить про великі фінансові ресурси, які спрямовані на забезпечення діяльності та функціонування адміністративного апарату Державної служби спеціального зв’язку та захисту інформації України. Ймовірно, це включає витрати на оплату праці, закупівлю технічних та програмних засобів, модернізацію інфраструктури та інші адміністративні витрати.

2. Головне управління урядового фельд’єгерського зв’язку Державної служби спеціального зв’язку та захисту інформації України: сума видатків на цей напрямок станом на 01.12.2023 року складає 578 млн.грн. Це менша сума порівняно з видатками на адміністрацію, що може вказувати на те, що ресурси для Головного управління урядового фельд’єгерського зв’язку використовуються для конкретних завдань, пов’язаних із забезпеченням фельд’єгерського зв’язку, доставкою кореспонденції та іншими сферами діяльності.

Враховуючи обидва напрямки видатків, можна припустити, що держава серйозно вкладає ресурси у підтримку та розвиток інфраструктури зв’язку та захисту інформації в умовах війни, спрямовуючи їх на різноманітні завдання, пов’язані з інформаційною безпекою країни.

На рис.2.8. представлено динаміку видатків на «Адміністрація Державної служби спеціального зв`язку та захисту інформації України» за 2019-2023 рік.

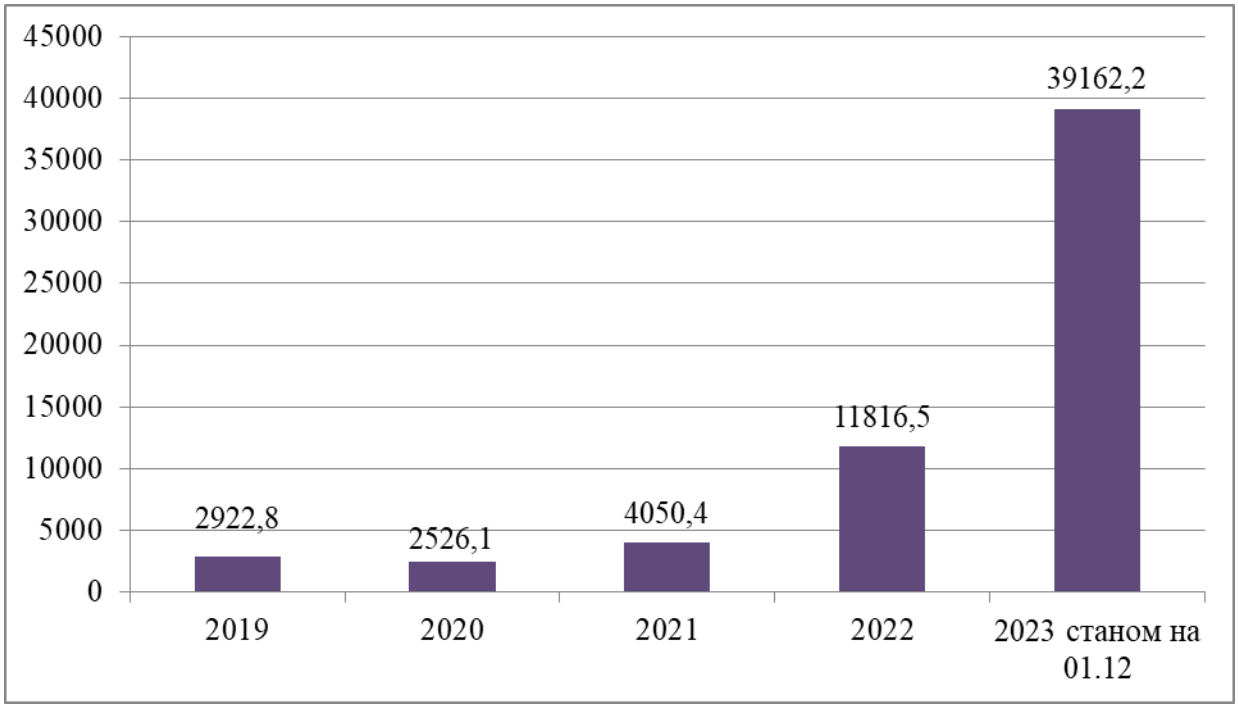

Рис.2.8. Динаміка видатків на «Адміністрація Державної служби спеціального зв`язку та захисту інформації України» за 2019-2023 рік, млн.грн.

З графіку можна побачити, що 2023 році видатки на «Адміністрація Державної служби спеціального зв`язку та захисту інформації України» значно збільшились порівно з попередніми роками і склали 39162,2 млн.грн. Вони розподіляються на: забезпечення функціонування державної системи спеціального зв’язку та захисту інформації; розвиток і модернізація державної системи спеціального зв’язку та захисту інформації; підготовка, перепідготовка та підвищення кваліфікації кадрів у сфері зв’язку закладами вищої освіти; Будівництво (придбання) житла для військовослужбовців Державної служби спеціального зв’язку та захисту інформації України.

На рис.2.9. представлено структур видатків на «Адміністрація Державної служби спеціального зв`язку та захисту інформації України» станом на 01.12.2023 року.

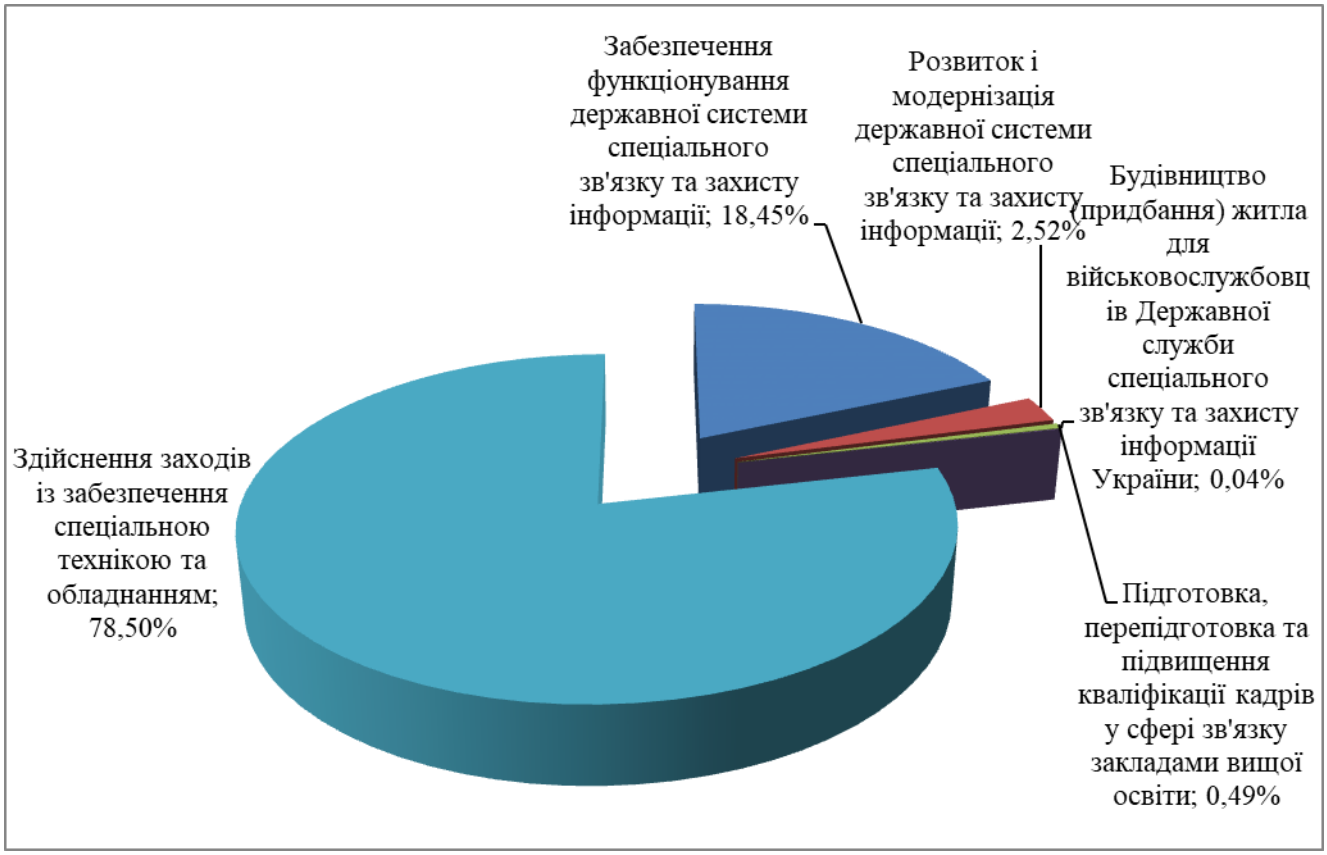

Рис.2.9. Структура видатків на «Адміністрація Державної служби спеціального зв`язку та захисту інформації України» станом на 01.12.2023 року,%

Станом на 01.12.2023 року, розподіл видатків свідчить про фокус на конкретні напрямки, які є стратегічно важливими для забезпечення ефективності та ефективності системи інформаційної безпеки в умовах війни. Зокрема:

1. Здійснення заходів із забезпечення спеціальною технікою та обладнанням: найбільша частина видатків, а саме 30742 млн.грн., спрямована на забезпечення спеціальною технікою та обладнанням. Це може включати закупівлю та модернізацію спеціальних засобів зв'язку, програмного забезпечення для захисту інформації, а також інфраструктурних рішень, спрямованих на підвищення стійкості інформаційних систем.

2. Забезпечення функціонування державної системи спеціального зв'язку та захисту інформації: до 18,45% видатків, тобто 7225,6 млн.грн., припадає на забезпечення функціонування державної системи спеціального

зв'язку та захисту інформації в рамках адміністративних витрат. Це може включати оплату праці персоналу, утримання інфраструктури, ремонт та технічне обслуговування засобів зв'язку, а також проведення навчань та тренінгів для персоналу.

Загальна сума видатків та їхній розподіл свідчать про серйозні заходи для забезпечення та підтримки дії інформаційної безпеки в умовах війни, включаючи не лише адміністративні аспекти, але й технічне забезпечення та модернізацію системи.

На рис.2.10 представлено видатки за напрямком «Головне управління урядового фельд'єгерського зв'язку Державної служби спеціального зв'язку та захисту інформації України» за 2019-2023 роки.

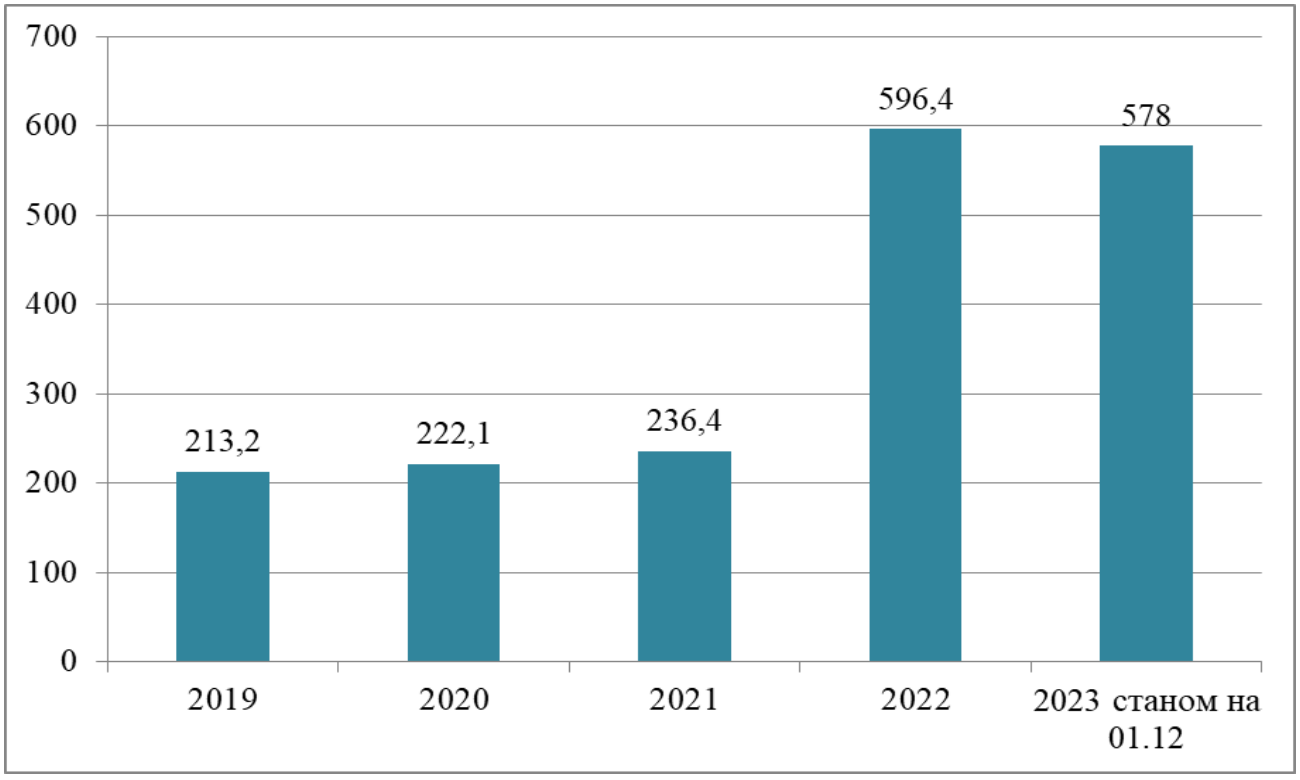

Рис.2.10. Видатки за напрямком «Головне управління урядового фельд'єгерського зв'язку Державної служби спеціального зв'язку та захисту інформації України» за 2019-2023 роки, млн.грн.

Видатки на «Головне управління урядового фельд'єгерського зв'язку Державної служби спеціального зв'язку та захисту інформації України» станом

на 01.12.2023 року склали 578 млн.грн., порівно з 2022 роком вони практично не змінились. Факт, що видатки на «Головне управління урядового фельд’єгерського зв’язку Державної служби спеціального зв’язку та захисту інформації України» станом на 01.12.2023 року залишились практично на тому ж рівні, що і в 2022 році (578 млн.грн.), може свідчити про стабільність фінансування цього напрямку. Збереження рівня фінансування може бути важливим для забезпечення надійності та ефективності функцій урядового фельд'єгерського зв'язку, особливо в умовах збільшеної активності та потреб у дипломатичній та службовій кореспонденції.

Розподіл видатків на «Доставку дипломатичної кореспонденції за кордон і в Україну» та «Доставку спеціальної службової кореспонденції органам державної влади» свідчить про важливі аспекти діяльності управління, зокрема:

1. Доставка дипломатичної кореспонденції за кордон і в Україну: фінансування цього напрямку може бути важливим для забезпечення конфіденційної та безпечної доставки дипломатичної кореспонденції, що є критичним в умовах геополітичної напруженості та дипломатичних відносин.

2. Доставка спеціальної службової кореспонденції органам державної влади: фінансування цього напрямку може включати в себе витрати на забезпечення безпеки та конфіденційності при передачі службової кореспонденції між різними органами державної влади.

Збереження стабільного рівня фінансування цих напрямків свідчить про важливість урядового фельд'єгерського зв'язку та підтримку його функцій, особливо в умовах, коли безпека та конфіденційність комунікацій стають надзвичайно важливими.

На рис.2.11 представлено структуру видатків на «Головне управління урядового фельд’єгерського зв’язку Державної служби спеціального зв’язку та захисту інформації України» станом на 01.12.2023 року.

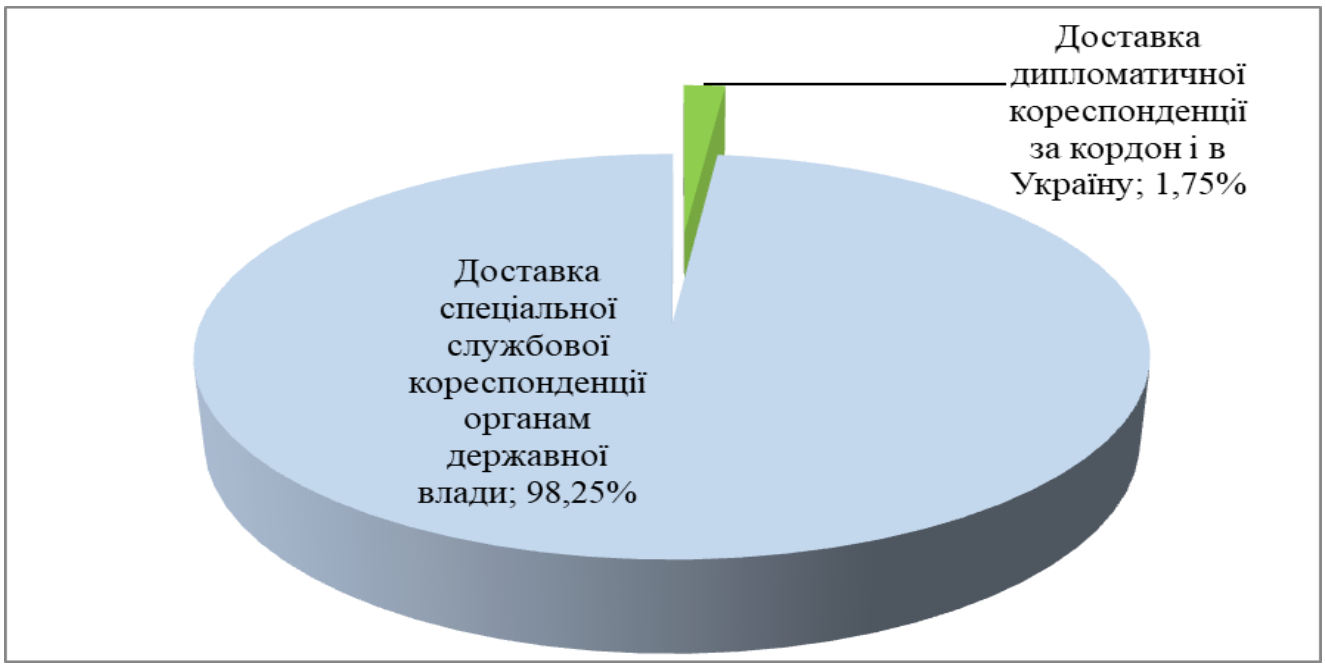

Рис.2.11. Структура видатків на «Головне управління урядового фельд'єгерського зв'язку Державної служби спеціального зв'язку та захисту інформації України» станом на 01.12.2023 року,%

Отже, найбільшу частку у видатках на «Головне управління урядового фельд'єгерського зв'язку Державної служби спеціального зв'язку та захисту інформації України» станом на 01.12.2023 року склали видатки на Доставку спеціальної службової кореспонденції органам державної влади, а саме 98,25%, це складає 567,9 млн.грн., на Доставка дипломатичної кореспонденції за кордон і в Україну видатки склали 10,1 млн.грн, їх частка 1,75%.

2.3. Інформаційна безпека в умовах воєнного стану

Інформація під час війни стає потужною зброєю. Неуважне ставлення до неї може призвести до серйозних наслідків – підриву державної безпеки або підігравання пропаганді країни-ворога. Розповідаємо, як цього не зробити та стати корисним на інформаційному фронті.

Що потрібно знати про інформацію у час війни?

- Поширюється надто динамічно. Через появу нових технологій (інтернету, соцмереж) інформація позбулася таких обмежень, як географія, час та швидкість отримання повідомлення. Тепер про те, що трапилося в одному куточку світу, за лічені секунди дізнаються в іншому. Під час війни інфоприводів більшає, тож інформація поширюється динамічніше.
- Поширюється у великих обсягах. Через збільшення інфоприводів збільшується і кількість фейків, які поширює РФ, аби приховати власні злочини та посіяти сумніви. Якщо до цього ще додати створення пропагандистами у соцмережах нових каналів і груп, що діють зі злочинною метою, то обсяг інформації збільшується у кілька разів. Наразі спостерігається така собі інфодемія 2.0.
- Війна відбувається також в інформаційному полі. Ворог провокує, поширює панічні повідомлення, розробляє та проводить інформаційно-психологічні операції, аби деморалізувати населення інформаційно.

Що не можна публікувати

Під час війни з’являються нові правила та обмеження в публікаціях. Усі вони наближають нашу перемогу, бо не дають ворогу інформацію, яку можна використати проти України. Адже під час війни російські спецслужби активно шукають в українському інфопросторі компромати, інфоприводи, геолокації, наслідки влучання тощо.

Тож Міністерство культури та інформаційної політики України застерігає не публікувати в реальному часі чи без офіційної інформації від державних органів України:

- фото та відео місцевості, де відбувся обстріл;
- відео з ракетами, що летять, моменти попадання снарядів;
- точні адреси та координати місць бойових дій;
- відео/фото з розпізнавальними знаками: таблички з назвами вулиць, станціями метро, автобусними зупинками, магазинами та супермаркетами, заводами й підприємствами, номери авто;
- роботу української ППО;

- відео та фото влучання ракет;
- будь-які дані про дії та переміщення українських військ, а також основні військові об’єкти;
- неперевірену інформацію про потерпілих чи загиблих;
- будь-яку інформацію, яка не верифікована державою та не з офіційних джерел;
- категорично заборонено стримити в прямому етері ракетний обстріл і бомбардування. Такими кадрами ви допоможете ворогу коригувати вогонь. Почекайте з публікацією;
- озвучувати та уточнювати дані в коментарях також заборонено.

Озвучувати такі дані можна лише після появи інформації про російську атаку та її наслідки від державних органів України.

Також, за рекомендаціями Міністерства оборони України, в жодному випадку не публікуйте в реальному часі:

- фото і відео пусків наших ракет протиповітряної оборони;
- фото і відео позицій наших засобів ППО;
- яка українська зброя де може стояти таякі об’єкти прикривати;
- скільки одиниць техніки бачили чи пусків ракет чули.

Росіяни використовують таку інформацію для розвідки, прокладання маршрутів застосування ракет для обходу наших ППО, коригування та завдання ударів по самих засобах ППО.

Також у Міністерстві внутрішніх справ закликають не поширювати фото та відео дронів, де видно їхні серійні номери. Будь-яка інформація про місце вибуху, про те, який конкретно дрон і з яким номером досягнув чи не досягнув мети, є також підказкою ворогу.

80% розвідінформації ворог отримує з відкритих джерел, і подібні повідомлення дають змогу коригувати вогонь.

Держспецзв’язку України також пропонує кілька порад, як не варто писати:

- *«Ракета влучила у школу №7».*

- *«Ракетою цілилися в вокзал, а влучили в лікарню, яка розташована поруч».*
- *«Ракета влучила в склад поряд із аеродромом».*

Такі повідомлення описують місцевість і дають ворогу додаткову інформацію щодо об’єктів на певній території.

Як не «зіграти на руку» російській пропаганді?

Правила публікацій переважно не надто відрізняються від загальноприйнятих журналістських норм у звичний мирний час. Проте у воєнний час деякі з них стають особливо важливими, аби не підіграти ненавмисно країні-ворогу та його пропаганді.

Не давайте хайпові, провокативні заголовки

Ними легко може скористатися ворог, адже це один із поширених способів маніпуляції російської пропаганди. Заголовки, які не вітаються у звичайний час, у воєнних умовах стають особливо небезпечними.

Користуйтесь офіційними джерелами

Не ведіться на панічні повідомлення з Facebook-груп, Telegram-каналів тощо. Не нагнітайте паніку публікаціями з посиланням на неперевірені джерела. Не допомагайте цим російській пропаганді, яка і так намагається посіяти паніку серед українців з допомогою різних інформаційно-психологічних операцій та інформаційних атак.

Крім того, з розквітом технологій розпочалася ера «диванних експертів». Тепер кожен може назвати себе «експертом», створивши лише профіль у соцмережі та коментуючи, як правило, все підряд.

Ще одна маніпуляція, що народжується під впливом соцмереж, — «соцмережі гнівно відреагували» і подібні повідомлення.

По-перше, дуже важко виявити, як насправді відреагували соцмережі, бо вони мають алгоритми, а отже інформаційні бульбашки (наприклад, у Facebook). І те, що бачите ви, необов’язково бачить хтось інший, відповідно й вам теж важко побачити альтернативну думку. Це ж стосується Telegram — хоч соцмережа дає можливість підписатися на певні сторінки та бачити

хронологічну стрічку в кожному каналі, ви не побачите, що публікують інші канали та яку думку просувають.

По-друге, навіть якщо говорити про коментарі під певним дописом, вони не можуть представляти думку більшості (хтось бачив цей допис, а когось він, наприклад, оминув алгоритмами). Загалом, ви ніколи не побачите повноцінної картини реакції людей на щось на основі лише реакцій та коментарів у соцмережах. Відповідно подібні повідомлення показують нерелевантні дані, які лише спотворюють реальну картину. Про думку більшості можуть говорити лише реальні статистичні дані, отримані в результаті досліджень соціологічними компаніями. Хоча не всі вони є достовірними. Перевірити, чи не використовуєте ви раптом маніпулятивну статистику, можна в базі псевдосоціологів від «Текстів».

Не поширюйте пропаганду як факт без спростувань і пояснень

Так ви допомагаєте збільшувати охоплення для пропагандистських дезінформаційних меседжів. У заголовках або матеріалах з використанням російських повідомлень вказуйте, що це неправдива або маніпулятивна інформація. Російське твердження беріть в лапки та поясніюйте, чому поширене російською пропагандою повідомлення є дезінформацією чи додавайте спростування від професійних фактчекінгових організацій.

Якщо робите спростування самостійно, то побудуйте його за принципом «сендвіча»:

- Факти, те, що сталося насправді.
- Зміст фейку.
- Спростування та завершення справжнім фактом.

Такий варіант розвінчування фейку допоможе не тиражувати сам фейк та не акцентувати на неправдивій інформації.

Лише з часом через знання правди та зменшення зацікавленості аудиторії зменшуватиметься його охоплення. Головне завдання спростування — попередити аудиторію про інформаційну загрозу, яка може чатувати на неї.

У час війни найважливіше — це співпраця. Якщо ви побачили в медіа ваших колег помилковий неправдивий контент — повідомте їм про це. А також перепубліковуйте спростування від професійних фактчекінгових організацій, аби воно дісталося якомога більшої аудиторії.

Не поспішайте перепубліковувати західні медіа

Аналізуйте та фільтруйте інформацію завжди, навіть отриману від західних ЗМІ. По-перше, російська пропаганда може ховатися і там. Адже вона має велику систему своїх «експертів» у всьому світі, що тиражують власні колонки, зокрема у західних ЗМІ, аби просувати кремлівські ідеї. Тож перед републікацією перевірте, хто автор статті, чи не просуває він російські наративи, чи не був замішаний у співпраці з Кремлем, які його попередні публікації та відгуки про нього.

По-друге, західні ЗМІ можуть мати певне нерозуміння щодо подій в Україні, тож можуть публікувати ненавмисний маніпулятивний контент.

По-третє, зважайте на рівень редакції та якість медіа. У західному інформаційному просторі також вистачає сайтів-сміттярок та російських пропагандистських сайтів, що мімікрують під достовірні західні медіа.

Перевірка на правдивість

Фактчекінг — це один з основних етапів створення журналістського матеріалу. Не нехтуйте цим етапом особливо у час війни! Уважно перевіряйте джерела та інформацію, яку публікуєте. Пам’ятайте: російські пропагандисти так само відстежують український інформаційний простір. А одна із їхніх цілей — шукати «підтвердження» російським наративам.

Наприклад, один із поширених російських меседжів серед чиновників, медіа та анонімних Telegram-каналів — «українські медіа поширюють фейки та дезінформують суспільство». Тож не давайте приводу російській пропаганді «підтверджувати» їхній меседж власною неуважністю чи недбалістю.

Як стати корисним на інформаційному фронті?

- Розповідайте світу про злочини російських окупантів. Після отримання офіційної інформації від державних органів України сповіщайте про

постраждалих унаслідок російських атак, зруйновані об’єкти архітектури та інші злочини РФ на території України. Світ має знати правду. Проте враховуйте у таких публікаціях рекомендації від державних органів України, наведені в цьому матеріалі.

- Якщо маєте важливу інформацію про місця перебування окупантів, дислокацію ворожої техніки, російські воєнні злочини, поділіться нею з відповідними державними органами України. Наприклад, невдовзі після початку повномасштабного російського вторгнення Міністерство цифрової трансформації створило чат-бот у Telegram «єВорог». З його допомогою можна повідомити про окупантів, колаборантів, російських вбивць і вибухонебезпечні предмети, які залишили окупанти.

Висновки до розділу 2

З початку 2023 року порівняно з IV кварталом 2022 року відзначається зменшенням загальної кількості кібератак, які організовують угруповання проросійських хактивістів. Однак, не дивлячись на це, систематичність та інтенсивність таких атак залишаються на високому рівні. Це свідчить про те, що хактивісти, спрямовані на розповсюдження проросійської агенди, продовжують активно використовувати кіберзброю для досягнення своїх цілей. Необхідно врахувати посилення інформаційних операцій, ініційованих Кремлем, щодо виправдання можливого вторгнення в Україну. Це створює умови для затяжної війни в Україні, що може призвести до збільшення інтенсивності та різноманітності кібератак на українські організації різних форм власності та галузей. З цим контекстом не можна вважати, що тренд до зменшення кількості кібератак залишиться стійким, іншими словами, цей різкий спад може бути тимчасовим, а не сталим явищем. У таких умовах важливо для організацій в Україні приділяти особливу увагу підвищенню рівня кібербезпеки та вживати заходів для ефективного виявлення, протидії та відновлення в разі кібератак.

Україна видає ресурси на забезпечення інформаційної безпеки, визнавши актуальність цього питання в умовах сучасного геополітичного та кібербезпекового середовища. За період з 2018 по 2023 роки спостерігається значне зростання обсягів фінансування на цей напрям, що свідчить не лише про постійний розвиток інформаційних технологій, але й про розуміння необхідності вдосконалення систем і заходів кіберзахисту. Основний акцент робиться на розвиток і модернізацію системи спеціального зв'язку, яка відіграє критичну роль у забезпеченні безпеки та конфіденційності обміну інформацією між владними органами. Зокрема, урядовий фельд'єгерський зв'язок отримав значне фінансування для доставки спеціальної службової кореспонденції органам державної влади, де частка видатків станом на 01.12.2023 року складає 98,25% або 567,9 млн.грн. Такий акцент свідчить про визнання важливості надійної і безпечної передачі інформації між ключовими структурами країни. Стабільність та сталість фінансування цих процесів є ключовим фактором, який вказує на систематичний та дбайливий підхід до забезпечення безпеки інформаційних потоків. Збільшення видатків у 2022 та 2023 роках, особливо в умовах повномасштабної війни, відображає гнучкість та адаптивність державних ресурсів до нових викликів та загостреної потреби в кіберзахисті в умовах геополітичних конфліктів. Загалом, фінансування інформаційної безпеки в Україні є стратегічно важливим елементом, що забезпечує не лише функціонування електронної інфраструктури, а й високий рівень конфіденційності та надійності комунікацій в умовах військових загроз та активності кіберзлочинців.

РОЗДІЛ 3
ШЛЯХИ УДОСКОНАЛЕННЯ ДЕРЖАВНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В УКРАЇНІ

3.1. Напрямки покращення державного управління інформаційної безпекою в Україні

Розвиток ефективного державного управління інформаційною безпекою в Україні є важливим завданням, спрямованим на забезпечення захисту національних інтересів та забезпечення стабільності кіберпростору. Для досягнення цієї мети необхідно визначити конкретні напрямки покращення державного управління в даній сфері.

Створення центрального органу інформаційної безпеки: важливим кроком у покращенні державного управління інформаційною безпекою є утворення централізованого органу, який би відповідав за розробку та впровадження стратегій і політики в галузі інформаційної безпеки. Цей центральний орган має об'єднувати зусилля всіх відомств та організацій, що займаються кібербезпекою, та визначати загальні стандарти та процедури.

Розробка та впровадження нових законодавчих засад: необхідно розглядати можливість створення нових законів, які регулюватимуть сферу інформаційної безпеки. Це включає в себе визначення відповідальності за кіберзлочини, правила обробки та зберігання критично важливої інформації, а також механізми співпраці з приватним сектором.

Забезпечення кадрового забезпечення та кваліфікаційного рівня спеціалістів: удосконалення системи підготовки та підвищення кваліфікації фахівців в галузі інформаційної безпеки визначається як необхідна умова. Розробка спеціалізованих програм навчання та стажування для працівників, а також підтримка наукових досліджень в цій області, сприятиме формуванню кваліфікованого кадрового резерву.

Розвиток механізмів міжнародної співпраці: у зв'язку з тим, що кіберзагрози не мають кордонів, важливо активно розвивати механізми співпраці з іншими країнами та міжнародними організаціями в галузі інформаційної безпеки. Обмін інформацією, створення спільних проектів та участь в міжнародних ініціативах дозволять спільно протидіяти загрозам кіберпростору.

Загальна координація зусиль у цих напрямках сприятиме зміцненню інфраструктури інформаційної безпеки в Україні, забезпечуючи стійкість та відповідність сучасним викликам у цій критично важливій сфері.

Створення Центрального Органу Інформаційної Безпеки (ЦОІБ) є стратегічним кроком для оптимізації державного управління інформаційною безпекою в Україні. Цей центральний орган має за мету об'єднати різноманітні напрямки та ініціативи, спрямовані на забезпечення кібербезпеки країни, та розвивати спільні стратегії для ефективного протидії сучасним викликам у кіберпросторі.

ЦОІБ візьме на себе відповідальність за розробку та впровадження комплексних стратегій і політик в галузі інформаційної безпеки. Його завданням буде не лише реагування на поточні загрози, а й активне прогнозування та врахування майбутніх тенденцій у кібербезпеці.

Одним із ключових аспектів роботи ЦОІБ буде координація зусиль різних відомств та організацій, що діють у сфері кібербезпеки. Це включає у себе співпрацю з військовими, правоохоронними органами, галузевими регуляторами, а також приватним сектором. Ця співпраця спрямована на обмін інформацією, розробку спільних проектів та стандартів, що дозволяє утворити єдиний фронт у протидії кіберзагрозам.

Створення ЦОІБ також передбачає визначення загальних стандартів та процедур в галузі інформаційної безпеки. Це створить єдиний фреймворк, який дозволить різним структурам ефективно взаємодіяти та спільно вирішувати завдання забезпечення кібербезпеки.

Утворення ЦОІБ стане стратегічним кроком для покращення державного управління інформаційною безпекою в Україні, роблячи країну більш стійкою та відповідною до вимог сучасного кіберсередовища.

Розробка та впровадження нових законодавчих засад у сфері інформаційної безпеки є стратегічним кроком для зміцнення правового регулювання та вдосконалення механізмів захисту кіберпростору в Україні.

– Визначення відповідальності за кіберзлочини: нові закони повинні чітко визначати відповідальність за кіберзлочини. Це включає у себе визначення кримінальних та цивільних санкцій за незаконний доступ до інформації, втручання у роботу інформаційних систем чи поширення шкідливих програм.

– Правила обробки та зберігання критично важливої інформації: закони повинні встановлювати чіткі правила щодо обробки та зберігання критично важливої інформації, зокрема, інформації, яка стосується національної безпеки, оборони та економіки. Важливо визначити стандарти захисту даних та забезпечити їх відповідність міжнародним стандартам.

– Механізми співпраці з приватним сектором: закони повинні стимулювати активну участь приватного сектору у захисті інформаційної безпеки. Це може бути досягнуто шляхом встановлення стимулів для компаній, які вживають заходів щодо кіберзахисту, а також розробкою механізмів обов'язкової звітності та обміну інформацією між публічним та приватним секторами.

– Створення організації захисту інформації: важливим елементом може бути створення спеціалізованої організації, відповідальної за захист інформації та координацію дій у сфері кібербезпеки. Ця організація може служити центральним пунктом для обробки інформації про кіберзагрози та розробки заходів їх запобігання.

Розробка та впровадження нових законодавчих норм дозволить створити прозорий та ефективний правовий фреймворк для боротьби з кіберзагрозами, забезпечуючи високий рівень інформаційної безпеки та захист важливих національних інтересів.

Забезпечення кадрового забезпечення та підвищення кваліфікаційного рівня фахівців у галузі інформаційної безпеки визнається важливим кроком для забезпечення ефективної оборони в кіберпросторі та вирішення викликів, пов'язаних із зростанням кількості та складності кіберзагроз.

– Розробка спеціалізованих програм навчання: створення і впровадження спеціалізованих програм навчання є ключовим елементом для підготовки кваліфікованих спеціалістів в області інформаційної безпеки. Ці програми повинні охоплювати широкий спектр тем, включаючи кіберзахист, криптографію, аналіз загроз, інцидент-менеджмент та етичне взаємодія з інформацією.

– Стажування та практичний досвід: додатково до теоретичної підготовки важливо розвивати систему стажування та надання практичного досвіду. Співпраця зі сферою бізнесу та організаціями забезпечить студентам та спеціалістам можливість отримати реальний досвід роботи з інформаційною безпекою та вирішувати конкретні завдання.

– Підтримка наукових досліджень: фінансування та підтримка наукових досліджень у галузі інформаційної безпеки є важливим стимулом для розвитку нових технологій та методів. Дослідження повинні спрямовуватися на виявлення нових загроз, розробку ефективних засобів захисту та вдосконалення існуючих практик.

– Створення кадрового резерву: розробка системи кадрового резерву для сфери інформаційної безпеки дозволить забезпечити стійку та динамічну кадрову базу. Це включає в себе програми підготовки лідерів, організацію курсів для розвитку управлінських навичок та формування планів кар'єрного росту.

Узагальнено, підвищення кваліфікації та забезпечення кадрового потенціалу в галузі інформаційної безпеки є важливою передумовою для ефективного протидії кіберзагрозам та зміцнення обороноздатності країни в кіберпросторі.

Розвиток механізмів міжнародної співпраці в галузі інформаційної безпеки визнається ключовим завданням у забезпеченні глобальної кібербезпеки, оскільки кіберзагрози є трансграничними і вимагають об'єднаних зусиль багатьох країн та організацій. Для досягнення цієї мети необхідно активно розвивати міжнародні механізми співпраці.

– Обмін інформацією: створення системи обміну інформацією про кіберзагрози та інциденти між країнами є першочерговим завданням. Ефективний обмін данними дозволяє своєчасно виявляти та реагувати на загрози, забезпечуючи швидше відновлення та мінімізацію шкоди.

– Створення спільних проектів та ініціатив: міжнародні партнерства мають сприяти створенню спільних проектів та ініціатив, які спрямовані на розробку нових технологій, методів захисту та стандартів кібербезпеки. Спільна робота сприятиме обміну досвідом і підвищенню ефективності заходів протидії кіберзагрозам.

– Участь в міжнародних ініціативах: активна участь в міжнародних ініціативах, таких як Глобальний інцидентний відгук (GCI), Кіберполіція INTERPOL, та інших, сприяє створенню об'єднаного фронту протидії кіберзагрозам на міжнародному рівні. Співпраця з іншими країнами в рамках міжнародних організацій дозволяє об'єднати ресурси та експертні знання.

– Розробка міжнародних кібернорм: створення міжнародних стандартів та кібернорм визначить правила поведінки країн у кіберпросторі. Це включає в себе визначення правил щодо використання кіберзброї, захисту критично важливих інфраструктур, та інших аспектів кібербезпеки.

Міжнародна співпраця в галузі інформаційної безпеки є ключовою для забезпечення глобальної стійкості та безпеки кіберпростору. Спільні зусилля країн у цьому напрямку допоможуть створити об'єднану і відповідальну кіберсереду, що забезпечить захист як окремих національних інтересів, так і міжнародної кібербезпеки.

3.2. Пріоритети формування політики кібербезпеки в Україні

У сучасному інформаційному суспільстві кіберпростір стає важливою складовою національної безпеки, вимагаючи системного та інтегрованого підходу до його захисту. Створення ефективної системи кіберзахисту в умовах воєнного стану є необхідністю, щоб гарантувати стійкість суспільства та захист важливих галузей. На рис.3.1. представлено пріоритети формування політики кібербезпеки в Україні.

Створення інтегрованої системи захисту кіберпростору

- Першочерговим завданням є розробка та впровадження комплексної системи кіберзахисту, орієнтованої на державні структури, критично важливу інфраструктуру, а також банківську та фінансову сферу. Ця інтегрована система повинна бути адаптивною та здатною ефективно реагувати на сучасні кіберзагрози.

Створення центру реагування на кіберзагрози

- Основною складовою системи повинен стати спеціалізований центр реагування на кіберзагрози, який відповідатиме за виявлення, аналіз та ліквідацію інцидентів. Цей центр має координувати зусилля різних відомств та організацій для ефективного вирішення кіберпроблем.

Забезпечення кібербезпеки критично важливих об’єктів

- Особлива увага повинна бути приділена розробці та впровадженню спеціальних заходів захисту для критично важливих об’єктів, таких як енергетика, транспорт, зв’язок та інші сфери. Це включає в себе розробку та реалізацію ефективних заходів для запобігання та реагування на кіберзагрози.

Розвиток національної системи кіберзахисту

- Створення та постійне удосконалення національної системи кіберзахисту – це важлива складова кібербезпечної політики. Ця система має включати в себе нормативно-правовий базис, технічні та організаційні заходи, а також регулярно оновлюватися відповідно до сучасних тенденцій у кібербезпеці.

Підвищення кваліфікації та свідомості користувачів

- Організація програм підвищення кваліфікації та інформаційної свідомості користувачів є ключовим елементом кібербезпекової політики. Інструктажі, навчання та регулярні кампанії з освіти сприятимуть запобіганню соціальним інженерним атакам та зниженню ризиків.

Міжнародна співпраця

- Активна участь в міжнародних ініціативах та обмін інформацією є важливою частиною ефективного протидії глобальним кіберзагрозам. Розробка спільних проектів та співпраця з іншими країнами та міжнародними організаціями сприятиме зміцненню колективної кібербезпеки.

Рис.3.1. Пріоритети формування політики кібербезпеки в Україні.

Ці пріоритети утворюють основу для розробки та впровадження комплексної політики кібербезпеки в Україні, спрямованої на стійке та безпечне функціонування кіберпростору країни в умовах сучасних викликів та загроз.

1. Створення інтегрованої системи захисту кіберпростору є пріоритетним завданням для забезпечення стійкості та ефективного функціонування кіберпростору України в умовах зростаючих кіберзагроз. Ця система має охоплювати різні сфери, включаючи державні структури, критично важливу інфраструктуру, банківську та фінансову сферу, забезпечуючи комплексний та надійний захист.

Державні структури: система повинна включати в себе ефективний механізм захисту державних інформаційних систем та даних. Це включає у себе розробку та впровадження високих стандартів кіберзахисту, регулярні аудити та тестування на вразливості.

Критично важлива інфраструктура: захист критично важливої інфраструктури, такої як енергетика, транспорт, зв’язок, медицина та інші, є невід’ємною частиною системи. Розробка та впровадження стандартів кіберзахисту для цих галузей, а також вдосконалення систем моніторингу та виявлення інцидентів, є критично важливими кроками.

Банківська та фінансова сфера: забезпечення безпеки фінансових та банківських систем є надзвичайно важливим аспектом. Інтегрована система повинна включати ефективний механізм захисту фінансових операцій, а також особистих та фінансових даних громадян.

Інтеграція та адаптивність: система має бути інтегрованою та адаптивною, здатною ефективно реагувати на постійно змінюючіся кіберзагрози. Це включає в себе розробку та впровадження технологій штучного інтелекту, машинного навчання та аналізу великих даних для виявлення та передбачення кіберзагроз.

Навчання та співпраця: система має передбачати програми навчання для фахівців з кібербезпеки, а також стимулювати активну співпрацю між

відомствами, компаніями та іншими зацікавленими сторонами. Це дозволить створити спільний фронт протидії кіберзагрозам.

Створення інтегрованої системи захисту кіберпростору є стратегічним завданням, що вимагає поєднання технічних, організаційних та нормативних заходів. Це забезпечить ефективний захист важливих секторів економіки та національної безпеки України від сучасних кіберзагроз.

2.Створення центру реагування на кіберзагрози є стратегічним заходом, спрямованим на швидке та координоване реагування на кіберінциденти. Цей центр повинен виконувати ключові функції для ефективної захисту кіберпростору та надання допомоги відповідальним структурам та організаціям. Основні аспекти цього завдання включають:

– Виявлення та моніторинг: центр повинен володіти сучасними засобами виявлення кіберзагроз, включаючи системи аналізу потоків даних, інтелектуального аналізу та штучного інтелекту. Автоматизована система виявлення допомагатиме оперативно визначати можливі інциденти та аномалії в кіберпросторі.

– Аналіз та діагностика: центр має мати кваліфікованих аналітиків, які в змозі проводити швидкий та точний аналіз кіберінцидентів. Це включає в себе діагностику інцидентів, визначення їх впливу та розробку стратегій ліквідації.

– Ліквідація та відновлення: центр повинен визначати та впроваджувати необхідні заходи для ліквідації кіберінцидентів. Координація з різними відомствами та партнерами забезпечить ефективну відповідь на загрозу. Після ліквідації інциденту важливо провести аналіз та вжити заходів для відновлення нормального функціонування систем.

– Координація та співпраця: центр повинен встановити ефективний механізм координації та співпраці з усіма відомствами, організаціями та компаніями, що мають значення для кібербезпеки. Регулярні тренування, спільні сценарії та обмін інформацією збільшать ефективність відповіді на кіберзагрози.

– Інформаційна кампанія та освіта: центр повинен брати активну участь в проведенні інформаційних кампаній та освітніх заходів для громадськості та бізнес-спільноти. Підвищення рівня кіберсвідомості сприятиме попередженню кіберзагроз та зменшенню ризиків.

Створення центру реагування на кіберзагрози є ключовим елементом національної системи кібербезпеки, спрямованим на ефективне управління та координування заходів з виявлення, аналізу та ліквідації кіберінцидентів.

3. Забезпечення кібербезпеки критично важливих об’єктів є пріоритетним завданням у сфері національної безпеки, оскільки ці об’єкти відіграють стратегічно важливу роль у функціонуванні країни. Розробка та впровадження спеціальних заходів захисту для цих сфер є необхідною складовою політики кібербезпеки, адаптованої до унікальних викликів, які ставлять кіберзагрози.

– Енергетика: розробка інтегрованих систем моніторингу та захисту енергетичних мереж від кіберзагроз. Впровадження стандартів кібербезпеки для критичних об’єктів енергетики, таких як електростанції та підстанції. Регулярне навчання та тренування персоналу енергетичних підприємств з питань кібербезпеки.

– Транспорт: захист систем автоматизації та керування транспортними мережами, включаючи авіаційні, морські, залізничні та автомобільні системи. Розробка заходів безпеки для транспортних інфраструктур, таких як аеропорти, порти, залізничні вузли та автомагістралі.

Визначення інформаційних вразливостей та впровадження заходів для захисту транспортних систем від кіберзагроз.

– Зв’язок: захист телекомунікаційних мереж та інфраструктури від кібератак, зокрема, від втручання в роботу мереж передачі даних та мобільного зв’язку. Впровадження кіберзахисту для дата-центрів та обладнання зв’язку.

Співпраця з операторами зв’язку для обміну інформацією про потенційні загрози та вдосконалення захисту.

– Інші критично важливі об’єкти: розробка та впровадження індивідуальних заходів кіберзахисту для об’єктів, що можуть мати великий

вплив на функціонування країни (включаючи медичні установи, водопостачання та інші). Визначення та оцінка ризиків для кожного об’єкта з метою розробки індивідуальних стратегій кіберзахисту.

Враховуючи сучасний характер кіберзагроз, важливо підтримувати постійно оновлювані та адаптовані стратегії кібербезпеки для критично важливих об’єктів. Такий підхід допоможе ефективно протистояти різноманітним викликам та забезпечить сталу безпеку країни.

.4. Розвиток національної системи кіберзахисту є важливою складовою національної політики кібербезпеки, спрямованою на створення ефективної та стійкої оборонної інфраструктури проти кіберзагроз. Цей процес включає в себе ряд ключових аспектів:

– Нормативно-правовий базис: розробка та удосконалення нормативних актів, які регулюють кібербезпеку на національному рівні. Визначення прав та обов’язків суб’єктів, включаючи державні інституції, приватний сектор та громадян, у сфері кіберзахисту.

– Технічні заходи: розробка та впровадження сучасних технічних засобів та інфраструктури для виявлення, запобігання та ліквідації кіберзагроз.

Створення механізмів для моніторингу та аналізу кіберподій для негайної відповіді на потенційні інциденти.

– Організаційні заходи: утворення спеціалізованих кіберзахисних відділів та команд для проведення регулярних аудитів та тестувань на вразливості. Розвиток системи співпраці та обміну інформацією між державними структурами, приватним сектором та міжнародними партнерами.

– Адаптація до сучасних тенденцій: врахування та адаптація системи до сучасних технологічних та кіберзагроз, таких як штучний інтелект, Інтернет речей (IoT) та інші інновації. Спроможність швидко реагувати на нові методи кібератак та впровадження заходів для їх запобігання.

– Оновлення та тренування персоналу: регулярне оновлення навичок та знань персоналу, включаючи військових, правоохоронців та фахівців з

кібербезпеки. Проведення тренувань та симуляцій для перевірки ефективності заходів кіберзахисту.

– Міжнародна співпраця: взаємодія та обмін досвідом з іншими країнами та міжнародними організаціями у галузі кібербезпеки. Участь в спільних проектах та ініціативах для ефективного протидії глобальним кіберзагрозам.

Створення та постійне удосконалення національної системи кіберзахисту є стратегічно важливим завданням, спрямованим на забезпечення безпеки та стабільності інформаційного простору країни в умовах невпинних змін технологій та загроз.

5. Підвищення кваліфікації та інформаційної свідомості користувачів є важливим напрямком для забезпечення кібербезпеки, оскільки люди є вразливим ланцюгом у цілісній системі захисту. Організація програм підвищення свідомості включає в себе різноманітні заходи:

– Інструктажі та навчання: організація регулярних навчань та інструктажів щодо базових принципів кібербезпеки, виявлення підозрілих активностей та застосування безпечних практик в роботі з комп’ютерами та Інтернетом. Надання конкретних прикладів соціальних інженерних атак та методів їх запобігання.

– Регулярні кампанії з освіти: проведення тематичних кампаній щодо кібербезпеки, які охоплюють широкий коло користувачів. Використання різноманітних медіаформатів (відео, інфографіка, брошури) для доступності та ефективності наданої інформації.

– Спеціалізовані програми для різних груп: розробка спеціальних програм для дітей, підлітків, старших груп населення, бізнес-спільноти та інших груп користувачів, з урахуванням їхніх особливих потреб та ризиків.

– Впровадження безпечних поведінкових звичок: поширення інформації щодо безпечних практик використання паролів, застосування двофакторної аутентифікації, оновлення програмного забезпечення та регулярних антивірусних перевірок. Підкреслення важливості обережності під

час обробки електронних повідомлень, відкриття відомих джерел та виявлення підозрілих дій.

– Ефективна комунікація: взаємодія зі спільнотою через різні канали зв’язку: соціальні мережі, вебінари, семінари, лекції та інші формати.

Сприяння взаємодії користувачів у вирішенні проблем та обміні досвідом.

– Співпраця з організаціями та спільнотами: співпраця з бізнес-організаціями, школами, університетами та громадськими групами для впровадження спільних програм з підвищення кібербезпеки. Створення партнерств з індустрією для впровадження найсучасніших технологій та методів.

Широкомасштабна і системна робота з підвищення кваліфікації та інформаційної свідомості користувачів є важливим елементом у збалансованій стратегії кібербезпеки, що спрямована на створення відповідального та бджільного кіберспільноти.

6. Активна участь в міжнародних ініціативах та співпраця з іншими країнами та міжнародними організаціями є ключовим елементом ефективної стратегії кібербезпеки. Це дозволяє спільно протистояти глобальним кіберзагрозам та покращувати стандарти та практики в цій області. Для досягнення цих цілей, важливо вживати наступні заходи:

– Участь у міжнародних форумах: активна участь у міжнародних конференціях, семінарах та робочих групах з кібербезпеки для обміну досвідом та вивчення найкращих практик. Залучення до діалогу з представниками інших країн для вирішення загальних проблем та обговорення важливих аспектів кібербезпеки.

– Створення міжнародних партнерств: розробка та підтримка багатосторонніх та двосторонніх партнерств з країнами, що мають великий досвід у сфері кібербезпеки. Спільна участь у проектах та ініціативах, спрямованих на розвиток та вдосконалення кіберзахисту.

– Обмін інформацією: створення механізмів для ефективного обміну інформацією про кіберзагрози та інциденти з іншими країнами. Участь у

глобальних платформах для обміну інформацією та створення спільних баз даних.

– Розробка спільних проектів: спільна розробка та впровадження проектів з кібербезпеки, які спрямовані на розвиток нових технологій, інструментів та методів захисту. Взаємна підтримка у проведенні досліджень та інновацій в галузі кібербезпеки.

– Постійна адаптація до змін: спільна реакція на нові та розвиваючіся кіберзагрози, включаючи взаємодію в умовах кіберкриз та розробку спільних стратегій відповіді. Постійна адаптація до змін у міжнародному кіберпросторі та вдосконалення співпраці для забезпечення глобальної кібербезпеки.

Міжнародна співпраця є необхідною для створення ефективної та стійкої глобальної кібербезпекової системи, спроможної ефективно протидіяти сучасним і майбутнім кіберзагрозам.

3.3. Розробка стратегії покращення державного управління інформаційною безпекою в Україні

Розробка стратегії покращення державного управління інформаційною безпекою країни є важливим завданням, яке вимагає системного підходу та узгодженої дії на різних рівнях. Це комплексне завдання передбачає аналіз та узагальнення різноманітних аспектів, включаючи технічні, правові, організаційні та кадрові питання. Одним із ключових напрямків удосконалення інформаційної безпеки є технічний аспект. Забезпечення надійності інформаційних систем, виявлення та усунення потенційних вразливостей, розробка та впровадження сучасних технологій кіберзахисту – це основні завдання, які ставляться перед технічними експертами. Врахування швидкого технологічного розвитку вимагає постійного оновлення заходів безпеки та активної участі у міжнародних ініціативах з цього питання. Не менш важливим аспектом є правове забезпечення інформаційної безпеки. Розробка та удосконалення законодавства, спрямованого на визначення прав та обов'язків у

сфері кібербезпеки, а також встановлення ефективної системи відповідальності за порушення правил безпеки, є необхідним елементом стратегії. Правова база повинна враховувати особливості інтернет-простору та забезпечувати прозорість та справедливість у вирішенні конфліктних ситуацій. Отже, стратегія покращення державного управління інформаційною безпекою країни передбачає взаємодію різних аспектів, щоб забезпечити комплексний та ефективний підхід до захисту інформаційних ресурсів та забезпечити стійкість країни у сучасному кіберпросторі.

В табл.3.1. представлено стратегію покращення державного управління інформаційною безпекою в Україні.

Таблиця 3.1

Стратегія покращення державного управління інформаційною безпекою в Україні

Стратегічні Цілі	**Операційні цілі**		**Інструменти досягнення**	**Очікувані результати**
Ціль 1 Забезпечення комплексного підходу	1.1.Створення уніфікованих стандартів для різних секторів	1.2.Розробка механізмів взаємодії між секторами та галузями	Створення міжгалузевого комітету, інформаційна платформа	Уніфіковані стандарти, підвищена ефективність міжгалузевої взаємодії
Ціль 2. Підвищення рівня свідомості та навичок населення	2.1.Запуск освітніх кампаній та тренінгів	2.2.Розробка навчальних програм для різних професій	Партнерства з освітніми установами, розробка онлайн-ресурсів	Збільшення інформаційної грамотності, підвищення свідомості
Ціль 3. Зміцнення захисту інфраструктури	3.1.Модернізація існуючих систем захисту	3.2.Впровадження передових технологій для виявлення кібератак	Аудит та оновлення захисних систем, інвестиції в інновації	Збільшення стійкості до кібератак, зменшення ризиків порушення
Ціль 4. Посилення законодавства	4.1.Розробка та вдосконалення законів	4.2.Впровадження відповідальності за порушення стандартів	Співпраця з парламентом, механізми контролю та санкцій	Ефективне правове середовище, зниження порушень стандартів
Ціль 5. Міжнародне співробітництво	5.1.Активна участь у міжнародних ініціативах	5.2.Розробка та підтримка міжнародних стандартів	Участь у конференціях, підписання міжнародних угод	Зміцнення позицій в глобальному кіберпросторі, встановлення стандартів на міжнародному рівні

Джерело: складено автором

Стратегічна ціль 1. Забезпечення комплексного підходу:

Операційна ціль 1.1: Розробка та впровадження уніфікованих стандартів інформаційної безпеки, націлених на різні сектори економіки та соціальні галузі.

Однією з основних операційних цілей є розробка та ефективне впровадження уніфікованих стандартів інформаційної безпеки, спрямованих на різні сектори економіки та соціальні галузі. Ця ціль має на меті створення консолідованого та систематизованого набору вимог та нормативів, які враховуватимуть специфічні особливості кожного сектору.

Першочерговим завданням є проведення глибокого аналізу поточного стану систем інформаційної безпеки в різних галузях економіки та сферах соціальної діяльності. Цей аналіз дозволить визначити основні виклики, уразливості та конкретні потреби кожного сектору.

На наступному етапі буде виконана розробка уніфікованих стандартів, які враховуватимуть різноманітні аспекти інформаційної безпеки, такі як захист від кібератак, управління ризиками, контроль доступу, шифрування та інші. Стандарти будуть враховувати специфіку кожного сектору, забезпечуючи оптимальний баланс між безпекою та ефективністю операцій.

Для успішного впровадження уніфікованих стандартів передбачається встановлення механізмів нагляду та відповідальності за їх дотримання в кожному секторі. Крім того, розробляться рекомендації щодо адаптації стандартів до конкретних особливостей організацій в межах кожного сектору, забезпечуючи гнучкість та практичність їх впровадження.

Очікуваним результатом є створення консолідованого фреймворку інформаційної безпеки, який забезпечить найвищий рівень захисту для різних секторів економіки та соціальних галузей, сприятиме сталому розвитку та зміцненню національної кібербезпеки.

Операційна ціль 1.2: Встановлення механізмів взаємодії між секторами та галузями для оптимізації координації та обміну інформацією з питань інформаційної безпеки.

Операційна ціль 1.2 передбачає впровадження механізмів, спрямованих на покращення взаємодії між різними секторами та галузями з метою оптимізації координації та ефективного обміну інформацією з питань інформаційної безпеки.

Спочатку необхідно провести аналіз поточних механізмів взаємодії та обміну інформацією між різними секторами та галузями. Це дозволить визначити наявні прогалини та визначити конкретні області для поліпшення.

Далі передбачається розробка та впровадження механізмів, які сприятимуть ефективній координації та обміну інформацією. Це може включати в себе створення спільних платформ для обміну даними, встановлення стандартів звітності, а також організацію регулярних нарад із залученням представників різних галузей та секторів.

Ключовим елементом буде впровадження системи моніторингу та звітності, що дозволить визначити ефективність механізмів взаємодії та вчасно реагувати на виникаючі проблеми. Паралельно із цим буде проводитися навчання та підвищення кваліфікації учасників системи взаємодії з питань інформаційної безпеки.

Очікуваними результатами реалізації цієї операційної цілі є покращення обміну інформацією між різними секторами та галузями, підвищення реагування на потенційні загрози, а також збільшення рівня співпраці, що в конечному підсумку сприятиме забезпеченню більш високого рівня інформаційної безпеки в країні.

Інструменти досягнення передбачають реалізацію конкретних заходів для ефективного досягнення операційної цілі стосовно встановлення механізмів взаємодії між секторами та галузями з питань інформаційної безпеки. Зокрема:

1. Створення міжгалузевого комітету для розробки стандартів: створення міжгалузевого комітету для розробки стандартів інформаційної безпеки є стратегічним кроком, спрямованим на консолідацію експертного потенціалу в різних секторах та галузях економіки. Ініціюючи цей процес, передбачено систематичне формування комітету з врахуванням різноманітності

представництва для забезпечення комплексного погляду на виклики інформаційної безпеки.

Розробка стратегічного плану дій комітету націлена на системне створення та уніфікацію стандартів інформаційної безпеки. Цей план визначає ключові завдання, кроки впровадження та критерії оцінки ефективності, враховуючи не лише технічні аспекти, але й організаційні та стратегічні аспекти управління інформаційною безпекою.

Визначення ролей та відповідальностей учасників комітету з урахуванням їхнього досвіду та експертизи спрямоване на створення ефективної командної динаміки. Це включає в себе ретельний аналіз компетенцій кожного учасника для оптимального внеску в розробку стандартів та забезпечення взаємної відповідальності за досягнення поставлених завдань. Загалом, дані заходи спрямовані на створення фундаментальної основи для забезпечення високого рівня інформаційної безпеки в усіх галузях та секторах економіки.

2. Запуск інформаційної платформи для обміну досвідом та кращими практиками.

Запуск інформаційної платформи для обміну досвідом та кращими практиками становить стратегічно важливий елемент для досягнення цілей у сфері інформаційної безпеки. Науково-технічний прогрес, впровадження новітніх технологій та зростання кількості цифрових викликів у сучасному світі наголошують на необхідності створення відкритого та ефективного механізму обміну інформацією між різними галузями та секторами.

Розробка інформаційної платформи передбачає вивчення кращих практик та розробку механізмів об'єднання цього досвіду в єдину систему. Централізований ресурс, розроблений з урахуванням сучасних стандартів безпеки, має сприяти консолідації та систематизації знань в сфері інформаційної безпеки.

Забезпечення доступу до платформи різним секторам та галузям передбачає розробку гнучких систем аутентифікації та авторизації, що

забезпечать безпеку обміну інформацією. Це дозволить представникам різних сфер ефективно користуватися ресурсом та активно взаємодіяти.

Організація вебінарів, конференцій та інших інтерактивних подій є ключовим елементом стратегії, оскільки сприяє активному обміну ідеями, аналізу кейсів та спільному пошуку рішень. Це не лише підвищує рівень інформаційної грамотності учасників, але й сприяє формуванню спільного розуміння важливих аспектів інформаційної безпеки.

Запровадження механізмів взаємодії на платформі включає створення ефективних інструментів для обговорення, обміну думками та стимулювання співпраці. Це передбачає використання форумів, чатів та інших інтерактивних засобів, які забезпечать плідну обміну думками.

Оцінка ефективності платформи включає в себе систему метрик та засобів збору фідбеку, які враховуватимуть активність користувачів, рівень задоволення, а також конкретні внески у загальний розвиток інформаційної безпеки. Цей інтегрований підхід до створення інформаційної платформи покликаний не лише поліпшити обмін знаннями в галузі інформаційної безпеки, а й сприяти інноваційному розвитку цієї важливої сфери в контексті загального комплексного підходу до забезпечення інформаційної безпеки в країні.

Ці інструменти спрямовані на створення ефективної інфраструктури для впровадження уніфікованих стандартів і обміну інформацією між різними секторами та галузями, що сприятиме досягненню стратегічної мети забезпечення комплексного підходу до інформаційної безпеки в країні.

Очікувані результати від стратегічної цілі 1.

Збільшення рівня інформаційної грамотності: передбачається значний приріст інформаційної грамотності серед різних сфер суспільства. Цей результат визначається як підвищення здатності та знань громадян у користуванні та розумінні інформації, пов'язаної з інформаційною безпекою.

Підвищення свідомості щодо кіберзагроз та методів їх запобігання: очікується активне підвищення рівня усвідомленості населення та фахівців

щодо потенційних кіберзагроз, а також ефективних методів їх передбачення та запобігання. Це включає розповсюдження актуальної інформації, проведення навчальних заходів та інших ініціатив, спрямованих на підвищення рівня обізнаності щодо кібербезпеки.

Стратегічна ціль 2. Підвищення рівня свідомості та навичок.

Операційна ціль 2.1:Запуск освітніх кампаній та тренінгів для робітників та громадян передбачає впровадження комплексу заходів з підвищення рівня інформаційної грамотності та свідомості щодо кіберзагроз серед робітників та громадян шляхом запуску освітніх кампаній та тренінгів. У межах цієї операційної цілі передбачено ретельне планування та реалізацію навчальних програм, спрямованих на надання конкретних знань та навичок у сфері кібербезпеки.

Першочерговим етапом є розробка навчальних програм, які охоплюватимуть широкий спектр аспектів кібербезпеки, враховуючи різноманітність аудиторії. Ці програми повинні бути відповідні рівню підготовки та специфіці робочих професій, сприяючи формуванню відповідальності та компетентності у сфері захисту інформації.

Важливою складовою є структурований підхід до проведення освітніх кампаній та тренінгів, який передбачає інтерактивні форми навчання, демонстраційні матеріали та практичні вправи. Взаємодія з робітниками та громадянами на практичному рівні сприятиме більш ефективному засвоєнню інформації та розвитку необхідних навичок у сфері кібербезпеки.

Попередньою умовою успішної реалізації цієї операційної цілі є врахування індивідуальних особливостей аудиторії, адаптація підходів до освіти до конкретних потреб та реалій робочого середовища. Загальний результат операції спрямований на вдосконалення інформаційної грамотності та формування високого рівня свідомості стосовно кіберзагроз, що визначатиме новий стандарт захисту інформації в сучасному соціально-економічному контексті.

Операційна ціль 2.2.:Розробка спеціалізованих навчальних програм для різних професій.

В межах операційної цілі 2.2 передбачено систематичний процес створення та впровадження спеціалізованих навчальних програм, орієнтованих на різні професії та сфери діяльності. Зазначена ініціатива має на меті оптимізацію процесу навчання та підвищення ефективності освітнього впливу на кібербезпеку.

– ідентифікація ключових професій та секторів: провести аналіз та ідентифікацію ключових професій та галузей, які вимагають специфічних знань у сфері кібербезпеки. Цей етап передбачає врахування особливостей роботи та взаємодії в різних сегментах економіки;

– розробка індивідуалізованих навчальних курсів: на основі виявлених потреб розробити спеціалізовані навчальні програми для кожної визначеної професії чи галузі. Це включає створення змісту, що відповідає конкретним завданням та ризикам, які виникають у відповідних сферах;

– впровадження інтерактивних форм навчання: враховуючи сучасні підходи до освіти, використовувати інтерактивні методи та педагогічні інструменти для ефективного засвоєння матеріалу. Ігрові та симуляційні елементи можуть сприяти активному навчанню та розумінню реальних ситуацій;

– постійне оновлення та адаптація програм: забезпечити систему постійного вдосконалення та адаптації навчальних програм до змін в кіберзагрозах, технологічних тенденціях та вимогах конкретних секторів;

– оцінка ефективності: здійснювати систематичну оцінку ефективності спеціалізованих навчальних програм з метою корекції та вдосконалення їх структури та змісту.

Загалом, ця операційна ціль націлена на створення індивідуалізованих освітніх можливостей, які відповідають потребам різних професій та галузей, та сприятимуть формуванню високого рівня кіберзахищеності в різних сферах суспільства.

Інструменти досягнення стратегічної цілі 2.

Партнерство з освітніми установами та тренінговими центрами: співпраця з ключовими освітніми установами та тренінговими центрами є важливим інструментом для досягнення цілей у сфері інформаційної безпеки. Партнерство з установами вищої освіти дозволить впровадження актуальних програм, забезпечуючи студентам та фахівцям доступ до передових знань у галузі кібербезпеки. Тренінгові центри стануть платформою для практичної підготовки, симуляцій та обміну досвідом.

Розробка онлайн-ресурсів та платформ для дистанційного навчання: розробка та впровадження онлайн-ресурсів та платформ для дистанційного навчання є ключовим елементом для забезпечення гнучкості та доступності освітніх матеріалів у сфері інформаційної безпеки. Ці ресурси включатимуть в себе електронні навчальні курси, відеолекції, вправи та тести для самоперевірки. Дистанційне навчання стане доступним для широкого кола аудиторії, забезпечуючи навчання в будь-якому місці та часі, що сприятиме ефективному розповсюдженню знань з кібербезпеки.

Очікувані результати від реалізації Стратегічної цілі 2.

Збільшення рівня інформаційної грамотності: заочукується систематичне підвищення рівня інформаційної грамотності серед різних верств населення. Це включає в себе зростання знань та навичок у сфері інформаційної безпеки, орієнтацію в сучасних технологіях та ефективне використання інформаційних ресурсів. Завдяки співпраці з освітніми установами та доступу до онлайн-ресурсів, індивіди зможуть систематично поповнювати свої знання, що відобразиться на загальному рівні інформаційної грамотності в суспільстві.

Підвищення свідомості щодо кіберзагроз та методів їх запобігання: очікується значне підвищення свідомості громадян та фахівців щодо потенційних кіберзагроз, а також вдосконалення їхнього розуміння ефективних методів запобігання. Інформованість населення про типові кіберзагрози, їхні можливі наслідки та заходи безпеки буде визначати високий ступінь готовності до відповіді на потенційні загрози. Ці результати вплинуть на загальний рівень

кібербезпеки в суспільстві та сприятимуть побудові стійкої кібербезпекової культури.

Стратегічна ціль 3: Зміцнення захисту інфраструктури.

Операційна ціль 3.1: Модернізація існуючих систем захисту інформації.

Мета цієї операційної стратегії полягає в систематичній модернізації існуючих систем захисту інформації з метою підвищення їх ефективності та відповідності сучасним стандартам кібербезпеки. Підходить, аналізується та оцінюється поточний стан захисту інформації з метою визначення пріоритетних областей для модернізації.

Стратегічно, операційна ціль передбачає проведення комплексного аналізу інфраструктури безпеки з урахуванням технічних, програмних та організаційних аспектів. На основі отриманих даних розробляється стратегія модернізації, включаючи в себе визначення необхідних технологічних змін, упровадження передових інновацій та вдосконалення процесів управління безпекою.

Ця операційна ціль сприяє не лише зміцненню захисту інформації від потенційних загроз, а й підвищенню загальної рівня кібербезпеки організації чи системи. Модернізація існуючих систем захисту інформації є ключовим елементом стратегії кібербезпеки, спрямованої на адаптацію до швидко змінюючого кіберсередовища та забезпечення стійкості та надійності у відповідь на сучасні виклики та загрози.

Операційні ціль 3.2: Впровадження передових технологій для виявлення та запобігання кібератак.

У світлі постійно зростаючого обсягу кіберзагроз, важливим напрямком у забезпеченні кібербезпеки є оптимізація систем виявлення та запобігання кібератак. Операційна ціль 2 визначає стратегію впровадження передових технологій, які не лише визнають наявні загрози, але й вчаться адаптуватися до нових форм атак, забезпечуючи прогнозовану та ефективну реакцію.

Системи виявлення оновлюються за допомогою передових алгоритмів штучного інтелекту, які виявляють навіть найтонші аномалії в мережі.

Одночасно із цим вдосконалюються засоби запобігання, що використовують адаптивні стратегії та машинне навчання для ефективного блокування та ізолювання потенційних загроз.

Партнерство з передовими технологічними компаніями та проведення пілотних проектів гарантує впровадження найбільш ефективних рішень. Крім того, завдяки постійному моніторингу і оновленню технічних рішень, система може швидко адаптуватися до нових варіантів кіберзагроз, забезпечуючи високий рівень кібербезпеки. Очікується, що впровадження передових технологій значно підвищить рівень захисту та відповідність до сучасних викликів у кіберпросторі.

Інструменти досягнення по стратегічній цілі 3.

Аудит та оновлення захисних систем: один із ключових інструментів для досягнення операційної цілі полягає у систематичних аудитах та оновленні захисних систем. Аудит безпеки є процесом глибокого аналізу та перевірки ефективності існуючих заходів безпеки. Цей процес включає в себе перевірку відповідності захисних механізмів вимогам сучасних стандартів та ідентифікацію можливих слабких місць. Цільовими результатами аудиту є виявлення потенційних вразливостей та розробка стратегій для їх виправлення.

Інвестиції в розробку та впровадження інноваційних кіберзахистових рішень: ефективність кіберзахисту значно підвищується завдяки інвестиціям у розробку та впровадження інноваційних кіберзахистових рішень. Цей інструмент передбачає активний підхід до використання передових технологій у сфері кібербезпеки. Інвестування у високотехнологічні розробки, такі як штучний інтелект, машинне навчання та аналітика в реальному часі, створює можливість розробки та впровадження передових рішень для виявлення та відповіді на загрози в онлайн середовищі.

Ці інструменти становлять основу для стійкого та прогресивного кіберзахисту, забезпечуючи адаптацію до найновіших загроз та викликів у цифровому середовищі. Регулярні аудити дозволяють підтримувати високий рівень безпеки шляхом виявлення та усунення слабких місць, водночас

інвестиції в інноваційні рішення стимулюють розвиток передових захисних механізмів, що відповідають сучасним викликам цифрової епохи.

Очікувані результати від впровадження стратегічно цілі 3:

Збільшення стійкості до кібератак: очікується покращення загальної стійкості інформаційної і кібернетичної інфраструктури до потенційних кібератак. Це включає удосконалення захисних механізмів, виявлення та ефективну реакцію на потенційні загрози, а також здатність до резилієнтності та відновлення в разі успішного нападу. Застосування інноваційних технологій та активна аудиторська діяльність сприятимуть підвищенню стійкості та непроникності систем.

Зменшення можливостей порушення безпеки: очікується зменшення імовірності та ефективності можливих порушень безпеки внаслідок кібератак. Це передбачає не лише попередження втрати конфіденційної інформації та відмов від доступу, але й активне усунення потенційних загроз ще до їхнього активного використання. Основні результати будуть визначатися швидкістю реагування на інциденти, ефективністю систем виявлення та нейтралізації загроз, а також удосконаленням оборонних стратегій та технологій.

Стратегічна ціль 4: Посилення законодавства:

Операційні ціль 4.1.Розробка та вдосконалення законів інформаційної безпеки.

Дана операційна ціль ставить за мету систематичне вдосконалення та розробку законодавства в галузі інформаційної безпеки для відповідності сучасним викликам кіберсередовища. Підходить до створення ефективної та комплексної правової бази, яка регулює захист інформації, протидію кіберзагрозам та визначає відповідальність за їхню порушення.

Стратегічно, це передбачає аналіз існуючого законодавства, виявлення прогалин та неспівробітності, а також розробку нових нормативних актів, що враховують швидкозмінювані технологічні та кібернетичні тенденції. Вдосконалення законів має за мету гармонізацію та узгодження правового середовища з найвищими стандартами інформаційної безпеки.

Застосування інструментів для досягнення цієї мети включає в себе консультації з експертами з правової сфери та інформаційної безпеки, проведення публічних обговорень для врахування різноманітних поглядів, а також взаємодію з міжнародними партнерами для узгодження стандартів та передових практик у цьому напрямку.

Очікується, що результатом цієї операційної цілі буде створення прогресивного та адаптивного законодавчого середовища, що сприятиме не лише ефективному регулюванню інформаційної безпеки, а й встановленню високих стандартів захисту в цифровому вимірі.

Операційні ціль 4.2.Впровадження відповідальності за порушення стандартів і захист інформації.

Операційна ціль 4.2 передбачає впровадження системи відповідальності за порушення стандартів та захист інформації в організації. Ця ціль спрямована на покращення безпеки та ефективності управління інформаційною безпекою. У рамках цієї операційної цілі визначаються та реалізуються механізми, які забезпечують відповідальність осіб за порушення встановлених стандартів та неналежний захист інформації.

Спочатку визначаються стандарти та політики щодо інформаційної безпеки, які повинні дотримуватися всіма працівниками організації. Потім впроваджуються механізми контролю та моніторингу, які дозволяють виявляти порушення цих стандартів. Це може включати в себе ведення журналів, аудит безпеки, системи виявлення вторгнень та інші технічні засоби.

Однак ключовим елементом є визначення відповідальності за порушення. Це може бути реалізовано через встановлення процедур внутрішнього розслідування, де особи, які порушили стандарти, притягуються до відповідальності. Це також може включати навчання та освіту працівників з питань інформаційної безпеки для забезпечення свідомості та відповідального ставлення до цих питань.

Впровадження відповідальності за порушення стандартів і захист інформації допомагає створити культуру безпеки в організації, підвищити

рівень свідомості працівників та зменшити ризики для інформаційних ресурсів компанії.

Інструменти досягнення для стратегічної цілі 4.

Співпраця з парламентом для розгляду та прийняття нових законів: забезпечення активної взаємодії та співпраці з парламентськими структурами для впровадження нових ініціатив у сфері інформаційної безпеки. Це включає проведення консультацій, представлення доказів необхідності змін, а також участь у парламентських слуханнях для збору обґрунтованих відгуків та підтримки законопроектів.

Створення механізмів контролю та санкцій за порушення законодавства: розробка ефективних механізмів контролю за дотриманням законодавства в галузі інформаційної безпеки. Це передбачає впровадження системи моніторингу та аудиту, а також визначення санкцій за порушення правил. Система санкцій повинна бути прозорою та пропорційною, спрямованою на запобігання порушень та стимулювання виконання законодавчих вимог.

Ці інструменти спрямовані на створення реально ефективної правової бази в галузі інформаційної безпеки, що базується на широкій підтримці та врахуванні потреб суспільства і експертної громадськості.

Очікувані результати від впровадження стратегічної цілі 4.

Цільовим результатом даної операційної стратегії є впровадження ефективного правового середовища, спрямованого на регулювання інформаційної безпеки. Передбачається, що розроблені та ухвалені нові законодавчі акти будуть відзначатися високою чіткістю, адаптивністю та спроможністю враховувати швидкозмінюючіться технологічні та кібернетичні реалії.

Очікується, що це правове середовище створить ефективний каркас для захисту інформації та боротьби з кіберзагрозами. Зокрема, прогресивні закони повинні сприяти запобіганню порушень стандартів інформаційної безпеки, а також забезпечити ефективні механізми контролю та санкцій у випадках їхнього порушення. Очікується, що ці заходи сприятимуть загальному підвищенню

рівня кібербезпеки, зниженню кількості порушень та створенню високих стандартів інформаційної безпеки в контексті сучасного цифрового середовища.

Стратегічна ціль 5. Міжнародне співробітництво.

Операційні ціль 5.1. Активна участь у міжнародних ініціативах з кібербезпеки.

Операційна ціль 5.1 орієнтована на розширення глобального впливу та взаємодії країни в сфері кібербезпеки через активну участь у міжнародних ініціативах. Це передбачає взаємодію та співпрацю з іншими країнами, міжнародними організаціями та експертами для спільного розв'язання глобальних проблем та вдосконалення підходів до кіберзахисту.

Активна участь у міжнародних ініціативах передбачає обмін інформацією про кіберзагрози, розробку та впровадження міжнародних стандартів, спільні навчальні програми та взаємну допомогу в разі кібератак. Мета полягає в створенні глобальної спільноти, що спільно працює над зміцненням кібербезпеки та відповіді на загрози цифрового віку.

Очікується, що ця участь допоможе країні висловити своє погляду на міжнародному рівні, сприятиме обміну кращими практиками, а також дозволить створити інтегровану систему захисту від кіберзагроз, яка враховує великий спектр викликів та можливостей в цифровому просторі.

Операційні ціль 5.2. Розробка та підтримка міжнародних стандартів у галузі інформаційної безпеки.

Операційна ціль 5.2 націлена на активну участь та лідерство організації у процесі розробки та підтримки міжнародних стандартів в галузі інформаційної безпеки. Зазначена ініціатива передбачає активну співпрацю з міжнародними стандартизаційними організаціями, науково-дослідними установами та іншими зацікавленими сторонами для спільного визначення та розвитку стандартів, які регулюють аспекти безпеки інформації на глобальному рівні.

Це включає в себе активне впливання на формування політики та нормативного середовища в галузі інформаційної безпеки, розробку міжнародних стандартів, які враховують сучасні технологічні виклики та

загрози, а також активну участь у процесі оновлення і вдосконалення існуючих стандартів. Підтримка таких міжнародних ініціатив сприяє створенню єдиного та уніфікованого підходу до забезпечення інформаційної безпеки на світовому рівні, сприяючи високому стандарту безпеки як для конкретної організації, так і для всієї глобальної спільноти.

Інструменти досягнення.

Участь в міжнародних конференціях та робочих групах: залучення до широкого кола міжнародних обговорень, конференцій та робочих груп є невід'ємною частиною стратегії. Це дозволяє не лише дізнатися про передові підходи та рішення в сфері кібербезпеки, а й активно співпрацювати з міжнародними партнерами, обмінюючи найкращими практиками та спільно вирішуючи виклики цифрової безпеки.

Підписання міжнародних угод з інформаційної безпеки: здійснення активних зусиль щодо укладання міжнародних угод з інформаційної безпеки відкриває можливості для взаємодії на міжнародному рівні. Це включає угоди про обмін інформацією, спільні дослідження, технічні стандарти та інші форми співпраці, спрямовані на підвищення стійкості та безпеки кіберпростору. Підписання таких угод визначає країну як активного учасника глобального кіберспільноти, що спільно працює над забезпеченням колективної кібербезпеки в еру цифрової трансформації.

Очікуваний результат від реалізації стратегічної цілі 5.

Зміцнення позицій країни у глобальному кіберпросторі: активна участь у міжнародних ініціативах прискорить визнання та зміцнення позицій країни у глобальному кіберпросторі. Це включає підвищення довіри спільноти, створення партнерств із визначеними лідерами, а також участь у спільних проектах, що сприяють сприйняттю країни як активного та впливового учасника у сфері кібербезпеки.

Встановлення стандартів безпеки на міжнародному рівні: підписання та активна реалізація міжнародних угод сприятиме встановленню високих стандартів безпеки на міжнародному рівні. Країна візьме активну участь у

формуванні правил та стандартів, що регулюють кіберпростір, сприяючи виробленню загальноприйнятих норм та принципів. Це сприятиме підняттю рівня кібербезпеки глобально та сприятиме визнанню країни як важливого учасника у визначенні майбутнього безпечного цифрового світу.

Висновки до розділу 3

Розробка та впровадження нових законодавчих засад у сфері інформаційної безпеки в Україні є ключовим кроком у забезпеченні стійкості та захищеності країни в кіберпросторі. Необхідно активно розглядати можливість створення нових законів, які визначатимуть відповідальність за кіберзлочини, встановлюватимуть правила обробки та зберігання критично важливої інформації, а також регулюватимуть механізми співпраці з приватним сектором Забезпечення кадрового забезпечення та підвищення кваліфікаційного рівня спеціалістів є важливим аспектом впровадження стратегії інформаційної безпеки. Удосконалення системи підготовки та підвищення кваліфікації фахівців, розробка спеціалізованих програм навчання та стажування, а також підтримка наукових досліджень в цій галузі сприятимуть формуванню кваліфікованого кадрового резерву. Розвиток механізмів міжнародної співпраці є важливою складовою стратегії інформаційної безпеки, оскільки кіберзагрози не знають кордонів. Активна участь в міжнародних ініціативах, обмін інформацією та спільні проекти з іншими країнами та міжнародними організаціями допоможуть ефективно протистояти загрозам кіберпростору. Загальна координація зусиль у цих напрямках сприятиме зміцненню інфраструктури інформаційної безпеки в Україні, забезпечуючи стійкість та відповідність сучасним викликам у цій критично важливій сфері. Такий комплексний підхід визначає стратегію як ключовий інструмент у створенні надійної та захищеної інформаційної інфраструктури в Україні.

Висновок стратегії покращення державного управління інформаційною безпекою в Україні є переконливим свідченням відданості країни побудові міцної та високоефективної системи захисту в інформаційному просторі.

Пропонована стратегія вирізняється системним підходом, що включає в себе широкий спектр заходів від створення уніфікованих стандартів до активної участі в міжнародних ініціативах. Стратегічні та операційні цілі, які визначені у документі, чітко орієнтовані на створення стійкої та адаптивної системи інформаційної безпеки, що враховує високий рівень кіберзагроз сучасності. Важливо відзначити акцент на співпраці, взаємодії між різними секторами та галузями, що сприятиме уніфікації підходів та підвищенню ефективності заходів. Інструменти досягнення цілей, такі як створення міжгалузевих комітетів, участь в міжнародних конференціях та робочих групах, підписання міжнародних угод, є детально розробленими та взаємодоповнюючими. Вони спрямовані на практичну реалізацію стратегії та досягнення очікуваних результатів. Очікувані результати, такі як зміцнення позицій у глобальному кіберпросторі та встановлення міжнародних стандартів безпеки, визначають стратегію як важливий інструмент для створення високоефективної системи інформаційної безпеки, яка відповідає викликам сучасності та підвищує рівень кіберстійкості України. Загалом, пропонована стратегія представляє собою ретельно розроблений та обгрунтований план, який, при вдалій реалізації, сприятиме створенню безпечного та надійного інформаційного середовища в Україні.

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

Державне управління інформаційною безпекою в сучасному світі визначається як невід'ємна частина державного управління, орієнтована на забезпечення високого рівня захисту інформаційних ресурсів та інфраструктури від можливих загроз. Це складний процес, який постійно змінюється та постійно і передбачає аналіз та оцінку різноманітних загроз, від розробки стратегій інформаційної безпеки до реалізації заходів з превентивного реагування та відновлення. Ключовими аспектами державного управління інформаційною безпекою є створення ефективної політики захисту, оперативна відповідь на інциденти та взаємодія з різними зацікавленими сторонами. Системний підхід включає в себе регулярний аналіз інформаційних загроз, розробку стратегій управління ризиками та вдосконалення механізмів виявлення та реагування на інциденти. Залучення та співпраця з різними суб'єктами, включаючи державні органи, приватний сектор та громадянське суспільство, вирішує завдання створення єдиної системи захисту від інформаційних загроз. У цьому контексті, законодавче забезпечення грає ключову роль у визначенні правового статусу та взаємодії учасників процесу, забезпечуючи ефективне функціонування системи інформаційної безпеки. Важливо також враховувати швидкі зміни технологій та їх вплив на загрози, що вимагає постійного вдосконалення стратегій та технічних засобів захисту національної інформаційної інфраструктури.

Організаційно-правовий механізм державного управління інформаційною безпекою в Україні, зокрема через діяльність Державної служби спеціального зв'язку та захисту інформації України, відіграє визначальну роль у забезпеченні безпеки та ефективності державних комунікаційних систем. Організація виконує ряд стратегічних завдань, спрямованих на гарантування захисту інформації та кібербезпеки, що є критичними аспектами національної безпеки, особливо в умовах сучасних кіберзагроз та гібридних конфліктів. Враховуючи важливість інформаційної безпеки, основні законодавчі акти, такі як Закони

України «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про державну таємницю», «Про захист персональних даних», і «Про основні засади забезпечення кібербезпеки України», становлять фундаментальний правовий каркас для регулювання цієї сфери. Державна служба спеціального зв'язку та захисту інформації України виступає ключовим ланцюгом у системі національної безпеки, забезпечуючи ефективне функціонування інформаційних систем та захист від кіберзагроз. Важливим аспектом є також наявність постанов КМУ, нормативних документів та державних стандартів, які регулюють технічний захист інформації та функціонування КСЗІ. У контексті постійно зростаючих загроз та швидкого технологічного розвитку, організаційно-правовий механізм вказаної служби потребує постійного вдосконалення, а також врахування міжнародних стандартів та передового досвіду для забезпечення оптимального рівня інформаційної безпеки в Україні.

Зарубіжний досвід державного управління інформаційною безпекою в особі таких країн, як Естонія, Ізраїль, США та Сінгапур, становить цінний джерело навчання для України у вдосконаленні власної системи кібербезпеки. Естонія, завдяки передовій інформаційній інфраструктурі та ефективним практикам у галузі кібербезпеки, може послужити прикладом для впровадження систем електронної ідентифікації та ефективного реагування на кібератаки. Ізраїль, з своєю активною роботою у сфері інновацій та ефективного управління, демонструє, як високий рівень кібербезпеки може поєднуватися з інноваційним підходом та успішною співпрацею між різними секторами суспільства. США визначаються своєю систематичною роботою у галузі кібербезпеки, включаючи захист критично важливої інфраструктури та протидію кіберзагрозам через національну стратегію. Сінгапур, з високотехнологічною економікою та активними заходами в плані кібербезпеки, надає важливі уроки з розвитку кадрового потенціалу та впровадження передових технологій. Цей досвід дозволяє визначити ключові аспекти, які можуть бути використані для оптимізації стратегій управління інформаційною

безпекою в Україні. Враховуючи високий рівень захисту інформації в зазначених країнах, Україна може взяти на увагу інноваційні методи та ефективні практики для забезпечення стійкості своєї інформаційної інфраструктури та ефективного впровадження заходів кібербезпеки. Такий підхід допоможе країні досягти найвищого рівня захисту в цифровому середовищі, а також сприятиме розвитку власного потенціалу в галузі кібербезпеки та інновацій.

З початку 2023 року порівняно з IV кварталом 2022 року відзначається зменшенням загальної кількості кібератак, які організовують угруповання проросійських хактивістів. Однак, не дивлячись на це, систематичність та інтенсивність таких атак залишаються на високому рівні. Це свідчить про те, що хактивісти, спрямовані на розповсюдження проросійської агенди, продовжують активно використовувати кіберзброю для досягнення своїх цілей. Необхідно врахувати посилення інформаційних операцій, ініційованих Кремлем, щодо виправдання можливого вторгнення в Україну. Це створює умови для затяжної війни в Україні, що може призвести до збільшення інтенсивності та різноманітності кібератак на українські організації різних форм власності та галузей. З цим контекстом не можна вважати, що тренд до зменшення кількості кібератак залишиться стійким, іншими словами, цей різкий спад може бути тимчасовим, а не сталим явищем. У таких умовах важливо для організацій в Україні приділяти особливу увагу підвищенню рівня кібербезпеки та вживати заходів для ефективного виявлення, протидії та відновлення в разі кібератак.

Україна видає ресурси на забезпечення інформаційної безпеки, визнавши актуальність цього питання в умовах сучасного геополітичного та кібербезпекового середовища. За період з 2018 по 2023 роки спостерігається значне зростання обсягів фінансування на цей напрям, що свідчить не лише про постійний розвиток інформаційних технологій, але й про розуміння необхідності вдосконалення систем і заходів кіберзахисту. Основний акцент робиться на розвиток і модернізацію системи спеціального зв'язку, яка відіграє

критичну роль у забезпеченні безпеки та конфіденційності обміну інформацією між владними органами. Зокрема, урядовий фельд'єгерський зв'язок отримав значне фінансування для доставки спеціальної службової кореспонденції органам державної влади, де частка видатків станом на 01.12.2023 року складає 98,25% або 567,9 млн.грн. Такий акцент свідчить про визнання важливості надійної і безпечної передачі інформації між ключовими структурами країни. Стабільність та сталість фінансування цих процесів є ключовим фактором, який вказує на систематичний та дбайливий підхід до забезпечення безпеки інформаційних потоків. Збільшення видатків у 2022 та 2023 роках, особливо в умовах повномасштабної війни, відображає гнучкість та адаптивність державних ресурсів до нових викликів та загостреної потреби в кіберзахисті в умовах геополітичних конфліктів. Загалом, фінансування інформаційної безпеки в Україні є стратегічно важливим елементом, що забезпечує не лише функціонування електронної інфраструктури, а й високий рівень конфіденційності та надійності комунікацій в умовах військових загроз та активності кіберзлочинців.

Розробка та впровадження нових законодавчих засад у сфері інформаційної безпеки в Україні є ключовим кроком у забезпеченні стійкості та захищеності країни в кіберпросторі. Необхідно активно розглядати можливість створення нових законів, які визначатимуть відповідальність за кіберзлочини, встановлюватимуть правила обробки та зберігання критично важливої інформації, а також регулюватимуть механізми співпраці з приватним сектором Забезпечення кадрового забезпечення та підвищення кваліфікаційного рівня спеціалістів є важливим аспектом впровадження стратегії інформаційної безпеки. Удосконалення системи підготовки та підвищення кваліфікації фахівців, розробка спеціалізованих програм навчання та стажування, а також підтримка наукових досліджень в цій галузі сприятимуть формуванню кваліфікованого кадрового резерву. Розвиток механізмів міжнародної співпраці є важливою складовою стратегії інформаційної безпеки, оскільки кіберзагрози не знають кордонів. Активна участь в міжнародних ініціативах, обмін

інформацією та спільні проекти з іншими країнами та міжнародними організаціями допоможуть ефективно протистояти загрозам кіберпростору. Загальна координація зусиль у цих напрямках сприятиме зміцненню інфраструктури інформаційної безпеки в Україні, забезпечуючи стійкість та відповідність сучасним викликам у цій критично важливій сфері. Такий комплексний підхід визначає стратегію як ключовий інструмент у створенні надійної та захищеної інформаційної інфраструктури в Україні.

Висновок стратегії покращення державного управління інформаційною безпекою в Україні є переконливим свідченням відданості країни побудові міцної та високоефективної системи захисту в інформаційному просторі. Пропонована стратегія вирізняється системним підходом, що включає в себе широкий спектр заходів від створення уніфікованих стандартів до активної участі в міжнародних ініціативах. Стратегічні та операційні цілі, які визначені у документі, чітко орієнтовані на створення стійкої та адаптивної системи інформаційної безпеки, що враховує високий рівень кіберзагроз сучасності. Важливо відзначити акцент на співпраці, взаємодії між різними секторами та галузями, що сприятиме уніфікації підходів та підвищенню ефективності заходів. Інструменти досягнення цілей, такі як створення міжгалузевих комітетів, участь в міжнародних конференціях та робочих групах, підписання міжнародних угод, є детально розробленими та взаємодоповнюючими. Вони спрямовані на практичну реалізацію стратегії та досягнення очікуваних результатів. Очікувані результати, такі як зміцнення позицій у глобальному кіберпросторі та встановлення міжнародних стандартів безпеки, визначають стратегію як важливий інструмент для створення високоефективної системи інформаційної безпеки, яка відповідає викликам сучасності та підвищує рівень кіберстійкості України. Загалом, пропонована стратегія представляє собою ретельно розроблений та обґрунтований план, який, при вдалій реалізації, сприятиме створенню безпечного та надійного інформаційного середовища в Україні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Антіпов І.Є. Засоби та системи технічного захисту інформації: навч. посіб. для студентів спец. 125 «Кібербезпека» спеціалізації «Системи технічного захисту інформації»; Харків. нац. ун-т радіоелектроніки. Харків: ХНУРЕ, 2019. 215 с.

2. Авер'янов В. Б. Державне управління в Україні : навч. посіб. / за заг. ред. В. Б. Авер'янова. К., 2009. 226 с.

3. Алещенко, В. Психологічні аспекти інформаційної війни Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки. 2022. № 2 (50). С. 27-31.

4. Архієреєв С.І. Державне та регіональне управління: навч. посіб. для студентів спец. 073 «Менеджмент»; Нац. техн. ун-т «Харків. політехн. ін.-т». Харків : Вид-во Іванченка І. С., 2018. 127 с.

5. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека». Правова інформатика. 2014. № 2(42). С.54-62.

6. Буйницька О. П. Інформаційні технології та технічні засоби навчання К.: Центр учбової літератури, 2012. 240 с.

7. Вараксін О.О. Кібербезпека мереж наступного покоління: навч. посіб. у галузі знань 1701 «Інформаційна безпека» за спец. 8.17010201 - Системи технічного захисту інформації, автоматизація її обробки. Одес. нац. акад. зв'язку ім. О. С. Попова, Каф. інформ. безпеки та передачі даних. О.: ОНАЗ ім. О. С. Попова, 2013. 238 с.

8. Впровадження європейської кібербезпеки: загальний огляд. ISACA URL: https://www.isaca.org/Knowledge-Center/Research/Documents/European-CybersecurityImplementation-Overview_res_Ukr_1215.pdf

9. Гнатюк С.О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. Безпека інформації. 2013. Т. 19, № 2. С. 118-129. URL: http://nbuv.gov.ua/UJRN/bezin_2013_19_2_8

10. Грищук Р.В. Інформаційна та кібернетична безпека : роль та місце в умовах гібридної війни: матеріали всеукр. наук.- практ. конф. (Одеса, 21 жовтня 2016 р.). Одеса : ОДУВС, 2016. С. 15-16.

11. Демедюк С.В. Адміністративно-правове регулювання відносин у сфері забезпечення кібербезпеки в Україні. Південноукраїнський правничий часопис. 2015. № 3. С. 119-123. URL: http://nbuv.gov.ua/UJRN/Pupch_2015_3_39

12. Дубов Д.В. Кібербезпека: світові тенденції та виклики для України. К.: НІСД, 2014. 30 с

13. Державне агентство з електронного врядування України. URL: https://www.e.gov.ua/ua.

14. Завдання Держспецзв'язку. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=89831&cat_id=89828.

15. Звіт за 2023 про роботу Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки URL: https://cip.gov.ua/services/cm/api/attachment/download?id=53656%20

16. Звоздецька, О. Дезінформація як загроза національній безпеці Європейського Союзу: проблеми та підходи Історико-політичні проблеми сучасного світу. 2021. Т. 43. С. 30-39. -

17. Інформайційно-воєнна безпека як елемент національної безпеки України Володимир Юрійович Артемов, Володимир Олексійович Хорошко, Юлія Євгеніївна Хохлачова, Володимир Володимирович Погорелов // Захист інформації. 2022. Т. 24, № 1.– С. 21-29

18. Кантур, О Досвід іноземних держав у питанні протидії інформаційним впливам Російської Федерації / Олександр Кантур // Вісник Київського національного університету імені Тараса Шевченка. Державне управління . 2022. Вип. 2 (16). С. 5-12.

19. Корнієнко Б.Я. Безпека інформаційно-комунікаційних систем та мереж: навч. посіб. для студентів спец. 125 «Кібербезпека»; Нац. авіац. ун-т. Київ : НАУ, 2018. 225 с.

20. Кібербезпека в сучасному світі: актуальні виклики: матеріали Всеукр. наук.-практ. конф., 29 листопада 2019 р. Одеса: Гельветика, 2019. 332 с.

21. Кібербезпека: віртуальна зброя держави. URL: https://biz.nv.ua/ukr/experts/kutsenko1/kiberbezpekazbroja-derzhavi-u-virtualnij-ploshchini-2014774.html.

22. Книженко О. О. Сучасний стан злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку в Україні. Бюлетень Міністерства юстиції України. 2014. № 7. С. 122–127

23. Конвенція про кіберзлочинність. Рада Європи; Конвенція, Міжнародний документ від 23.11.2001 р. URL: http://zakon4.rada.gov.ua/laws/show/994_575

24. Кондакова С.В. Кібербезпека в Великобританії. Бизнес и безопасность. 2019. № 1. С.67-80

25. Курінний, Є. В. Адміністративно-правове забезпечення інформаційної гігієни під час воєнного стану в Україні / Євген Володимирович Курінний. Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2023. № 1 (122). С. 38-43.

26. Меркель: Уряд Німеччини актуалізував стратегію кібербезпеки URL: https://vgolos.com.ua/news/merkel-uryad-nimechchyny-aktualizuvav-strategiyu-kiberbezpeky_256173.html

27. Мельник С.В., Тихомиров О.О., Лєнков О.С. До проблеми формування понятійно-термінологічного апарату кібербезпеки: зб. матер. наук.-практ. конф. [Актуальні проблеми управління інформаційною безпекою держави], (Київ, 22 березня 2011 р.). К. : Вид-во НА СБ України, 2011. Ч. 2. С. 43-48

28. Методологічні основи інформаційної безпеки країни з урахуванням умов сучасного періоду її державотворення / Юрій Федорович Кучеренко, Олександр Валерійович Александров, Андрій Михайлович Носик, Дмитро

Олександрович Камак // Збірник наукових праць Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки. 2022. Вип. 4 (14). С. 99-109

29. Онопрієнко, С. Функції забезпечення інформаційної безпеки публічного адміністрування в Україні за умов повномасштабної збройної агресії Російської Федерації. Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки. 2022. № 2 (50). С. 95-98.

30. Офіційний сайт «Державної служби спеціального зв'язку та захисту інформації України» URL: https://cip.gov.ua/ua

31. Петров В.В. Щодо формування національної системи кібербезпеки України. Стратегічні пріоритети. 2013. № 4 (29). С. 127-130.

32. Пилипчук В.Г. Забезпечення інформаційної безпеки України: сучасні тенденції та проблеми: матеріали наук.-практ. конф. "Запобігання новим викликам та загрозам інформаційній безпеці України: правові аспекти", (Київ, 6 жовтня 2016 р.). НТУУ «КПІ імені Ігоря Сікорського». К.: Вид-во «Політехніка», 2016. С. 24-28.

33. Про внесення змін до Закону України "Про основи національної безпеки України" : проект Закону України щодо кібернетичної безпеки України від 07.03.13 р. № 2483.URL: //www.w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=45998

34. Про Стратегію кібербезпеки України: Указ Президента України від 15.03.2016 № 96/2016 // Офіційний вісник Президента України. 2016 р. № 10. – Ст. 198

35. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» URL: https://zakon.rada.gov.ua/laws/show/96/2016#n11

36. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIIIURL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657.

37. Рудь І. Закон про кібербезпеку: основні положення, оцінки експертів та розвиток вітчизняного інформаційного простору. Україна: події, факти, коментарі. 2017. № 19. С. 42–48.

38. Сучасний стан і напрями протидії кіберзлочинності в Україні. Вісник Кримінологічної асоціації України URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/3848/Suchasnyi%20stan%20i%20napriamy%20protydii%20kiberzlochynnosti%20v%20Ukraini%20_Kravtsova_2018.pdf?sequence=1&isAllowed=y

39. Співробітництво Україна. ЄС – НАТО з протидії гібридним загрозам у кіберсфері. Київ, 2019. 28 с. URL: https:// geostrategy.org.ua/ua/analitika/item/1565- cooperation-ukraine-nato.

40. Трофименко О.Л., «Моніторинг стану кібербезпеки в Україні», Правове життя сучасної України: матер. міжнар. наук.-практ. конф., 17 травня 2019 р., Т. 1, Одеса: Видавничий дім «Гельветика»,2019. С. 642-646

41. У Держспецзв'язку відбулося відкриття найпотужнішого в ЄС Центру реагування на кіберзагрози. URL: http:// www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=286338&cat_id=284576.

42. Функції захисту персональних даних покладено на уповноваженого. URL: http://www.ombudsman.gov.ua/ua/page/ zpd/.

43. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. Інформація і право. 2012. № 2. С. 162-169.

44. Хорошко, В. О. Інформаційна зброя як інструмент інформаційної війни / Володимир Олексійович Хорошко, Юлія Євгеніївна Хохлачова, Тіна Павлівна Пірцхалава, Ігор Сергійович Іванченко // Захист інформації. 2022. Т. 24, № 2. С. 50-58.

45. Чаркіна А.О. Державне управління. Територіальна організація влади в Україні: курс лекцій / А. О. Чаркіна. Київ : Персонал, 2018. 259 с.

46. Шеломенцев В.П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення. Боротьба з

організованою злочинністю і корупцією (теорія і практика). 2012. № 1. С. 312-320.

47. About National Cybersecurity and Communications Integration Center. Офіційний сайт Міністерства внутрішньої безпеки США.URL: https://www.dhs.gov/about-nationalcybersecurity-communications-integration-center

48. Cyber Security Strategy for Germany. Berlin : Federal Ministry of the Interior. 2011. 15 с. URL: www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_ download.pdf?__blob=publicationFile

49. Cyber security strategy. – Commonwealth of Australia: Australian Government, 2009. URL: www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber %20Security%20Strategy%20-%20for%20website.pdf

50. Cyberbezpieczeństwo / Ministerstwo Cyfryzacji Official website. URL: https://www.gov.pl/cyfryzacja/cyberbezpieczenstwo

51. Cyber security strategy of Latvia 2014-2018 URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss

52. Cyber Power Index. Аналітичний проект.URL: http://cyberhub.com

53. China publishes first national cybersecurity-strategy URL: http://www.usito.org/news/china-publishes-first-national-cybersecurity-strategy.

54. Siobhan G. NSA Chief Seeks Bigger Cybersecurity Role // The Wall Street Journal, vol. 8, URL: http://www.wsj.com/articles/SB10001424052970203833004577247710881763168

55. Stubley D. What is Cyber Security? URL: //www.7elements.co.uk/resources/blog /what-is-cyber-security

56. The national strategy to secure cyberspace. Washington, 2003. 60 с. URL: www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

57. History of the EDL CU URL: http://www.kaitseliit.ee/en/historyof-the-edl-cu

58. Information systems defence and security: France’s strategy. – French Network and Information Security Agency. 2011. C. 23.URL: //www.gouvernement.fr/sites /default/files/fichiers_joints/livre-blanc-sur-la-defense-et-la-securite-nationale_2013.pdf

59. Franscella J. Cybersecurity vs. Cyber Security: When, Why and How to Use the Term / J. Franscella. URL: //www.infosecisland.com/blogview/23287-Cybersecurity-vsCyberSecurity-When-Why-and-How-to-Use-the-Term.html

60. Welcome to GCHQ.Pioneering a new kind of security for an ever more complex world URL: www.gchq.gov.uk

61. Zemessardzes Kiberaizsardzī bas vienī ba URL: http://www.zs.mil.lv/Zemessardzes%20vienibas/kiberaizsardzibas_vieniba.aspx