Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи магістра

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

спеціальність *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*

освітньо-наукова програма *Кібербезпека*
(назва освітньої програми)

на тему: *Методи протидії кібервпливам в умовах гібридної війни*

Виконавець: студентка ІІ курсу, групи КБм-21

Валентина ОРТО
(підпис) (ім'я ПРІЗВИЩЕ)

	Прізвище, ініціали	**Підпис**
Науковий керівник	Іван ПАРХОМЕНКО	
Нормоконтроль	Сергій ДАКОВ	

Київ 2023

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Сергій ТОЛЮПА
« 24 » жовтня 2022р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*

Здобувача(ки) КБм-21 *Орто Валентини Віталіївни*
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи: *Методи протидії кібервпливам в умовах гібридної війни*

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ
Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 3 від 20.10.2022.

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень: *процес зменшення кіберризиків та їх впливу на інформаційне середовище у розрізі гібридної війни*

Предмет досліджень: *кіберризики та їх вплив на державне та корпоративне середовище під час гібридної війни*

Мета досліджень: *розробка комплексу заходів для процесу управління кіберризиками та мінімізацію їх негативного впливу на інфраструктуру інформаційних технологій*

Вихідні дані для проведення роботи: *дослідження інцидентів безпеки, які відбувались з початку гібридної війни, контролі безпеки, що застосовуються для зниження рівня кіберризиків, та практичні приклади реалізованих інструментів, методів та моделей*

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна: *удосконалено підхід до управління кіберризиками шляхом вивчення кібервпливу та наявністю індивідуального підходу;*

Практична цінність: *можливість впровадження концептуальної моделі в системах будь-якого масштабу та галузі*

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота виконана у повному обсязі відповідно до теми.

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів роботи	Строки виконання робіт (початок-кінець)
Уточнення постановки задачі	24.10.2022
Розробка плану для досягнення мети роботи	25.10.2022 – 04.12.2022
Аналіз літературних джерел	05.12.2022 – 03.02.2023
Аналіз інцидентів безпеки, які відбулись з початку гібридної війни	04.02.2023 – 19.02.2023
Узагальнення методів та способів управління кіберризиками та їх впливом	20.02.2023 – 25.02.2023
Вивчення контролів безпеки, що можуть бути використані для управління кіберризиками	26.02.2023 – 08.03.2023
Розробка комплексу заходів для процесу управління кіберризиками та їх впливом поетапно з доданням технічних рішень	09.03.2023 – 28.03.2023
Обґрунтування специфіки використання методів	29.03.2023 – 10.04.2023
Оформлення пояснювальної записки	11.04.2023 – 14.05.2023
Підготовка до захисту кваліфікаційної роботи	15.05.2023 – 19.05.2023

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект: *Зменшення поверхі та кількості кібератак та відповідно їх впливу, нанесених через інциденти безпеки*

Соціальний ефект: *Підвищення обізнаності щодо управління кіберризиками завдяки впровадження ефективного та структурованого процесу сучасними методами*

7. ДОДАТКОВІ ВИМОГИ

Завдання видав		*Іван ПАРХОМЕНКО*
	(підпис)	(прізвище, ініціали)
Завдання прийняла до виконання		*Валентина ОРТО*
	(підпис)	(прізвище, ініціали)

Дата видачі завдання: 24.10.2022 р.

Термін подання кваліфікаційної роботи до ЕК: 19.05.2023 р.

УДК. 004.588

РЕФЕРАТ

Пояснювальна записка кваліфікаційно роботи «Методи протидії кібервпливам в умовах гібридної війни» містить 77 сторінок, список використаних джерел з 45 найменувань.

Об’єкт дослідження: процес зменшення кіберризиків та їх впливу на інформаційне середовище у розрізі гібридної війни.

Мета кваліфікаційної роботи: розробка комплексу заходів для процесу управління кіберризиками та мінімізацію їх негативного впливу на інфраструктуру інформаційних технологій.

Методи дослідження: методи наукової абстракції, індукції та дедукції, аналізу, максимальної правдоподібності та синтезу, структурування, алгоритмізація та макетування.

В роботі проведено аналіз інцидентів безпеки, пов’язаних з людським фактором, визначено характерні особливості поведінки людини. Запропоновано застосування сучасних методів управління кіберризиками для зменшення поверхні атак.

Практичне значення роботи полягає у розробці нових та удосконаленні наявних методів зменшення поверхні атак, спричинених людським фактором.

Результати здійснених у кваліфікаційній роботі досліджень можуть бути використані для впровадження запропонованого методу в організації та інтеграція з наявними рішеннями.

Наукова новизна дослідження полягає в удосконаленні підходу до управління кіберризиками шляхом вивчення кібервпливу та наявністю індивідуального підходу.

Ключові слова: кіберризики, кібербезпека, вразливість, реагування на інциденти, методи захисту, гібридна війна, протидія кібервпливу.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРЧЕНЬ

ACL	—	Access Control List
AI	—	Artificial Intelligence
ENISA	—	European Union Agency for CyberSecurity
IoT	—	Internet of Things
SIEM	—	Security Information and Event Management System
DevSecOps	—	Development, Security, Operations
IT	—	Інформаційні технології
ПЗ	—	Програмне забезпечення
НАТО	—	North Atlantic Treaty Organization

ЗМІСТ

ВСТУП

Зважаючи на суттєве зростання інформаційної складової гібридної війни проти України, проблема зростання кіберзагроз стає вкрай актуальною і для свого розв’язання потребує ефективних заходів з оптимізації системи кібербезпеки держави. Реальна ситуація у сфері кібербезпеки України сформована масштабними кібернетичними атаками на інформаційні ресурси держави, метою яких є отримання даних про плани та оцінки українських органів державної влади щодо врегулювання конфлікту на Сході України та дій владних структур у зв’язку з цим. За таких умов питання зменшення кіберризиків надзвичайно актуальні для України, а заходи з протидії викликам і загрозам у зазначеній сфері потребують комплексного характеру, адже кібербезпека має бути невід'ємною і нерозривною частиною технологічного прогресу.

Як вже показало наше сьогодення, зневажання державою питаннями власної кібербезпеки спричиняє не лише значні матеріальні збитки через втрату або спотворення стратегічно важливої інформації, а й може породити техногенні катастрофи, збитки цивільної, фінансової і військової інфраструктури аж до втрати суверенітету держави.

Незважаючи на актуальність даної проблеми, сьогодні існує ряд недоліків в управлінні кіберризиками в організаціях. Наприклад, багато організацій не проводять ранжирування інформаційних систем за ступенем значущості. Це призводить до спроб захистити все, через що одні системи будуть «перезахищені», в той час як інші – «недозахищені».

Таким чином, кіберризиків неможливо уникнути, ними можна керувати лише шляхом впровадження відповідних засобів контролю. Рішенням проблеми кібератак є введення кіберризиків у загальну систему оцінки ризиків, яку проводить служба внутрішнього контролю. Незважаючи на актуальність даної теми, кіберризики внутрішнього контролю практично не розглядаються дослідниками та практиками.

Актуальність теми – кіберризики особливо актуальні сьогодні через зростаючу залежність суспільств і економік від цифрових технологій. З розвитком Інтернету речей (IoT), штучного інтелекту (AI) та інших нових технологій розширюється зона атак для кіберзлочинців і спонсорованих державою акторів, що ускладнює захист від впливу кіберризиків.

Об'єкт дослідження – процес зменшення кіберризиків та управління їх впливом у розрізі гібридної війни.

Предмет дослідження – кіберризики та їх вплив на державне та корпоративне середовище під час гібридної війни.

Метою даної роботи є розробка комплексу заходів для процесу управління кіберризиками та мінімізацію їх негативного впливу на IT-інфраструктуру.

Для досягнення мети кваліфікаційної роботи поставлені окремі завдання:

- проаналізувати наслідки гібридної війни, спричинені кібератаками та наявністю вразливостей;
- провести аналіз сучасних міжнародних підходів до аналізу та зменшення кіберризиків;
- провести аналіз українських підходів до аналізу та зменшення кіберризиків;
- формалізувати принципи побудови системи захисту від кіберризиків та їх впливу;
- дослідити підходи управління кіберризиками та їх впливом на середовище організацій та держави.

При вирішенні поставлених завдань у кваліфікаційній роботі використані: методи наукової абстракції, індукції та дедукції, аналізу (при розкритті основних особливостей управління кіберризиками); метод синтезу (при дослідженні окремих технологій, засобів та заходів для побудови надійної системи безпеки).

Теоретична і методична значущість отриманих результатів:

- удосконалено підхід до управління кіберризиків та зменшення поверхні впливу на корпоративне та державне середовище;

- розроблено сучасні методи побудови захисту інформаційних технологій, що базується на залученні сучасних технологій, які розвинулися чи розвивають на ряду з IoT.

Практична цінність роботи полягає в розробці методики побудови процесу управління кіберризиками в системах будь-якого масштабу та галузі.

Запропоновані методи можуть бути покладені в основу створення процесу зменшення поверхні атак, пов’язаних з гібридною війною.

Основні наукові положення і результати доповідалися та обговорювалися на V Міжнародно-науковій конференції «Проблеми кібербезпеки інформаційно-телекомунікаційних систем (PCSITS)» (Київ, 2022), VI Міжнародно-науковій конференції «Проблеми кібербезпеки інформаційно-телекомунікаційних систем (PCSITS)» (Київ, 2023).

РОЗДІЛ 1
ДОСЛІДЖЕННЯ КІБЕРРИЗИКІВ У КОНТЕКСТІ ЗАХИСТУ ДЕРЖАВИ ТА ОРГАНІЗАЦІЙ

Організації та держави є залежними від комп'ютерних систем та мереж, щоб зберігати та обробляти конфіденційну інформацію, керувати процесами та здійснювати інші операції. Проте, вони також стають мішенями для кібератак, включаючи крадіжку даних, шантаж, розповсюдження шкідливих програм та інших видів кіберзлочинів.

Державні та організаційні системи містять велику кількість конфіденційної інформації, такої як фінансові дані, медичні записи, персональні дані, які можуть бути вкрадені або пошкоджені в результаті кібератаки. Це може призвести до серйозних наслідків, включаючи втрату великих сум грошей, порушення конфіденційності та витоку даних.

Крім того, державні системи містять важливу інформацію про національну безпеку та оборону. Якщо ця інформація потрапить у руки кіберзлочинців або ворожих країн, це може завдати серйозного шкоди національній безпеці.

Тому, дослідження важливості захисту держави та організацій від кіберризиків є критично важливим. Дослідження допоможуть визначити найбільші кіберризики та визначити заходи, які потрібно вживати, щоб запобігти кібератакам та зменшити вплив випадків кіберзлочинності.

Крім виявлення кіберризиків, дослідження також допоможуть в оцінці потенційних наслідків кібератак і визначенні найбільш уразливих місць у системах. Це дасть можливість розробити та впровадити ефективні заходи з кібербезпеки, щоб запобігти атакам, виявити їх на ранніх стадіях та забезпечити швидку реакцію на подібні інциденти.

Дослідження важливості захисту від кіберризиків також допоможуть визначити необхідні ресурси для покращення кібербезпеки. Це включає фінансування на розробку та впровадження захисних технологій, навчання персоналу, вдосконалення

політик безпеки та встановлення ефективних механізмів виявлення та реагування на інциденти.

Подальше дослідження також може сприяти співпраці між державами та організаціями в області кібербезпеки. В обличчі постійно мінливих загроз, обмін інформацією про нові типи атак, розроблені інструменти та найкращі практики може бути важливим фактором у виявленні загроз та вдосконаленні захисних заходів.

Нарешті, дослідження важливості захисту від кіберризиків допоможуть підвищити освіченість і свідомість щодо кібербезпеки. Це може стимулювати організації та індивідуальних користувачів до вживання кроків забезпечення безпеки та практик, які знижують ризик стати жертвою кібератак..

1.1 Аналіз поняття кіберризиків та кібервпливу

Поняття кіберризиків відноситься до потенційних загроз та небезпек, пов'язаних з використанням інформаційних технологій і кіберпростору. Кіберризики включають широкий спектр можливих атак, порушень безпеки, крадіжок даних, кібершпигунство, вимагання викупу та багато інших діянь, що можуть призвести до втрати конфіденційної інформації, порушення приватності, втрати фінансових коштів, недоступності систем або пошкодження репутації.

Кіберризики можуть стосуватися як індивідуальних користувачів, так і організацій, урядових установ, критично важливих інфраструктур, мереж, систем управління та інших компонентів кіберінфраструктури. Зростання кількості та складності кіберзагроз спонукає організації та індивідів активно займатися кібербезпекою та приймати заходи для запобігання, виявлення та відповіді на кібератаки [1].

Звичайно, у контексті гібридної війни кіберризики стосуються неочікуваних і неконтрольованих подій, які можуть вплинути на кіберінфраструктуру країни чи організації. Ці ризики можуть бути викликані навмисними кібератаками або стихійними лихами та можуть спричинити широкомасштабні збої та пошкодження критично важливих систем.

Нижче наведені основні приклади кіберризиків [2]:

▪Широкомасштабні кібератаки: у гібридній війні кібератаки можуть бути використані як інструмент для руйнування або виведення з ладу критичної інфраструктури, такої як електромережі, транспортні мережі, фінансові системи та системи зв'язку. Ці атаки можуть бути спонсоровані іншою державою або недержавними суб'єктами та мати руйнівний вплив на постраждалу країну чи організацію.

▪Стихійні лиха: стихійні лиха, такі як урагани, землетруси та повені, також можуть становити значний ризик для кіберінфраструктури. Ці події можуть спричинити перебої в електропостачанні, пошкодити центри обробки даних і порушити комунікаційні мережі, що призведе до втрати даних, простою системи та інших кіберризиків.

▪Збої в ланцюгах поставок: у гібридній війні ланцюги поставок можуть стати мішенню злочинців або суб'єктів, спонсорованих іншою державою, що призведе до збоїв у потоці товарів і послуг. Це може вплинути на діяльність підприємств і критичну інфраструктуру, що призведе до фінансових втрат та інших кіберризиків.

▪Людська помилка: людська помилка також може становити значний кіберризик, особливо в контексті гібридної війни. Співробітники можуть ненавмисно натиснути фішингові посилання або інші зловмисні вкладення, що призведе до витоку даних або інших наслідків. Крім того, співробітники можуть стати мішенню атак соціальної інженерії, коли злочинці видають себе за надійні джерела, щоб отримати доступ до конфіденційної інформації або систем.

▪Пандемії: такі пандемії, як пандемія COVID-19, можуть призвести до сплеску віддаленої роботи, що призведе до збільшення кіберризиків. Віддалена робота може призвести до таких вразливостей, як незахищені домашні мережі, незахищені пристрої та незахищені канали зв'язку.

▪Дії уряду: такі дії уряду, як регулювання, обмеження та припинення роботи, можуть порушити бізнес-операції, що призведе до кіберризиків. Наприклад, припинення роботи уряду може призвести до закриття центрів обробки даних, що призведе до втрати критичних даних і послуг.

▪Технологічні збої: технологічні збої, такі як помилки програмного забезпечення, збої апаратного забезпечення та збої системи, можуть призвести до кіберризиків. Наприклад, помилка програмного забезпечення може призвести до збою системи, що призведе до втрати критичних даних і служб.

Кібервплив означає навмисне використання цифрових платформ, технологій і тактик для формування, маніпулювання або контролю громадської думки, поведінки та процесів прийняття рішень. Це передбачає використання онлайн-каналів для поширення інформації, часто з наміром сформувати наративи, змінити громадське сприйняття або просувати конкретні плани.

Кампанії кібервпливу можуть включати широкий спектр тактик, як-от поширення дезінформації, дезінформації, пропаганди або застосування методів соціальної інженерії для маніпулювання окремими особами чи групами. Наслідки кібервпливу значні та далекосяжні. Рекомендується перелік ключових аспектів, які слід враховувати при оцінці масштабу впливу:

Дезінформація та дезінформація: кампанії кібервпливу часто передбачають поширення неправдивої або оманливої інформації. Це можна зробити через платформи соціальних мереж, веб-сайти фейкових новин або інші онлайн-канали. Навмисне поширення дезінформації та дезінформації може підірвати довіру до інституцій, маніпулювати громадською думкою та створити плутанину.

Соціально-політична маніпуляція: кампанії кібервпливу можуть бути спрямовані на політичні, соціальні чи культурні проблеми, щоб формувати суспільні настрої та маніпулювати результатами. Використовуючи розбіжності в суспільстві, поширюючи суперечливі наративи або посилюючи екстремістські погляди, ці кампанії можуть розпалювати поляризацію та сіяти розбрат у громадах і націях.

Втручання у вибори: кібервплив використовувався як інструмент для втручання у виборчі процеси. Поширюючи дезінформацію, зламуючи або витікаючи конфіденційну інформацію або маніпулюючи соціальними мережами, зловмисники можуть намагатися вплинути на поведінку виборців, підірвати демократичні процеси та підірвати довіру суспільства до виборів.

Економічний вплив: кампанії кібервпливу можуть мати економічні наслідки. Наприклад, поширення негативних наративів про підприємства чи галузі може зашкодити репутації, вплинути на ціни акцій і створити економічну нестабільність. Крім того, крадіжка інтелектуальної власності та економічне шпигунство можуть бути частиною заходів кібервпливу, спрямованих на отримання конкурентної переваги.

Ризики для кібербезпеки: кампанії кібервпливу можуть мати прямі наслідки для кібербезпеки. Фішингові атаки, розповсюдження зловмисного програмного забезпечення або методи соціальної інженерії можуть використовуватися для отримання несанкціонованого доступу до мереж, зламу систем або викрадення конфіденційних даних. Ці кампанії також можна використовувати як димову завісу для відволікання від інших зловмисних дій, таких як кібершпигунство чи саботаж.

Громадська довіра та впевненість: одним із важливих наслідків кібервпливу є ерозія суспільної довіри та впевненості. Коли люди постійно стикаються з неправдивою або оманливою інформацією, стає складно відрізнити правду від вигадки. Це може підірвати довіру до засобів масової інформації, інституцій і навіть демократичних процесів, призводячи до суспільної недовіри та поляризації [6].

Щоб подолати виклики, пов’язані з кібервпливом, важливо реалізувати комплексні стратегії, які передбачають співпрацю між урядами, технологічними компаніями, організаціями громадянського суспільства та окремими особами. Ці стратегії мають бути зосереджені на підвищенні цифрової грамотності, сприянні критичному мисленню, зміцненні заходів кібербезпеки та вихованні культури відповідальної поведінки в Інтернеті. Розвиваючи стійкість і обізнаність, суспільства можуть краще протистояти впливу кібервпливу та приймати обґрунтовані рішення в епоху цифрових технологій.

Загалом кіберризики та їх вплив у контексті гібридної війни є непередбачуваними та можуть мати далекосяжні наслідки. Організації та країни повинні вживати проактивних заходів для захисту своєї кіберінфраструктури, зокрема впроваджувати потужні заходи кібербезпеки, регулярно перевіряти свої

системи на наявність вразливостей і створювати надійні плани реагування на інциденти [3].

1.2 Приклади кіберризиків у світі

За даними досліджень [36], кількість кібератак у світі зростає щороку, а їхні види та форми стають більш складними та спрямованими. Кіберзагрози можуть бути направлені на різні об'єкти: від індивідуальних користувачів та маленьких компаній до великих корпорацій, установ та державних структур.

Крім того, кіберзагрози можуть мати далекосяжні наслідки для суспільства в цілому, зокрема для критично важливих інфраструктур, таких як енергетика, транспорт, медична техніка, телекомунікації та ін.

Найбільш загрозливі тенденції у кібербезпеці на сьогоднішній день [7]:

Фішингові атаки – спроби шахраїв отримати конфіденційну інформацію, таку як паролі та номери кредитних карт, як правило, через електронну пошту або соціальні мережі. Наприклад, шахраї можуть надіслати електронного листа від імені відомої компанії або банку і запросити користувача ввести свої логін та пароль на фішинговому сайті.

Шкідливе програмне забезпечення (ПЗ) – зловмисний код, який блокує доступ до файлів на комп'ютері або мережі та вимагає викупу в обмін на відновлення доступу до них. Шкідливе ПЗ може поширюватися через електронну пошту, соціальні мережі, веб-сайти чи інші канали.

Атаки на хмарні сервіси – зростаюча популярність хмарних технологій призвела до збільшення кількості атак на хмарні сервіси, такі як Dropbox, Google Drive, Amazon Web Services та інші. Нападники можуть отримати доступ до конфіденційної інформації, використовуючи вразливості в цих сервісах.

Атаки на Інтернет речей (IoT) – IoT пристрої, такі як розумні домашні пристрої, медичні прилади та інші, можуть бути під управлінням зловмисників, які можуть використовувати їх для здійснення кібератак. Зловмисники можуть використовувати вразливості цих пристроїв для виконання різних кібератак, таких як знищення даних

або використання пристроїв для створення ботнету для інших атак. Також це може призвести до крадіжки конфіденційної інформації, блокування пристроїв або навіть витоку особистих даних.

Соціальні мережі – є одним з основних каналів комунікації для мільйонів користувачів, але вони також можуть бути використані зловмисниками для збирання інформації про користувачів та їх діяльність. Наприклад, шахраї можуть використовувати соціальні мережі, щоб дізнатися про приватні дані користувачів та використовувати їх для різних кібератак.

Атаки на критичну інфраструктуру – цільові атаки на критичну інфраструктуру, зокрема електропостачання, транспортні системи, комунікаційні мережі та інші, можуть бути дуже небезпечними. Наприклад, атака на електропостачання може спричинити зупинку роботи підприємств, виробництв, господарства, а також призвести до скачку цін на електроенергію.

Кібершпигунство – зловмисники можуть використовувати його, щоб збирати конфіденційну інформацію про корпорації, урядові структури, дипломатичні мережі та інші організації. Ця інформація може бути використана для створення конкурентної переваги або навіть для впливу на геополітичні процеси.

Кібертероризм – використання кібератак для терористичних цілей. Наприклад, зловмисники можуть використовувати кібератаки для знищення важливої інфраструктури або для поширення страху та паніки серед населення.

Кібершантаж – це використання кібератак для вимагання грошової винагороди від жертви. Наприклад, зловмисники можуть зашифрувати важливі файли на комп'ютері жертви та вимагати винагороду за їх розшифрування.

Витік даних – ситуація, коли конфіденційна інформація, така як паролі, номери кредитних карт, медична інформація та інші, стає доступною зловмисникам. Це може статися через кібератаки, несанкціонований доступ або інші методи.

Це лише деякі з численних кіберризиків, з якими стикається сучасний світ. Для запобігання таким атакам, потрібно забезпечити належний рівень кібербезпеки для всіх систем та пристроїв, які використовуються в повсякденному житті.

Зважаючи на широкий діапазон потенційних загроз, багато кібератак можуть бути успішними, оскільки вони можуть бути спрямовані на використання слабкостей у програмному забезпеченні, людські помилки та інші вразливості [4]:

- Кібератака на SolarWinds

У грудні 2020 року сталася кібератака на підприємство SolarWinds, яке постачає програмне забезпечення для управління мережами і системами. Атака призвела до компрометації програми Orion, яка використовується для моніторингу мереж та систем. Ця атака, яку приписують російським хакерам, була виконана шляхом вставки шкідливого коду в оновлення програми. Як наслідок, хакери змогли отримати доступ до важливих даних більше, ніж 18 тисяч компаній та організацій у США, включаючи державні агентства та підприємства.

Інцидент вирішувався у співпраці з різними компаніями, державними органами, включаючи Федеральне бюро розслідувань (FBI), Національний центр кібербезпеки (CISA), та інші. Вони зосередили свої зусилля на встановленні розміру та обсягу вторгнення, визначенні точки входу та виду діяльності зловмисників. Для відновлення контролю над зараженими системами компанія SolarWinds випустила патч, який видаляє шкідливе ПЗ.

- Кібератака на Microsoft Exchange Server [4]

У березні 2021 року була виявлена кібератака на Microsoft Exchange Server, електронну пошту та групові календарі якої використовуються в установах державного сектору та приватних компаніях. Атака, яку також приписують китайським хакерам, виконувалася за допомогою чотирьох вразливостей, які були використані для встановлення шкідливого ПЗ на серверах Exchange.

Для вирішення цього інциденту Microsoft випустила патчі, які закривають вразливості, а також надала рекомендації щодо безпеки та виявлення шкідливих програм на серверах. Крім того, Microsoft співпрацювала з державними органами, включаючи FBI, для виявлення та ідентифікації зловмисників. Крім того, компанія надала додаткову підтримку для організацій, які могли бути компрометовані в результаті атаки.

▪ Кібератака на Colonial Pipeline

У травні 2021 року сталася кібератака на компанію Colonial Pipeline, яка забезпечує постачання палива в Східному узбережжі США. Атака призвела до припинення роботи трубопроводу та призупинення постачання палива в декількох штатах. Атаку виконала група кіберзлочинців з Росії, яка вимагала викупу у розмірі 4,4 мільйонів доларів.

Для вирішення цього інциденту Colonial Pipeline співпрацювала з Федеральною комісією з енергетичних регуляторів (FERC), Національним центром кібербезпеки та Інфраструктурою (CISA), Федеральним бюро розслідувань (FBI) та іншими державними та приватними організаціями. Компанія також заплатила викуп, але після того, як було встановлено, що вони змогли відновити контроль над своїми системами.

▪ SolarWinds Supply Chain Attack [5]

В грудні 2020 року було виявлено масштабну кібератаку на десятки урядових організацій та приватних компаній, яка стала відома як SolarWinds Supply Chain Attack. Атака була спрямована на додаток підприємства SolarWinds, який використовується для моніторингу мереж та систем, та була спрямована на отримання доступу до конфіденційних даних. Зловмисники використовували складну технологію для обходу механізмів безпеки та перехоплення даних.

Для вирішення цього інциденту десятки організацій уклалися в спільну роботу, включаючи Федеральне бюро розслідувань (FBI), Департамент кібербезпеки та інфраструктури (CISA), Національний центр кібербезпеки та інфраструктури (NCSC), а також приватні компанії з кібербезпеки. Для ідентифікації та вирішення проблеми було залучено кращих експертів з кібербезпеки, які використовували найсучасніші методики та технології для виявлення та видалення шкідливого програмного забезпечення.

▪ WannaCry Ransomware Attack

У травні 2017 року, шкідлива програма WannaCry поширилась по всьому світу, заражаючи мільйони комп'ютерів у десятках країн. Ця атака використовувала уразливість в операційній системі Windows, що була використана для швидкого

поширення шкідливого програмного забезпечення. Атака вимагала викуп в обмін на дешифрування даних.

Для вирішення цієї кризи, Міністерство зв'язку та інформаційних технологій Великої Британії працювало разом з приватними організаціями, які надавали рекомендації щодо заходів з захисту та запобігання подібним атакам. Також, було створено додаткові інструменти та патчі для виправлення уразливостей, які були використані для поширення WannaCry.

Усі ці атаки показують, що кібербезпека є важливою складовою державної безпеки, та що організації мають бути готовими до подібних інцидентів та мати механізми для їх вирішення. Крім того, ці атаки наголошують на важливості співпраці між державами та приватними організаціями для боротьби з кіберзлочинністю та попередження подібних інцидентів.

Для запобігання атакам, організації мають приймати заходи з підвищення своєї кібербезпеки, такі як регулярне оновлення програмного забезпечення, використання сильних паролів та багатофакторної аутентифікації, моніторинг мережі та систем на виявлення підозрілих дій, резервне копіювання даних та розробка планів надзвичайних ситуацій.

Крім того, державні органи мають приділяти увагу кібербезпеці та розробляти стратегії для захисту своїх систем та інформації. Вони також повинні співпрацювати з іншими країнами та організаціями для обміну інформацією про нові загрози та спільного розроблення рішень для боротьби з кіберзлочинністю.

Тому забезпечення кібербезпеки та боротьба з кіберзагрозами та їх впливом стають все більш важливим завданням для компаній, установ та державних структур. Для захисту від кіберризиків необхідно використовувати комплексний підхід, що включає в себе не лише технічні заходи, але й культурні, організаційні та правові аспекти.

1.3 Наслідки неналежного управління кіберризиками у розрізі гібридної війни в Україні

Точкою відліку у кібервійні для України називають грудень 2015 року. Хакерам вдалося успішно атакувати системи одразу трьох енергопостачальних систем нашої країни.

Тоді 250 тисяч мешканців заходу України близько шести годин просиділи без електрики. Як пояснили у Прикарпаттяобленерго, "систему фактично хакнули". Атака відбулася з використанням троянської програми BlackEnergy, яка, ймовірно, потрапила у корпоративну систему компанії з комп'ютера одного зі співробітників. Таким чином злочинцям протягом декількох місяців вдалося непомітно збирати дані, які потім використали, щоб перехопити контроль за управлінням системою.

Паралельно подібні атаки сталися на Чернівціобленерго та Київобленерго, але вже з меншими наслідками. Ці випадки стали першими у світовій історії, коли відключення електроенергії сталося з вини хакерів. Як вдалося з'ясувати, атаки були заздалегідь сплановані та скоординовані з єдиного центру, розміщеного в росії.

"Це стало потужним сигналом для населення України про його вразливість до віддалених атак, а світу – про дедалі вищу майстерність російських хакерів", – написали про цей інцидент у виданні Wired [8].

Головною подією кібервійни проти України став вірус, який згодом отримав назву NotPetya. Наприкінці червня 2017 року російські хакери використали зламані сервери української бухгалтерської фірми Linkos Group. Її програмним забезпеченням MTdoc користується більшість бухгалтерів нашої країни, тому вірус майже миттєво поширився на приблизно 10% усіх комп'ютерів в Україні.

Його жертвами стали як приватні компанії, так і урядові установи країни та частина інфраструктури – Кабмін, Мінінфраструктури, Податкова служба, Держконцерн Антонов, Ощадбанк та Укртелеком, аеропорти Бориспіль та Жуляни, Укргазвидобування, WOG, ДТЕК, Укрпошта, Укррічфлот, Київський метрополітен, Київенерго, Нова Пошта та навіть Чорнобильська атомна електростанція.

15 лютого Україна пережила найбільшу у своїй історії DDoS-атаку. Це спричинило збої у роботі Приват24 та Ощадбанку, а також сайтів Міноборони та ЗСУ. Голова Мінцифри Михайло Федоров зазначив, що атаку готували наперед, а вартість такого замовлення – мільйони доларів [9].

Атака була здійснена з метою здирства, крадіжки даних шляхом отримання доступу до мережі через навантаження, а також з метою шантажу або психологічного впливу.

До того ж, неналежне управління кіберризиками в Україні може мати додаткові наслідки на різних рівнях, включаючи національну безпеку, економічну стабільність та особисту конфіденційність [10]:

Ризики для національної безпеки: Україна в минулому зазнавала кібератак зі значними наслідками для національної безпеки. Неналежне управління кіберризиками може призвести до вразливості критичної інфраструктури, такої як енергетичні мережі, транспортні системи та урядові мережі. Успішні кібератаки на ці системи можуть порушити роботу основних служб, скомпрометувати конфіденційну інформацію та підірвати національну безпеку.

Економічний вплив: кібератаки можуть мати серйозні економічні наслідки для України. Вони можуть порушити бізнес-операції, призвести до фінансових втрат і завдати шкоди репутації організацій. Атаки, спрямовані на фінансові установи, платформи електронної комерції або державні установи, можуть призвести до значної фінансової шкоди та втрати довіри до економіки.

Витоки даних і порушення конфіденційності: неадекватне управління кіберризиками може призвести до витоку даних і порушень конфіденційності, що ставить під загрозу особисту інформацію громадян України. Це може призвести до крадіжки особистих даних, шахрайства та інших форм кіберзлочинності. Порушення даних також може підірвати довіру громадськості до організацій та їх здатність захищати конфіденційну інформацію.

Порушення роботи державних послуг: неправильне управління кіберризиками може призвести до збоїв у роботі державних послуг, таких як охорона здоров’я, освіта та державні послуги. Атаки, спрямовані, наприклад, на системи охорони здоров’я,

можуть перешкоджати наданню важливих медичних послуг і поставити під загрозу життя.

Геополітичні наслідки: враховуючи геополітичний ландшафт і регіональний контекст України, кібератаки можуть мати ширші геополітичні наслідки. Спонсоровані іншими державами атаки або атаки з боку іноземних кіберзлочинців можуть бути політично вмотивованими та викликати ескалацію напруженості між державами [11].

Кібервійна та гібридні загрози: Україна є об'єктом кібервійни та гібридних загроз. Неналежне управління кіберризиками може зробити країну більш сприйнятливою до кіберзагроз, включаючи спонсоровані державою атаки та кампанії з дезінформації. Ці дії можуть бути спрямовані на дестабілізацію країни, втручання в її політичні процеси та маніпулювання громадською думкою.

Промислове шпигунство та крадіжка інтелектуальної власності: Україна має значний технологічний сектор і є домом для багатьох інноваційних компаній. Неналежне управління кіберризиками може наражати ці організації на промислове шпигунство, коли зловмисники намагаються викрасти цінну інтелектуальну власність, комерційні секрети та дані досліджень і розробок. Це може завдати шкоди конкурентоспроможності та інноваційному потенціалу українського бізнесу.

Пошкодження репутації: успішні кібератаки та витоки даних можуть серйозно зашкодити репутації організацій і навіть країни в цілому. Сприйняття неадекватних заходів кібербезпеки може стримувати іноземних інвесторів, впливати на міжнародне співробітництво та перешкоджати економічному зростанню. Відновлення довіри та авторитету після значного кіберінциденту може бути складним і тривалим процесом.

Політична нестабільність і соціальні заворушення: кібератаки, спрямовані на критичну інфраструктуру та державні системи, можуть призвести до політичної нестабільності та соціальних заворушень. Якщо державні послуги порушуються або скомпрометовані, громадяни можуть розчаруватися і вимагати відповідальності від уряду. Це може мати ширші наслідки для стабільності країни та її управління.

Міжнародні санкції та наслідки: у випадках, коли кібератаки походять з України або приписуються їй, неналежне управління кіберризиками може призвести

до міжнародних наслідків. Це може включати дипломатичну напруженість, економічні санкції або обмеження на експорт технологій. Такі заходи можуть мати серйозні економічні та політичні наслідки для країни.

Щоб подолати ці виклики, Україна має зосередитися на посиленні своїх можливостей у сфері кібербезпеки. Це включає покращення правової бази, інвестування в дослідження та розробки в галузі кібербезпеки, сприяння міжнародній співпраці для обміну інформацією та нарощування потенціалу, а також сприяння освіті та обізнаності з питань кібербезпеки серед громадян і організацій. Крім того, співпраця між державними установами, організаціями приватного сектору та міжнародними партнерами має вирішальне значення для комплексної та ефективної стратегії управління кіберризиками [12].

1.4 Забезпечення кібербезпеки України в умовах гібридної війни

Забезпечення кібербезпеки України в умовах гібридної війни – це складний та багатоаспектний процес, який включає в себе різноманітні заходи з протидії кіберзагрозам та кібератакам, а також забезпечення безпеки інформаційних систем державних органів та критично важливих об'єктів.

Один з найважливіших аспектів забезпечення кібербезпеки в Україні – взаємодія між державними органами, компаніями та науковими установами, що працюють в галузі кібербезпеки. Така взаємодія забезпечує обмін інформацією, координацію дій та спільні зусилля в протидії кіберзагрозам.

Для забезпечення кібербезпеки в Україні існує цілий ряд органів та структур, які відповідають за різні аспекти цієї проблеми. Зокрема, це Державна служба спеціального зв'язку та захисту інформації України, Центр кібербезпеки Державної служби спеціального зв'язку та захисту інформації України, Міністерство цифрової трансформації України та інші [13].

Протидія кіберризикам в умовах гібридної війни вимагає постійного моніторингу, аналізу та вдосконалення заходів з кібербезпеки, а також гнучкості і швидкості реагування на нові та еволюціонуючі загрози. Важливо розвивати

інтелектуальні здібності та аналітичні навички, щоб виявляти та передбачати кібератаки, а також швидко реагувати на них.

Загалом, забезпечення кібербезпеки в умовах гібридної війни вимагає комплексного підходу, включаючи вдосконалення технічних, правових, організаційних та людських аспектів. Це вимагає постійного аналізу загроз, оновлення стратегій та планів дій, а також співпраці всіх зацікавлених сторін, як на національному, так і на міжнародному рівні.

Гібридна війна включає кібероперації, які використовуються як інструмент інформаційної війни, шпигунства та диверсій.

Для протидії цим кіберзагрозам Україна створила Національний координаційний центр кібербезпеки, який є централізованим органом, відповідальним за координацію та управління зусиллями країни у сфері кібербезпеки. Центр співпрацює як з державними, так і з приватними організаціями для розробки та впровадження політики та стратегій кібербезпеки.

Росія опинилася в невигідному становищі, оскільки Україна винесла уроки з руйнівних кібератак, здійснених в 2014 і 2016 роках. Найважливішими елементами української оборони були підготовка та зміцнення ймовірних цілей, партнерство та допомога з боку іноземних спеціалістів, а також швидке реагування на звести нанівець атаки, виявлені моніторингом [14].

Українські відомства відігравали провідну роль в обороні, але оборона не повністю спиралася на державні чи навіть українські засоби. Україна мала мережу партнерів (як урядів, так і компаній), які могли забезпечити навчання та допомогу, включаючи дистанційний моніторинг та пом’якшення наслідків, до вторгнення та після його початку. Технічні компанії надали неоціненну допомогу. Колективні дії, які поєднували національне та іноземне, урядове та приватне, дали Україні перевагу в моніторингу та швидкому реагуванні на блокування атак та відновлення або усунення вразливостей. Російські нападники часто розчаровувалися у своїх спробах, і навіть у разі успіху успіх був недовгим. Урок полягає в тому, щоб розвивати міжнародні відносини та інтегрувати партнерів за допомогою дій, які виходять за

рамки зустрічей і семінарів і включають планування та навчання задовго до будь-якої атаки.

У 2016 році Україна опублікувала національну стратегію кібербезпеки та встановила ступінь резервування та стійкості даних і розширила використання шифрування. Будь-який периметр мережі може бути зламаний, і все програмне забезпечення має недоліки, які можна використати.

Україна використовувала сторонню домовленість про хостинг для переміщення деяких даних і послуг за межі географічних кордонів конфлікту. Якщо ніщо інше, це ускладнювало та обмежувало російське планування. Комерційні операції в Інтернеті не завжди дотримуються географічних кордонів. Це розповсюдження зростатиме, оскільки уряди будуть покладатися на хмарні та інші дистанційні служби (включаючи програмне забезпечення як послугу та супутникове підключення). Атака на ці віддалені служби, розташовані в країнах, які не беруть участі в бойових діях, створює ризик наслідків, яких зловмисник може забажати уникнути.

Україна також запровадила низку технічних заходів для захисту свого кіберпростору, включаючи покращення безпеки мережі, посилення шифрування конфіденційних даних і створення можливостей моніторингу та реагування на кібербезпеку. Країна також співпрацює з міжнародними партнерами, включаючи НАТО та Сполучені Штати, для обміну інформацією та координації зусиль із кіберзахисту.

Протидія дезінформації та пропагандистським кампаніям також є важливим аспектом кібербезпеки в контексті гібридної війни. Кампанії з дезінформації можуть бути такими ж шкідливими, як і кібератаки, і можуть підірвати суспільну довіру та впевненість у демократичних інститутах. Створено Департамент стратегічних комунікацій для протидії російській пропаганді та кампаніям дезінформації та працює над підвищенням медіаграмотності серед громадян, щоб сприяти критичному мисленню та усвідомленню дезінформації [15].

Щоб захистити свій кіберпростір, Україна застосувала комплексний підхід, який включає як технічні, так і політичні заходи. Цей підхід визнали ефективною

стратегією експерти з кібербезпеки, які відзначили, що важливо мати скоординований і централізований орган, відповідальний за управління зусиллями з кібербезпеки.

Співпраця з міжнародними партнерами має вирішальне значення для захисту, оскільки ці загрози часто перетинають національні кордони. Встановлення партнерства та угод про обмін інформацією допомогло Україні краще визначати кіберзагрози та реагувати на них.

Загалом війна в Україні підкреслила необхідність застосування країнами комплексного підходу до кібербезпеки та готовності до дедалі складнішої та багатогранної природи сучасної війни.

Запорукою створення надійної системи інформаційної безпеки сьогодні може бути лише зміцнення самої Української держави та її державних органів, відповідальних за забезпечення інформаційної безпеки в країні. У зв’язку з цим постають масштабні завдання щодо розвитку системи захисту інформації, пошуку принципово нових, нестандартних форм організації, взаємодії, координації діяльності, удосконалення всіх засобів, спрямованих на забезпечення процесу управління загрозами та небезпеками.

Головну мету забезпечення інформаційної безпеки слід визначати на основі широкого розуміння цього поняття як важливої складової національної безпеки та системного чинника в усіх сферах життєдіяльності особистості, суспільства, держави, політичної, економічної, соціальної та культурної, науково-технічної, військової, екологічної, інформаційної та ін., складових національної безпеки.

Висновки за розділом 1

Важливо застосувати комплексний підхід до кібербезпеки під час війни, включаючи інвестиції в технічні можливості, створення централізованих координаційних органів, сприяння міжнародній співпраці та обміну інформацією, а також протидію дезінформації та пропагандистським кампаніям. Україна продемонструвала, що кіберзагрози можуть бути такими ж згубними, як і традиційні військові операції, і що кібербезпеку потрібно сприймати серйозно як частину сучасної війни.

РОЗДІЛ 2
АНАЛІЗ ТА МІНІМІЗАЦІЯ КІБЕРРИЗИКІВ У РОЗРІЗІ ГІБРИДНОЇ ВІЙНИ

Аналіз кіберризиків в контексті гібридної війни допоможе ідентифікувати потенційні загрози та розробити відповідні стратегії та тактики для їх протидії. Це включає оцінку можливих джерел атак, визначення цілей та мотивів нападників, а також виявлення можливих вразливостей і слабких місць у системах оборони.

Окрім того, аналіз кіберризиків у гібридній війні може допомогти відновити національну реагувальну здатність у разі кібератак та розробити стратегії відновлення після інциденту. Це може включати розробку резервних планів, впровадження систем резервного копіювання та відновлення даних, а також планування процедур реагування та координації між різними органами влади та секторами.

Додатково, мінімізація кіберризиків у гібридній війні вимагає широкої співпраці між різними секторами суспільства, включаючи державні органи, галузеві організації, приватний сектор та академічну громадськість. Тільки через спільні зусилля можна розробити ефективні стратегії кібербезпеки, обмінюватися інформацією про нові загрози та використовувати найкращі практики в області кібербезпеки.

Мінімізація кіберризиків у гібридній війні також включає розвиток та впровадження передових технологій кібербезпеки. Це може включати розробку потужних систем виявлення та захисту, а також використання штучного інтелекту і аналізу даних для виявлення вразливостей та попередження атак. Такі технології можуть забезпечити швидку реакцію на загрози та покращити загальну кібербезпеку.

Важливим аспектом мінімізації кіберризиків є також розвиток кадрів у сфері кібербезпеки. Необхідно залучати талановитих фахівців з кібербезпеки та забезпечувати їхнє постійне навчання та розвиток. Також потрібно підтримувати академічні програми, дослідження та ініціативи, щоб забезпечити постійний прогрес у сфері кібербезпеки та відповідати на зростаючі загрози.

Крім того, співпраця між країнами є ключовою у мінімізації кіберризиків у гібридній війні. Обмін інформацією про виявлені загрози, спільне проведення навчань та тренувань, а також взаємна підтримка в разі кібератак є важливими елементами колективної оборони від кіберзагроз.

Загалом, аналіз та мінімізація кіберризиків у розрізі гібридної війни є необхідними для забезпечення національної безпеки та захисту інтересів держави.

2.1 Опис поточної ситуації

Зараз, у світі спостерігається постійне зростання кіберризиків та їх впливу на різні сфери діяльності. Швидкий розвиток інформаційних технологій, зростання кількості підключених до мережі пристроїв та поширення хмарних технологій створюють нові можливості для кіберзлочинців та кібершпигунів.

Національні уряди та міжнародні організації дедалі більше усвідомлюють необхідність ефективного управління кіберризиками. Вони розробляють політики, законодавство та стандарти з кібербезпеки, спрямовані на захист критично важливої інформації, захист інфраструктури та протидію кібератакам. Такі організації, як Міжнародний союз зв'язку (ITU), Організація з безпеки та співробітництва в Європі (ОБСЄ), тощо, активно працюють над розробкою та реалізацією міжнародних стандартів та політик кібербезпеки [16].

Однак, незважаючи на зусилля, ситуація з керуванням кіберризиками залишається викликом. Кіберзлочинці постійно вдосконалюють свої технології та тактики, що ускладнює виявлення та протидію їхнім атакам. Постійно зростає кількість інцидентів кібербезпеки, включаючи великі та комплексні кібератаки, які можуть мати серйозні наслідки для держав, організацій та громадян.

За нинішньої політичної ситуації вкрай важливо посилити кібербезпеку виборчих систем та критичної інфраструктури, сприяти реалізації Стратегії кібербезпеки України, посилювати реагування на кіберінциденти.

Доцільно докладати більше зусиль для встановлення державно-приватного партнерства, розробленню та запровадженню механізму обміну інформацією між

державними органами, приватним сектором і громадянами стосовно загроз критичній інформаційній інфраструктурі. Задля своєчасного реагування на кіберінциденти і здійснення практичних заходів зі зміцнення володіння ситуацією у кіберпросторі важливо організовувати проведення тренінгів з підготовки висококваліфікованих фахівців у галузі кібербезпеки та цифрової криміналістики із залученням міжнародних фахівців.

Критично важливі інфраструктурні компанії мають дотримуватись принципу «безпека понад усе» (security-first thinking). Оскільки понад 90% усіх несанкціонованих доступів, уражень і атак відбувається через людський фактор, то на підприємствах потрібно ввести прості регламентні норми, щоб максимально мінімізувати можливі витоки загроз і уражень [17].

Кіберризики неможливо обмежити якоюсь однією сферою, це вимагає від усіх зацікавлених сторін всебічної обізнаності з факторами ризику, умінь і навиків для їхнього вирішення та відповідних заходів для запобігання кібератак ще до їх початку. Україна активно залучає провідні організації до підвищення ступеня обізнаності комерційних підприємств і неприбуткових організацій щодо кібербезпеки на всіх рівнях.

Аналіз показує, що у разі продовжування та активації започаткованої трансформації протягом двох-трьох років можна досягти стійкого рівня кіберстійкості, де безпека стане «звичайним бізнесом», вбудованим у структуру організацій. Забезпечення кібербезпеки можливе тільки за рахунок комплексного і безперервного застосування організаційно-правових та технічних методів захисту на різних рівнях реалізації.

Правовим регулюванням держава має сприяти підвищенню відповідальності провайдерів і власників сайтів щодо розміщення недостовірної та завідомо шкідливої інформації, а також закріплювати механізм впливу на недобросовісних суб’єктів інформаційних правовідносин в кіберпросторі.

Крім того, необхідною умовою також є уникнення правових колізій та прогалин в законодавстві, наслідком чого є несвоєчасне і неадекватне реагування правоохоронних органів на факти заподіяння шкоди інформації, інформаційно-

телекомунікаційним мережам, репутації громадян тощо. Забезпечення кібербезпеки все частіше розглядається, у якості стратегічного завдання держави, що охоплює увесь спектр правового регулювання.

Кібербезпека України умовно розглядається у двох площинах [18]:

- технологічний прогрес, який не лише сприяє стрімкому розвиткові інформаційних комунікацій та послуг, а й формує свої специфічні кіберризики, що є надбанням усього глобального людства та певним чином невідворотною кармою сучасного інформаційного суспільства;
- Україна у стані війни, яка характеризується агресивними нападами не лише у воєнній сфері, інша складова агресії проти України, можливо навіть попереду всього іншого, базується на сучасних інформаційних технологіях і гібридизує усталені конвенційні канони війни.

Таким чином, сучасний стан розвитку суспільних відносин у кіберпросторі для України характеризується низкою як загальноцивілізаційних ознак, характерних інформаційному суспільству, так і певними особливостями, що є результатом гібридної агресії на територію України. Дуалізм зазначеної характеристики кіберпростору для вітчизняних користувачів інформаційно-телекомунікаційними системами, перш за все, притаманний безпековій складовій інформаційних суспільних відносин.

2.2 Сучасні підходи до аналізу та зменшення кіберризиків

Сучасний підхід до інформаційної безпеки підприємства у площині дії кіберризиків визначається наступними етапами [19]:

- визначення кількості кіберризиків та їх категорювання;
- проведення емпірикостатистичної та аналітичної оцінок кіберризиків;
- вчасна ідентифікація нових кіберризиків;
- розробка плану дій та превентивних заходів щодо мінімізації кіберризиків;
- реалізація системи контролю та внесення інноваційних підходів до вчасного аудиту кіберризиків на підприємстві.

Сучасні кіберризики підкреслюють нагальну потребу у співпраці між державами для попередження постійних загроз в інтернеті, забезпечення кращого розслідування, затримання і переслідування зловмисних агентів, мінімізації кіберризиків, адже сучасні суспільства глобально взаємопов'язані, а кібератаки можуть призвести до значних економічних і соціальних збитків. Саме тому міжнародні зусилля у мінімізації кіберризиків та захисту критично важливих інформаційних інфраструктур мають бути узгоджені.

Ці підходи зосереджені на проактивних заходах для запобігання та пом'якшення потенційних кіберзагроз. Також рекомендується дотримуватись основних контролів для мінімізації кіберризиків [20]:

Оцінка та управління ризиками. Організації проводять всебічну оцінку ризиків, щоб визначити й визначити пріоритетність потенційних загроз і вразливостей. Це передбачає оцінку ймовірності атаки, потенційного впливу та ефективності існуючих засобів контролю безпеки. Структури управління ризиками, такі як NIST Cybersecurity Framework або ISO 27001, надають рекомендації щодо систематичного управління кіберризиками.

Інтелектуальні дані про загрози: організації використовують служби та інструменти аналізу загроз для збору інформації про нові загрози, методи атак і зловмисників. Аналізуючи цю інформацію, організації можуть заздалегідь визначати потенційні ризики та вживати відповідних заходів для зміцнення свого захисту.

Управління вразливостями: регулярні оцінки вразливості та тестування на проникнення допомагають виявити слабкі місця в мережах, системах і програмах. Швидко усуваючи ці вразливості, організації можуть зменшити ймовірність успішних атак. Інструменти автоматичного сканування вразливостей і програми винагород за помилки зазвичай використовуються для постійного керування вразливістю.

Навчання з питань безпеки: навчання співробітників передовим практикам кібербезпеки має вирішальне значення для зниження ризику. Програми навчання охоплюють такі теми, як розпізнавання фішингових електронних листів, створення надійних паролів і безпечна обробка конфіденційних даних. Співробітники

відіграють важливу роль у запобіганні кіберзагрозам, тому їхня обізнаність і розуміння мають першочергове значення.

Поглиблений захист: цей підхід передбачає реалізацію кількох рівнів контролю безпеки для захисту від різних векторів атак. Він включає в себе поєднання таких технологій, як брандмауери, системи виявлення та запобігання вторгненням, антивірусне програмне забезпечення та безпечні конфігурації. Принцип полягає в тому, щоб гарантувати, що якщо один шар виходить з ладу, інші рівні все ще можуть забезпечити захист.

Планування реагування на інциденти. Наявність чітко визначеного плану реагування на інциденти допомагає організаціям ефективно реагувати на кіберінциденти. Він включає кроки для виявлення, локалізації, викорінення та відновлення після порушень безпеки. Регулярні настільні вправи та моделювання допомагають перевірити та підвищити ефективність плану реагування.

Автоматизація та оркестровка безпеки: використання технологій автоматизації та управління може оптимізувати операції безпеки та процеси реагування. Автоматизоване виявлення загроз, сортування інцидентів і робочі процеси реагування можуть значно скоротити час, витрачений на виявлення та пом’якшення кіберризиків.

Безперервний моніторинг і аналітика: організації використовують інструменти та рішення моніторингу безпеки, щоб виявляти загрози та реагувати на них у реальному часі. Системи керування інформацією про безпеку та подіями (SIEM) збирають і аналізують дані журналу з різних джерел для виявлення потенційних інцидентів безпеки. Аналітика безпеки та методи машинного навчання дозволяють ідентифікувати шаблони та аномалії для раннього виявлення.

Архітектура нульової довіри: нульова довіра – це підхід, який передбачає відсутність прихованої довіри всередині чи поза периметром мережі. Він наголошує на перевірці користувачів, пристроїв і мережевого трафіку, незалежно від їхнього місцезнаходження. Впровадження принципів нульової довіри може мінімізувати потенційний вплив скомпрометованих систем і несанкціонованого доступу.

Хмарна безпека та DevSecOps [21]: із зростаючим впровадженням хмарних служб і гнучких методологій розробки включення безпеки в хмарні середовища та життєвий цикл розробки програмного забезпечення є надзвичайно важливим. Впровадження практик DevSecOps, включаючи автоматизоване тестування безпеки та інтеграцію засобів контролю безпеки в процес розробки, допомагає зменшити ризики, пов’язані з хмарними рішеннями та програмами.

Сучасні підходи до аналізу та зменшення кіберризиків враховують розмаїття та складність кіберзагроз, які постійно зростають у світі інформаційних технологій. Це може охоплювати технічні заходи, такі як застосування сучасних захисних технологій та систем моніторингу, а також організаційні заходи, такі як політики, процедури та навчання персоналу.

2.3 Державне регулювання кібербезпеки

На державному рівні Україна приділяє значну увагу кібербезпеці і має ряд заходів для її керування [22]:

Стратегія та політика кібербезпеки: Україна розробляє і впроваджує національну стратегію кібербезпеки, яка визначає стратегічні цілі, пріоритети та завдання в галузі кібербезпеки. Також формулюються національна політика та плани дій для забезпечення безпеки кіберпростору.

Інституційні рамки: Україна створила спеціалізовані організації, що відповідають за керування кібербезпекою на державному рівні. Національний кіберцентр, розташований при Держсервізі України, відповідає за моніторинг, аналіз та реагування на кіберзагрози, розробку політик та стандартів безпеки. Крім того, існує Кіберполіція, яка займається розслідуванням кіберзлочинів.

Міжнародне співробітництво: Україна активно співпрацює з міжнародними партнерами у сфері кібербезпеки, такими як Європейський Союз, НАТО та Інтерпол.

Безпека критичної інфраструктури: Україна звертає особливу увагу на захист критичної інфраструктури, такої як енергетика, транспорт, фінансова система тощо.

Здійснюються заходи для ідентифікації критичних об'єктів, розробки та впровадження заходів з кіберзахисту цих об'єктів.

Усвідомлення та навчання: Україна проводить інформаційні кампанії, навчальні заходи та тренінги з кібербезпеки для населення, бізнесу та державних службовців. Мета полягає в усвідомленні загроз та підвищенні рівня кіберграмотності серед користувачів.

Координація та співпраця: В Україні існує механізм координації дій між різними органами влади, поліцією, бізнес-сектором та іншими зацікавленими сторонами. Це сприяє виявленню, аналізу та реагуванню на кіберзагрози, а також обміну інформацією та кращій координації заходів з кібербезпеки.

Також Україна має ряд законів та інших документів, які регулюють кібербезпеку на державному рівні, наприклад [23]:

- Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" – встановлює правила захисту інформації в ІТС, зокрема заборону несанкціонованого доступу, використання та поширення інформації, що містить державну таємницю.
- Стратегія кібербезпеки України – описує стратегічні цілі та завдання держави щодо забезпечення кібербезпеки, встановлює рекомендації щодо захисту інформації та кіберінфраструктури.
- Національний кіберцентр при Держсервізі України – центральний орган виконавчої влади, який забезпечує функціонування інформаційної та кібербезпеки в Україні.
- Кіберполіція – спеціалізована поліцейська служба, яка займається розслідуванням кіберзлочинів, проведенням профілактичної роботи та співпрацею з міжнародними партнерами з кібербезпеки.
- Державне агентство з питань електронного урядування - забезпечує розробку та впровадження технічних засобів для захисту інформації та забезпечення кібербезпеки урядових систем.

Ці інститути та законодавчі акти спільно працюють для забезпечення кібербезпеки в Україні. Однак, важливо зауважити, що кібербезпека є процесом, який

постійно розвивається, і вимагає постійного оновлення. Україна продовжує займатися вдосконаленням своїх кібербезпечних зусиль, впровадженням нових технологій та розробкою стратегічних планів для забезпечення стійкої кібербезпеки на державному рівні.

Застосування заходів з кібербезпеки на практиці включає різноманітні дії та ініціативи. Зокрема, як Україна впроваджує кібербезпеку на практиці [24]:

Реагування на інциденти: Україна впровадила систему реагування на кіберінциденти, яка дозволяє виявляти, аналізувати та реагувати на кібератаки. Ця система допомагає швидко виявляти загрози та приймати заходи щодо їх нейтралізації.

Санкції: Україна впровадила законодавчі заходи для протидії кіберагресії та злочинної діяльності в кіберпросторі. Це включає можливість застосування санкцій проти осіб та організацій, які здійснюють кібератаки на інтереси України.

Створення захисних центрів: Україна розвиває мережу кіберзахисних центрів на різних рівнях – від державних до регіональних та секторальних. Ці центри забезпечують моніторинг, аналіз та реагування на кіберзагрози відповідно до своєї компетенції.

Заходи з кіберграмотності: Україна активно проводить навчання та інформаційні кампанії з кібербезпеки для громадян, бізнесу та державних службовців. Це включає проведення тренінгів, розповсюдження практичних порад щодо безпеки в Інтернеті та популяризацію кіберграмотності серед широкої громадськості.

Співпраця з міжнародними партнерами: Україна активно співпрацює з міжнародними організаціями у сфері кібербезпеки. Ця співпраця включає обмін інформацією про кіберзагрози, проведення спільних навчань та тренувань, а також розробку спільних проектів з кібербезпеки.

Захист критичної інфраструктури: Україна зосереджує зусилля на захисті критичної інфраструктури від кіберзагроз. Це включає розробку та впровадження заходів з кіберзахисту для енергетичних систем, транспорту, банківської системи та інших важливих секторів.

Участь у міжнародних ініціативах: Україна приєдналася до різних міжнародних ініціатив у сфері кібербезпеки. Наприклад, Україна брала участь у глобальних кібернормативних процесах, таких як робота в Групі з роботи з питань кібербезпеки ООН та інших форумах, для формування міжнародних стандартів та правил у кіберпросторі.

Державне регулювання кібербезпеки в Україні є невід'ємною складовою розвитку і захисту інформаційно-комунікаційних систем країни. Україна визнає значення кібербезпеки та впроваджує широкий спектр заходів для запобігання та протидії кіберзагрозам.

2.4 Комерційне регулювання кібербезпеки

Регулювання комерційної кібербезпеки стосується встановлених урядом правил і стандартів, яких організації повинні дотримуватися, щоб забезпечити безпеку своїх цифрових активів і захистити конфіденційну інформацію. Ці правила спрямовані на встановлення мінімального рівня вимог до кібербезпеки, просування найкращих практик і захист критичної інфраструктури та даних споживачів. Специфіка регулювання комерційної кібербезпеки може відрізнятися в різних країнах і юрисдикціях, але існують деякі загальні аспекти [25]:

Нормативна база: уряди встановлюють нормативну базу, яка визначає вимоги та зобов’язання комерційних організацій щодо кібербезпеки. Ці рамки можуть бути введені в дію через законодавчі акти, виконавчі накази або спеціальні нормативні акти для галузі. Вони забезпечують правову основу для дотримання стандартів кібербезпеки.

Вимоги до відповідності: правила комерційної кібербезпеки зазвичай окреслюють конкретні заходи безпеки, засоби контролю та практики, які організації повинні впроваджувати. Ці вимоги можуть охоплювати широкий діапазон сфер, таких як безпека мережі, контроль доступу, захист даних, реагування на інциденти та конфіденційність. Очікується, що організації будуть відповідати цим вимогам і демонструвати їх дотримання за допомогою аудитів та оцінок.

Регуляторні органи: регуляторні органи або агентства відповідають за нагляд і виконання комерційних правил кібербезпеки. Ці органи можуть мати повноваження проводити аудити, розслідування та оцінки для забезпечення відповідності. Вони також можуть надавати керівництво та підтримку організаціям у розумінні та впровадженні заходів кібербезпеки.

Звітування та сповіщення: комерційні організації можуть бути зобов'язані повідомляти про інциденти кібербезпеки або порушення до регуляторних органів протягом визначеного періоду часу. Це допомагає регуляторним органам відстежувати характер і вплив кіберзагроз і вживати відповідних заходів. Деякі нормативні акти також можуть вимагати від організацій сповіщати постраждалих осіб або клієнтів про порушення даних, які можуть вплинути на їхню особисту інформацію.

Штрафи та правозастосування [26]: Недотримання правил комерційної кібербезпеки може призвести до штрафів і санкцій. Регуляторні органи можуть мати повноваження накладати штрафи, накладати обмеження або скасовувати ліцензії чи сертифікати. Ці покарання стимулюють організації серйозно ставитися до кібербезпеки та забезпечувати відповідність.

Спеціальні нормативні акти для окремих галузей: у деяких галузях або секторах, як-от фінанси, охорона здоров'я та критична інфраструктура, можуть діяти додаткові правила кібербезпеки, адаптовані до їхніх унікальних ризиків і вимог. Ці галузеві норми можуть накладати додаткові стандарти, заходи відповідності або зобов'язання щодо звітності для вирішення конкретних проблем кібербезпеки.

Міжнародні стандарти та гармонізація: правила комерційної кібербезпеки часто узгоджуються з міжнародними стандартами та найкращими практиками кібербезпеки. Наприклад, від організацій може вимагатися дотримання таких стандартів, як ISO 27001 (система управління інформаційною безпекою) або NIST Cybersecurity Framework. Зусилля щодо гармонізації спрямовані на встановлення узгодженості та сумісності між правилами кібербезпеки різних юрисдикцій.

Співпраця та державно-приватне партнерство: уряди часто співпрацюють із зацікавленими сторонами галузі, експертами з кібербезпеки та професійними

асоціаціями для розробки та вдосконалення комерційних правил кібербезпеки. Державно-приватне партнерство може допомогти в обміні даними про загрози, сприянні обміну інформацією та сприянні співпраці для спільного вирішення проблем кібербезпеки.

Важливо зазначити, що специфіка регулювання комерційної кібербезпеки може значно відрізнятися залежно від країни та регіону. Організації повинні бути в курсі застосовних норм у їхніх юрисдикціях і працювати над їх відповідністю, щоб забезпечити безпеку своїх цифрових активів і захистити конфіденційну інформацію.

Існує багато комерційних рішень для захисту від кіберризиків, які пропонують різні компанії та постачальники послуг, наприклад [27]:

- Антивірусне програмне забезпечення: це програмне забезпечення дозволяє виявляти та блокувати шкідливі програми, які можуть завдати шкоди комп'ютеру або мережі. Деякі з найвідоміших виробників антивірусного ПЗ - McAfee, Norton, Kaspersky та Bitdefender.
- Фаєрвол: це програмне або апаратне забезпечення, яке забезпечує контроль доступу до мережі та забезпечує захист від небажаних з'єднань або атак. Деякі з найпопулярніших виробників файерволів – Cisco, Juniper Networks та Fortinet.
- Системи виявлення та запобігання вторгненням (IDS/IPS): ці системи дозволяють виявляти та блокувати небажані з'єднання та атаки на мережу. Деякі з провідних виробників IDS/IPS систем – IBM, McAfee, Check Point та Palo Alto Networks.
- Системи управління безпекою інформації (ISMS): ці системи дозволяють організаціям забезпечувати стандарти безпеки та управляти ризиками на всіх рівнях. Деякі з провідних виробників ISMS – Symantec, RSA та Microsoft.
- Системи аутентифікації та авторизації: ці системи дозволяють забезпечувати контроль доступу до систем та даних. Деякі з провідних виробників систем аутентифікації та авторизації – RSA, Microsoft та Okta.
- Системи захисту від DDoS-атак: ці системи дозволяють захищати мережу від DDoS-атак, що можуть завдати значної шкоди. Деякі з провідних виробників систем захисту від DDoS-атак – Akamai

▪Системи захисту від шпигунського програмного забезпечення та шпигунських атак: ці системи дозволяють виявляти та блокувати шкідливі програми та атаки, які спрямовані на отримання конфіденційної інформації. Деякі з провідних виробників систем захисту від шпигунського ПЗ та атак – McAfee, Symantec тощо.

▪Системи захисту від фішингу та інших соціальних інженерних атак: ці системи дозволяють виявляти та блокувати атаки, які спрямовані на отримання конфіденційної інформації шляхом маніпулювання людьми. Деякі з провідних виробників систем захисту від фішингу та соціальних інженерних атак - Proofpoint, KnowBe4 та Cofense.

▪Системи захисту від кібератак на критичну інфраструктуру [22]: ці системи дозволяють захистити критичну інфраструктуру від кібератак, які можуть завдати значної шкоди. Деякі з провідних виробників систем захисту від кібератак на критичну інфраструктуру - Dragos, CyberX та Indegy.

▪Системи захисту від зломів веб-додатків: ці системи дозволяють захистити веб-додатки від атак, які спрямовані на отримання несанкціонованого доступу до даних або системи. Деякі з провідних виробників систем захисту від зломів веб-додатків - Imperva, F5 Networks та Akamai.

2.5 Міжнародні контролі захисту від кіберризиків

З метою покращення захисту від кіберризиків та забезпечення безпеки в кіберпросторі створено багато міжнародних організацій та ініціатив [28].

Європейська загальна регламентація про захист даних (GDPR): Ця регламентація встановлює стандарти захисту даних та приватності для організацій, які збирають та обробляють персональні дані громадян Європейського Союзу.

Кібербезпекова рада НАТО (NCSC NATO): Ця рада є форумом для обміну інформацією та співпраці між членами НАТО у галузі кібербезпеки. Вона сприяє виробленню норм та стандартів безпеки, обміну найкращими практиками та спільним навчанням.

Рамкова програма Європейського Союзу з кібербезпеки (EU Cybersecurity Framework): Ця програма спрямована на забезпечення високого рівня кібербезпеки в Європейському Союзі шляхом розробки політик, стандартів та координації дій між державами-членами.

Група фінансової діяльності з нормативного регулювання (Financial Action Task Force, FATF): FATF є міжнародною організацією, що займається боротьбою з фінансуванням тероризму та відмиванням грошей. Вона встановлює рекомендації щодо захисту фінансової системи від кіберзагроз, зокрема, вимоги до кібербезпеки у фінансовому секторі.

Ініціатива "Інформаційна безпека на Інтернеті" (Cybersecurity on the Internet Initiative, CII): Ця ініціатива, започаткована Організацією Об'єднаних Націй (ООН), має на меті сприяти зміцненню кібербезпеки та захисту від кіберризиків шляхом співпраці між державами, громадськими організаціями та приватним сектором.

Європейська агенція з кібербезпеки (European Union Agency for Cybersecurity, ENISA): ENISA є агентством Європейського Союзу, яке сприяє підвищенню рівня кібербезпеки в Європі. Вона займається розробкою та поширенням настанов, рекомендацій та інформації щодо кібербезпеки.

Міжнародна організація зі стандартизації (International Organization for Standardization, ISO): ISO розробляє стандарти в різних сферах, включаючи кібербезпеку. Наприклад, стандарт ISO/IEC 27001 встановлює вимоги до систем управління інформаційною безпекою.

Основні цілі цих організацій включають [29]:

- Розробка стандартів і рекомендацій: Ці організації встановлюють стандарти, які організації та держави можуть використовувати як референсні точки для впровадження ефективних заходів кібербезпеки. Вони розробляють рекомендації щодо найкращих практик, методологій та процедур для захисту від кіберризиків.
- Сприяння співпраці та обміну інформацією: Ці організації створюють платформи для співпраці між країнами, державними установами, приватним сектором та іншими зацікавленими сторонами. Вони сприяють обміну інформацією про кіберзагрози, інциденти та найкращі практики.

▪Зміцнення свідомості та навчання: Ці організації виконують роль у підвищенні свідомості щодо кібербезпеки та наданні навчальних матеріалів та ресурсів. Вони сприяють освіті та підвищенню кваліфікації професіоналів у галузі кібербезпеки.

▪Координація та розробка стратегій: Ці організації координують зусилля міжнародного співтовариства щодо кібербезпеки. Вони допомагають у розробці національних та міжнародних стратегій, планів дій та політик для ефективного захисту від кіберризиків.

Тобто метою цих організацій є створення безпечного та надійного кіберпростору, захист інформації, захист критично важливих інфраструктур та протидія кіберзагрозам. Вони також сприяють підвищенню довіри в електронному середовищі, забезпеченню конфіденційності, цілісності та доступності даних, а також протидії кіберзлочинності.

Організації цілеспрямовано співпрацюють з урядами, громадськими організаціями, академічними установами та приватним сектором, щоб спільно розробляти та впроваджувати стратегії, політики та технологічні рішення для захисту від кіберризиків. Вони також сприяють побудові міжнародної співпраці, обміну інформацією та спільним навчанням для ефективного реагування на кіберзагрози.

Відповідно, зменшення кіберризиків контролюється законом за допомогою різних нормативних актів і законодавства, які встановлюють вимоги та практику кібербезпеки. Ці закони спрямовані на захист конфіденційних даних, критичної інфраструктури та конфіденційності особи від кіберзагроз і атак [30]:

Загальний регламент захисту даних (GDPR): GDPR – це нормативний акт Європейського Союзу (ЄС), який встановлює вказівки щодо збору, обробки та зберігання персональних даних, містить вимоги щодо захисту персональних даних та створення спеціальних заходів для боротьби з кіберзлочинністю. Він вимагає від організацій впроваджувати належні заходи безпеки для захисту персональних даних і повідомляти про порушення даних протягом 72 годин.

Закон про обмін інформацією про кібербезпеку (CISA): CISA – це закон США, який заохочує організації обмінюватися інформацією про загрози кібербезпеці між

собою та з урядом. Він також уповноважує федеральні агентства розробляти та впроваджувати заходи кібербезпеки для захисту федеральних систем.

Закон про перенесення та підзвітність медичного страхування (HIPAA): HIPAA – це закон США, який вимагає від організацій охорони здоров'я захищати конфіденційність і безпеку інформації про здоров'я пацієнтів. Він зобов'язує впроваджувати адміністративні, фізичні та технічні заходи захисту для захисту електронної захищеної медичної інформації (ePHI).

Правила захисту критичної інфраструктури (CIP): Правила CIP – це набір обов'язкових стандартів, розроблених Північноамериканською корпорацією з надійності електроенергії (NERC), які вимагають від електричних енергокомпаній впровадження заходів безпеки для захисту від кіберзагроз.

Стандарт безпеки даних платіжних карток (PCI DSS): PCI DSS – це набір стандартів безпеки, розроблений великими компаніями, що випускають кредитні картки, для захисту від шахрайства з платіжними картками. Він зобов'язує впроваджувати заходи безпеки для захисту від витоку даних, який може поставити під загрозу інформацію платіжної картки.

Загалом закони та нормативні акти відіграють вирішальну роль у контролі та зниженні кіберризиків, встановлюючи вимоги та методи кібербезпеки. Організації, які не дотримуються цих законів і правил, можуть зіткнутися з юридичними та фінансовими наслідками, включаючи штрафи, пені та судові позови.

Зважаючи на те, що кіберзагрози є досить серйозною проблемою в сучасному світі, на міжнародному рівні було додатково прийнято багато ініціатив та контролів для захисту від них. Ось декілька прикладів:

Європейська стратегія кібербезпеки: ця стратегія була розроблена Європейською комісією та містить рекомендації щодо захисту від кіберзагроз, забезпечення кібербезпеки та зміцнення співпраці між державами-членами.

Конвенція про кібербезпеку Організації з безпеки та співробітництва в Європі (ОБСЄ): ухвалена у 2001 році, ця конвенція містить вимоги щодо боротьби з кіберзлочинністю та забезпечення кібербезпеки.

Конвенція про кіберзлочинність (Budapest Convention): Ця конвенція, прийнята Радою Європи, має на меті боротьбу з кіберзлочинністю шляхом розробки міжнародних норм та співпраці між країнами.

Ініціатива з кібербезпеки США: американський уряд активно розробляє ініціативи щодо захисту від кіберзагроз та боротьби з кіберзлочинністю, такі як Національна стратегія кібербезпеки та Закон про кібербезпеку.

Міжнародні контролі захисту від кіберризиків є критично важливими для забезпечення безпеки та стійкості в цифровому світі. Кіберзагрози не мають кордонів, і їх вплив може мати глобальні наслідки, тому спільні зусилля на міжнародному рівні є невід'ємною частиною ефективного керування кібербезпекою.

2.6 Порівняння державного, комерційного і міжнародного регулювання

Кіберризики стають все більшою загрозою для суспільства, організацій та індивідуальних користувачів. У зв'язку з цим стає все важливішим визначення ефективних методів регулювання цих ризиків та мінімізації їх впливу.

- Державне регулювання [25]

Державне регулювання кіберризиків передбачає втручання держави у формі законодавчих актів, політик та нагляду. Однією з основних переваг державного регулювання є забезпечення безпеки країни та її громадян у кіберпросторі. Держави можуть приймати закони, що регулюють кібербезпеку, встановлюють вимоги до захисту інформації, забороняють кібератаки та встановлюють відповідальність за порушення законодавства. Державне регулювання може бути корисним для забезпечення базового рівня захисту, координації та співпраці між організаціями та відповідних секторів господарства.

Однак, недоліком може бути недостатня гнучкість, пов'язана зі швидкими змінами в кіберзагрозах та технологічному розвитку. Державні структури можуть виявляти складнощі в оперативному впровадженні нових політик та законодавства, а також в адаптації до мінливого середовища.

▪Комерційне регулювання [27]

Комерційне регулювання кіберризиків передбачає впровадження внутрішніх політик та процедур організаціями та підприємствами. Компанії можуть встановлювати свої стандарти кібербезпеки, проводити аудит та аналіз ризиків, розробляти плани реагування на інциденти та впроваджувати заходи захисту інформації. Комерційне регулювання може бути ефективним у гнучкості та швидкому реагуванні на зміни в кіберризиках. Компанії можуть використовувати нові технології та інноваційні підходи до захисту своїх активів.

До недоліків комерційного регулювання входить відсутність стандартизації, відсутність координації між організаціями та можливість ігнорування кібербезпеки з боку деяких суб'єктів.

▪Міжнародне регулювання [30]

Міжнародне регулювання кіберризиків відбувається через співпрацю між державами та міжнародними організаціями. Вони можуть укладати договори та угоди, розробляти міжнародні стандарти та рекомендації з кібербезпеки. Міжнародна співпраця допомагає вирішувати глобальні кіберзагрози, встановлювати мінімальні стандарти безпеки та спільні підходи до реагування на кібератаки. Однією з переваг міжнародного регулювання є можливість обміну інформацією та досвідом між країнами, спільна розробка рішень та впровадження найкращих практик.

Однак, є складність досягнення консенсусу між різними країнами, різниця в правових системах та можливість використання кіберзагроз як засобу геополітичного впливу.

Державне, комерційне і міжнародне регулювання кіберризиків мають свої переваги та виклики. Державне регулювання забезпечує нормативну базу та координацію на національному рівні, комерційне регулювання дозволяє організаціям впроваджувати індивідуальні підходи та інновації, а міжнародне регулювання сприяє співпраці та координації між країнами.

Врахування наступних аспектів у розгляді порівняння різних форм регулювання кіберризиків дозволить забезпечити більш повне розуміння та

комплексний підхід до кібербезпеки, що буде сприяти забезпеченню стабільності та безпеки в цифровому середовищі [26]:

Роль громадськості: Поміж різних форм регулювання слід враховувати роль громадськості у контексті кібербезпеки. Активна участь громадських організацій, наукових спільнот та громадян може сприяти підвищенню освітнього рівня, забезпеченню ефективної свідомості та підтримці впровадження заходів кібербезпеки.

Міжсекторальний підхід: Важливо розглядати вплив кіберризиків та регулювання їх у контексті міжсекторального підходу. Зв'язок та співпраця між державними органами, приватним сектором, академічними установами та громадськістю є ключовим для ефективного розуміння, виявлення та вирішення кіберризиків.

Технологічний прогрес: Швидкий темп технологічного прогресу викликає постійні зміни в кіберпросторі та появу нових кіберзагроз. Регулювання повинно бути гнучким та адаптивним до цих змін, а також стимулювати розробку та впровадження нових технологій для захисту від кіберризиків.

Міжнародна співпраця в області правозастосування: Поміж міжнародного регулювання варто наголосити на важливості співпраці між правоохоронними органами та правозастосовними установами різних країн. Обмін інформацією, спільне розслідування та навчання допомагають ефективно протидіяти кіберзлочинності та міжнародним кіберзагрозам.

Етичні аспекти: У контексті кіберризиків існують етичні питання, пов'язані з використанням кіберзброї та маніпуляцією даними. Регулювання повинно враховувати ці аспекти та сприяти розробці етичних принципів, які забезпечать відповідальне та етичне використання кібертехнологій.

Рівень ресурсів: Важливо враховувати рівень доступних ресурсів у кожній формі регулювання. Державне регулювання може мати більше фінансових, технічних та людських ресурсів, що дозволяє йому проводити більш широкі та комплексні заходи з кібербезпеки. У той же час, комерційне регулювання може бути більш

гнучким та швидким у впровадженні нових заходів, оскільки приватні компанії мають більшу відповідальність за захист своїх власних інформаційних активів.

Географічний контекст: Регулювання кіберризиків може розрізнятися залежно від географічного контексту. Різні країни та регіони можуть мати різні законодавчі рамки, політичні пріоритети та культурні особливості, що впливають на спосіб регулювання кібербезпеки. Міжнародне регулювання може включати угоди та стандарти, які дозволяють забезпечити гармонізацію підходів між країнами та забезпечити міжнародну співпрацю у сфері кібербезпеки.

Зв'язок з іншими секторами безпеки: Кібербезпека тісно пов'язана з іншими аспектами безпеки, такими як національна безпека, економічна безпека, кримінальна безпека тощо. Важливо розглядати вплив кіберризиків на ці сектори та забезпечувати взаємозв'язок і співпрацю між ними. Державне регулювання може бути більш орієнтоване на загальну національну безпеку, комерційне регулювання може більше акцентувати на економічних аспектах, а міжнародне регулювання може ставити акцент на міжнародну співпрацю та обмін інформацією.

Співпраця і координація: Ефективне управління кіберризиками вимагає співпраці та координації між різними стейкхолдерами, включаючи урядові органи, приватний сектор, академічну громадськість та міжнародні організації. Регулювання повинно сприяти створенню механізмів співпраці та обміну інформацією між цими стейкхолдерами, а також підтримувати створення міжнародних форумів та ініціатив для обговорення та спільного розроблення політик та стандартів.

Для ефективного управління кіберризиками необхідно забезпечити постійну співпрацю між різними суб'єктами, встановити міжнародні стандарти та рекомендації, розвивати технічні засоби та здібності для виявлення, відповіді та мінімізації кіберризиків. Тільки шляхом поєднання зусиль на рівні держав, організацій та міжнародної спільноти можна досягти ефективного управління кіберризиками та забезпечити безпеку в кіберпросторі [19].

Висновки за розділом 2

Для успішного захисту від кіберризиків, важливо розуміти, що це довгостроковий процес, який потребує системного підходу. Захист від кібератак повинен бути вбудований в усі аспекти бізнесу та повинен бути підтриманий високої керівництвом.

Крім того, необхідно пам'ятати, що технології не є єдиним рішенням. Управління кіберризиками та їх впливом повинно включати в себе як технічні, так і не технічні засоби захисту.

Також важливо розуміти, що захист від кіберризиків є постійним процесом, який потребує регулярного оновлення та адаптації до нових загроз. Тому важливо планувати та вдосконалювати свої стратегії та плани реагування на кібератаки та тестувати їх регулярно.

РОЗДІЛ 3
РОЗРОБКА МЕТОДІВ УПРАВЛІННЯ КІБЕРРИЗИКАМИ

Методи управління ризиками є важливим інструментом для ефективного управління кібербезпекою та мінімізації ризиків в організаціях. Вони дозволяють ідентифікувати, оцінювати та контролювати ризики, пов'язані з кібербезпекою, що дозволяє вчасно виявляти та запобігати можливим загрозам.

Методи управління ризиками допомагають організації визначити, які інформаційні активи потребують захисту, оцінити потенційні загрози та ризики, пов'язані з цими активами, а також розробити та впровадити стратегії та заходи з мінімізації цих ризиків. Також вони допомагають організації виявляти слабкі місця в системах кібербезпеки та вдосконалювати їх для покращення захисту.

Використання методів управління ризиками також допомагає забезпечувати відповідність організації з вимогами законодавства та стандартами з кібербезпеки. Багато держав та регуляторних органів вимагають від організацій дотримання певних стандартів та практик з кібербезпеки, і модель управління ризиками допомагає виконувати ці вимоги.

Тобто, управління ризиками є необхідним інструментом для ефективного керування кібербезпекою та зниження ризиків в організаціях. Вони допомагають ідентифікувати, оцінювати, контролювати та мінімізувати кіберризики, а також забезпечують оптимальне використання ресурсів, підвищують свідомість про кібербезпеку та сприяє постійному вдосконаленню системи захисту.

Важливо пам'ятати, що методи управління ризиками повинні бути гнучкими і адаптивними до мінливих умов та нових загроз. Вони потребують постійного оновлення, моніторингу та аналізу, а також активної співпраці між відділами кібербезпеки, високого рівня управлінської підтримки та залучення всього персоналу організації.

Необхідно також враховувати, що методи управління ризиками є лише однією з частин комплексної стратегії кібербезпеки. Крім них, важливо розглядати інші

аспекти, такі як технічні заходи безпеки, навчання персоналу, обмін інформацією та співпрацю зі сторонніми експертами та організаціями.

3.1 Вхідні дані та постановка завдання

Забезпечення кібербезпеки стає все більш важливим завданням у сучасному цифровому світі. Зростання кіберзагроз, залежність від інформаційних технологій, економічні наслідки кібератак та регуляторні вимоги є чинниками, які вимагають розробки ефективних методів управління кіберризиками.

Одним з основних чинників, що ведуть до необхідності розробки методів управління кіберризиками, є зростання кіберзагроз. У сучасному світі кібератаки стають все більш складними та витонченими, а зловмисники використовують нові технології та методи для злому систем і крадіжки даних. Це ставить під загрозу безпеку організацій та індивідуальних користувачів, що вимагає розробки нових стратегій та методів захисту [31].

Крім того, залежність від інформаційних технологій є іншим фактором, що підкреслює необхідність розробки методів управління кіберризиками. Організації та державні установи зберігають і обробляють значні обсяги конфіденційної інформації, яка потребує надійного захисту. Зростання кількості IoT-пристроїв також створює нові ризики та вразливості. Розробка методів управління кіберризиками допомагає забезпечити безпеку цих інформаційних систем та пристроїв.

Економічні наслідки кібератак є ще одним фактором, що вимагає розробки методів управління кіберризиками. Кібератаки можуть призвести до втрати даних, порушення роботи систем, витоку конфіденційних даних, шахрайства та інших негативних наслідків для бізнесу і економіки. Втрати, пов'язані з кібератаками, можуть бути значними і мати серйозний вплив на фінансову стабільність організацій. Розробка методів управління кіберризиками спрямована на зменшення ризиків та підвищення рівню кібербезпеки, що сприяє зниженню втрат і збереженню репутації організацій.

Крім того, регуляторні вимоги стосовно кібербезпеки стають все більш жорсткими і обов'язковими. Багато країн встановлюють законодавство та регуляції, які вимагають від організацій виконувати певні стандарти кібербезпеки, забезпечувати конфіденційність та цілісність даних, інформувати про кіберінциденти тощо. Розробка методів управління кіберризиками є необхідною для відповідності цим регуляторним вимогам та запобігання можливим штрафам та правовим наслідкам.

Тобто зростання кіберзагроз, залежність від інформаційних технологій, економічні наслідки кібератак та регуляторні вимоги становлять фундаментальні чинники, які ведуть до необхідності розробки ефективних методів управління кіберризиками. Це вимагає постійного вдосконалення стратегій, технологій та процесів, а також залучення відповідних експертів та ресурсів для забезпечення надійного захисту від кіберзагроз.

Для вибору методів управління кіберризиками та їх впливом, необхідно врахувати наступні ключові елементи [32]:

- Аналіз ризиків: Першим кроком є проведення комплексного аналізу кіберризиків, що охоплює оцінку потенційних загроз, вразливостей системи, імовірність виникнення інцидентів та можливі наслідки. Це дозволяє ідентифікувати основні ризики та їх потенційний вплив на організацію чи державу.
- Розробка стратегії: На основі аналізу ризиків створюється стратегія управління кіберризиками, яка визначає загальні цілі, принципи та підходи до кібербезпеки. Вона повинна бути відповідною до особливостей організації чи держави, її мети та потенційних загроз.
- Реалізація політики кібербезпеки: Основою методів управління кіберризиками є політика кібербезпеки, яка встановлює правила, процедури, стандарти та практики для захисту від кіберзагроз. Реалізація цієї політики вимагає встановлення захисних заходів, впровадження технологій, навчання персоналу та забезпечення відповідності стандартам кібербезпеки.
- Моніторинг та оцінка: Ефективні методи управління кіберризиками вимагають постійного моніторингу та оцінки стану кібербезпеки. Це включає

виявлення потенційних загроз, вимірювання ефективності заходів безпеки, аналіз інцидентів та оновлення стратегії та політики на основі отриманих даних.

▪Внутрішні та зовнішні комунікації: Важливим аспектом управління кіберризиками є встановлення ефективних комунікаційних каналів. Це охоплює внутрішню комунікацію між всіма рівнями організації чи держави, спілкування зі зацікавленими сторонами та обмін інформацією про потенційні загрози та заходи безпеки.

▪Планування відновлення після інциденту: Методи управління кіберризиками повинні включати план відновлення після інциденту, що охоплює процедури відновлення систем, відновлення даних, комунікацію зі зацікавленими сторонами та оцінку наслідків інциденту. Це допомагає забезпечити швидке відновлення після атаки та зменшення впливу на діяльність організації чи держави.

▪Система нагляду та аудиту: Ефективні методи управління кіберризиками включають систему нагляду та аудиту, яка забезпечує контроль за дотриманням політики кібербезпеки, оцінку ефективності заходів безпеки, виявлення слабких місць та розробку рекомендацій для покращення.

▪Постійне вдосконалення: Кіберзагрози постійно змінюються, тому методи управління кіберризиками повинні бути гнучкими і піддаватися постійному вдосконаленню. Це включає оновлення стратегій, політик, процедур та технологій з урахуванням нових загроз та передових методів захисту.

Загалом, для створення моделі управління кіберризиками та їх впливом потрібні: аналіз ризиків, стратегія управління, політика кібербезпеки, моніторинг та оцінка, комунікації, планування відновлення після інциденту, система нагляду та аудиту, а також постійне вдосконалення. Крім перерахованих чинників, ще декілька факторів впливають на необхідність розробки методів управління кіберризиками:

Зміна характеру загроз: Кіберзагрози постійно змінюються і еволюціонують. Зловмисники швидко пристосовуються до нових захисних заходів і розробляють нові методи атак. Це вимагає постійного моніторингу, аналізу та розробки нових методів управління ризиками для виявлення, попередження та впорядкування кіберзагроз.

Глобалізація та взаємозалежність: Висока взаємозалежність між країнами, організаціями та системами створює потенційні ризики для кібербезпеки. Кібератаки можуть мати транскордонний характер, поширюючись швидко і впливаючи на багато різних суб'єктів. Тому розробка методів управління кіберризиками повинна враховувати глобальний контекст і співпрацювати з міжнародними партнерами.

Технологічний розвиток: Швидкий темп технологічного розвитку вносить нові виклики в сферу кібербезпеки. Розширення IoT, штучний інтелект, блокчейн та інші нові технології відкривають нові можливості, але одночасно створюють нові ризики. Розробка методів управління кіберризиками повинна бути гнучкою і адаптивною до таких змін, забезпечуючи захист нових технологій та інфраструктури.

Соціальний фактор: Люди є одним з найвразливіших ланок у системі кібербезпеки. Соціальна інженерія, фішинг, інсайдерські загрози та інші види атак, спрямовані на людей, є поширеними методами зловмисників. Недостатня обізнаність, необережність при використанні технологій, слабкі паролі і недостатнє усвідомлення ризиків створюють потенційні вразливості. Розробка методів управління кіберризиками повинна включати ініціативи з підвищення свідомості, навчання та підготовки персоналу, щоб зменшити людський фактор в кібербезпеці.

Необхідність розробки методів управління кіберризиками визначається широким спектром факторів, які включають зміну характеру загроз, глобалізацію та взаємозалежність, технологічний розвиток та соціальний фактор. Розуміння цих факторів допомагає організаціям і державам розробляти ефективні стратегії та методи управління кіберризиками для забезпечення стійкості в умовах постійного мінливого середовища [33].

3.2 Управління кіберризиками та їх впливом

В сучасному цифровому світі, де кіберзагрози стають все більш поширеними та складними, управління кіберризиками та їх впливом стає необхідністю для держав та організацій. Зростання кіберзагроз, зокрема в умовах гібридної війни, вимагає

розробки та впровадження ефективних методів управління кібербезпекою для забезпечення стійкості та безпеки.

Управління кіберризиками передбачає комплексний підхід до ідентифікації, оцінки, управління та зменшення ризиків, пов'язаних з кібербезпекою. Це необхідно для забезпечення безпеки державних структур, критично важливих інфраструктур та організацій у різних секторах.

Один з ключових елементів управління кіберризиками є розуміння потенційних загроз. Необхідно проводити систематичний аналіз та оцінку потенційних кіберзагроз, їх імовірності та впливу на діяльність організації. Це дозволяє виявити вразливості та вжити заходи для їх запобігання та мінімізації впливу.

Однак, розуміння загроз само по собі недостатнє. Для ефективного управління кіберризиками необхідно мати методи управління ризиками. Це включає в себе систему процесів, методик та інструментів для ідентифікації, аналізу, оцінки та управління кіберризиками та допомагає організаціям визначати та реалізовувати стратегії та заходи, спрямовані на мінімізацію ризиків і забезпечення безпеки [34].

Одним із важливих етапів управління кіберризиками є розробка політики кібербезпеки. Ця політика визначає цілі, принципи та підходи до захисту від кіберзагроз та кібервпливу. Вона повинна бути відповідною до потреб організації та враховувати регуляторні вимоги. Політика кібербезпеки встановлює рамки та вказівки для реалізації стратегії безпеки, впровадження технологічних рішень та процедур безпеки.

Паралельно з політикою кібербезпеки, необхідно встановити технічні та організаційні заходи безпеки. Це можуть бути технічні рішення, такі як фаєрволи, антивіруси, системи виявлення вторгнень та системи моніторингу. Також важливо розробити процедури безпеки, які включають політики доступу, управління інцидентами, навчання персоналу та аудит безпеки.

Свідомість та навчання персоналу є невід'ємною частиною управління кіберризиками. Персонал повинен бути навчений розпізнавати підозрілу активність, виявляти потенційні загрози та надавати звітність про можливі інциденти. Регулярні

тренування та оновлення навичок допомагають забезпечити високу рівень кіберсвідомості в організації [35].

Не менш важливим елементом управління кіберризиками є моніторинг та реагування. Системи моніторингу та виявлення кіберзагроз дозволяють оперативно виявляти підозрілу активність та реагувати на неї. Плани реагування на інциденти дозволяють швидко реагувати, відновлювати та усувати наслідки кібервпливу.

На останньому етапі управління кіберризиками стоїть завдання постійного вдосконалення. Кібервплив є постійно змінюваною сферою, тому необхідно постійно вдосконалювати підходи, заходи та процеси управління кібервпливом. Це включає оновлення політик, технологій та навичок персоналу.

Управління кібервпливом є важливим завданням для держав, організацій та інших суб'єктів, які працюють в цифровому просторі. Для ефективного управління кіберризиками та їх впливом необхідно мати ясну стратегію, політику безпеки, впроваджувати технічні та організаційні заходи, навчати та підтримувати кіберсвідомість персоналу та постійно вдосконалювати підходи управління.

Управління кіберризиками та їх впливом на інфраструктуру додатково має включати наступні етапи [36]:

Оцінка ризиків: спочатку необхідно визначити потенційні загрози та ризики, які можуть виникнути. Це можна зробити шляхом проведення аналізу зразків кібератак, вивчення статистичних даних, звітів про виявлені уразливості та зломи систем.

Розробка стратегії: після оцінки ризиків, необхідно розробити стратегію управління кіберризиками, яка включає в себе детальний план дій, щоб уникнути чи зменшити наслідки кібератаки.

Визначення команди реагування: для ефективного управління кіберризиками, необхідно визначити команду, яка буде відповідальною за реагування на кібератаку. Ця команда повинна включати експертів з інформаційної безпеки, комунікаційних технологій, управління кризами та інших відповідних галузей.

Підготовка до реагування: необхідно підготувати системи та персонал до можливих екстрених ситуацій. Це включає в себе проведення тренувань та симуляцій,

щоб перевірити ефективність планів реагування, а також забезпечення належного рівня захисту системи [38].

Реагування на кібератаку: у разі виникнення кібератаки, команда реагування повинна діяти відповідно до стратегії, яка була розроблена на етапі 2. Це може включати в себе блокування доступу до системи, відновлення даних

Аналіз наслідків: після того, як кібератаку було зупинено, необхідно проаналізувати її наслідки. Це може допомогти удосконалити стратегії та плани реагування на подібні події в майбутньому.

Вдосконалення: останнім етапом є вдосконалення системи управління кіберризиками. Це може включати в себе зміну планів реагування та стратегій на основі результатів аналізу наслідків.

Одним з можливих підходів до управління кіберризиками є створення цілеспрямованої команди, яка відповідає за управління ризиками та реагування на кібератаки. Команда повинна мати ясну роль та обов'язки, а також виконувати регулярні тренування та симуляції.

Також можна розглянути використання сучасних технологій та рішень для захисту від кібератак, таких як інтелектуальні системи аналізу поведінки, системи виявлення вторгнень та інші. Однак, важливо пам'ятати, що технології не можуть бути єдиним рішенням та їх використання повинне бути вписано в загальну стратегію управління кіберризиками.

З іншої сторони, зменшення кіберризиків вимагає комплексного та проактивного підходу до кібербезпеки. Важливо використовувати наступні рекомендації щодо зменшення кіберризиків [37]:

Проведення регулярних оцінок ризиків: регулярні оцінки ризиків допоможуть виявити потенційні кіберризики, зокрема вразливі місця в апаратному забезпеченні, програмному забезпеченні та мережах. Це допоможе визначити пріоритети та ефективно розподілити ресурси.

Застосування суворих заходів безпеки: такі як брандмауери, системи виявлення вторгнень і антивірусне програмне забезпечення, щоб запобігати та виявляти

кібератаки. Крім того, рекомендується використовувати надійні паролі, багатофакторну автентифікацію та шифрування для захисту конфіденційних даних.

Навчання співробітників найкращим практикам кібербезпеки: регулярні тренінги з кібербезпеки для співробітників допоможуть підвищити обізнаність про кіберризики та навчать виявляти потенційні кібератаки та реагувати на них. Це допоможе запобігти людським помилкам і мінімізувати вплив кіберінцидентів.

Розробка плану реагування на інциденти: плани реагування на інциденти мають описувати як реагувати на потенційні кіберінциденти, зокрема, з ким зв'язатися, які кроки вжити та як відновитися після атаки. Потрібно регулярно тестувати ці плани, щоб переконатися в їх ефективності, або ж, за потреби, оновити.

Регулярне створення резервних копій важливих даних: необхідно регулярно створювати резервні копії важливих даних та зберігати їх у безпечному місці, або ж у декількох. Це гарантує можливість відновити важливі дані у разі кіберінциденту.

Моніторинг оновлень і виправлень безпеки: рекомендується регулярно встановлювати виправлення та оновлення системи безпеки для всього програмного забезпечення та систем, що використовуються у IT-інфраструктурі, аби запобігти використанню відомих уразливостей.

Проведення оцінки ризиків третьої сторони: необхідно для того, щоб оцінити стан безпеки постачальників та інших партнерів. Це допоможе забезпечити відповідність їхніх методів безпеки корпоративним стандартам і зменшить ризик злому через третю сторону.

Загалом, зменшення кіберризиків потребує багатогранного підходу, який залучає технології, людей і процеси. Виконуючи ці рекомендації, зменшується ймовірність та вплив кіберінцидентів, підтримується безпека систем та стабільність бізнес операцій [27].

3.3 Контролі кіберризиками та їх впливом

Для протидії кібервпливу, зокрема, коли йдеться про боротьбу з дезінформацією, дезінформацією та онлайн-пропагандою пропонуються наступні контролі [38]:

Ідентифікація активів: На початковому етапі необхідно всі важливі активи, що потребують захисту, включаючи інформаційні системи, мережі, даних та інші ресурси.

Оцінка загроз: Визначення потенційних загроз, які можуть вплинути на активи. Дослідження відомих кіберзагроз, включаючи шкідливі програми, хакерські атаки, фішинг, соціальний інжиніринг тощо.

Оцінка вразливостей: Визначте вразливості в системах та інфраструктурі, які можуть бути використані загрозами для атаки. Розгляньте слабкі місця в мережах, програмному забезпеченні, політиках безпеки та людському факторі.

Аналіз ризиків: Оцінка потенційного впливу загроз та вразливостей на активи. Визначення ймовірності виникнення інцидентів та можливі збитки, які можуть виникнути внаслідок кібератак.

Розробка стратегій мінімізації ризиків: Розробка плану заходів для зменшення ризиків кібербезпеки. Це може включати встановлення технічних заходів безпеки, розробку політик та процедур безпеки, навчання персоналу та забезпечення відповідного плану реагування на інциденти.

Впровадження та контроль: Реалізація запланованих заходів з мінімізації ризиків та забезпечення їх ефективне впровадження. Контроль стану безпеки систем, виявлення можливих проблем або вразливостей, та вжиття відповідних заходів для їх виправлення.

Виявлення та відповідь на інциденти: Розробка процедури виявлення, реагування та відновлення в разі кіберінциденту. Інтеграція механізму моніторингу та реагування на підозрілу активність, швидку ідентифікацію та відповідь на інциденти, а також плани відновлення після атаки.

Оцінка та оновлення: Проведення регулярної оцінки ризиків, аналізу результатів контролю та інцидентів, ініціація необхідних змін в стратегіях та заходах з мінімізації ризиків. Постійне оновлення моделі управління ризиками, щоб відповідати новим тенденціям та загрозам.

Комунікація та свідомість: Забезпечення ефективної комунікації зі всіма зацікавленими сторонами, включаючи керівництво, співробітників та стейкхолдерів. Підвищення свідомості про кібербезпеку серед персоналу, проведення навчання та освітніх заходів.

Систематичність та неперервність [39]: Підхід до управління кіберризиками як до постійного процесу, забезпечуючи систематичну оцінку, планування та впровадження заходів. Впровадження циклу безперервного вдосконалення, привертаючи увагу до нових загроз, технологічних змін та навчання з новими методами атак.

Співпраця та обмін інформацією: Встановлення механізму співпраці зі сторонніми експертами, іншими організаціями та урядовими органами, для обміну інформацією про нові загрози, вразливості та кращі практики. Активна участь у відповідних форумах та групах, співпраця зі спеціалізованими службами безпеки.

Визначення відповідальності: Визначення ролей та відповідальності різних зацікавлених сторін у процесі управління кіберризиками. Забезпечення ясності щодо обов'язків, звітності та виконання стратегій безпеки.

Бюджетування та ресурси: Забезпечення належного фінансування та ресурсів для виконання заходів з управління кіберризиками. Врахування витрат на захист, навчання персоналу, технологічне оновлення та забезпечення відповідного обладнання та інструментів.

Звітність та аудит: Регулярна звітність про стан кібербезпеки, проведення аудитів та оцінки відповідності. Забезпечення розуміння керівництва та зацікавлених сторін про ефективність стратегій та заходів з мінімізації ризиків.

Непередбачувані ситуації та резервність: Планування та підготовка до непередбачуваних ситуацій та інцидентів. Розробка плану неперервної роботи та

відновлення після інцидентів, забезпечуючи наявність резервних копій даних, систем та процесів.

Свідоме впровадження технологій: У відповідь на зростаючі загрози кібербезпеки, необхідне впровадження нових технологій та інновацій, які можуть поліпшити захист від кіберризиків. Розгляд застосування штучного інтелекту, машинного навчання та інших передових методів для виявлення та запобігання атакам.

Постійне навчання та розвиток персоналу: Забезпечення неперервного навчання персоналу з питань кібербезпеки. Організація тренінгів, семінарів та інших освітніх заходів для підвищення свідомості про загрози та навичок безпеки.

Еволюція та адаптація: Кіберзагрози постійно змінюються, тому модель управління кіберризиками повинна бути гнучкою та адаптованою до нових викликів. Постійний перегляд, аналіз та вдосконалення підходу та заходів з мінімізації ризиків.

Свідоме прийняття ризиків: Важливо зрозуміти та прийняти певний рівень ризику, виходячи з бізнес-потреб, вартості реалізації заходів з мінімізації ризиків та потенційних наслідків. Варто ретельно оцінити, коли ціна мінімізації ризику перевищує можливі збитки від можливого інциденту.

Забезпечення згоди з правовими та регуляторними вимогами: Дотримання усіх відповідних правових та регуляторних вимог, пов'язаних з кібербезпекою. Розробка політики та процедури відповідно до законодавства, дотримання стандартів безпеки та забезпечення відповідності з органами регулювання.

Культура кібербезпеки [40]: Створення культури безпеки в організації, де кожен працівник відчуває відповідальність за кібербезпеку. Залучення всіх співробітників до процесу управління ризиками, навчання їх базовим заходам безпеки та сприяння формуванню свідомої поведінки в онлайн-середовищі.

Своєчасне виявлення та реагування: Розробка механізмів для своєчасного виявлення кібератак та інцидентів безпеки. Встановлення системи моніторингу, інтрузійного виявлення, аналізу вразливостей та реагування на події. Розробка плану реагування на інциденти та проведення регулярних тренувань для персоналу.

Запобігання внутрішнім загрозам: Приділення уваги не лише зовнішнім, а й внутрішнім загрозам безпеки. Розробка політики та процедури для контролю доступу до систем та даних, моніторингу активності персоналу та виявлення ненормальної поведінки. Забезпечення надійної аутентифікації та авторизації користувачів.

Захист критично важливих інфраструктур: Визначення критично важливої інфраструктури, яка впливає на національну безпеку та економіку, і забезпечення ефективного захисту від кіберризиків. Розробка стратегії захисту, плану відновлення та співпраця з урядовими органами та критичними інфраструктурами.

Систематичне тестування та валідація: Регулярне проведення тестування безпеки, включаючи тест на проникнення, валідацію безпеки додатків та інших компонентів системи. Це дозволить виявити потенційні слабкі місця та помилки в заходах з мінімізації ризиків, щоб їх вчасно виправити та покращити безпеку системи.

Контроль та аудит: Встановлення механізму контролю та аудиту, щоб переконатися, що політики та процедури безпеки дотримуються. Проведення регулярних перевірок виконання стандартів безпеки, аналіз журналу подій та моніторинг активності в системі. Це дозволить виявити некоректні дії, вразливості та інші потенційні загрози.

Застосування методів управління кіберризиками є критично важливим для забезпечення кібербезпеки в будь-якій організації. Вона дозволяє забезпечити прозорість і довіру в управлінні кіберризиками шляхом оцінки ризиків та прийняття рішень щодо їх керування.

Оцінка ризиків є ключовим етапом управління кібербезпекою, що дозволяє виявити потенційні загрози, визначити рівень потенційної шкоди та ризику та прийняти необхідні заходи для зниження ризику до прийнятного рівня. Цей підхід дозволяє зосередитися на найбільш критичних об'єктах та ризиках, знизити витрати на управління кібербезпекою та забезпечити ефективний захист.

Також важливою складовою моделі управління кіберризиками є розробка та впровадження плану надзвичайних ситуацій, який містить процедури відновлення після кібератак та надзвичайних ситуацій [27].

Застосування цих методів дозволяє забезпечити ефективність та прозорість управління кіберризиками, зменшити можливість виникнення кібератак, знизити ризик та забезпечити захист важливих даних та інфраструктури.

3.4 Виклики при впровадженні та шляхи вирішення

Управління кіберризиками та їх впливом є складною задачею, яка потребує великої уваги та зусиль від керівництва організації. На шляху впровадження методів можуть виникати різні виклики, які, в свою чергу, можуть суттєво ускладнити процес інтеграції [41].

- Недостатня підтримка керівництва

Одним з основних викликів, з якими можуть стикнутися організації при впровадженні методів управління кіберризиками та їх впливом, є недостатня підтримка керівництва. Це може бути пов'язано з тим, що керівництво не розуміє необхідності впровадження такої моделі або не бажає витрачати ресурси на її реалізацію.

Один з можливих способів подолання цього виклику полягає у створенні бізнес-кейсу, який демонструє потенційні переваги впровадження моделі управління кіберризиками та їх впливом для організації. Цей бізнес-кейс може включати аналіз потенційних загроз та ризиків, що можуть бути відвернуті завдяки впровадженню моделі, а також оцінку можливих втрат, які можуть виникнути в разі її невикористання. Це також включає підвищення кіберсвідомості серед керівництва та їх участь у навчальних програмах.

- Недостатня знайомість з кібербезпекою

Іншим викликом може бути недостатня знайомість з кібербезпекою у всіх рівнях організації. Багато співробітників можуть не розуміти потенційні кіберризики та їх вплив на діяльність організації. Це може створювати вразливості та зростаючий ризик кібератак.

Важливо створити канали зв'язку та систему звітності, які дозволять співробітникам повідомляти про можливі кіберінциденти та надавати відповідні рекомендації щодо їх запобігання та вирішення.

Забезпечення постійного навчання та підвищення кваліфікації співробітників у сфері кібербезпеки є важливим кроком у вирішенні цього виклику. Організації можуть розглядати внутрішні програми навчання, підвищення свідомості та проведення симуляційних тренувань для персоналу. Крім того, співпраця з університетами, професійними асоціаціями та експертами з кібербезпеки може забезпечити доступ до актуальних знань та навичок.

- Постійна зміна кіберзагроз

Кіберзагрози постійно змінюються та стають все складнішими. Це означає, що впровадження моделі управління кіберризиками повинно бути гнучким та адаптивним до нових загроз. Організації повинні постійно вдосконалювати свої заходи безпеки та оновлювати свої стратегії, щоб підтримувати рівень безпеки.

Один зі способів подолання цього виклику полягає у встановленні системи моніторингу та оцінки кіберзагроз. Це допоможе виявляти нові ризики та аналізувати їх вплив на організацію. Також важливо підтримувати постійний контакт з експертами з кібербезпеки, брати участь у конференціях та нових дослідженнях, щоб бути в курсі останніх тенденцій та технологій.

- Співпраця та обмін інформацією

Управління кіберризиками не є виключно внутрішньою задачею організації. Важливо співпрацювати з іншими організаціями, ділитися інформацією про кіберінциденти та використовувати спільні ресурси для підвищення кібербезпеки в цілому.

Для забезпечення ефективної співпраці варто розглянути можливість приєднання до альянсів та об'єднань, які сприяють обміну інформацією та спільним діям для запобігання кібератакам. Також важливо встановити механізми обміну інформацією з іншими організаціями та владними структурами, щоб швидко реагувати на загрози та спільно працювати над їх вирішенням.

- Недостатнє фінансування [42]

Брак необхідних фінансових ресурсів може обмежити здатність організації до ефективного управління кіберризиками.

Для подолання цього виклику організація повинна ретельно оцінити свої потреби, включаючи інвестиції в необхідні інструменти, технології та навчання персоналу. Крім того, варто розглянути можливість залучення зовнішніх ресурсів, таких як партнери, фонди або державні програми фінансування, для підтримки кібербезпеки.

▪Складність ландшафту кіберзахисту

Швидкий розвиток технологій та різноманітність кіберзагроз створюють складність у кіберзахисті. Організації повинні пристосовуватися до постійно мінливого ландшафту кібербезпеки, оновлювати свої захисні стратегії та технології. Ефективне використання інструментів моніторингу, виявлення загроз та реагування може допомогти виявити вразливості та негайно реагувати на кібератаки.

Використання стандартів та рамок кібербезпеки, таких як ISO 27001, NIST Cybersecurity Framework або CIS Controls, може допомогти організаціям впоратися з цим викликом. Реалізація принципів та практик кібербезпеки, таких як сегрегація мережі, контроль доступу, захист даних, моніторинг та виявлення загроз, допоможуть підвищити рівень безпеки і зменшити вразливості інфраструктури.

▪Глобальний інтернет

Віртуальний характер кіберпростору і глобальне поширення Інтернету створюють виклики управлінню кіберризиками. Кібератаки можуть приходити з будь-якої точки світу, а інциденти можуть мати міжнародний вплив.

Співпраця з іншими організаціями, урядами та міжнародними організаціями є важливим аспектом ефективного управління кіберризиками. Обмін інформацією, спільні ініціативи та створення міжнародних стандартів можуть покращити спроможність виявлення та протидії кібератакам.

Ці виклики не є вичерпним списком, але вони відображають деякі ключові фактори, які організації повинні враховувати при управлінні кіберризиками. Зрозуміння цих викликів та впровадження відповідних стратегій та заходів може

допомогти забезпечити ефективний захист від кіберзагроз і знизити їх вплив на організацію.

Загалом, вирішення викликів управління кіберризиками вимагає комплексного підходу, який включає в себе технологічні, організаційні та людські аспекти. Необхідно активно співпрацювати зі зацікавленими сторонами, сприяти обміну інформацією та знаннями, а також регулярно оновлювати та вдосконалювати підходи до кібербезпеки [43].

Управління кіберризиками та їх впливом є важливою складовою успішної кібербезпеки для будь-якої організації. Подолання викликів, з якими можна стикнутися під час впровадження моделі управління кіберризиками, вимагає комбінації культурної, технічної та стратегічної роботи. З усвідомленням цих викликів та впровадженням відповідних стратегій організації зможуть підвищити свою кібербезпеку та зменшити ризик впливу кіберінцидентів.

3.5 Найкращі практики при впровадженні методів управління кібererризиками

Методи управління кіберризиками та протидії кібервпливу, про які було згадано раніше, містять у собі кілька особливостей, які сприяють їх ефективності. Основні функції, пов’язані з описаними методами [44]:

Проактивний підхід: ці методи використовують проактивний підхід для боротьби з кібервпливом. Замість того, щоб просто реагувати на дезінформацію чи дезінформацію після її поширення, вони зосереджуються на запобіганні та пом’якшенні впливу неправдивих наративів до того, як вони набудуть значного поширення.

Розширення можливостей і навчання: методи наголошують на наданні людям знань і навичок для ефективного орієнтування в цифровому середовищі. Вони спрямовані на підвищення критичного мислення, медіаграмотності та цифрової грамотності серед широкої громадськості, щоб вони могли робити обґрунтовані судження щодо інформації, з якою вони стикаються.

Співпраця та партнерство: співпраця та партнерство лежать в основі протидії кібервпливу. Ці методи визнають необхідність співпраці між різними зацікавленими сторонами, включаючи уряди, організації громадянського суспільства, технологічні компанії та наукові кола. Використовуючи колективний досвід і ресурси, вони можуть досягти ширшого охоплення та ефективніших результатів.

Мультидисциплінарний підхід: протидія кібервпливу потребує мультидисциплінарного підходу, який поєднує елементи технології, психології, комунікацій, права та політики. Ці методи ґрунтуються на досвіді з різних галузей для розробки комплексних стратегій, спрямованих на комплексний характер кібервпливу.

Адаптивність і безперервне вдосконалення: Методи віддають пріоритет адаптивності та безперервному вдосконаленню. Враховуючи постійний розвиток тактики кібервпливу, стратегії необхідно регулярно оновлювати та вдосконалювати. Гнучкість і здатність реагувати на нові тенденції та виклики є критично важливими.

Практики, що ґрунтуються на фактах [45]: ці методи ґрунтуються на практиках, що ґрунтуються на фактах, включаючи перевірку фактів, аналіз даних і дослідження, для боротьби з кібервпливом. Вони підкреслюють важливість об’єктивної інформації, фактів, які можна перевірити, і прийняття рішень на основі доказів у протидії неправдивим наративам.

Глобальна перспектива: протидія кібервпливу часто потребує глобальної перспективи, оскільки кампанії з дезінформації можуть виходити за національні кордони. Міжнародне співробітництво, обмін інформацією та співробітництво мають вирішальне значення для вирішення проблеми транснаціонального характеру кампаній кібервпливу.

Баланс між свободою слова та відповідальністю: ці методи визнають важливість досягнення балансу між захистом прав на свободу слова та сприянням відповідальному обміну інформацією. Протидіяючи кібервпливу, вони спрямовані на боротьбу зі шкідливою дезінформацією, одночасно захищаючи свободу вираження думок і зберігаючи відкритість Інтернету.

Ці функції разом сприяють комплексному та багатогранному підходу до протидії кібервпливу, що дозволяє ефективніше реагувати на виклики, пов’язані з дезінформацією та дезінформацією в епоху цифрових технологій.

Також модель може бути адаптована для державного регулювання, інтегрувавши її у нормативні рамки та політику [22]:

Проактивний підхід: державні регулюючі органи можуть застосувати проактивний підхід, включивши заходи пом’якшення кібервпливу в свою нормативну базу. Це включає виявлення потенційних ризиків кібервпливу в різних секторах і галузях і розробку нормативних актів, які врегульовують ці ризики. Передбачаючи виклики кібервпливу та вирішуючи їх за допомогою нормативних актів, уряди можуть пом’якшити їхній вплив і захистити суспільні інтереси.

Розширення можливостей і навчання: державні регулюючі органи можуть віддати пріоритет наділення окремих осіб і організацій знаннями та навичками для розпізнавання кібервпливу та протидії йому. Цього можна досягти шляхом встановлення нормативних вимог щодо навчання з питань кібербезпеки, сприяння медіаграмотності та критичного мислення, а також надання освітніх ресурсів зацікавленим сторонам. Уповноважені особи та організації можуть відігравати активну роль у зниженні ризиків кібервпливу та дотриманні нормативних вимог.

Співпраця та партнерство: Співпраця та партнерство є важливими в державному регулюванні для ефективної протидії кібервпливу. Регулятори можуть співпрацювати з галузевими асоціаціями, експертами з кібербезпеки та технологічними компаніями, щоб розробити правила, які вирішують проблеми кібервпливу, що виникають. Ці партнерства можуть також сприяти обміну інформацією, кращим досвідом і спільним ініціативам для боротьби з кібервпливом.

Міжгалузевий: державні регулюючі органи повинні застосувати міжгалузевий підхід, залучаючи до процесу регулювання експертів із різних галузей. Сюди входять спеціалісти з кібербезпеки, експерти з права та фахівці з комунікацій. Колективна експертиза може сприяти розробці комплексних нормативних актів, що враховують технічні, правові, соціальні та психологічні аспекти кібервпливу.

Адаптивність і постійне вдосконалення: державні регулятори повинні постійно оцінювати та оновлювати свої нормативні рамки, щоб не відставати від тактики кібервпливу, що розвивається. Це вимагає моніторингу мінливого ландшафту, участі в поточних дослідженнях і отримання відгуків від зацікавлених сторін. Адаптувавши нормативні акти для вирішення нових ризиків, регулятори можуть ефективно пом'якшувати кібервплив і підтримувати відповідність своєї нормативної бази.

Практика, що ґрунтується на фактичних даних: державні нормативні акти мають ґрунтуватися на практичних засадах, що ґрунтуються на фактичних даних, і базуватися на надійних даних і дослідженнях. Регулятори можуть встановлювати вимоги щодо прозорості та розкриття інформації щодо ризиків кібервпливу, сприяючи точному звітуванню та обміну інформацією. Норми, засновані на фактичних даних, гарантують, що рішення ґрунтуються на надійній інформації та можуть ефективно протидіяти викликам кібервпливу.

Глобальна перспектива: враховуючи транснаціональний характер кібервпливу, урядові регулятори повинні розглянути міжнародну співпрацю та координацію. Це передбачає узгодження регуляторних підходів із міжнародними стандартами, обмін інформацією та розвідданими з іншими країнами та участь у міжнародних ініціативах із боротьби з кібервпливом. Співпраця на глобальному рівні підвищує ефективність державного регулювання у протидії кібервпливу.

Адаптувавши ці методи до державного регулювання, регулятори можуть розробити надійні системи, які ефективно протидіють ризикам кібервпливу. Включення моделі до нормативних актів допоможе захистити окремих осіб, організації та суспільство в цілому від згубних наслідків кібервпливу, забезпечуючи безпечніше та стійкіше цифрове середовище.

Управління кіберризиками – це складне завдання, але необхідне для забезпечення безпеки організації в сучасному цифровому світі. Впровадження ефективних стратегій та найкращих практик управління кіберризиками стикається зі своїми викликами, такими як недостатні ресурси, низька кіберсвідомість, швидка зміна загроз та технологій. Проте, існують шляхи вирішення цих викликів, такі як залучення керівництва, створення культури кібербезпеки, здійснення регулярної

оцінки ризиків і використання найкращих практик, які відповідають специфіці організації [35].

Для успішного управління кіберризиками необхідно поєднувати технологічні, організаційні та людські аспекти. Це вимагає постійного вдосконалення, оновлення політик та процедур, а також навчання та підвищення кіберсвідомості працівників. Застосування найкращих практик управління кіберризиками сприятиме забезпеченню безпеки, захисту важливої інформації та підтримці неперервності бізнесу.

Висновки за розділом 3

Протидія кібервпливу вимагає багатогранного та проактивного підходу, який охоплює кілька ключових особливостей. Розширюючи можливості людей через освіту та обізнаність, сприяючи співпраці та партнерству, а також приймаючи міждисциплінарну перспективу, можна розробити ефективні стратегії. Адаптивність і безперервне вдосконалення, що базується на науково-обґрунтованих практиках, допомагають боротися з постійним характером кампаній кібервпливу.

Крім того, вкрай важливо знайти баланс між захистом прав на свободу слова та сприянням відповідальному обміну інформацією. Включаючи ці функції, методи протидії кібервпливу можуть ефективно пом’якшувати поширення дезінформації та онлайн-пропаганди, сприяючи більш поінформованому та стійкому цифровому суспільству.

ВИСНОВКИ

Кіберризики та їх вплив в контексті гібридної війни є актуальними, оскільки вони можуть мати значний вплив на безпеку, стабільність і стійкість країн і організацій. У гібридній війні кібератаки та інші ризики часто використовуються як інструмент для отримання стратегічної переваги над опонентами, руйнування критичної інфраструктури та спричинення хаосу та плутанини.

Наслідки та експлуатація кіберризиків можуть бути серйозними та далекосяжними, включаючи втрату даних, простої системи, фінансові втрати та репутаційну шкоду. У випадку критичної інфраструктури, такої як електромережі та транспортні мережі, кібератаки можуть призвести до серйозних збоїв, що вплине на повсякденне життя мільйонів людей.

Дослідження показало, щоб подолати ці виклики, країна та організації повинні прийняти комплексний і проактивний підхід до кібербезпеки, який включає регулярну оцінку ризиків, жорсткі заходи безпеки та плани реагування на інциденти. Таким чином вони можуть краще пом’якшити вплив кіберризиків і підтримувати безпеку та стабільність своїх операцій.

У кваліфікаційній роботі розв’язано актуальне питання стосовно зменшення поверхі та кількості кібератак та відповідно їх впливу, нанесених через інциденти безпеки. У ході розв’язання поставлених задач були отримані наступні наукові та практичні результати:

- Проаналізовано наслідки гібридної війни, спричинені кібератаками та наявністю вразливостей. Виокремлено та проаналізовано інциденти безпеки, які мали найбільший кібервплив на українську ІТ-інфраструктуру.
- Проведено аналіз сучасних міжнародних підходів до аналізу та зменшення кіберризиків, причини та наслідки успішних кібератак на великі міжнародні компанії.
- Проведено аналіз українських підходів до аналізу та зменшення кіберризиків. Проаналізовано наслідки неналежного управління кіберрризиками та причини успішних кібератак на українську ІТ-інфраструктуру.

- Формалізовано принципи побудови системи захисту від кіберризиків та їх впливу. Досліджено інструменти, методи та засоби управління кіберризиками для зменшення їх негативного впливу.
- Досліджено підходи управління кіберризиками та їх впливом на середовище організацій та держави. Методи управління кіберризиками повинні враховувати особливості інфраструктури, співпрацю з іншими експертами, реалістичні сценарії вторгнення та забезпечувати постійний моніторинг нових загроз для підтримання встановленого рівня кібербезпеки.

Кіберризики широко поширені та постійно зростають, що вимагає від організацій, урядів та користувачів приділяти особливу увагу заходам захисту. Технологічні рішення, міжнародна співпраця та регулярні навчання є ключовими елементами в ефективному управлінні кіберризиками та забезпеченні стійкості кіберпростору.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Абу, Т.М., Хеліфі, А., Барачі, М., та Орманджієва, О. (2012). Посібник із ISO 27001: практичне дослідження ОАЕ. Проблеми інформатики та інформаційних технологій, 9(19), 331–349.

2. Бугайчук, К,. & Shoroxova, G. (2018). Забезпечення кібербезпеки як умова протидії терористичній діяльності: нормативно-правові аспекти / О.В. Протидія терористичній діяльності: міжнародний досвід та його актуальність для України: матеріали ІІ Міжнародної науково-практичної конференції (15.12.2017). К.: Національна академія прокуратури України, С. 135–138.

3. Данильян О. (2002). Національна безпека України: сутність, структура та напрями реалізації : навч. Харків: Фоліо.

4. Доктрина інформаційної безпеки України (2017): введено в дію Указом Президента України: від 25.02.2017, 47/2017. Отримано з: http://www.president.gov.ua.

5. Гуровський В. (2014). Роль органів державної влади у сфері інформаційної безпеки України. Вісник Української академії державного управління при Президентові України, 3, 21–31.

6. Левченко, О. (2014). Проблеми і шляхи формування системи інформаційної безпеки держави / О.В. Zbirnyk naukovyx pracz Xarkivskogo universytetu Povitryanyx Syl, 2(39), 166–168.

7. Ліпкан В. (2006). Інформаційна безпека України в умовах євроінтеграції : навчальний посібник. Київ: КНТ

8. Марутян Р. (2018). Інформаційна складова гібридної війни проти України: сучасні виклики та загрози [Електронний ресурс]. — Режим доступу до документа: https://matrix-info.com

9. Олійник О. (2016). Принципи забезпечення інформаційної безпеки України / О.В. Юридичний вісник повітряне і космічне право, 4(41).

10. Сенченко, М. (2014). Запорука національної безпеки в умовах інформаційної війни. Вісник Книжкової палати, 6, 3–9.

11. Фон Солмс, Р. (1999). Управління інформаційною безпекою: чому стандарти важливі, Управління інформацією та комп'ютерна безпека, 7(1), 50–58.

12. Вітмен, М., і Матторд, Х. (2014). Управління інформаційною безпекою. Бостон: Курс Технологія Cengage Learning.

13. Cyber security of critical infrastructures / L.A. Maglaras [та ін.]. – ICT Express, 2018 [Електронний ресурс]. — Режим доступу до документа: https://doi.org/10.1016/j.icte.2018.02.001.

14. Cyber security management model for critical infrastructure / Limba T., Plėta T., Agafonov K., Damkus M. – Entrepreneurship and Sustainability Issues, 2017, [Електронний ресурс]. — Режим доступу до документа: https://doi.org/10.9770/jesi.2017.4.4(12).

15. The WIRED Guide to Cyberwar [Електронний ресурс]. — Режим доступу до документа: https://www.wired.com/story/cyberwar-guide

16. Казарян С. Кібератаки. Як Україна і світ борються з руйнівною діяльністю хакерів / Казарян С. – Telegraf.Design, 2022 [Електронний ресурс]. — Режим доступу до документа: https://telegraf.design/kiberataky-yak-ukrayina-i-svit-boryutsya-z-rujnivnoyu-diyalnistyuhakeriv/.

17. Максименко Ю.Є. Правове регулювання національної безпеки України: окремі аспекти // Імперативи розвитку юридичної та безпекової науки : матеріали міжнародної науково-практичної інтернет-конференції (Київ, 15 квітня 2010 р.). — К. : О.С. Ліпкан, 2010. — 102 с.

18. Грищук Р., Охрімчук В., Ахтирцева В. Джерела первинних даних для розроблення шаблонів потенційно небезпечних кібератак Захист інформації. 2016. Вип. 18(1). С.21-29.

19. Рубан І.В. Мартовицький В.О., Партика С.О. Класифікація методів виявлення аномалій в інформаційних системах. Системи озброєння і військова техніка. 2016. Вип. 3(47). С. 100–105.

20. Антонюк А.О. Моделювання систем захисту інформації: монографія. Ірпінь: Національний університет ДПС України, 2015. 273 с

21. Козубцов І.М., Козубцова Л.М., Куцаєв В.В., Терещенко Т.П. Методика оцінки кібернетичної захищеності системи зв’язку організації. Сучасні інформаційні технології у сфері безпеки та оборони. 2018. Вип. 1 (31). С. 43-46.

22. Кучернюк П.В., Довгаль А.О. Модель загроз безпеки в інформаційно-комунікаційних системах на основі регресійного аналізу. Електроніка та зв'язок. 2017. Вип., № 2(97), т. 22. С. 79–84

23. Мірошник М.А. Розробка методів оцінки ефективності захисту інформації в розподілених комп’ютерних системах. Інформаційно-керуючі системи на залізничному транспорті. 2015. Вип. 4(113). С. 39–43.

24. Впровадження європейської кібербезпеки: загальний огляд. ISACA. [Електронний ресурс]. — Режим доступу до документа: https://www.isaca.org /Knowledge-Center/Research/Documents/European-CybersecurityImplementation-Overview_res_Ukr_1215.pdf.

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

26. Лівенцев С.П., Сторчак А.С. Виявлення комп’ютерних атак в інформаційно-телекомунікаційних системах на основі методів індуктивного прогнозування станів. Information Technology And Security. 2012. Вип. 1(1). С.100–104.

27. Лантвойт О.Б., Гришин С.П., Винярський Я.Я. Інформаційне забезпечення комплексного керування захистом складних систем управління. Сучасна спеціальна техніка. 2011. Вип.2(25). С.112–117.

28. Мірошник М.А. Розробка методів оцінки ефективності захисту інформації в розподілених комп’ютерних системах. Інформаційно-керуючі системи на залізничному транспорті. 2015. Вип. 4(113). С. 39–43.

29. Сторчак А.С., Сальник С.В., Крамський А.Є. Аналіз вразливостей та атак на державні інформаційні ресурси, що обробляються в інформаційнотелекомунікаційних системах. Системи обробки інформації. 2019. Вип. 2(157). С. 121-128

30. Застосування моделей оцінювання ризиків інформаційної безпеки в інформаційно-телекомунікаційних системах / О. Г. Пузиренко, С. О. Івко // Системи обробки інформації. Л.: Академія сухопутних військ імені гетьмана Петра Сагайдачного, 2015. Вип. 3 (128). С. 75–79.

31. Микитенко Т. Проблеми інформаційної безпеки суб'єктів господарювання в Україні та можливі шляхи їх вирішення в сучасних умовах / Т. Микитенко, І. Петровська, П. Рогов, А. Гаркуша // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2016. № 2. С. 24–31.

32. Пузиренко О. Г. Аналіз процесу управління ризиками інформаційної безпеки в забезпеченні живучості інформаційнотелекомунікаційних сис- тем / О. Г. Пузиренко, С. О. Івко, О. О. Лаврут // Системи обробки інформації. Л.: Академія сухопутних військ імені гетьмана Петра Сагайдачно го, 2014. Вип. 8 (124). С. 128–134.

33. Jain P., Pasman H. J., Waldram S., Pistikopoulos E. N., Mannan M. S. Process Resilience Analysis Framework (PRAF): A systems approach for improved risk and safety management. Journal of Loss Prevention in the Process Industries. 2018. Vol. 53. P. 61–73

34. Terje Aven. Risk assessment and risk management: Review of recent advances on their foundation. European Journal of Operational Research. 2016. Vol. 253. Issue 1. P. 1–13.

35. Cyber war and Ukraine / James Andrew Lewis // Center for Strategic and International Studies [Електронний ресурс]. — Режим доступу до документа: https://www.csis.org/ analysis/cyber-war-and-ukraine

36. Defending Ukraine: Early Lessons from the Cyber War / Brad Smith // Microsoft. [Електронний ресурс]. — Режим доступу до документа: https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/

37. Russia's war on Ukraine: Timeline of cyber-attacks [Електронний ресурс]. — Режим доступу до документа: https://www.europarl.europa. eu/thinktank/en/document/EPRS_BRI(2022)733549

38. Why Russia's cyber war in Ukraine hasn't played out as predicted / David Szondy // New Atlas [Електронний ресурс]. — Режим доступу до документа: https://newatlas.com/military/russia-cyber-war-ukraine/

39. WeLiveSecurity ESET Threat Report T3 2021 [Електронний ресурс]. — Режим доступу до документа: https://www.welivesecurity.com/2022/02/09/eset-threat-report-t32021/

40. Ransomware Uncovered: Attackers' Latest Methods [Електронний ресурс]. — Режим доступу до документа: https://www.groupib.com/whitepapers/ ransomware-uncovered.html.

41. Усков А. В. Іванніков А. Д. Усков В. Л. Технології забезпечення інформаційної безпеки корпоративних освітніх мереж // Освітні технології і суспільство. - 2008. -Т.11, №1. - С. 472 – 479

42. Батечко С. В., Лебедєва О. Ю. Методика оцінки захищеності інформаційних систем. Інформатика та математичні методи в моделюванні. 2021. Т. 11, № 3.

43. Stine K. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (Ukrainian Translation). National Institute of Standards and Technology, 2022 [Електронний ресурс]. — Режим доступу до документа: https://doi.org/10.6028/nist.cswp.04162018uk

44. Мехед Д., Ткач Ю., Базилевич В., Гур'єв В., Усов Я. Аналіз вразливостей корпоративних інформаційних систем Захист інформації. 2018. Вип. 20(1). С.61-66. DOI: 10.18372/2410-7840.20.12453.

45. Ільяшов О.А., Бурячок В.Л. До питання захисту інформаційнотелекомунікаційної сфери від стороннього кібернетичного впливу. Наука і оборона. 2010. Вип. 4. С.35–40.

ДОДАТОК А
СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Тези наукових доповідей:

- Orto Valentyna ANALYSIS OF HYBRID WAR IMPACT ON THE UKRAINIAN CYBERSPACE / Volodymyr Nakonechnyi, Valentyna Orto // “Problems of Cybersecurity of Information and Telecommunication Systems” (PCSITS): Collection of reports and abstracts; Kyiv city, 27-28 October 2022 year; Taras Shevchenko National University of Kyiv / Editorial board.: V.V. Il′chenko, Dr. Phys.-Math. Sc., Prof., (Head); and others. – K.: PPC "Kyiv University", 2022. – 159 pages (40-42 pages)
- Orto Valentyna ANALYSIS AND MINIMIZATION OF CYBER RISKS AS PART OF HYBRID WARFARE / Ivan Parkhomenko, Valentyna Orto // “Problems of Cybersecurity of Information and Telecommunication Systems” (PCSITS): Collection of reports and abstracts; Kyiv city, 27 April 2023 year; Taras Shevchenko National University of Kyiv / Editorial board.: V.V. Il′chenko, Dr. Phys.-Math. Sc., Prof., (Head); and others. – K.: PPC "Kyiv University", 2023. – 166 pages (74-75 pages)