Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО

«17» травня 2024 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи

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 оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури»

Виконавець: студент ІІ курсу, групи КБм-21

_____ **Євгеній РИЖИЙ**
(підпис) (Ім'я, ПРІЗВИЩЕ)

	Ім'я, ПРІЗВИЩЕ	**Підпис**
Науковий керівник	Володимир НАКОНЕЧНИЙ	
Нормоконтроль	Сергій ДАКОВ	

Київ 2024

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
_____ Іван ПАРХОМЕНКО
«17» листопада 2023 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*

Здобувача КБм-21 (група) Рижому Євгенію Віталійовичу (прізвище ім'я по-батькові)

Тема кваліфікаційної роботи Методи оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 5 від 15.11.2023 р.

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень	Процес кількісного та якісного оцінювання ризиків кібербезпеки.
Предмет досліджень	Методи та інструментальні засоби оцінювання ризиків кібербезпеки інформаційних систем ОКІ.
Мета	Дослідження теоретичного базису та практичних аспектів процесу оцінювання ризиків кібербезпеки інформаційних систем ОКІ. Удосконалення відомих підходів до ризик-менеджменту в кібербезпеці.
Вихідні дані для проведення роботи	Методи та інструментальні засоби оцінювання ризиків кібербезпеки інформаційних систем ОКІ.

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна	удосконалено метод управління ризиками кібербезпеки, який використовує стандарт FMECA та систему індикаторів критичності (діаграми Ісікави та Парето, матриці критичності).
Практична цінність	створення спеціалізованого програмного забезпечення на основі запропонованого методу дозволить, крім якісного і кількісного оцінювання ризику, автоматизовано оцінювати важливість ОКІ в різних галузях та секторах критичної інфраструктури.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота виконана у повному обсязі відповідно до теми.

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Уточнення постановки задачі	17.11.2023 – 20.01.2024
Аналіз літературних джерел	21.01.2024 – 10.02.2024
Ознайомлення з основними поняттями, структурою та змістом інформаційної безпеки	11.02.2024 – 20.02.2024
Визначення ролі та місця інформаційної безпеки в системі національної безпеки держави	21.02.2024 – 27.02.2024
Дослідження стратегій кібербезпеки, захисту об’єктів критичної інфраструктури та управління ризиками в інших державах	28.02.2024 – 10.03.2024
Огляд FMECA як одного з ефективних підходів у ризик-менеджменті	11.03.2024 – 17.03.2024
Дослідження практичних підходів до побудови системи управління інформаційною безпекою	18.03.2024 – 27.03.2024
Розгляд основних підходів до аналізу ризиків кібербезпеки	28.03.2024 – 10.04.2024
Огляд інструментарію для оцінки ризиків	11.04.2024 – 17.04.2024
Розроблення методу оцінювання ризиків кібербезпеки інформаційних систем ОКІ на основі FMECA	18.04.2024 – 28.04.2024
Оформлення пояснювальної записки згідно методичних рекомендацій	29.04.2024 – 12.05.2024
Подача пакету документів на розгляд ЕК	13.05.2024 – 18.05.2024

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект	Ефективніший перерозподіл інвестицій в кібербезпеку певних ОКІ в умовах обмежених матеріальних та інших ресурсів
Соціальний ефект	Ідентифікація першопричин та пріоритезація ризиків дозволить краще аналізувати динаміку та реагувати на зміни трендів в кібербезпеці для ІС ОКІ.

7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ Володимир НАКОНЕЧНИЙ
(підпис) (Ім'я, ПРІЗВИЩЕ)

Завдання прийняв
до виконання _____ Євгеній РИЖИЙ
(підпис) (Ім'я, ПРІЗВИЩЕ)

Дата видачі завдання: 17.11.2023 р.
Термін подання кваліфікаційної роботи до ЕК 17.05.2024 р.

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи «Методи оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури»: 87 сторінок, 5 рисунків, 7 таблиць та 86 літературних джерел.

Об’єкт дослідження – процес кількісного та якісного оцінювання ризиків кібербезпеки.

Мета роботи – дослідження теоретичного базису та практичних аспектів процесу оцінювання ризиків кібербезпеки інформаційних систем ОКІ, а також удосконалення відомих підходів до ризик-менеджменту в кібербезпеці.

Методи дослідження – методи кількісного та якісного оцінювання ризиків, методи прийняття рішень, методи управління ризиками.

У роботі досліджено процес кількісного та якісного оцінювання ризиків кібербезпеки.

Наукова новизна: удосконалено метод управління ризиками кібербезпеки, який використовує стандарт FMECA та систему індикаторів критичності (діаграми Ісікави та Парето, матриці критичності), що дозволяє пріоритезувати ризики та ідентифікувати їх першопричини, аналізувати динаміку й реагувати на зміни трендів.

Актуальність теми: Вивченню питань розробки, реагування, аналізу та дослідження загроз інформаційній безпеці присвячено низку публікацій вітчизняних і закордонних науковців. Проте, багато питань з розробки, реагування, аналізу та дослідження загроз інформаційній безпеці залишаються не повністю дослідженими (зокрема, в контексті захисту ОКІ, що є надзвичайно важливим для України в умовах кібервійни з агресором), а отже, тема цієї роботи є актуальною і важливою у галузі кібербезпеки та захисту інформації.

Цю роботу було апробовано у наступному видані:

Рижий Є.В., Наконечний В.С.. Methods and tools for assessing cyber security risks of information systems of critical infrastructure objects - V Всеукраїнська студентська наукова конференція «Науковий простір: аналіз, сучасний стан, тренди та перспективи» (ISBN: 978-617-8312-44-2) Вінниця «UKRLOGOS Group» 2024 с. 361-363.

Ключові слова: кібербезпека, критичність, об’єкти критичної інфраструктури, ризики, захист, security.

ЗМІСТ

ВСТУП

Актуальність. Сьогодні у користуванні організацій і підприємств присутня велика кількість інформації та різноманітних інформаційних ресурсів, також все більше уваги приділяється питанню захисту даних та кібербезпеці. Основне завдання забезпечення інформаційної безпеки (кібербезпеки) все більше вирішується в результаті впровадження різноманітних методів і дотримання вимог міжнародних і національних нормативно-правових актів, удосконалення процесу управління інформацією на основі застосування організаційних заходів.

Сучасні інформаційні системи наражаються на низку загроз (кіберзагроз), що є результатом несанкціонованого доступу, модифікації, підробки, видалення або розкриття інформації з боку зловмисника (порушника інформаційної безпеки). Щоб захистити інформаційні ресурси та сервіси від потенційних загроз, необхідно застосовувати відповідні методи (заходи) з управління ризиками кібербезпеки, які можуть бути якісними чи кількісними, або їх поєднанням (найбільш оптимальний підхід). Якісні оцінки часто використовуються для отримання загального рівня ризику та визначення ключових ризиків. Крім того, може знадобитися більш кількісний або детальний аналіз значних ризиків, особливо на ОКІ.

Вивченню питань розробки, реагування, аналізу та дослідження загроз інформаційній безпеці присвячено низку публікацій вітчизняних і закордонних науковців, зокрема, Дж. Едвардс, С. Гончар, Г. Вівер, С. Казмірчук, Ю. Яремчук, С. Толюпа, О. Архіпов, Р. Грищук, А. Банафа, І. Опірський, В. Бурячок, В. Мохор, В. Лахно та ін. Проте, багато питань залишаються не повністю дослідженими (зокрема, в контексті захисту ОКІ, що є надзвичайно важливим для України в умовах кібервійни з агресором), а отже, тема цієї роботи є актуальною і важливою у галузі кібербезпеки та захисту інформації.

Мета роботи – дослідження теоретичного базису та практичних аспектів процесу оцінювання ризиків кібербезпеки інформаційних систем ОКІ, а також удосконалення відомих підходів до ризик-менеджменту в кібербезпеці.

Для досягнення поставленої мети необхідно розв’язати такі задачі**:**

1. Проаналізувати основні поняття та базові аспекти захисту даних в інформаційних системах ОКІ;

2. Дослідити основні підходи до ризик-менеджменту в інформаційних системах ОКІ держави;

3. Дослідити ефективні методи кількісного та якісного оцінювання ризиків кібербезпеки інформаційних систем ОКІ.

Об’єктом дослідження є процес кількісного та якісного оцінювання ризиків кібербезпеки.

Предмет дослідження – це методи та інструментальні засоби оцінювання ризиків кібербезпеки інформаційних систем ОКІ.

Методи досліджень. Для розв’язання поставлених задач у даній кваліфікаційній роботі використано: методи кількісного та якісного оцінювання ризиків, методи прийняття рішень, методи управління ризиками.

Наукова новизна одержаних результатів. Удосконалено метод управління ризиками кібербезпеки, який використовує стандарт FMECA та систему індикаторів критичності (діаграми Ісікави та Парето, матриці критичності), що дозволяє пріоритезувати ризики та ідентифікувати їх першопричини, аналізувати динаміку й реагувати на зміни трендів.

Практичне значення отриманих результатів. Створення спеціалізованого програмного забезпечення на основі запропонованого методу дозволить, крім якісного і кількісного оцінювання ризику, автоматизовано оцінювати важливість ОКІ в різних галузях та секторах критичної інфраструктури. У свою чергу, це дасть змогу здійснювати перерозподіл інвестицій в кібербезпеку певних ОКІ в умовах обмежених матеріальних та інших ресурсів.

Практична цінність результатів роботи підтверджена відповідним актом впровадження (Додаток А).

РОЗДІЛ 1
АНАЛІЗ ПОНЯТЬ ТА БАЗОВИХ АСПЕКТІВ ЗАХИСТУ ДАНИХ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1. Основні поняття та визначення

Для детального розуміння процедури управління ризиками в кібербезпеці, проаналізуємо базові поняття та аспекти в галузі, висвітлені у стратегіях (концепціях) кібербезпеки і управління ризиками різних держав [1-48], а також іншій науковій літературі [24, 50-52, 54-68]:

Кіберзагроза або загроза кібербезпеці – це зловмисні дії, спрямовані на пошкодження даних, викрадення даних або порушення цифрового життя в цілому. До кіберзагроз належать комп'ютерні віруси, витоки даних, атаки типу «відмова в обслуговуванні» (DoS) та інші вектори атак.

Захист інформації – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї [54-59].

Інформація: Абстрактне поняття, яке стосується того, що має здатність інформувати. На найфундаментальнішому рівні воно стосується інтерпретації (можливо, формальної) того, що можна відчути, або їхніх абстракцій. Можна сказати, що будь-який природний процес, який не є повністю випадковим, і будь-яка закономірність, яку можна спостерігати в будь-якому середовищі, передає певну кількість інформації. У той час як цифрові сигнали та інші дані використовують дискретні знаки для передачі інформації, інші явища та артефакти, такі як аналогові сигнали, вірші, картини, музика чи інші звуки, а також течії передають інформацію в більш безперервній формі. Інформація - це не знання як таке, а значення, яке може бути отримане з представлення через інтерпретацію.

Інформаційна безпека – це набір процедур та інструментів безпеки, які в цілому захищають конфіденційну інформацію підприємства від зловживань, несанкціонованого доступу, витоку або знищення. Інфобезпека охоплює фізичну та екологічну безпеку, контроль доступу та кібербезпеку.

Інформаційна війна – це використання на полі бою та управління інформаційно-комунікаційними технологіями (ІКТ) з метою отримання конкурентної переваги над супротивником. Вона відрізняється від кібервійни, яка атакує комп'ютери, програмне забезпечення та системи управління.

Інформаційне забезпечення – це підтримка засобами інформаційних систем процесів виробництва, торгівлі, керування, навчання, наукових досліджень та будь-якої іншої діяльності у всіх сферах життя суспільства, які спрямовані на створення умов для задоволення інформаційних потреб людини, суспільства та держави.

Інформаційна загроза – вхідні дані, початково призначені для активізації в інформаційній системі алгоритмів, що відповідають за звичайний режим функціонування.

Інформаційна зброя – сукупність спеціально організованої інформації та інформаційних технологій, яка дозволяє цілеспрямовано змінювати (знищувати, спотворювати), копіювати, блокувати інформацію, долати системи захисту, обмежувати допуск законних користувачів, здійснювати дезінформацію, порушувати функціонування носіїв інформації, дезорганізовувати роботу технічних засобів комп’ютерних систем та інформаційно-обчислювальних мереж, що застосовується в ході інформаційної війни (боротьби) для досягнення поставлених цілей.

Інформаційна інфраструктура – це сукупність взаємодіючих систем виробництва, накопичення, збереження і розвитку інформаційних продуктів та їх доставки, виробництво інформаційних технологій, сервісного обслуговування інфраструктури і системи підготовки кадрів.

Інформаційний захист досягається шляхом внесення в порядку законодавчої ініціативи законопроектів, здійснення судового захисту, проведення оперативних заходів силами і засобами інформаційної безпеки.

Інформаційна кооперація – форма забезпечення інформаційної безпеки між рівноправними суб’єктами інформаційного процесу (фізичними, юридичними, міжнародними), яка включає сукупність їхніх взаємоузгоджених дій, спрямованих на одержання відомостей про дестабілізуючі фактори, дестабілізуючі й інформаційні загрози та захист від них доступними законними способами і засобами.

Інформаційне поле**:** 1) сукупність енергетичних субстанцій окремих об'єктів, які є елементами інформаційного поля Землі та Всесвіту; 2) просторово-часові вібрації (інформаційно-розпорядницькі структури), що містять відомості про минуле, сьогодення і майбутнє Всесвіту.

Інформаційний простір – це тип інформаційного дизайну, в якому репрезентації інформаційних об'єктів розташовуються в принциповому просторі. У принциповому просторі місцезнаходження і напрямок мають значення, так що стає можливим картографування і навігація [63-68]**.**

Інформаційні ресурси означає інформацію та пов'язані з нею ресурси, такі як персонал, обладнання, кошти та інформаційні технології.

Інформаційний суверенітет – здатність держави контролювати і регулювати потоки інформації поза межами держави з метою додержання законів України, прав і свобод громадян, забезпечення національної безпеки держави.

Інформаційне суспільство**:** можна визначити як суспільство, в якому інформаційні та комунікаційні технології (ІКТ) широко використовуються та інтегровані в різні аспекти життя людей. Воно характеризується можливістю швидко та ефективно отримувати доступ до інформації, обробляти її та обмінюватися нею.

Інформаційне середовище – сфера діяльності суб’єктів, пов’язана зі створенням, перетворенням і використанням інформації.

Інформаційна система – це організаційно впорядкована сукупність інформаційних ресурсів та інформаційних технологій і засобів забезпечення інформаційних процесів.

Інформаційні технології**:** це сукупність пов'язаних між собою галузей, які охоплюють комп'ютерні системи, програмне забезпечення, мови програмування, а також обробку та зберігання даних та інформації. ІТ є частиною інформаційно-комунікаційних технологій (ІКТ).

Ризик – це ймовірність того, що може статися щось погане. Ризик пов'язаний з невизначеністю щодо наслідків/впливу діяльності на те, що люди цінують (наприклад, здоров'я, добробут, багатство, власність або навколишнє середовище), часто зосереджуючись на негативних, небажаних наслідках.

Управління ризиками – це процес виявлення, оцінки та контролю фінансових, юридичних, стратегічних і безпекових ризиків для капіталу та прибутків організації. Управління кіберризиками стало життєво важливою частиною більш широких зусиль з управління корпоративними ризиками. Сьогодні компанії різних галузей залежать від інформаційних технологій для виконання ключових бізнес-функцій, що робить їх вразливими до кіберзлочинців, помилок співробітників, стихійних лих та інших загроз кібербезпеці. Ці загрози можуть вивести з ладу критичні системи або спричинити хаос в інший спосіб, що призведе до втрати доходів, викрадення даних, довгострокової шкоди репутації та штрафів з боку регуляторних органів. Ці ризики неможливо усунути, але програми управління кіберризиками можуть допомогти зменшити вплив і ймовірність загроз. Компанії використовують процес управління ризиками кібербезпеки, щоб визначити найбільш критичні загрози та обрати правильні заходи ІТ-безпеки для захисту інформаційних систем від кібератак та інших цифрових і фізичних загроз, виходячи з їхніх бізнес-пріоритетів, ІТ-інфраструктури та рівня ресурсів.

Ризик кібербезпеки – це потенційна можливість піддатися впливу або зазнати збитків внаслідок кібератаки або витоку даних вашої організації. Він

передбачає виявлення потенційних загроз і вразливостей у цифрових системах і мережах вашої організації.

Управління кіберризиками, яке також називають управлінням ризиками кібербезпеки, - це процес виявлення, визначення пріоритетів, управління та моніторингу ризиків для інформаційних систем.

1.2. Структура та зміст інформаційної безпеки

Інфобезпека займається захистом інформації в різних формах, включаючи цифрову, фізичну і навіть вербальну. Вона охоплює широкий спектр заходів, таких як адміністративний, технічний та фізичний контроль, для захисту даних від несанкціонованого доступу, розкриття, порушення, модифікації або знищення. Інфобезпека стосується безпеки даних під час зберігання, обробки та передачі.

Кібербезпека, з іншого боку, зосереджена на захисті цифрової інформації, комп'ютерних систем, мереж та електронних пристроїв від кіберзагроз. Ця сфера передусім стосується захисту від зловмисних атак, таких як хакерство, шкідливе програмне забезпечення, програми-вимагачі та фішинг, що походять з Інтернету або інших цифрових каналів. Кібербезпека охоплює різні аспекти, включаючи мережеву безпеку, безпеку додатків, безпеку кінцевих точок і реагування на інциденти. Хоча інформаційна безпека та кібербезпека мають спільні цілі, такі як збереження конфіденційності, цілісності та доступності інформації, їхні сфери застосування відрізняються. Інфобезпека має ширшу перспективу, яка охоплює всі форми інформації, в той час як кібербезпека є більш спеціалізованою сферою, яка концентрується на цифрових активах. На практиці кібербезпека може розглядатися як підгалузь інфобезпеки, яка конкретно стосується загроз та вразливостей. [70-73].

Ось найпоширеніші види інформаційної безпеки в сучасних організаціях:

Мережева безпека. Цей тип безпеки охоплює захист комп'ютерних мереж від несанкціонованого доступу або зловживань. Мережева безпека включає в себе ряд технологій, таких як брандмауери, системи виявлення/запобігання

вторгненням, віртуальні приватні мережі (VPN) та безпечні протоколи для забезпечення конфіденційності, цілісності та доступності даних.

Безпека додатків. Безпека додатків передбачає захист програмних додатків від кіберзагроз, таких як шкідливе програмне забезпечення, атаки на SQL-ін'єкції та міжсайтовий скриптинг (XSS). Рішення для захисту додатків включають безпечне кодування, тестування на проникнення та оцінку вразливостей.

Безпека даних - це практика захисту конфіденційних даних від несанкціонованого доступу, використання, розкриття або знищення. Безпека даних включає в себе ряд технологій, таких як шифрування, контроль доступу, процедури резервного копіювання та відновлення, для забезпечення конфіденційності, цілісності та доступності даних.

Безпека кінцевих точок зосереджена на захисті кінцевих точок, таких як ноутбуки, настільні комп'ютери, сервери та мобільні пристрої, від кіберзагроз. Традиційні технології захисту кінцевих точок включають антивірусне та антивірусне програмне забезпечення і брандмауери. Сучасна безпека кінцевих точок включає в себе передові рішення, такі як виявлення та реагування на кінцевих точках (EDR), які можуть захистити від загроз «нульового дня».

Мобільна безпека. Мобільна безпека - це захист мобільних пристроїв, додатків і даних від несанкціонованого доступу або використання. Рішення для мобільної безпеки включають програмне забезпечення для управління мобільними пристроями (MDM), безпечну розробку мобільних додатків і захищені протоколи зв'язку.

Хмарна безпека передбачає захист хмарних даних, додатків та інфраструктури. Вона охоплює різноманітні проблеми безпеки, включаючи конфіденційність даних, контроль доступу, управління загрозами та відповідність нормативним вимогам.

Безпека Інтернету речей. Безпека Інтернету речей передбачає захист мереж, пристроїв і даних, пов'язаних з Інтернетом речей (IoT). Безпека IoT охоплює цілий ряд питань безпеки, включаючи конфіденційність даних, контроль доступу, автентифікацію пристроїв і мережеву безпеку.

Інформаційна безпека виступає як характеристика стабільного, стійкого стану системи, яка при впливі внутрішніх та зовнішніх загроз та небезпек зберігає суттєво важливі характеристики для власного існування. До характеристик, за допомогою яких можна описати дану систему, належать:

- доступність – Здатність зробити інформацію та пов'язані з нею фізичні та логічні ресурси доступними в міру необхідності, коли вони потрібні і де вони потрібні.

- цілісність визначається як «точність, узгодженість і надійність інформаційного контенту, процесів і систем для підтримки здорової інформаційної екосистеми».

- конфіденційність означає збереження санкціонованих обмежень на доступ та розкриття інформації, включаючи засоби захисту особистої приватності та службової інформації.

1.3. Основи управління ризиками кібербезпеки та кращі практики

Управління ризиками інформаційної безпеки – це процес виявлення, оцінки, визначення пріоритетів та зменшення ризиків, пов'язаних з інформаційними активами та IT-інфраструктурою організації. Метою управління ризиками інформаційної безпеки є захист конфіденційності, цілісності та доступності інформаційних активів при мінімізації впливу інцидентів безпеки на діяльність організації, її репутацію та юридичні зобов'язання.

Процес зазвичай складається з наступних кроків:

- Ідентифікація активів: Створіть інвентаризацію інформаційних активів, таких як обладнання, програмне забезпечення, дані та мережеві компоненти, і визначте їхню цінність для організації.
- Виявлення загроз та вразливостей: Проаналізуйте потенційні загрози та вразливості, які можуть поставити під загрозу безпеку інформаційних активів. Загрози можуть надходити з різних джерел, таких як хакери, шкідливе програмне

забезпечення, стихійні лиха або людські помилки. Вразливості - це слабкі місця в системах, процесах або політиках, які можуть бути використані загрозами.

- Оцініть ризики: Оцініть ймовірність і потенційний вплив виявлених загроз і вразливостей на інформаційні активи. Це можна зробити за допомогою якісних або кількісних методів, таких як матриці ризиків, системи оцінювання або ймовірнісні моделі.
- Визначте пріоритетність ризиків: Проранжуйте виявлені ризики на основі їхнього потенційного впливу та ймовірності, зосереджуючись на найбільш значущих ризиках, які потребують негайної уваги та ресурсів.
- Розробляйте стратегії пом'якшення наслідків: Розробіть та впровадьте засоби контролю безпеки, політики та процедури для зменшення пріоритетних ризиків. Вони можуть включати превентивні заходи (наприклад, брандмауери, шифрування), заходи виявлення (наприклад, системи виявлення вторгнень, моніторинг журналів) та коригувальні заходи (наприклад, плани реагування на інциденти, резервні копії).
- Моніторинг та аналіз: Постійно відстежуйте ефективність впроваджених засобів контролю безпеки та переглядайте процес управління ризиками, щоб переконатися, що він залишається актуальним та сучасним. Це передбачає постійне інформування про нові загрози та вразливості, а також про зміни в активах, операціях та законодавчих вимогах організації.
- Звітувати та комунікувати: Регулярно звітуйте про стан ризиків інформаційної безпеки та зусилля щодо їх зменшення зацікавленим сторонам, зокрема вищому керівництву, членам ради директорів та аудиторам. Чітке інформування допомагає гарантувати, що всі в організації розуміють свої ролі та обов'язки в підтримці інформаційної безпеки.

Кращі практики

- Розробити план реагування на інциденти. План реагування на інциденти готує організацію до ефективного управління та реагування на інциденти безпеки, мінімізуючи потенційний вплив і забезпечуючи швидке повернення до нормальної роботи. Визначаючи чіткі ролі та обов'язки, окреслюючи процедури

реагування та сприяючи постійному вдосконаленню, план реагування на інциденти допомагає організаціям підтримувати сильну позицію безпеки та захищати свої критичні активи.

- Впроваджуйте DevSecOps. DevSecOps, що розшифровується як «Розробка, Безпека та Операції», інтегрує практики безпеки протягом усього життєвого циклу розробки програмного забезпечення. Включаючи безпеку як невід'ємну частину процесу розробки, DevSecOps має на меті зменшити вразливості, забезпечити швидке реагування на інциденти безпеки та сприяти розвитку культури спільної відповідальності за безпеку в межах всієї організації.
- Створіть червону та синю команди. Вправи «червона команда - синя команда» передбачають спільну роботу двох груп над зміцненням системи безпеки організації. Червона команда імітує реальні атаки, в той час як синя команда захищається від цих атак, виявляє вторгнення та зменшує загрози. Беручи участь у таких вправах, організації можуть зміцнити свою систему безпеки, покращити можливості реагування на інциденти та сформувати культуру спільної відповідальності за безпеку.
- Проведення тестування на проникнення. Тестування на проникнення передбачає імітацію реальних кібератак на системи, мережі або додатки організації для виявлення вразливостей та оцінки їхнього захисту. Регулярно проводячи тести на проникнення, організації можуть виявити слабкі місця в своїх засобах контролю безпеки, оцінити їхню стійкість до атак і усунути проблеми до того, як вони будуть використані.
- Автоматизуйте управління вразливостями. Впровадження автоматизованих інструментів управління вразливостями, таких як сканери вразливостей і системи управління виправленнями, допомагає організаціям регулярно виявляти, оцінювати, визначати пріоритети і усувати вразливості безпеки в своїх системах. Цей безперервний процес зменшує вікно можливостей для зловмисників використовувати відомі вразливості та покращує загальний стан безпеки організації.

- Впроваджуйте шифрування даних. Шифрування даних захищає конфіденційні дані від несанкціонованого доступу та забезпечує конфіденційність і цілісність цих даних як під час передачі, так і в стані спокою.
- Використовуйте надійну автентифікацію. Впровадження надійних механізмів автентифікації, таких як багатофакторна автентифікація (MFA), допомагає гарантувати, що лише авторизовані користувачі можуть отримати доступ до конфіденційних даних і систем. MFA поєднує в собі кілька методів перевірки, наприклад, щось, що користувач знає (пароль), щось, що користувач має (токен безпеки або смартфон), або щось, чим користувач є (біометричні дані). Такий багаторівневий підхід значно знижує ризик несанкціонованого доступу через скомпрометовані облікові дані.
- Навчайте та тренуйте користувачів. Людські помилки часто є важливим фактором порушення інформаційної безпеки. Регулярне навчання співробітників, підрядників і партнерів з питань безпеки допомагає сформувати культуру безпеки і гарантує, що користувачі розуміють свої обов'язки щодо захисту даних організації. Теми таких тренінгів можуть включати обізнаність про фішинг, безпечні паролі та способи повідомлення про підозри щодо інцидентів, пов'язаних з безпекою.

1.4. Роль та місце інформаційної безпеки в системі національної безпеки України

Роль та місце інформаційної безпеки в системі національної безпеки нашої держави визначаються відповідно до Закону України «Про основи національної безпеки України» (Рис.1.1).

Інформаційна безпека є невід’ємною складовою національної безпеки у всіх без виключення сферах життєдіяльності особи, суспільства та держави, оскільки безпосередньо впливає на стан їх захищеності та розвитку.

В процесі забезпечення інформаційної безпеки об’єктами захисту є [77]:

- інформація (особиста, конфіденційна, з обмеженим доступом);

- інформаційно-телекомунікаційна інфраструктура (суб’єкти та засоби створення, поширення інформації та передавання даних);

- свідомість (особи, групи осіб, суспільства).

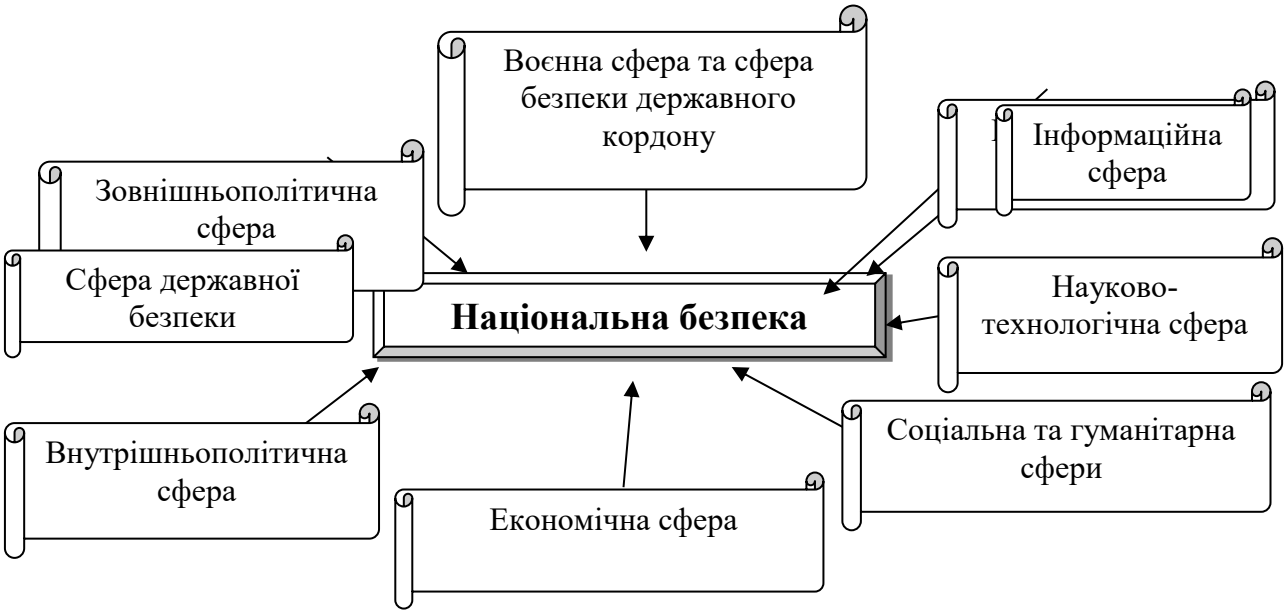


Рисунок 1.1 – Місце інформаційної безпеки в системі національної безпеки України

Основні загрози:

Внутрішні загрози (інсайдерські)

Внутрішні загрози - це ризики для безпеки, які походять зсередини організації і стосуються осіб, які мають санкціонований доступ до конфіденційної інформації, систем або ресурсів. Це можуть бути теперішні або колишні працівники, підрядники чи ділові партнери. Внутрішні загрози можуть бути навмисними (зловмисні інсайдери) або ненавмисними (недбалі інсайдери).

Навмисні інсайдерські загрози пов'язані з особами, які навмисно завдають шкоди організації шляхом крадіжки або витоку конфіденційної інформації, саботажу систем або полегшення несанкціонованого доступу для зовнішніх зловмисників. Ненавмисні внутрішні загрози виникають через недбалість, необізнаність або людські помилки, що призводить до інцидентів безпеки або витоку даних.

Запобігання внутрішнім загрозам передбачає поєднання технічних,

адміністративних та організаційних заходів:

Перевірка біографічних даних: Проводьте ретельну перевірку анкетних даних працівників і підрядників під час процесу найму, включаючи перевірку судимостей і перевірку історії працевлаштування.

Контроль доступу на основі ролей (RBAC): Обмежуйте доступ до конфіденційної інформації та ресурсів на основі ролі користувача в організації. Надавайте доступ лише тим, хто потребує його для виконання своїх посадових обов'язків.

Регулярний аудит і моніторинг: Регулярно перевіряйте дії користувачів, особливо тих, хто має підвищені привілеї. Відстежуйте поведінку користувачів, щоб виявити незвичні або підозрілі дії, які можуть свідчити про потенційні інсайдерські загрози.

Фішингові атаки

Фішингові атаки - це різновид тактики соціальної інженерії, коли зловмисники намагаються обманом змусити людей розкрити конфіденційну інформацію або виконати дії, що ставлять під загрозу безпеку.

Зазвичай фішингові атаки передбачають використання шахрайських електронних листів, миттєвих повідомлень або веб-сайтів, які імітують легітимні організації, такі як банки, онлайн-сервіси або державні установи. Зловмисники намагаються обманом змусити користувачів надати облікові дані для входу в систему, особисту інформацію або фінансові дані, а також натиснути на шкідливі посилання або завантажити інфіковані шкідливим програмним забезпеченням вкладення.

Ось кілька стратегій для запобігання фішинговим атакам:

Освіта та обізнаність: Регулярно навчайте працівників і користувачів, як розпізнавати та уникати фішингових атак. Ознайомте їх із загальними індикаторами фішингу, такими як підозрілі адреси електронної пошти, погана граматика та термінові запити на особисту інформацію.

Спам-фільтри: Впроваджуйте та налаштовуйте надійні спам-фільтри для автоматичного виявлення та блокування фішингових листів, зменшуючи

ймовірність того, що вони потраплять до поштових скриньок користувачів.

Автентифікація електронної пошти: Використовуйте стандарти автентифікації електронної пошти, такі як Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) та Domain-based Message Authentication, Reporting and Conformance (DMARC), щоб запобігти підробці електронної пошти та зменшити кількість фішингових листів, які потрапляють до користувачів.

Використовуйте безпечні з'єднання: Заохочуйте користувачів отримувати доступ до веб-сайтів через безпечні HTTPS-з'єднання та перевіряти наявність сертифікату безпеки веб-сайту.

Розподілені атаки на відмову в обслуговуванні (DDoS)

Розподілена атака на відмову в обслуговуванні (DDoS-атака) - це тип кібератаки, коли кілька скомпрометованих систем, часто контрольованих ботнетом, використовуються для того, щоб наводнити цільову систему, мережу або сервіс величезним обсягом трафіку або запитів.

Основна мета DDoS-атаки - перевантажити ресурси цілі, позбавивши її можливості обробляти законні запити, спричинити простої або порушити нормальну роботу. DDoS-атаки можуть бути спрямовані на веб-сайти, онлайн-сервіси або критично важливу мережеву інфраструктуру.

Щоб запобігти або пом'якшити вплив DDoS-атак, розгляньте можливість впровадження наступних стратегій:

Моніторинг та аналіз трафіку: Регулярно відстежуйте мережевий трафік, щоб виявити незвичні шаблони або сплески активності, які можуть свідчити про підготовку DDoS-атаки. Використовуйте інструменти та аналітику для виявлення та розрізнення легітимного та зловмисного трафіку.

Резервування та масштабованість: Розробіть свою інфраструктуру таким чином, щоб мати надлишкові компоненти, такі як сервери, мережеві канали або центри обробки даних, щоб розподілити навантаження і мінімізувати вплив атаки. Впроваджуйте масштабовані хмарні рішення, щоб поглинати сплески трафіку та зменшити ризик перебоїв у роботі сервісів.

Мережева архітектура: Проектування багаторівневої мережевої архітектури

для розподілу трафіку між різними ресурсами та мінімізації впливу атаки на будь-який окремий компонент. Впровадження балансування навантаження, мереж доставки контенту (CDN) та кешування може допомогти в цьому відношенні.

Атаки з вимогою викупу

Атаки з вимогою викупу - це тип шкідливого програмного забезпечення, яке шифрує дані або файли жертви, роблячи їх недоступними. Потім зловмисник вимагає сплатити викуп, зазвичай у криптовалюті, як-от біткойн, щоб отримати ключ дешифрування, який розблокує зашифровані дані.

Атаки з вимогою викупу можуть бути спрямовані на фізичних осіб, підприємства або державні установи і можуть призвести до значних фінансових втрат, перебоїв у роботі та шкоди для репутації.

Щоб запобігти або пом'якшити наслідки атак зловмисників, розгляньте можливість впровадження наступних стратегій:

Регулярне резервне копіювання даних: Створюйте та регулярно зберігайте резервні копії критично важливих даних і систем, зберігаючи їх у безпечних, автономних або віддалених місцях. Це дозволить вам відновити дані без сплати викупу в разі атаки.

Оновлюйте та виправляйте системи: Оновлюйте все програмне забезпечення, операційні системи та додатки найновішими патчами безпеки, щоб мінімізувати вразливості, які можуть використовувати програми-вимагачі.

Антивірусне та антивірусне програмне забезпечення: Використовуйте надійне антивірусне та антивірусне програмне забезпечення для виявлення та блокування програм-вимагачів та іншого шкідливого програмного забезпечення. Переконайтеся, що ці інструменти регулярно оновлюються найновішими сигнатурами шкідливих програм.

Безпека електронної пошти: Впроваджуйте надійні заходи безпеки електронної пошти, такі як фільтри спаму, протоколи автентифікації електронної пошти та захищені поштові шлюзи, щоб мінімізувати ймовірність потрапляння електронних листів з вимогами до поштових скриньок користувачів.

Сучасні постійні загрози (APT-атаки)

APT-атаки - це складні, цілеспрямовані кібератаки, що здійснюються висококваліфікованими та добре фінансованими суб'єктами загроз, часто за підтримки національних держав або організованих кіберзлочинних угруповань. Метою APT-атак є отримання та утримання несанкціонованого доступу до мережі або систем жертви протягом тривалого періоду часу, зазвичай з метою викрадення конфіденційної інформації, шпигунства або порушення роботи.

Запобігання або пом'якшення наслідків APT-атак вимагає комплексного, багаторівневого підходу до безпеки. Ось кілька стратегій, які варто розглянути:

Впровадьте надійну систему безпеки: Прийміть стратегію глибокого захисту, яка включає в себе кілька рівнів заходів безпеки, таких як брандмауери, IDPS, сегментація мережі та шифрування даних.

Моніторинг мережі та виявлення аномалій: Постійно відстежуйте мережевий трафік і системні журнали на предмет незвичної або підозрілої активності, яка може вказувати на присутність актора APT. Впроваджуйте інструменти виявлення аномалій для виявлення потенційних вторгнень.

Захист кінцевих точок: Посильте безпеку кінцевих точок за допомогою рішень, призначених для виявлення та реагування на атаки, які часто пропускаються традиційними системами безпеки, наприклад, виявлення та реагування на кінцеві точки (EDR).

Аналітика загроз: Використовуйте канали та служби розвідки загроз, щоб бути в курсі останніх дій, тактик та індикаторів компрометації (IOC), що дозволить вам проактивно захищатися від нових загроз.

Видавання себе за користувача

Видавання себе за користувача, також відоме як підробка ідентифікаційних даних або маскування, - це зловмисна діяльність, коли зловмисник видає себе за легітимного користувача, привласнюючи його особистість, часто з наміром отримати несанкціонований доступ до конфіденційної інформації, систем або мереж.

Видавання себе за користувача може набувати різних форм, залежно від методів і прийомів, які використовує зловмисник. Деякі поширені типи видачі

себе за користувача включають в себе

Крадіжка облікових даних: Отримання облікових даних користувача, таких як імена користувачів і паролі, за допомогою фішингу, кейлоггінгу або інших хакерських методів, і використання їх для отримання несанкціонованого доступу до систем і даних.

Захоплення сеансу: Перехоплення та отримання контролю над активним сеансом користувача, часто шляхом використання вразливостей у протоколах зв'язку або перехоплення токенів сеансу, що дозволяє зловмиснику видавати себе за користувача в межах скомпрометованого сеансу.

Атаки типу «людина посередині» (MitM): Розміщення між користувачем і системою для перехоплення та маніпулювання комунікаціями, потенційно видаючи себе за обидві сторони, щоб отримати доступ до конфіденційної інформації або модифікувати дані під час передачі.

Атаки на передачу хешу: Захоплення та використання хешованих даних пароля замість отримання відкритого пароля, щоб видати себе за користувача та отримати несанкціонований доступ до систем.

Ескалація привілеїв: Використання вразливостей або неправильних конфігурацій в системі для підвищення привілеїв доступу та видавання себе за користувача з вищим рівнем авторизації.

Соціальна інженерія

Соціальна інженерія - це техніка маніпуляції, яка використовує людську психологію та поведінку, щоб обманом змусити людей розкрити конфіденційну інформацію, надати несанкціонований доступ або виконати дії, які вигідні зловмиснику. Замість того, щоб використовувати технічні вразливості в системах або мережах, соціальна інженерія націлена на найслабшу ланку в ланцюгу безпеки - людей.

Зловмисники часто використовують переконання, побудову довіри або маніпуляції, щоб переконати жертв поділитися конфіденційними даними, такими як паролі, фінансові реквізити або особиста інформація. До поширених тактик соціальної інженерії належать

Фішинг: надсилання шахрайських електронних листів або повідомлень, які виглядають як такі, що надходять з легітимних джерел, обманом змушуючи одержувачів натискати на шкідливі посилання, завантажувати шкідливе програмне забезпечення або надавати конфіденційну інформацію.

Вигадані приводи: Створення сфабрикованого сценарію або видавання себе за авторитетну особу, щоб увійти в довіру та отримати інформацію від жертви.

Заманювання: Спонукання жертви до певної дії, наприклад, до завантаження шкідливого програмного забезпечення, шляхом пропозиції чогось привабливого, наприклад, безкоштовного програмного забезпечення або завантаження медіафайлів.

Послуга за послугу: Пропонування послуги або послуги в обмін на інформацію або доступ жертви, наприклад, видавання себе за службу технічної підтримки, щоб отримати облікові дані для входу в систему.

Тейлгейтинг: Отримання несанкціонованого доступу до зон з обмеженим доступом шляхом слідування за уповноваженою особою, часто під виглядом працівника або кур'єра.

1.5. Забезпечення інформаційної безпеки держави та захист критичної інфраструктури

Забезпечення інформаційної безпеки – це комплекс заходів, необхідний для досягнення такого стану інформаційного розвитку (духовного, соціально-політичного, технічного) та захищеності особи, суспільства, держави, за якого сторонні інформаційні впливи не завдають суттєвої шкоди національним інтересам.

Об’єкти забезпечення інформаційної безпеки можуть бути як об’єктами захисту, так і засобами проведення заходів, що впливають на стан інформаційної безпеки.

Основу системи забезпечення інформаційної безпеки України складають відповідні органи та сили, які вживають адміністративно-правових,

інформаційно-аналітичних, організаційно-управлінських, та інших заходів, спрямованих на забезпечення стійкого функціонування системи державного управління в інформаційній сфері.

Система суб'єктів забезпечення інформаційної безпеки – це організована державою сукупність суб’єктів державних органів, громадських організацій, посадових осіб та окремих громадян, об’єднаних цілями та завданнями щодо захисту національних інтересів в інформаційній сфері, що здійснюють узгоджену діяльність у межах законодавства України.

Принципи забезпечення інформаційної безпеки України [74-78]:

- свобода збирання, зберігання, використання та поширення інформації;
- достовірність, повнота та неупередженість інформації;
- обмеження доступу до інформації виключно на підставі закону;
- гармонізація особистих, суспільних і державних інтересів;
- запобігання правопорушенням в інформаційній сфері;
- економічна доцільність;
- гармонізація українського законодавства в інформаційній сфері з міжнародним;
- пріоритетність національної інформаційної продукції.

Розрізняють два аспекти забезпечення інформаційної безпеки – активний та пасивний. Забезпечення інформаційної безпеки як активна функція загальнодержавної системи забезпечення інформаційної безпеки включає [79]:

- на фізичному рівні – розвиток потужної ІКС, підтримка діяльності вітчизняних ЗМІ, розвитку видавничої справи, кінематографу, побудова мережі корпунктів за кордоном;
- на інформаційному рівні – інформаційна підтримка геополітичних позицій держави, що відповідають національним інтересам, формування позитивного міжнародного іміджу держави, створення власного конкурентного інформаційного продукту, забезпечення свободи слова та доступу громадян до інформації, реалізація права на повноту і достовірність інформації, патріотичне виховання громадян.

Пасивний аспект (захист) передбачає:

- на фізичному рівні – захист ІКС від монополізації, використання з розвідувальною чи іншою метою, що становить загрозу національній безпеці, захист інформації (на матеріальних носіях, в мережах) від несанкціонованого доступу, модифікації, блокування, захист інформації з обмеженим доступом;

- на інформаційному рівні – захист свідомості особи, групи осіб, суспільства, захист інтелектуальної власності.

Система забезпечення інформаційної безпеки передбачає формування відповідної системи протидії загрозам, яка складаєтьсяз чотирьох складових [80]:

1. Нормативно-правова складова повинна забезпечувати формування й удосконалення системи правових норм протидії загрозам інформаційної безпеки та механізмів їх реалізації. Вона утворюється сукупністю нормативних правових актів, інших нормативних документів, які регулюють відносини у сфері виявлення загроз безпеці індивідуальної, групової та масової свідомості громадян і протидії цим загрозам, що забезпечує реалізацію конституційних прав та свобод, їх законних обмежень, охорону психічного здоров'я громадян, збереження соціального спокою в суспільстві.

2. Організаційна складова системи забезпечення інформаційної безпеки має установлювати функціональну структуру громадських організацій і державних органів, що займаються реалізацією правових норм у цій сфері, й відносини між ними, а також між цими організаціями й органами, з одного боку, та громадянами – з іншого. При цьому найважливішою частиною організаційної складової системи мають бути відповідні структури громадянського суспільства. Організаційна складова є важливою частиною загальної системи забезпечення інформаційної безпеки, конфігурація якої має бути позначена в Доктрині інформаційної безпеки країни. Система забезпечення інформаційної безпеки повинна будуватися на основі тісної взаємодії глави держави, органів законодавчої, виконавчої й судової влади, а також громадських організацій, що займаються установленою законом діяльністю в цій сфері.

3. Технологічна складова цієї системи повинна забезпечувати можливість

вільного та безпечного інформаційного обміну між громадянами, членами груп, групових асоціацій і запобігання протиправному інформаційному впливу на них; своєчасне виявлення загроз інформаційній безпеці особи, суспільства та держави, оцінку можливого й завданого збитку цій безпеці та організацію ефективної протидії таким загрозам.

4. Кадрова складова має забезпечити формування й підтримання кадрового потенціалу суспільства та держави, необхідного для ефективного функціонування системи забезпечення інформаційної безпеки.

1.6. Висновки до розділу 1

У цьому розділі було проведено аналіз базових концептів та ключових аспектів кібербезпеки та управління ризиками інформаційної безпеки. Визначено, що основні аспекти управління ризиками кібербезпеки включають:

- Ідентифікація ризиків: Визначення вразливостей, загроз і можливих точок доступу, які можуть використовувати зловмисники. Це включає в себе інвентаризацію активів та їхню класифікацію за важливістю.
- Оцінка ризиків: Вимірювання ймовірності кожного ризику та його можливого впливу на організацію. Ця оцінка допомагає встановити пріоритети та планувати стратегії реагування.
- Розробка стратегії пом'якшення ризиків: Визначення заходів для зменшення впливу ризиків, таких як впровадження політик безпеки, використання брандмауерів, шифрування та навчання персоналу.
- Впровадження заходів: Реалізація планів пом'якшення ризиків, таких як удосконалення систем моніторингу, оновлення програмного забезпечення, налаштування обмежень доступу та створення плану дій на випадок інцидентів.
- Моніторинг та виявлення загроз: Безперервний моніторинг систем для виявлення та попередження нових загроз або підозрілої активності.

- Оцінка ефективності: Аналіз і перегляд ефективності впроваджених заходів для забезпечення актуальності та дієвості. Це може включати регулярне тестування, проведення аудитів або симуляцію атак (пентест).
- Реагування на інциденти: Розробка планів швидкого реагування та мінімізації шкоди під час кіберінциденту. Це передбачає відновлення системи, сповіщення відповідних сторін і проведення розслідування.
- Навчання та підвищення обізнаності: Підготовка співробітників щодо ризиків кібербезпеки та правильного поводження з інформацією, щоб знизити ризик фішингових атак або інших соціальних маніпуляцій.

РОЗДІЛ 2
ТЕОРЕТИЧНІ ОСНОВИ РИЗИК-МЕНЕДЖМЕНТУ В ІНФОРМАЦІЙНИХ СИСТЕМАХОБЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

2.1. Методи забезпечення інформаційної безпеки, загрози та ризики

Серед методів забезпечення інформаційної безпеки можна виділити наступні [52, 63, 71-75, 80-84]:

- однорівневі методи будуються на підставі одного принципу управління інформаційної безпеки;

- багаторівневі методи будуються на основі декількох принципів управління інформаційною безпекою, кожний з яких слугує вирішення власного завдання. При цьому приватні технології не пов’язані між собою і спрямовані лише на конкретні чинники інформаційних загроз;

- комплексні методи – багаторівневі технології, які об’єднані до єдиної системи координуючими функціями на організаційному рівні з метою ЗІБ виходячи з аналізу сукупності чинників небезпеки, які мають семантичний зв’язок або генеруються з єдиного інформаційного центру інформаційного впливу;

- інтегровані високоінтелектуальні методи – багаторівневі, багатокомпонентні технології, які побудовані на підставі могутніх автоматизованих інтелектуальних засобів із організаційним управлінням.

Дестабілізуючі чинники інформаційної безпеки – явища та процеси природного та штучного походження, що породжують інформаційні загрози.

Загрози інформаційній безпеці – це сукупність умов і чинників, що створюють небезпеку життєво важливим інтересам особистості, суспільства і держави в інформаційній сфері.

Основні загрози інформаційній безпеці поділяються на [71]:

- загрози впливу неякісної інформації на особистість, суспільство, державу;

- загрози несанкціонованого і неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси;

- загрози інформаційним правам і свободам особистості.

Чинники загроз за видовою ознакою поділяються на:

- політичні,

- економічні

- організаційно-технічні.

Витік інформації – це втрата інформації за рахунок її перехоплення за допомогою технічних засобів розвідки.

Втрата інформації можлива за наявності каналів розголошення або витоку. Канал витоку інформації означає перехід цінних відомостей від джерела до конкурента або зловмисника, чи до третьої особи в несанкціонованому режимі.

Під третьою особою розуміються будь-які особи, які одержали знання конфіденційної інформації через обставини або в результаті безвідповідальності персоналу. Варто враховувати, що ці особи не зацікавлені в отриманій інформації.

Канали витоку інформації поділяються на [78]:

- візуально-оптичні;

- акустичні;

- електромагнітні.

Несанкціонований доступ – це протиправне навмисне оволодіння конфіденційною інформацією особою, що не має права доступу до відомостей.

Основні шляхи несанкціонованого доступу до інформації:

- перехоплення електронних випромінювань;

- примусове електромагнітне опромінення (підсвічування) ліній зв'язку з метою одержання паразитної модуляції несучої частоти;

- застосування підслухових пристроїв (закладок);

- дистанційне фотографування;

- перехоплення акустичних випромінювань і відновлення тексту принтера;

- читання залишкової інформації в пам'яті системи після виконання санкціонованих запитів;

- копіювання носіїв інформації з подоланням мір захисту;

- маскування під зареєстрованого користувача;

- маскування під запити системи;

- використання програмних пасток;

- використання недоліків мов програмування й операційних систем;

- незаконне підключення до апаратури й ліній зв'язку спеціально розроблених апаратних засобів, що забезпечують доступ до інформації;
злочинний вивід з ладу механізмів захисту;

- розшифровка спеціальними програмами зашифрованої інформації.

Безпосередні шляхи несанкціонованого доступу до інформації:

- розкрадання носіїв інформації й документів;

- ініціативне співробітництво;

- схиляння до співробітництва з боку зломщика;

- підслуховування;

- спостереження.

2.2. Порушники інформаційної безпеки

Порушником інформаційної безпеки є будь-хто або будь-що, що намагається отримати доступ до будь-якої частини вашої комп'ютерної системи. Порушника зазвичай називають хакером. Відомо, що хакери використовують автоматизовані комп'ютерні програми для компрометації системи безпеки вашого комп'ютера.

Порушення можуть бути: ненавмисні; зловмисні.

Особливу небезпеку варто очікувати від зловмисних порушників, які в силу тих або інших причин, перебувають під впливом: кримінальних осіб та їх угруповань; бізнесменів, комерсантів та їх об'єднань; політичних діячів і партій; агентів спецслужб інших держав, або самі входять у їх склад.

Кваліфікація порушника – це сукупність певних знань і вмінь порушника, які він використовує для реалізації несанкціонованого доступу до ІКС.

Можна відзначити кілька типів кваліфікації порушників, що дозволять йому успішно реалізувати загрози ІКС [80-83]:

1. Порушник володіє інформацією щодо функціональних особливостей ІКС взагалі, уміє користуватися штатними засобами;

2. Порушник має високий рівень знань і досвід роботи в технічному обслуговуванні аналогічних ІКС;

3. Порушник володіє високим рівнем знань в галузі обчислювальної техніки (зокрема, криптографії, теорії алгоритмів та паралельних обчислень тощо) і програмування на мовах розробки програмного забезпечення ІКС чи її аналога;

4. Порушник досконало володіє необхідними знаннями і навиками роботи з обладнанням, що використовується в ІКС;

5. Порушник має доступ до глобальних обчислювальних мереж, суперкомп'ютера чи квантового комп'ютера, за допомогою якого може реалізувати, наприклад, силову атаку на ІКС.

Загальна класифікація порушників ІБ приведена на рис. 2.1.

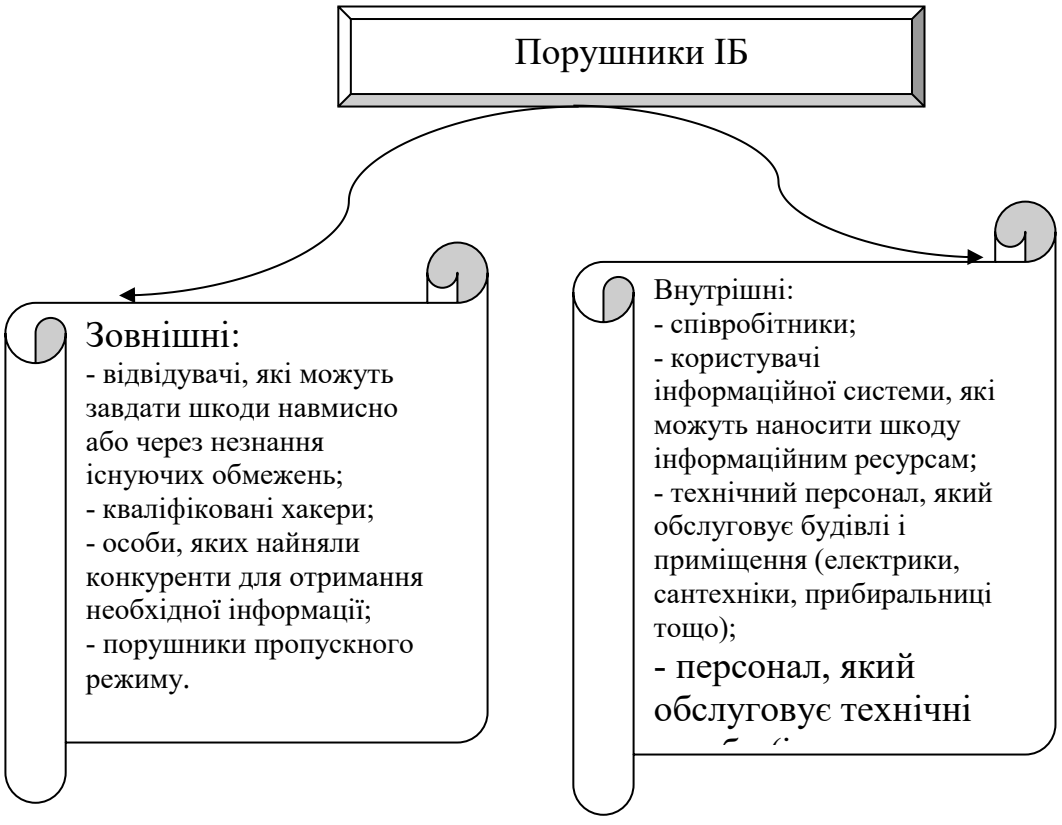


Рисунок 2.1 – Класифікація порушників інформаційної безпеки

Можливості порушника щодо впливу на ІКС можна представити у вигляді ієрархічної класифікації [63]:

1. Порушник має можливість запуску певного обмеженого набору програмного забезпечення, що реалізує певні функції з обробки інформації в ІКС (перший рівень можливостей);

2. Порушник може створювати власне програмне забезпечення та модифікувати існуюче, що дозволить створити нові функції обробки інформації і подальшого одержання частини необхідної інформації (другий рівень можливостей);

3. Порушник має змогу управляти функціонуванням ІКС, тобто безпосередньо впливати на програмне забезпечення, склад та конфігурацію технічного забезпечення ІКС (третій рівень можливостей);

4. Порушник має весь обсяг можливостей легітимних користувачів, тому може розробляти та впроваджувати в експлуатацію технічні ІКС, а також інтегрувати власні технічні засоби з метою подальшого отримання корисної інформації (четвертий рівень можливостей);

Ступінь ризику, щодо можливої реалізації загроз та нанесення шкоди в залежності від зазначених робочих функцій працівників [56]:

- найбільший ризик: системний адміністратор; адміністратор бази даних; адміністратор безпеки;

- високий ризик: оператор системи; оператор введення й підготовки даних; менеджер обробки даних; системний програміст;

- середній ризик: інженер системи; менеджер програмного забезпечення;

- обмежений ризик: прикладний програміст; інженер і оператор зв'язку; інженер по устаткуванню; оператор периферійного устаткування; бібліотекар системних магнітних носіїв; користувач-програміст; користувач-операціоніст;

- низький ризик: інженер по периферійному устаткуванню; бібліотекар магнітних носіїв користувачів.

Можливою метою порушника є:

- особиста авторизація;

- авторизувати інших осіб;

- знайти прихильників або довірених осіб серед персоналу або користувачів ІС.

При відсутності можливості або безуспішності реалізації вищенаведених дій, порушник може мати наміри [84]:

1. Одержання атрибутів доступу авторизованих користувачів шляхом використання технічних засобів, крадіжок, купівлі, або одержання іншим шляхом;

2. Проникнення на місця розміщення тих або інших компонентів, елементів або ресурсів ІКС шляхом подолання будівельних конструкцій, охорони або охоронної сигналізації;

3. Зміни режимів функціонування ІКС, її ресурсів та послуг системи;

4. Установки фізичних засобів у місцях розміщення елементів ІКС (технічних закладок) чи інших засобів технічної розвідки (у тому числі й віддалених, наприклад в елементах комунікаційної мережі зв'язку) для перехвату інформації;

5. Установки фізичних засобів у місцях розміщення елементів ІС (технічних закладок) або інших засобів (у тому числі й віддалених, наприклад в елементах комунікаційної мережі зв'язку) для генерації хибних сигналів, інформаційних символів або спотворених повідомлень;

6. Установки програмних засобів (програмних закладок або вірусів) зйому інформації з метою її використання;

7. Установки програмних засобів (програмних закладок або вірусів) для модифікації системного програмного забезпечення так і інформації ІКС, шляхом введення програмних вірусів, спотворених сигналів, інформаційних символів або хибних повідомлень із метою перевантаження систем і порушення, таким чином, доступності компонентів ІС;

8. Здійснення спроб несанкціонованого доступу до обчислювальних та інформаційних ресурсів, базового й прикладного програмного забезпечення;

9. Здійснення спроб несанкціонованого доступу до системи захисту інформації, як частини ІКС, так і до її телекомунікаційної підсистеми, шляхом

подолання системи управління доступом.

Порушник може використовувати сукупність релевантних знань, умінь та навиків, для прикладу [67-68]:

- досконале знання математичного апарату дозволить створити нові методи криптоаналізу відповідно до рівня криптографічного захисту;

- знання мов програмування (програмної інженерії) дозволить реалізувати створені методи криптоаналізу, а також модифікувати існуюче програмне забезпечення легітимних користувачів;

- знання основ фізики, електроніки і т.п. дасть змогу порушнику підібрати відповідну специфічну атаку і отримати корисну інформацію;

- знання методів соціального інжинірингу дозволить порушнику без ґрунтовних знань математики, фізики та програмування обійти будь-які системи захисту.

Важливість кібербезпеки:

- Захист ідентичності: Кібербезпека гарантує, що особистість людини захищена, а автентичність зберігається під час використання технологій.
- Збереження конфіденційності: Кібербезпека задовольняє вимогу, щоб інформація або контент, які є конфіденційними, були надзвичайно захищеними. Користувачі можуть довіряти використанню технології.
- Захист конфіденційного контенту: Конфіденційна інформація є найбільш вразливою до загроз безпеці. Атаки на конфіденційну інформацію, таку як банківська інформація, є найбільш поширеними і здійснюються з метою грошового шахрайства.

Найпоширенішою загрозою безпеці є атака зловмисника. Зловмисників часто називають хакерами, і вони є найбільш шкідливими факторами, що сприяють вразливості системи безпеки. Вони володіють величезними знаннями і глибоким розумінням технологій і безпеки. Зловмисники порушують приватність користувачів і мають на меті викрасти конфіденційну інформацію користувачів. Потім викрадену інформацію продають третім особам, які мають на меті зловживати нею для власної особистої чи професійної вигоди.

2.3. Дослідження стратегій кібербезпеки, захисту ОКІ та управління ризиками в різних державах

У роботах [1-48] було відображено сучасні стратегії кібербезпеки та захисту об’єктів критичної інфраструктури у контексті ризик-менеджменту.

І. Держави Європи. Стратегія кібербезпеки Німеччини (Cyber Security Strategy for Germany) 2011 року створена з метою кримінального переслідування кібератак та запобігання їх виникнення, а також запобігання виходу з ладу IT-обладнання через випадкові чинники. Передбачено такі загрози: кібератаки та виведення з ладу критичних інформаційних ресурсів. До принципів забезпечення кібербезпеки віднесено узгодження набору інструментів для реагування на кібератаки; регулярна оцінка ситуації, ризиків та прийняття відповідних засобів захисту; регулярні тренування персоналу та тестування обладнання; зміцнення IT-безпеки в сфері держуправління. Наведено дефініції таких понять як кіберпростір, кібератака, кібершпіонаж, кіберсаботаж, кібербезпека, цивільна та військова кібербезпека, критична інфраструктура (критичні ресурси). Міжнародна співпраця і партнерство, регулярна перевірка мети стратегії на рівень її досягнення та оновлення відповідно до стану поточної ситуації є пріоритетними.

Стратегія кібербезпеки Угорщини (National Cyber Security Strategy of Hungary), що була прийнята 2013 року, спрямована на розвиток вільного та безпечного кіберпростору і захист національного суверенітету в національному та міжнародному контексті, який зазнав значних змін у зв’язку із появою кіберпростору, що став новим ключовим чинником у XXI сторіччі. Крім того, вона спрямована на захист діяльності та забезпечення безпеки національної економіки і суспільства, адаптації технологічних інновацій для полегшення економічного зростання і міжнародного співробітництва в цій галузі відповідно до національних інтересів Угорщини. Дефініцій понять у документі не наведено. Пріоритетними є співпраця на різних рівнях, підвищення рівня обізнаності та освіченості громадян в сфері кібербезпеки, захист дітей у кіберпросторі, розвиток нормативно-правової та технічної бази, мотивація комерційного сектору.

Стратегія кібербезпеки Чорногорії (Strategy on Cyber Security of Montenegro to 2017) була прийнята 2013 року. Мета документу – побудувати інтегрований, функціональний та ефективний кіберпростір, відповідно до міжнародних стандартів і принципів. У документі наведено дефініції таких понять: кіберпростір, ІБ, комп'ютерна безпека, Інтернет-безпека, мережева безпека, кібербезпека, кібероборона, кіберзлочин, кібертероризм, кібершпіонаж, кібервійна. Визначено такі загрози: DoS і DDoS-атака, атаки на сайти з метою несанкціонованої модифікації їх змісту, несанкціонований доступ до розвинутих ІКТ державних органів та їх бази даних, фішинг. До принципів забезпечення кібербезпеки віднесено визначення інституційної та організаційної структури в сфері кібербезпеки в державі, захист критичних інформаційних структур, зміцнення потенціалу державних правоохоронних органів, реагування на інциденти, посилення ролі Міністерства оборони та військових Чорногорії в кіберпросторі, державно-приватне партнерство, підвищення обізнаності громадськості та захисту користувачів. Пріоритетними визначено такі завдання: моніторинг ризиків на національному рівні, розробка чіткої структури управління, створення механізмів розслідування інцидентів, встановлення балансу між безпекою і повагою приватного життя, створення конфіденційних механізмів обміну інформацією, встановлення основних вимог до кібербезпеки, відповідальність за кіберзлочинність, зміцнення програм освіти і професійної підготовки, підвищення обізнаності громадськості з питань кібербезпеки тощо.

Метою Стратегії кібербезпеки Естонії (Cyber Security Strategy) 2014 року є опис методів забезпечення безперебійної експлуатації та стійкості важливих сервісів і захист критичних інформаційних інфраструктур від кіберзагроз на період до 2017 року. У документі наведено дефініцію поняття кібербезпека. Головним пріоритетом у забезпеченні кібербезпеки є прогноз як запобігання можливості виникнення загрози, так і ефективного реагування на загрози, які матеріалізуються. Визначено такі загрози: кібератаки, шпіонаж, кіберзлочини. Принципи забезпечення кібербезпеки: кібербезпека є невід'ємною частиною національної безпеки, підтримує функціонування держави і суспільства,

конкурентоспроможність економіки та інновацій, забезпечується на основі принципу пропорційності, беручи до уваги існуючі та потенційні ризики і ресурси; гарантується дотриманням основних прав і свобод, а також захисту особистої інформації та особистості; починається з індивідуальної відповідальності за безпечне використання засобів ІКТ; підтримується інтенсивністю і конкурентоспроможністю досліджень і розвитку на міжнародному рівні; забезпечується на узгодженій основі в рамках співпраці між державним, приватним та третім сектором, беручи до уваги взаємозв'язок і взаємозалежність існуючої інфраструктури і сервісів в кіберпросторі; забезпечується за допомогою міжнародного співробітництва з союзниками і партнерами. Завдяки співпраці, Естонія сприяє зміцненню глобальної кібербезпеки і підвищує рівень своєї компетенції.

Стратегія кібербезпеки Австрії (Austrian Cyber Security Strategy) 2013 року має на меті визначення ролей, обов'язків та повноваженнь державних і недержавних суб'єктів у кіберпросторі, а також створення адекватних структурованих умов для співпраці між усіма суб'єктами. Визначено такі загрози: маніпулювання у каналах зв'язку; маніпулювання в системах фінансових операцій; DDoS-атаки; відсутність правової основи; відсутність безпеки, обізнаності та стандартів; систематична крадіжка цифрових персональних даних; махінації в соцмережах; недостатня кількість експертів; виробничий кібершпіонаж, відсутність систематичного оцінювання технологічного впливу; шкідливе ПЗ, проблемні і несумісні коди ПЗ; непевна відповідальність в урядових системах, потреба в стратегії мережевої інфраструктури. До принципів забезпечення кібербезпеки віднесено наступне: дотримання закону, самоврегулювання, пропорційність, ієрархічність, конфіденційність, цілісність, автентичність, доступність, приватність і захист даних. Стратегією передбачено такі пріоритети покращення стійкості критичних інфраструктур: посилення культури кібербезпеки; зміцнення досліджень Австрії в сфері кібербезпеки; ефективна співпраця з Європою та світом у сфері кібербезпеки.

Стратегія кібербезпеки Польщі (Cyberspace Protection Policy of the Republic of Poland) була ухвалена 2013 року. Відповідно до документу, інфраструктура ІКТ повинна бути захищена від атак з кіберпростору, знищення, пошкодження та несанкціонованого доступу. Наведено дефініції таких понять: експлуатація з порушенням норм, кіберпростір, кіберзлочин, безпека кіберпростору, кібератака, кібертероризм, CERT, кіберпростір Республіки Польща, користувач кіберпростору, інцидент комп'ютерної безпеки, ризик-менеджмент тощо. Принципи забезпечення кібербезпеки, дотримання яких є пріоритетними: принцип законодавчих заходів, принцип процедурних і організаційних заходів (система менеджменту), принцип виховання, навчання та підвищення обізнаності в галузі безпеки, принцип технічних дій (збільшення кількості команд для реагування на інциденти безпеки у державних установах, тестування рівня безпеки, розвиток системи попередження, запобігання інцидентам і прийняття профілактичних рішень).

II. Держави Африки. Стратегія кібербезпеки Кенії (Cybersecurity Strategy) була затверджена 2014 року. Метою є чітке визначення бачення кібербезпеки Кенії, цілі та завдання для забезпечення захисту кіберпростору держави, продовжуючи сприянню використання для економічного зростання Кенії. Визначено такі загрози: ботнети, організована злочинність, DoS-атаки, кібертероризм, шкідливі коди та спеціально націлене шкідливе ПЗ. У стратегії наведено дефініції понять CERT, кіберпростір, кібербезпека, електронне урядування, критична інфраструктура, уряд, ІКТ, інсайдерська загроза, соціальний інжиніринг тощо. Пріоритетними напрямками визначено електронне урядування, підвищення кібербезпеки Кенії, оновлення стратегії, її цілей і завдань.

Стратегія кібербезпеки Маврикія (National Cyber Security Strategy 2014-2019) була затверджена 2014 року. Метою документу є інтеграція ІБ в базові структури для розвитку інформаційного суспільства. Підхід до виконання стратегії базується на задачах кібербезпеки: побудова безпеки за функціональними і технічними вимогами, робота системи моніторингу

кіберзагроз, яка сприяє кращому реагуванню, моніторингу та координації кіберзагроз на національному рівні у режимі 24/7, покращення ризик-менеджменту, покращення і замовлення експертиз та їх супровід. Дефініцій понять і загроз у стратегії не наведено. Пріоритетними є вибір правильного фокусу для створення безпечного комп'ютеризованого середовища, оприлюднення механізму для видалення нелегального контенту, посилення правоохоронної спроможності в кібербезпеці, міжнародна і регіональна співпраця, посилення безпеки в кіберпросторі, створення тестувальної системи для мережі безпеки, сприяння розробці ПЗ, сприяння виконанню стандартів ІБ в цивільних справах, проведення аудитів, співробітництво з промисловістю для пошуку покращень, створення тренінгових програм, покращення кіберосвіти та обізнаності людей у цій сфері, організація щорічних заходів, присвячених міжнародній кібербезпеці.

III. Держави Азії та Океанії. Стратегія кібербезпеки Катару (Qatar's National Cyber Security Strategy) була прийнята 2014 року та являє собою план для поліпшення ІБ держави. Метою документу є встановлення і підтримка безпечного кіберпростору для захисту національних інтересів і збереження основних прав та цінностей суспільства Катару. У документі визначено такі загрози: інсайдерські атаки, хактивізм, кібератаки, кіберзлочини, APT-загрози. Наведено дефініції понять: інформаційна кампанія, функціональні можливості, критична інформаційна інфраструктура, кіберзлочин, критичний сектор, організація критичного сектору, кібербезпека, контроль кібербезпеки, кіберпростір, персональна інформація, здатність до відновлення нормального функціонування, ненавмисні інсайдери. Стратегією визначено наступні принципи забезпечення кібербезпеки: катарський уряд несе відповідальність за захист своєї інформації, систем і мереж; інвестиції в людські ресурси, процеси і технології, необхідні для забезпечення функціонування сервісів, на які опирається суспільство; визначення напрямку для подальшого економічного розвитку Катару; можливість підприємств захищати свою інформацію і мережі від кіберзагроз, впровадження передового досвіду. До пріоритетів віднесено наступне: мінімізація ризиків,

сприяння встановленню високого рівня кібербезпеки в Катарі, забезпечуючи стратегічний напрямок для зусиль в області кібербезпеки, і тісна співпраця із організаціями для повного виконання цілей і вимог стратегії, чітке дотримання плану дій тощо.

Концепція кібербезпеки Сінгапуру (National Cyber Security Masterplan 2018) затверджено 2013 року. Вона спрямована на створення безпечного і стійкого середовища інфокомунікацій та динамічної екосистеми кібербезпеки. Документом передбачено такі загрози: APT-загрози, фішинг, соціальний інжиніринг, DDoS-атаки, шкідливе ПЗ. Дефініцій понять у концепції не наведено. Пріоритетом є підвищення рівня готовності та реагування на значні кібератаки на національному рівні, оцінка безпеки ІКТ, які мають вирішальне значення для функціонування критичних інфраструктур, збільшення людських та інтелектуальних ресурсів тощо.

Стратегія кібербезпеки Бангладешу (The National Cybersecurity Strategy of Bangladesh) була прийнята 2014 року. Метою документу є створення цілісного уявлення про Бангладеш як про безпечну та процвітаючу державу у координації уряду, приватного сектору, громадян та міжнародних зусиль в обороні кіберпростору до 2021 року. У документі визначено такі принципи забезпечення кібербезпеки: дослідження атак; внутрішня і зовнішня співпраця; створення законів, які взаємодіють між собою і застосовуються глобально; створення організацій кібербезпеки; тренування навиків персоналу; визначення правової та оперативної основи для комплексної та повної координації державного партнерства з приватним сектором у сфері кібербезпеки; захист урядової інфраструктури; можливість вчасного реагування на інциденти ІБ. Дефініцій понять у документі не наведено. Крім того, визначено загрози від шпіонажу до фішингу, DoS-атаки, інші кіберзлочини. Визначено такі пріоритети держави: покращення законодавства; технічні і процедурні заходи (організаційні структури і політика кіберзлочинності, спостереження, оповіщення і реагування на інциденти, а також створення загальної та універсальної цифрової системи

ідентифікації); організаційні структури (фокус на національні межі протоколів безпеки, стандартів і схем акредитації ПЗ).

Концепція кібербезпеки Індії (National Cyber Security Policy) була затверджена 2013 року. Метою документу є побудова захищеного і стійкого кіберпростору, захист інформації та інформаційної інфраструктури в кіберпросторі, створення можливості для реагування і запобігання кіберзагрозам, зменшення уразливостей і мінімізація шкоди від кіберінцидентів. Завдання кібербезпеки, які є пріоритетними для Індії – створення безпечної кіберекосистеми; створення системи ресурсів; заохочення відкритих стандартів; збільшення можливостей регулюючих структур; створення механізмів захисту від нових загроз, управління уразливостями реагування на загрози безпеці; захист електронних урядових сервісів; захист і стійкість критичної інформаційної інфраструктури; розвиток людських ресурсів; поширення інформації та співпраця тощо.

IV. Держави Америки. Стратегія кібербезпеки США (International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World) 2011 року визначає контекст підходу для розуміння пріоритетів держави, способів досягнення її безпечного кіберпростору та боротьби з кібератаками. У якості загроз визначено шантаж та вимагання коштів, шахрайство, крадіжки та експлуатація дітей, крадіжка інтелектуальної власності. Дефініцій понять у документі не наведено. Забезпечення кібербезпеки держави базується на таких принципах: дотримання основних свобод; приватність особистого життя; вільний потік інформації; повага до різних форм власності; захист від злочинів; відповідна законодавча база; взаємодія на глобальному рівні; багатостороннє управління. Пріоритетами США у цій сфері є захист інтелектуальної власності, у тому числі комерційних таємниць; взаємодія та відповідність технічних стандартів, встановлених експертами; сприяння співробітництву та партнерству; управління інцидентами, стійкість і можливості відновлення інформаційної інфраструктури; проведення консультацій з промисловим сектором; участь у розробці міжнародних стандартів; фокусування законів про кіберзлочинність на боротьбі з

незаконною діяльністю; створення і розширення вже існуючих військових союзів для протистояння потенційним загрозам в кіберпросторі; заохочення міжнародного співробітництва для ефективного комерційного захисту конфіденційних даних.

Концепція кібербезпеки Канади (Action Plan 2010-2015 for Canada's Cyber Security Strategy) 2013 року призначена для спрямування зусиль уряду для створення безпечного кіберпростору для канадців. У документі визначено такі принципи забезпечення кібербезпеки: захист державних систем; співпраця з метою захисту ключових систем від кібератак, що знаходяться за межами федерального уряду; забезпечення безпеки канадців в онлайн-мережі. У якості загроз визначено різного роду кіберзлочини та кібератаки. Дефініцій понять не наведено. Пріоритетними визначено наступні дії: безпечне зберігання особистої інформації канадців онлайн, а також ІКТ, інфраструктури уряду; боротьба з кіберзлочинністю; посилення безпеки кіберсистем федерального рівня та підвищення інформованості суспільства в галузі кібербезпеки.

Стратегія кібербезпеки Ямайки (Jamaica National Cyber Security Strategy) була прийнята 2015 року. Мета документу – взяти до уваги забезпечення ведення онлайн та оффлайн справ. Визначено такі загрози: викрадення персональних даних; фішинг; підроблені банківські застосунки; атаки на комп'ютерні дані та системи; поширення дитячого сексуального насильства; шахрайські Інтернет-аукціони, віруси, ботнети, внутрішні загрози тощо. Наведено дефініції понять: ботнет, критична інфраструктура, кіберзлочин, кібербезпека, ІБ, CERT, відмова в обслуговуванні, фішинг, саморегулювання, несанкціонований доступ, несанкціонована зміна. Пріоритети держави у цій сфері – інформованість населення в сфері кібербезпеки; розвиток культури кібербезпеки; захист національної критичної інфраструктури; тренінги для громадськості тощо.

Отже, проаналізувавши стратегії та з огляду на постійне збільшення ризику виникнення нових кіберзагроз та їх еволюції, збільшення впливу на особу, суспільство, кожній державі необхідно мати продуману та чітко сформульовану, комплексну стратегію кібербезпеки. Оскільки загрози такого типу не мають

кордонів, потрібно постійно підтримувати тісне міжнародне співробітництво, що є необхідним не лише для підготовки до кібератак, а й для своєчасного реагування на них. Провівши аналіз ключових положень національних стратегій кібербезпеки держав світу та врахувавши сучасний стан цієї галузі в Україні, доцільно сформулювати практичні рекомендації для нашої держави (див. другий розділ роботи).

2.4. FMECA як сучасний ефективний підхід у ризик-менеджменті

Основні програмні засоби для управління ризиками кібербезпеки включають:

- SIEM (Security Information and Event Management): Інтеграційні рішення, які збирають та аналізують дані з різних систем, забезпечуючи виявлення та реагування на загрози в режимі реального часу. Приклади: Splunk, IBM QRadar, ArcSight.
- GRC (Governance, Risk, and Compliance): Платформи, які допомагають керувати політиками та контролями безпеки, проводити аудити, керувати ризиками та відповідати вимогам регуляторів. Приклади: RSA Archer, ServiceNow GRC.
- Платформи управління вразливостями: Інструменти для сканування мережі, систем та застосунків на предмет вразливостей, з подальшим аналізом та рекомендаціями щодо їх усунення. Приклади: Tenable Nessus, Rapid7 InsightVM, Qualys.
- EDR (Endpoint Detection and Response): Засоби моніторингу та реагування на загрози на кінцевих пристроях, таких як комп'ютери та сервери. Приклади: CrowdStrike Falcon, Carbon Black, Microsoft Defender.
- Платформи управління конфігураціями: Інструменти, які перевіряють, чи відповідає конфігурація систем та мереж політикам безпеки та стандартам, допомагаючи виявити можливі ризики. Приклади: Tripwire, Chef InSpec.

- DLP (Data Loss Prevention): Засоби запобігання витоку даних, які допомагають виявляти та захищати конфіденційну інформацію, контролюючи її переміщення по мережі або на пристрої. Приклади: Symantec DLP, McAfee Total Protection.
- Платформи управління привілейованим доступом (PAM): Інструменти, що обмежують доступ до критично важливих ресурсів лише для авторизованих користувачів та забезпечують моніторинг їхньої активності. Приклади: CyberArk, BeyondTrust.
- SOAR (Security Orchestration, Automation, and Response): Інтегровані платформи, що об'єднують різні засоби кібербезпеки для автоматизації рутинних завдань, прискорення реагування на інциденти та покращення співпраці між командами. Приклади: Splunk Phantom, IBM Resilient. Використання цих засобів дозволяє організаціям забезпечити комплексний підхід до управління ризиками кібербезпеки, допомагаючи виявляти, оцінювати та мінімізувати ризики ефективніше.

Крім використання програмних засобів, існують різні методики управління ризиками кібербезпеки. Ось кілька основних підходів:

- NIST Cybersecurity Framework: Структура Національного інституту стандартів і технологій США надає п'ятиступеневий підхід до управління ризиками: ідентифікувати, захищати, виявляти, реагувати та відновлювати. Він також включає глибокі рекомендації щодо кожного етапу.
- ISO/IEC 27001: Стандарт міжнародної організації з сертифікації забезпечує систему управління інформаційною безпекою (ISMS), що включає ідентифікацію, оцінку та пом'якшення ризиків.
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation): Методологія аналізу кіберризиків, яка фокусується на ідентифікації критичних активів, загроз та вразливостей. Вона складається з декількох етапів, включаючи оцінку безпеки та визначення пріоритетів ризиків.

- FAIR (Factor Analysis of Information Risk): Модель, що дозволяє оцінити фінансові наслідки кіберризиків, допомагаючи встановити пріоритети в управлінні безпекою з точки зору впливу на бізнес.
- STRIDE: Модель загроз від Microsoft для ідентифікації та категоризації потенційних загроз за типами: підміна (Spoofing), спотворення (Tampering), відмова (Repudiation), розкриття (Information Disclosure), відмова в обслуговуванні (Denial of Service) та підвищення привілеїв (Elevation of Privilege).
- Threat Modeling: Методика моделювання загроз, яка допомагає створити сценарії можливих атак на систему та розробити ефективні контрзаходи.
- Risk Register: Використання реєстру ризиків для систематичного документування та відстеження виявлених ризиків, а також пов'язаних з ними стратегій управління.
- FMEA/FMECA (Failure Modes and Effects Analysis / Failure Modes, Effects, and Criticality Analysis): Методи визначення можливих типів збоїв у системі, оцінки їх впливу та ймовірності виникнення для планування заходів з пом'якшення ризиків.

Розглянемо більш детально останній підхід.

FMECA (Failure Modes, Effects, and Criticality Analysis) є методологією аналізу ризиків, яка може бути ефективно застосована для управління ризиками кібербезпеки. Ось основні кроки, як її використовувати [49, 53, 69, 85, 86]:

1. Визначення системи: Спершу необхідно визначити систему, яка підлягає аналізу. Це може бути окрема програма, мережа, або інша інформаційна система.

2. Ідентифікація компонентів: Складіть список всіх компонентів системи, які можуть бути потенційними точками вразливості.

3. Виявлення можливих збоїв (Failure Modes): Для кожного компонента визначте можливі збої, які можуть виникнути в результаті кіберзагроз. Це можуть бути збої через атаки програм-вимагачів, фішингові атаки або несанкціонований доступ.

4. Аналіз впливів (Effects Analysis): Оцініть вплив кожного типу збою на компонент і всю систему загалом. Враховуйте, як збої можуть призвести до втрати конфіденційності, цілісності або доступності даних.

5. Аналіз критичності (Criticality Analysis): Розрахуйте критичність кожного збою, враховуючи частоту його виникнення і серйозність впливу на систему. Це допоможе визначити, які збої мають найвищий пріоритет для усунення.

6. Розробка плану пом'якшення ризиків: На основі аналізу критичності розробіть плани пом'якшення ризиків для пріоритетних збоїв. Це можуть бути заходи з резервного копіювання даних, покращення захисту від фішингу або впровадження системи багатофакторної автентифікації.

7. Оцінка ефективності: Регулярно переглядайте та оновлюйте FMECA, щоб відображати нові загрози і вразливості. Переконайтеся, що заходи пом'якшення ризиків дієві та ефективні. Ця методологія дозволяє отримати структуроване уявлення про ризики кібербезпеки, оцінити критичність кожного ризику та запровадити відповідні заходи для захисту інформаційних систем.

Переваги використання FMECA над іншими підходами в управлінні ризиками кібербезпеки полягають у кількох аспектах [69, 85, 86]:

1. Систематичність: FMECA забезпечує структурований та детальний аналіз усіх можливих збоїв і їхніх наслідків, що дозволяє не пропустити потенційні загрози та вразливості.

2. Пріоритезація ризиків: Аналіз критичності допомагає оцінити кожен збій з точки зору ймовірності виникнення та впливу на систему. Це дозволяє визначити пріоритетні ризики для негайного вирішення, оптимізуючи використання ресурсів.

3. Ідентифікація першопричин: FMECA дозволяє виявити кореневі причини збоїв та запобігти їх повторенню шляхом усунення основних вразливостей.

4. Планування заходів: Завдяки аналізу можливих наслідків кожного збою, FMECA допомагає створити конкретні плани пом'якшення ризиків та заходи з попередження майбутніх атак.

5. Універсальність: Цей підхід можна адаптувати до різних типів систем та індустрій, використовуючи єдиний підхід для оцінки ризиків і для малих, і для великих організацій.

6. Виявлення ланцюгових реакцій: Аналіз дозволяє зрозуміти взаємозв'язки між компонентами системи та передбачити, як один збій може призвести до інших проблем.

7. Динамічність: FMECA може бути інтегрована в постійний процес оцінки ризиків, що дозволяє регулярно переглядати та оновлювати ризик-профілі.

Ці переваги роблять FMECA ефективним інструментом для управління ризиками кібербезпеки у складних та критичних системах. З огляду на це, в наступному розділі буде розроблятись і досліджуватись метод управління ризиками кібербезпеки саме на основі FMECA [49, 53].

2.5. Висновки до розділу 2

У цьому розділі було досліджено основні програмні засоби для управління ризиками кібербезпеки, зокрема SIEM (Security Information and Event Management), GRC (Governance, Risk, and Compliance), Платформи управління вразливостями, EDR (Endpoint Detection and Response), Платформи управління конфігураціями, DLP (Data Loss Prevention), Платформи управління привілейованим доступом (PAM), SOAR (Security Orchestration, Automation, and Response).

Проаналізовано стратегії і концепції кібербезпеки та управління ризиками в різних державах. Ідентифіковано методики управління ризиками кібербезпеки, серед яких NIST Cybersecurity Framework, ISO/IEC 27001, OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), FAIR (Factor Analysis of Information Risk), FMEA/FMECA (Failure Modes and Effects Analysis / Failure Modes, Effects, and Criticality Analysis), STRIDE, Threat Modeling, Risk Register.

РОЗДІЛ 3
ПРАКТИЧНІ АСПЕКТИ АНАЛІЗУ ТА ОЦІНЮВАННЯ РИЗИКІВ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ОБЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

3.1. Практичний підхід до побудови системи управління інформаційною безпекою

В світовій практиці є розроблені моделі систем управління ІБ, наприклад, «Information Security Management Maturity Model» (ISM3 від ISECOM) або Systems Security Engineering Capability Maturity Model» або стандарт NIST SP800-33. Існує також ряд міжнародних стандартів. Серед них: ISO/IEC 17799:2005 [5] і перший стандарт нової серії ISO/IEC 27001, що прийшов на зміну англійському стандарту BS7799-2:2002 [50-52].

Проте пряме використання цих моделей і стандартів ISO/IEC 27001 та ISO/IEC 17799:2005 для побудови СУІБ дуже складно. Вони або дуже конкретизовані, а в будь-якій організації, як правило, вже існує певна система процесів, ролей, організаційно-розпорядчих документів інформаційної безпеки, які необхідно інтегрувати в систему управління ІБ, або навпаки, рекомендації носять дуже загальний характер.

Підхід до побудови систем управління ІБ, включаючи розробку процесів забезпечення ІБ, базується на наступних методичних рекомендаціях і директивах:

- рекомендації ITIL (Information Technology Infrastructure Library, кращий світовий досвід в галузі організації роботи IT-служби), а також моделі управління IT-ресурсами та IT-сервісами Microsoft Operations Framework (MOF);
- рекомендації Microsoft Service Management Function (SMF);
- стандарт ISO 27001.

Доцільність використання рекомендацій з управління IT-ресурсами та IT-послугами (і в першу чергу процесів управління інцидентами, змінами) при

побудові СУІБ обумовлена тим, що процеси забезпечення інформаційної безпеки нерозривно пов'язані з процесами захисту, а тому управління інформаційними системами повинні бути тісно інтегровані з процесами управління ІТ.

Інтеграція процесу управління безпекою в систему процесів управління ІТ-ресурсами та ІТ-послугами і застосування сервісно-ресурсного підходу при побудові СУІБ (коли забезпечення ІБ розглядається як сервіс з певним рівнем якості, надання якої забезпечується певними фінансовими, технічними, людськими ресурсами) дає цілий ряд переваг.

При побудові СУІБ необхідно використовувати наведені вище рекомендації і стандарти і на їх основі будувати процесну модель СУІБ, що містить три рівні процесів:

1. Процеси стратегічного рівня – управління ризиками, управління безперервністю ведення бізнесу, розробка і розвиток політики ІБ верхнього рівня.

2. Тактичні процеси – розробка і розвиток процедур ІБ, технічної архітектури системи ІБ, класифікація ІТ-ресурсів, моніторинг і управління інцидентами.

3. Процеси операційного рівня – управління доступом, управління мережною безпекою, перевірка відповідності.

Визначаються взаємозв'язки процесів. В результаті ми одержуємо процесно-сервісну трьохрівневу модель системи управління ІБ, відповідно вимогам стандарту ISO 27001, на яку накладається ролева модель.

3.2. Основні поняття та визначення ризик-менеджменту

Для покращення розуміння співвідношення понять, розглянемо безові визначення згідно відомих джерел [24, 55, 62, 70-76]:

Загроза – сукупність умов і факторів, які можуть стати причиною порушення цілісності, доступності й конфіденційності інформації.

Вразливість – слабкість у системі захисту, що уможливлює реалізацію загрози.

Ризик порушення безпеки – можливість реалізації загрози.

Базовий аналіз ризиків – аналіз ризиків, проведений відповідно до вимог базового рівня захищеності. Прикладні методи аналізу ризиків, орієнтовані на даний рівень, звичайно не враховують цінність ресурсів і не оцінюють ефективність контрзаходів. Методи даного класу застосовуються у випадках, коли до інформаційної системи не пред'являється підвищених вимог в області ІБ.

Повний аналіз ризиків – аналіз ризиків для інформаційних систем що пред'являють підвищені вимоги в області ІБ (більше високі, чим базовий рівень захищеності). Містить у собі визначення цінності інформаційних ресурсів, оцінку загроз і вразливостей, вибір адекватних контрзаходів, оцінку їхньої ефективності.

Оцінка ризиків – ідентифікація ризиків, вибір параметрів для їхнього опису й одержання оцінок по цих параметрах.

Клас ризиків – безліч загроз ІБ, виділених по певній ознаці (наприклад, що ставляться до певної підсистеми або типу ресурсу).

Аналіз ризиків – це процес визначення загроз, вразливостей і можливого збитку безпеки корпоративної інформаційної системи.

Ціль аналізу ризиків полягає в тому, щоб виявити існуючі ризики й оцінити їхню величину (дати їм кількісну оцінку). Ризик визначається ймовірністю заподіяння збитку й величиною збитку, що наноситься ресурсам корпоративної інформаційної системи (КІС), у випадку здійснення загрози безпеці. Визначення набору адекватних контрзаходів здійснюється в ході керування ризиками.

3.3. Основні підходи до аналізу ризиків кібербезпеки

Вибір підходу до аналізу ризиків цілковито залежить від рівня вимог і характеру прийнятих до уваги загроз.

Розрізняють два рівні вимог:

- мінімальні вимоги до режиму ІБ;

- підвищені вимоги до режиму ІБ.

Мінімальним вимогам до режиму ІБ відповідає базовий рівень інформаційної безпеки. Звичайним середовищем використання цього рівня є типові проектні рішення. Аналіз ризиків проводиться за спрощеною схемою: розглядається стандартний набір найпоширеніших загроз безпеки без оцінки їхньої ймовірності. Існує ряд стандартів і специфікацій, у яких розглядається мінімальний (типовий) набір найбільш імовірних загроз, таких як віруси, збої в роботі устаткування, несанкціонований доступ.

Для нейтралізації цих загроз обов'язково повинні бути прийняті контрзаходи незалежно від ймовірності їхнього здійснення й уразливості ресурсів. Тому характеристики загроз на базовому рівні розглядати не обов'язково.

Підвищені вимоги до режиму ІБ застосовуються в тих випадках, коли порушення режиму інформаційної безпеки призводять до важких наслідків й базовий рівень вимог до режиму ІБ є недостатнім.

Для того щоб сформулювати підвищені вимоги до режиму ІБ, необхідно:

- визначити цінність ресурсів;

- доповнити стандартний набір списком загроз, актуальних для досліджуваної інформаційної системи;

- оцінити ймовірності загроз;

- визначити вразливість ресурсів.

Основні етапи аналізу ризиків:

- ідентифікація ключових ресурсів КІС;

- визначення важливості тих або інших ресурсів;

- ідентифікація існуючих загроз безпеки й вразливостей, що роблять можливим здійснення загроз;

- обчислення ризиків, пов'язаних зі здійсненням загроз безпеки.

Ресурси КІС діляться на три категорії:

- інформаційні ресурси;

- програмне забезпечення;

- технічні засоби (файлові сервери, робочі станції, мости, маршрутизатори).

Вартість ресурсу визначається величиною збитку, що виникає у випадку порушення конфіденційності, цілісності або доступності цього ресурсу. У ході оцінки вартості ресурсів визначається величина можливого збитку для кожної категорії ресурсів, наприклад:

- дані були розкриті, змінені, вилучені або стали недоступні;
- апаратури була ушкоджена або зруйнована;
- порушена цілісність ПЗ.

3.4. Інструментарій для оцінки інформаційних ризиків

Метод *CRAMM* (CCTA Risk Analysis and Managment Method) був розроблений Агентством з комп'ютерів та телекомунікацій Великобританії (Central Computer and Telecommunications Agency) за завданням Британського уряду й узятий на озброєння як державний стандарт. Він використовується, починаючи з 1985 р., урядовими й комерційними організаціями Великобританії. За цей час CRAMM набув популярності в усьому світі. Фірма Insight Consulting Limited займається розробкою й супроводом однойменного програмного продукту, що реалізує метод CRAMM.

CRAMM дозволяє, крім аналізу ризиків, вирішувати також і ряд інших аудиторських завдань, включаючи:

- проведення огляд ІС і випуск супровідної документації на всіх етапах його проведення;
- проведення аудиту, відповідно до вимог Британського уряду, а також стандарту BS 7799:1995;
- розробка політики безпеки й плану забезпечення безперервності бізнесу.

В основі методу CRAMM лежить комплексний підхід до оцінки ризиків, поєднуючи кількісні і якісні методи аналізу. Метод є універсальним і підходить як для великих, так і для дрібних організацій, як урядового, так і комерційного сектора. Версії програмного забезпечення CRAMM, орієнтовані на різні типи організацій, відрізняються один від одного своїми базами знань (profiles). Для комерційних організацій є Комерційний профіль (Commercial Profile), для урядових організацій – Урядовий профіль (Government profile). Урядовий варіант профілю, також дозволяє проводити аудит на відповідність вимогам американського стандарту ITSEC.

Використовуючи метод CRAMM стає можливим одержання економічного обґрунтування витрат організації на забезпечення інформаційної безпеки й безперервності бізнесу. Економічно обґрунтована стратегія керування ризиками дозволяє, в кінцевому результаті, заощаджувати засоби, уникаючи невиправданих витрат. CRAMM припускає поділ всієї процедури на три послідовних етапи. Завданням першого етапу є відповідь на питання: «Чи досить для захисту системи застосування засобів базового рівня, що реалізують традиційні функції безпеки, або необхідне проведення більш детального аналізу?» На другому етапі виробляється ідентифікація ризиків й оцінюється їхня величина. На третьому етапі вирішується питання про вибір адекватних контрзаходів.

Методика CRAMM для кожного етапу визначає набір вихідних даних, послідовність заходів, анкети для проведення інтерв'ю, списки перевірки й набір звітної документації.

Програмний пакет RiskWatch є потужним засобом аналізу й керування ризиками. У сімейство RiskWatch входять програмні продукти для проведення різних видів аудита безпеки. Воно містить у собі наступні засоби аудиту й аналізу ризиків:

- RiskWatch for Physical Security – для фізичних методів захисту ІС;

- RiskWatch for Information Systems – для інформаційних ризиків;

- HIPAA-WATCH for Healthcare Industry – для оцінки відповідності вимогам стандарту HIPAA (US Healthcare Insurance Portability and Accountability Act);

- RiskWatch RW17799 for ISO 17799 – для оцінки вимогам стандарту ISO 17799.

У методі RiskWatch як критерії для оцінки й керування ризиками використовуються пророкування річних втрат (Annual Loss Expectancy, ALE) та оцінка повернення від інвестицій (Return on Investment, ROI). Сімейство програмних продуктів RiskWatch має масу переваг,а саме: допомагає провести аналіз ризиків і зробити обґрунтований вибір мір і засобів захисту. Методика використана в програмі містить у собі 4 фази.

На відміну від CRAMM, програма RiskWatch більше орієнтована на точну кількісну оцінку співвідношення втрат від загроз безпеки й витрат на створення системи захисту. Треба також відзначити, що в цьому продукті ризики в сфері інформаційної й фізичної безпеки комп'ютерної мережі підприємства розглядаються разом. В основі продукту RiskWatch перебуває методика аналізу ризиків, що складається із чотирьох етапів.

Перший етап – визначення предмета дослідження. Тут описуються такі параметри, як тип організації, склад системи, яку досліджують, базові вимоги в області безпеки. Для полегшення роботи аналітика, у шаблонах, що відповідають типу організації («комерційна інформаційна система», «державна/військова інформаційна система»), є списки категорій ресурсів, що захищають, втрат, загроз, уразливостей і заходів захисту. З них потрібно вибрати ті, що реально присутні в організації.

Наприклад, категорії втрат:

- затримки й відмова в обслуговуванні;
- розкриття інформації;
- прямі втрати (наприклад, від знищення устаткування вогнем);
- життя й здоров'я (персоналу, замовників);
- зміна даних;
- непрямі втрати (наприклад, витрати на відновлення);
- репутація.

Другий етап – уведення даних, що описують конкретні характеристики системи. Дані можуть вводитися вручну або імпортуватися зі звітів, створених інструментальними засобами дослідження вразливості комп'ютерних мереж. На даному етапі докладно описуються ресурси, втрати й класи інцидентів. Класи інцидентів отримують шляхом зіставлення категорії втрат і категорії ресурсів. Для виявлення можливих уразливостей використовується опитувальна книга, база якої містить більше 600 питань, які пов'язані з категоріями ресурсів. Задається частота виникнення кожної з виділених загроз, ступінь вразливості й цінність ресурсів. Все це використовується надалі для розрахунку ефекту від впровадження засобів захисту.

Третій етап – кількісна оцінка. На цьому етапі розраховується профіль ризиків, і вибираються міри забезпечення безпеки. Спочатку встановлюються зв'язки між ресурсами, втратами, загрозами й уразливостями, виділеними на попередніх кроках дослідження (ризик описується сукупністю цих чотирьох параметрів). RiskWatch містить у собі бази з оцінками LAFE й SAFE, а також узагальнений опис різних типів засобів захисту.

Четвертий етап – генерація звітів.

Розрізняють такі типи звітів:

- короткі підсумки;
- повні та короткі звіти про елементи, описані на першій та другій стадіях.
- звіт від вартості ресурсів, що захищають, і очікуваних втратах від реалізації загроз.
- звіт про загрози й міри протидії.
- звіт про результати аудита безпеки.

Компанія MethodWare розробила свою власну методику оцінки й керування ризиками й випустила ряд відповідних інструментальних засобів.

До цих засобів відносяться:

- ПЗ аналізу й керування ризиками Operational Risk Builder й Risk Advisor. Методика відповідає австралійському стандарту Australian/New Zealand Risk Management Standard (AS/NZS 4360:1999) і стандарту ISO17799.

- ПЗ керування життєвим циклом інформаційної технології відповідно до Cobi Advisor 3rd Edition (Audit) і Cobi 3rd Edition Management Advisor. У посібниках по користуванню Cobi істотне місце приділяється аналізу й керуванню ризиками.

- ПЗ для автоматизації побудови різноманітних опитувальних листів Questionnaire Builder.

Компоненти:

Опис ризиків. Задається матриця ризиків на основі деякого шаблона. Ризики оцінюються по якісній шкалі й поділяються на прийнятні та неприйнятні. Потім вибираються керуючі впливи контрзаходу з обліком зафіксованої раніше системи критеріїв, ефективності контрзаходів й їхньої вартості. Вартість й ефективність також оцінюються в якісних шкалах.

Опис загроз. На початку формується список загроз. Загрози певним чином класифікуються, потім описується зв'язок між ризиками й загрозами. Опис також робиться на якісному рівні й дозволяє зафіксувати їхній взаємозв'язок.

Опис втрат. Описуються події (наслідки), пов'язані з порушенням режиму інформаційної безпеки. Втрати оцінюються в обраній системі критеріїв.

Аналіз результатів. У результаті побудови моделі можна сформувати докладний звіт (близько 100 розділів), подивитися на екрані агреговані опису у вигляді графів-ризиків.

Розглянута методика дозволяє автоматизувати різні аспекти керування ризиками компанії. При цьому оцінки ризиків даються в якісних шкалах. Докладний аналіз факторів ризиків не передбачений. Сильною стороною розглянутої методики є можливість опису різних зв'язків, адекватний облік багатьох факторів ризику й істотно менша трудомісткість у порівнянні з CRAMM.

Методика аналізу ризиків, розроблена корпорацією Microsoft. Згідно цієї методики ризик розглядається, як можливість зазнати збитків через порушення

безпеки мережі зсередини або ззовні. Ефективне керування ризиками підприємства в сфері комп'ютерної безпеки вимагає виконання чотирьох етапів:

- розпізнавання (ідентифікація) ризиків;
- визначення розміру ризику;
- розробка плану керування ризиками;
- поточний контроль і керування ризиками.

При обмеженому часі як спосіб ідентифікації ризиків рекомендується застосовувати методики одержання знань від експертів, зокрема, метод «мозкового штурму». Для кожного виявленого ризику потрібно оцінити його вартість (тобто визначити збиток у тому випадку, якщо розглянута небажана подія відбулася) і ймовірність виникнення ризику.

3.5. Розроблення методу оцінювання ризиків кібербезпеки інформаційних систем ОКІ на основі FMECA

На основі FMECA було побудовано удосконалений метод визначення рівня важливості об’єктів КІІ, який реалізується в такі етапи:

1. Визначення компонентів системи та встановлення рівня деталізації;
2. Визначення функцій кожного виявленого компонента системи;
3. Визначення переліку можливих переривань роботи кожного компонента системи;
4. Визначення наслідків кожного можливого переривання роботи;
5. Ідентифікація ознак виявлення переривань роботи;
6. Ідентифікація способів виявлення переривань роботи;
7. Побудова тривимірної матриці критичності;
8. Розрахунок рангу критичності ймовірних переривань;
9. Виділення переліку найбільш значущих (критичних) переривань роботи;
10. Формування переліку коригувальних заходів;

11. Складання звіту про ризики ОКІ.

Визначимо вхідні дані методу:

- структурно-функціональні схеми аналізованої системи і її компонентів або етапи процесу;
- інформація про функціонування кожного етапу процесу або компонента системи;
- докладний опис всіх параметрів, які можуть впливати на функціонування системи;
- відомості про результати переривання роботи;
- хронологічні дані про переривання роботи, включаючи доступні дані про інтенсивність переривання роботи.

Реалізувавши всі зазначені етапи методу, отримаємо такі *вихідні дані*:

- перелік видів переривань роботи для кожного компонента системи;
- інформація про причини виникнення та наслідки переривання роботи для кожного компонента системи;
- матриця критичності, яка за зібраними попередніми даними графічно відображає критичність компонентів системи;
- діаграма Парето, яка візуально зображує рівень критичності в середині системи та дає можливість порівняти декілька різних систем;
- результати ранжування – перелік найбільш значущих (критичних) переривань роботи; причинно-наслідкова діаграма Ісікави, що дозволяє виділити пріоритетні напрямки розробки коригувальних заходів для переривань роботи;
- список коригувальних заходів для зменшення критичності найбільш значущих переривань роботи.

Умови функціонування ІС швидко і суттєво змінюються із впровадженням сучасних технологій обробки, передачі та збереження інформації, що забезпечують підвищення рівня захисту. Найбільшого захисту потребують ресурси ОКІ. Розглянемо детально кожен з етапів реалізації запропонованого методу, а для оцінювання критичності та ризиків ОКІ оберемо з кожної із категорій одну систему/підсистему.

Етап 1 – Визначення компонентів системи та встановлення рівня деталізації

На основі структурно-функціональних схем аналізованої ІС складається перелік усіх компонентів системи у процесі функціонування. Встановлюється мінімальний рівень деталізації для їх опису та декомпозиції.

Цей етап реалізується у 5 кроків:

Крок 1. Введемо повну множину ОКІ $\mathbf{S}$:

$$\mathbf{S} = \{\bigcup_{i=1}^{n} \mathbf{S}_i\} = \{\mathbf{S}_1, \mathbf{S}_2, \ldots, \mathbf{S}_n\}, \tag{3.1}$$

де $\mathbf{S}_i \subseteq \mathbf{S}$, $(i = \overline{1,n})$ – клас систем ОКІ, n – загальна кількість класів систем.

Крок 2. Множина $\mathbf{S}_i$ може бути представлена у вигляді множини систем:

$$\mathbf{S}_i = \{\bigcup_{j=1}^{m_i} \mathbf{S}_{ij}\} = \{\mathbf{S}_{i1}, \mathbf{S}_{i2}, ..., \mathbf{S}_{im_i}\}, \tag{3.2}$$

де $\mathbf{S}_{ij} \subseteq \mathbf{S}_i$ $(i = \overline{1,n},\ j = \overline{1,m_i})$ – системи i-го класу, m_i – кількість систем i-го класу.

З урахуванням (3.2), вираз (3.1) можна представити у такому вигляді:

$$\begin{gathered}\mathbf{S} = \{\bigcup_{i=1}^{n} \mathbf{S}_i\} = \{\bigcup_{i=1}^{n} \{\bigcup_{j=1}^{m_i} \mathbf{S}_{ij}\}\} = \{\{\mathbf{S}_{11}, \mathbf{S}_{12}, ..., \mathbf{S}_{1m_1}\}, \\ \{\mathbf{S}_{21}, \mathbf{S}_{22}, ..., \mathbf{S}_{2m_2}\}, ..., \{\mathbf{S}_{n1}, \mathbf{S}_{n2}, ..., \mathbf{S}_{nm_n}\}\}, (i = \overline{1,n},\ j = \overline{1,m_i}).\end{gathered} \tag{3.3}$$

Крок 3. Множина $\mathbf{S}_{ij}$ може бути представлена у вигляді множини підсистем:

$$\mathbf{S}_{ij} = \{\bigcup_{k=1}^{r_{ij}} S_{ijk}\} = \{S_{ij1}, S_{ij2}, ..., S_{ijr_{ij}}\}, \tag{3.4}$$

де $S_{ijk} \subseteq \mathbf{S}_{ij}$ $(i = \overline{1,n},\ j = \overline{1,m_i},\ k = \overline{1,r_{ij}})$ – множина підсистем системи $\mathbf{S}_{ij}$, r_{ij} – кількість підсистем ij-го класу.

З урахуванням (3.4), вираз (3.3) можна представити у такому вигляді:

$$\mathbf{S} = \{\bigcup_{i=1}^{n} \mathbf{S}_i\} = \{\bigcup_{i=1}^{n} \{\bigcup_{j=1}^{m_i} \mathbf{S}_{ij}\}\} = \{\bigcup_{i=1}^{n} \{\bigcup_{j=1}^{m_i} \{\bigcup_{j=1}^{r_{ij}} S_{ijk}\}\}\} =$$

$$= \{\{\{S_{111}, S_{112}, ..., S_{11r_{11}}\}, \{S_{121}, S_{122}, ..., S_{12r_{12}}\}, ..., \{S_{1m_11}, S_{1m_12}, ..., S_{1m_1r_{nm_1}}\}\},$$

$$\{\{S_{211}, S_{212}, ..., S_{21r_{21}}\}, \{S_{221}, S_{222}, ..., S_{22r_{22}}\}, ..., \{S_{2m_21}, S_{2m_22}, ..., S_{2m_2r_{nm_2}}\}\}, ...,$$

$$\{\{S_{n11}, S_{n12}, ..., S_{n1r_{n1}}\}, \{S_{n21}, S_{n22}, ..., S_{n2r_{n2}}\}, ..., \{S_{nm_11}, S_{nm_12}, ..., S_{nm_nr_{nm_n}}\}\}\}. \quad (3.5)$$

Крок 4. Введемо множину компонентів $\mathbf{C}$, що характеризуватиме $\mathbf{S}_{ij} / S_{ijk}$:

$$\mathbf{C} = \{\bigcup_{i=1}^{b} C_i\} = \{C_1, C_2, ..., C_b\}, \quad (3.6)$$

де $C_i \subseteq \mathbf{C}$, $(i = \overline{1,b})$ – компоненти, b – загальна кількість компонентів ij -ї системи.

Крок 5. Встановимо мінімальний рівень деталізації $(Det_{\min})$ для опису та декомпозиції системи. Метою аналізу S_{ij} / S_{ijk} є визначення рівня критичності можливих видів переривань роботи компонентів, що спричиняють втрату їх функціональності (у концепції управління безперервністю бізнесу BCP/DRP за ISO 22301), з'ясування їх причин виникнення, наслідків, способів виявлення та рекомендацій щодо зменшення їх критичності.

Етап 2 – Визначення функцій кожного виявленого компонента системи

На основі структурно-функціональних схем ОКІ обраного рівня деталізації визначимо функції F_i, які виконує кожен з перелічених компонентів C_i. Представимо повну множину функцій $\mathbf{F}$ у такому вигляді:

$$\mathbf{F} = \{\bigcup_{i=1}^{l} F_i\} = \{F_1, F_2, ..., F_l\}, \quad (3.7)$$

де $F_i \subseteq \mathbf{F}$, $(i = \overline{1,l})$ – функції компонентів ОКІ, l –загальна кількість функцій.

Етап 3 – Визначення переліку можливих переривань роботи кожного компонента системи

Для кожного ідентифікованого компонента C_i на основі наявних класифікаторів переривання роботи (i-го класу ОКІ), апріорних даних, інженерного аналізу, досвіду і знань експертів формується перелік можливих переривань роботи. Для визначення переліку можливих переривань роботи

кожного компонента C_i введемо множину переривань роботи **D** у наступному вигляді:

$$\mathbf{D} = \{\bigcup_{i=1}^{p} D_i\} = \left\{D_1, D_2, ..., D_p\right\}, \tag{3.8}$$

де $D_i \subseteq \mathbf{D}$, $(i = \overline{1, p})$ – переривання роботи компонента C_i, p – загальна кількість переривань роботи.

Етап 4 – Визначення наслідків кожного можливого переривання роботи

Для кожного виду D_i обраного компонента C_i визначаються його можливі наслідки на даному та наступних (сусідніх/вищих) рівнях. Якщо наслідки D_i компонентів нижчого рівня не можуть бути виражені у вигляді впливу на функціонування компонентів розглянутого рівня, то такі компоненти розглядаються як самостійні види переривань на цьому рівні.

Наслідки D_i компонентів за впливом на системи/класу ОКІ вищих рівнів деталізації класифікуються на:

- локальні, які викликають переривання роботи лише C_i;
- проміжні, пов'язані з перериванням роботи компонентів рівня S_{ij};
- кінцеві, що призводять до переривання роботи класу ОКІ $\mathbf{S}_i$.

Для визначення наслідків кожного можливого D_i введемо множину наслідків **E**:

$$\mathbf{E} = \{\bigcup_{i=1}^{q} E_i\} = \left\{E_1, E_2, ..., E_q\right\}, \tag{3.9}$$

де $E_i \subseteq \mathbf{E}$, $(i = \overline{1, q})$ – наслідки D_i, q – загальна кількість наслідків D_i.

Етап 5 – Ідентифікація ознак виявлення переривання роботи

Для кожного виду D_i обраного компонента C_i визначимо ознаки виявлення D_i. Введемо множину ознак **O**:

$$\mathbf{O} = \{\bigcup_{i=1}^{r} O_i\} = \left\{O_1, O_2, ..., O_r\right\}, \tag{3.10}$$

де $O_i \subseteq \mathbf{O}$, $(i = \overline{1,r})$ – ознаки виявлення D_i, r – загальна кількість ознак виявлення D_i.

Для кожної виявленої ознаки O_i кожного можливого переривання роботи D_i введемо функцію еквівалентності (3.11), яка приймає значення «1» при виявленні ознаки D_i та «0» при не виявленні відповідної ознаки D_i:

$$E(O_i, D_i) = \begin{cases} 1, \textit{ при } O_i = D_i; \\ 0, \textit{ при } O_i \neq D_i. \end{cases} \tag{3.11}$$

Етап 6 – Ідентифікація способів виявлення переривань роботи

Для визначення способів виявлення кожного можливого D_i введемо множину способів виявлення $\mathbf{W}$:

$$\mathbf{W} = \{\bigcup_{i=1}^{s} W_i\} = \{W_1, W_2, ..., W_s\}, \tag{3.12}$$

де $W_i \subseteq \mathbf{W}$, $(i = \overline{1,s})$ – способи виявлення D_i, s –загальна кількість способів виявлення D_i.

Етап 7 – Побудова тривимірної матриці критичності

Для побудови матриці критичності необхідно для кожного виду D_i визначити якісний параметр, що характеризує рівень ймовірності виникнення (ймовірність).

За ступенем тяжкості кінцевих наслідків D_i поділяють на чотири категорії:

- катастрофічне (I);
- істотне, що призводить до невиконання об'єктом своїх функцій (II);
- проміжне, що призводить до економічних втрат (III);
- незначне (IV).

Після цього оцінювання необхідно доповнити частотним аналізом, при якому враховується ймовірність настання D_i (наприклад, частковий (A), ймовірний (B), рідкісний (C), дуже рідкісний (D), неможливий (E)). Можливі значення ймовірності виникнення виду переривань роботи регламентовані в табл. 3.1.

Таблиця 3.1 – Рівні ймовірності виникнення переривань роботи

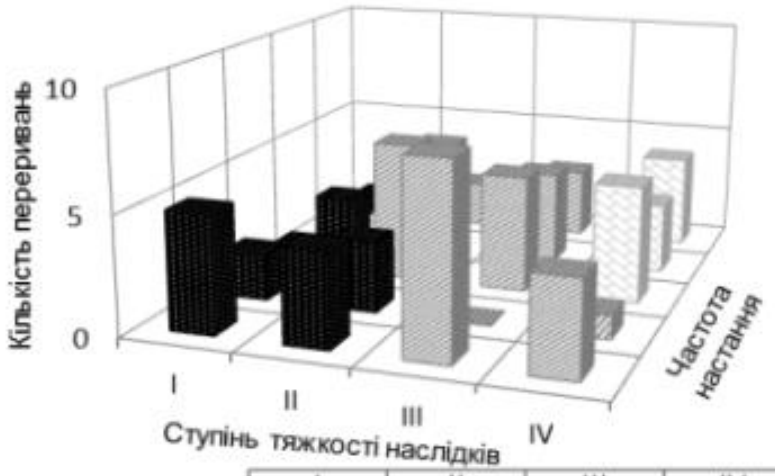
Рівень ймовірності виникнення D_i	Опис	Ймовірність виникнення D_i за час роботи
A	Часткове	> 0,2
B	Ймовірне	0,1 … 0,2
C	Можливе	0,01 … 0,1
D	Рідкісне	0,001 … 0,01
E	Малоймовірне	< 0,001

У табл. 3.2 представлена класифікаційна матриця оцінки частоти і значущості переривань роботи за категоріями I-IV.

Таблиця 3.2 – Оцінка значимості переривання роботи

Очікувана частота D_i	Категорія D_i			
	I	**II**	**III**	**IV**
Частковий	A	A	C	C
Ймовірний	A	A	B	C
Рідкісний	A	B	B	D
Дуже рідкісний	A	B	B	D
Неймовірний	B	C	C	D

Причини переривань роботи, що потрапили в групу A, підлягають безумовному усуненню при проектуванні шляхом зміни конструкції, збільшення відповідних запасів, стійкості тощо, пом'якшення умов експлуатації та ін. Причини, що потрапили в групу B і C, вимагають подальшого аналізу, уточнення механізмів D_i, дослідження характеру деградаційних процесів та інших факторів, важливих для більш повного опису D_i, а групи D не вимагають додаткового аналізу. Третій параметр – кількість D_i, з’являється під час заповнення таблиці (рис. 3.1) при фіксованій категорії і частоті.



	I	II	III	IV
A – Частковий	5	4	8	4
B – Ймовірний	2	3	0	1
C – Рідкісний	1	6	5	5
D – Дуже рідкісний	2	5	4	3
E – Неможливий	1	2	3	4

Рисунок 3.1 – Приклад побудови тривимірної матриці критичності

Етап 8 – Розрахунок рангу критичності ймовірних переривань

Для визначення рангу критичності R_i для кожного з перерахованих видів переривань роботи D_i розраховується показник рангу критичності переривання. Для цього введемо множину значень рангу критичності $\mathbf{R}$ у наступному вигляді:

$$\mathbf{R} = \{\bigcup_{i=1}^{w} R_i\} = \{R_1, R_2, ..., R_w\}, \tag{3.13}$$

де $R_i \subseteq \mathbf{R}$, $(i = \overline{1, w})$ – ранги критичності D_i, w –загальна кількість показників рангів критичності.

Ранг критичності D_i компонента C_i розраховується таким чином:

$$R_i = B_{1i} B_{2i} B_{3i}. \tag{3.14}$$

Крок 1. Для визначення показника B_{1i} (оцінка частоти (ймовірності) настання потенційного D_i компонента C_i) введемо відповідну множину:

$$\mathbf{B}_1 = \{\bigcup_{i=1}^{z} B_{1j}\} = \{B_{11}, B_{12}, ..., B_{1z}\}, \tag{3.15}$$

де $B_{1j} \subseteq \mathbf{B}_1$, $(j = \overline{1, z})$, значення z знаходяться за відповідною таблицею, сформованою апріорі у залежності від типу ОКІ. У табл. 3.3 наведені значення

коефіцієнта B_1 у загальному вигляді, де $B_{11}, B_{12}, ..., B_{1z}$ – значення j-х коефіцієнтів, <*value*> – числове значення частоти D_i, а <*frequency*> – лінгвістична змінна, що характеризує асоційовану інтенсивність D_i.

Таблиця 3.3 – Апріорні значення коефіцієнта B_1

Характеристика частоти D_i	Асоційована інтенсивність D_i	Значення $B_{1,}$ бали
<*frequency*>	<*value*>	$B_{11}, B_{12}, ..., B_{1z}$

Крок 2. Для визначення показника B_{2i} (оцінка ймовірності виявлення D_i компонента C_i до його проявлення) введемо відповідну множину:

$$\mathbf{B}_2 = \{\bigcup_{j=1}^{x} B_{2j}\} = \{B_{21}, B_{22}, ..., B_{2x}\}, \tag{3.16}$$

де значення x знаходяться аналогічно за таблицею, сформованою апріорі в залежності від типу ОКІ. У табл. 3.4 наведені значення коефіцієнта B_2 у загальному вигляді, де $B_{21}, B_{22}, ..., B_{2x}$ – значення j-х коефіцієнтів, <*probability*> – лінгвістична змінна, що характеризує ймовірність виявлення D_i.

Таблиця 3.4 – Апріорні значення коефіцієнта B_2

Характеристика ймовірності виявлення D_i	Значення
<*probability*>	$B_{21}, B_{22}, ..., B_{2x}$

Крок 3. Аналогічним чином, як і у виразах (3.15), (3.16) для визначення показника B_{3i} (оцінка тяжкості D_i компонента C_i) введемо множину:

$$\mathbf{B}_3 = \{\bigcup_{j=1}^{c} B_{3j}\} = \{B_{31}, B_{32}, ..., B_{3c}\}, \tag{3.17}$$

де значення c знаходяться аналогічно до табл. 3.3 та табл. 3.4 (див. табл. 3.5, у якій <*Consequence*> – лінгвістична змінна, що характеризує наслідки переривань D_i).

Таблиця 3.5 – Апріорні значення коефіцієнта B_3

Наслідки переривання D_i	Значення B_3, бали
<Consequence>	$B_{31}, B_{32}, ..., B_{3c}$

Крок 4. Розрахунок рангу критичності R_i кожного з перерахованих видів переривань роботи D_i за допомогою (3.14) та занесені отриманих даних до звіту (етап 11, табл. 3.7).

Етап 9 – Виділення переліку найбільш значущих (критичних) переривань роботи

Виділення найбільш значущих D_i здійснюється шляхом порівняння рангу критичності переривання R_i з деякими граничними значеннями R_0 та R_k. Згідно (3.14) і табл. 3.3, табл. 3.4, табл. 3.5, критичність змінюється в діапазоні від $R_{\min} = B_{11}B_{21}B_{31}$ до $R_{\max} = B_{1z}B_{2x}B_{3c}$.

Зазвичай у якості граничного значення призначають $R_k = \frac{1}{2}(B_{1z}B_{2x}B_{3c})$, при чому $R_{\min} < R_k < R_{\max}$. До того ж, для прикладу, $R_{\min} = 1$, $R_{\max} = 10^3$, $R_k = 125$, а рекомендоване значення $R_0 = 60$. Введемо правила для визначення критичності D_i $criticality\ (D_i) \in \{High, Middle, Low\}$:

$$criticality\ (D_i) = \begin{cases} High, при\ R_i > R_k; \\ Middle, при\ R_0 < R_i \le R_k; \\ Low, при\ R_i \le R_0, \end{cases} \qquad (3.18)$$

де, якщо $R_i > R_k$, то D_i визнається критичним $(High)$, отже, його причини підлягають обов'язковому усуненню; якщо $R_0 < R_i \le R_k$, то необхідні коригувальні заходи для зменшення критичності $(Middle)$, наприклад, зміна регламенту технічного обслуговування та ремонту, які заносяться до відповідного переліку для подальшого аналізу і контролю; якщо $R_i \le R_0$, то D_i є незначним і не вимагає розробки та імплементації додаткових заходів (Low).

Крім того, на цьому етапі для виділення переліку найбільш значущих (критичних) D_i використовується стовпчаста діаграма Парето (рис. 3.2), яка будується окремо для кожної з S_{ij} (з метою ранжування найбільш значущих (критичних) D_i по горизонтальній осі діаграми відкладаються D_i, а по вертикальній – розраховане значення R_i), якщо $R_i > R_k$, то D_i на діаграмі позначається чорним кольором, якщо $R_0 < R_i \le R_k$, то D_i на діаграмі позначається сірим кольором, якщо $R_i \le R_0$, то D_i на діаграмі позначається світло-сірим кольором.

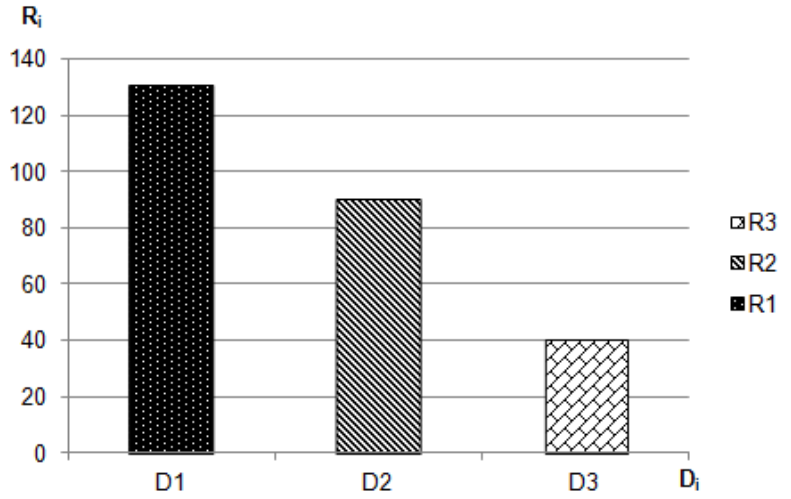


Рисунок 3.2 – Приклад побудови стовпчастої діаграми Парето

Діаграма Парето допомагає виділити перелік найбільш значущих (критичних) D_i підсистеми, а також дає можливість порівняти окремі підсистеми за обчисленим R_i та виділити підсистему, що є більш критичною для ОКІ взагалі.

Етап 10 – Формування переліку коригувальних заходів

Після виконання попереднього етапу проводиться аналіз R_i переривань D_i і необхідно імплементувати відповідні корегувальні заходи (напрямки розробки цих заходів випливають з (3.14) – (3.17), тобто якщо у добутку (3.14) один із множників є найбільшим, то, очевидно, що мета коригувальних заходів має полягати в зниженні саме цього коефіцієнта).

Для складання переліку коригувальних заходів відбувається виявлення причинно-наслідкових закономірностей за діаграмою Ісікави (рис. 3.3), яка для кожного критичного переривання роботи R_{begin} системи S_{ij} відображає характеристики, з якими пов'язане виникнення D_i і підвищує ефективність розробки коригувальних заходів. Причинно-наслідкова діаграма Ісікави поділяє всі ідентифіковані D_i за основними причинами (параметрами) їх виникнення, а саме через помилки: користувачів (a), програмного забезпечення (b), апаратного забезпечення (c), мережевих технологій (d).

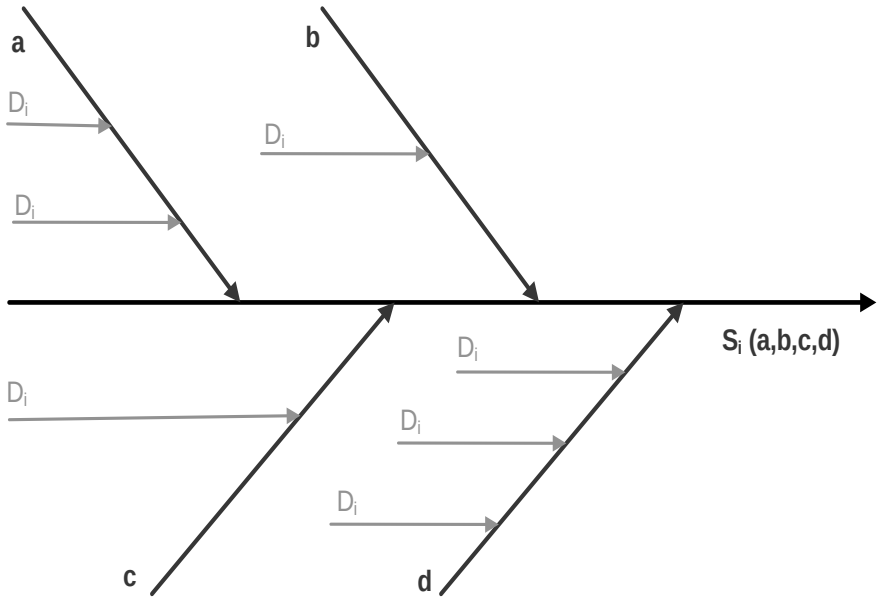


Рисунок 3.3 – Приклад побудови причинно-наслідкової діаграми Ісікави

Для визначення переліку можливих коригувальних заходів кожного C_i введемо множину коригувальних заходів $\mathbf{K}$:

$$\mathbf{K} = \{\bigcup_{i=1}^{g} K_i\} = \{K_1, K_2, ..., K_g\}, \tag{3.19}$$

де $K_i \subseteq \mathbf{K}$, $(i = \overline{1,g})$ – коригувальні заходи, g –загальна кількість коригувальних заходів. Оцінка ефективності коригувальних заходів проводиться шляхом повторного розрахунку R_i (див. етап 8). Далі, оперуємо початковим значенням

R_{begin} (до імплементації коригувальних заходів) і кінцевим R_{finish} (після імплементації коригувальних заходів): якщо $R_{finish} < R_k$ то коригувальні заходи, спрямовані на підвищення КБ, можна рекомендувати до використання. Перелік K_i для досліджуваних S_{ij} формуємо у вигляді табл. 3.8.

Таблиця 3.6 – Перелік коригувальних заходів

S_{ijk}	D_i	R_{begin}	K_i	R_{finish}
$S_{ij1}, S_{ij2}, ..., S_{ijr_{ij}}$	$D_1, D_2, ..., D_p$	$R_1, R_2, ..., R_w$	$K_1, K_2, ..., K_g$	$R_{finish.1}, R_{finish.2}, ..., R_{finish.w}$

Етап 11 – Складання звіту щодо ризиків ОКІ

На цьому етапі відбувається систематизація даних, отриманих на попередніх етапах ($\mathbf{S}_i, S_{ij}, C_i, F_i, D_i, E_i, O_i, W_i$ та R_i), візуалізація якісних та обчислення кількісних значень критичності ОКІ. Етап передбачає систематизацію всієї інформації у вигляді табл. 3.7.

Таблиця 3.7 – Звіт для всіх рівнів аналізу у загальному вигляді

$\mathbf{S}_i / S_{ij} / S_{ijk}$	C_i	F_i	D_i	E_i	O_i	W_i	**R**			
							B_1	B_2	B_3	R_i
$\mathbf{S}_1, \mathbf{S}_2, \ldots, \mathbf{S}_n$ $\mathbf{S}_{i1}, \mathbf{S}_{i2}, ..., \mathbf{S}_{im_i}$ $S_{ij1}, S_{ij2}, ..., S_{ijr_{ij}}$	C_1, C_2, ..., C_b	F_1, F_2, ..., F_l	D_1, D_2, ..., D_p	E_1, E_2, ..., E_q	O_1, O_2, ..., O_r	W_1, W_2, ..., W_s	B_{11}, B_{12}, ..., B_{3z}	B_{21}, B_{22}, ..., B_{2x}	B_{31}, B_{32}, ..., B_{3c}	R_1, R_2, ..., R_w

Таким чином, у табл. 3.7 систематизовано такі вихідні дані запропонованого методу як:

- перелік компонентів системи, їх функції, види переривань роботи для кожного компонента системи;

- інформація про причини виникнення та наслідки переривань роботи для кожного компонента системи;
- розрахунки рангів критичності, результати ранжування – перелік найбільш значущих (критичних) переривань роботи, які відображаються у формалізованому і зручному для експертів вигляді.

Інші вихідні дані отримані на різних етапах реалізації методу, зокрема, матриця критичності, яка за зібраними попередніми даними графічно відображає критичність компонентів системи (етап 7), діаграма Парето, яка показує рівень критичності в середині системи та дає можливість порівняти декілька різних систем (етап 9), причинно-наслідкова діаграма Ісікави, що дозволяє виділити пріоритетні напрямки розробки відповідних коригувальних заходів (етап 10).

Таким чином, розроблено метод визначення рівня важливості об’єктів КІІ, який, за рахунок введення базової множини систем та відповідних підмножин підсистем, компонентів, функцій, порушень безперервності роботи, їх ознак і наслідків, а також побудови тривимірної матриці критичності, діаграми Парето, причинно-наслідкової діаграми Ісікави та розрахунку додаткових вагових коефіцієнтів критичності, дає можливість проводити оцінювання рівня важливості ОКІ, оцінювати ризики і ранжувати ОКІ як за кількісними, так і за якісними параметрами та пропонує множину коригувальних заходів для зменшення виявленого рівня критичності.

3.6. Висновки до розділу 3

Таким чином, у третьому розділі було удосконалено метод управління ризиками кібербезпеки, який використовує стандарт FMECA та систему індикаторів критичності (діаграми Ісікави та Парето, матриці критичності), що дозволяє пріоритезувати ризики та ідентифікувати їх першопричини, аналізувати динаміку й реагувати на зміни трендів. Цей метод відрізняється від відомих (зокрема від оригінальної методики FMECA) тим, що за рахунок введення базової

множини систем та відповідних підмножин підсистем, компонентів, функцій, порушень безперервності роботи, їх ознак і наслідків, а також побудови тривимірної матриці критичності, діаграми Парето, причинно-наслідкової діаграми Ісікави та розрахунку додаткових вагових коефіцієнтів критичності, дає можливість проводити оцінювання рівня важливості ОКІ, оцінювати ризики і ранжувати ОКІ як за кількісними, так і за якісними параметрами та пропонує множину коригувальних заходів для зменшення виявленого рівня критичності.

ВИСНОВКИ

1. Основні аспекти управління ризиками кібербезпеки включають:

- Ідентифікація ризиків: Визначення уразливостей, загроз і можливих точок доступу, які можуть використовувати зловмисники. Це включає в себе інвентаризацію активів та їхню класифікацію за важливістю.
- Оцінка ризиків: Вимірювання ймовірності кожного ризику та його можливого впливу на організацію. Ця оцінка допомагає встановити пріоритети та планувати стратегії реагування.
- Розробка стратегії пом'якшення ризиків: Визначення заходів для зменшення впливу ризиків, таких як впровадження політик безпеки, використання брандмауерів, шифрування та навчання персоналу.
- Впровадження заходів: Реалізація планів пом'якшення ризиків, таких як удосконалення систем моніторингу, оновлення програмного забезпечення, налаштування обмежень доступу та створення плану дій на випадок інцидентів.
- Моніторинг та виявлення загроз: Безперервний моніторинг систем для виявлення та попередження нових загроз або підозрілої активності.
- Оцінка ефективності: Аналіз і перегляд ефективності впроваджених заходів для забезпечення актуальності та дієвості. Це може включати регулярне тестування, проведення аудитів або симуляцію атак (пентест).
- Реагування на інциденти: Розробка планів швидкого реагування та мінімізації шкоди під час кіберінциденту. Це передбачає відновлення системи, сповіщення відповідних сторін і проведення розслідування.
- Навчання та підвищення обізнаності: Підготовка співробітників щодо ризиків кібербезпеки та правильного поводження з інформацією, щоб знизити ризик фішингових атак або інших соціальних маніпуляцій.

2. Основні програмні засоби для управління ризиками кібербезпеки включають:

- SIEM (Security Information and Event Management): Інтеграційні рішення, які збирають та аналізують дані з різних систем, забезпечуючи виявлення та реагування на загрози в режимі реального часу. Приклади: Splunk, IBM QRadar, ArcSight.
- GRC (Governance, Risk, and Compliance): Платформи, які допомагають керувати політиками та контролями безпеки, проводити аудити, керувати ризиками та відповідати вимогам регуляторів. Приклади: RSA Archer, ServiceNow GRC.
- Платформи управління вразливостями: Інструменти для сканування мережі, систем та застосунків на предмет вразливостей, з подальшим аналізом та рекомендаціями щодо їх усунення. Приклади: Tenable Nessus, Rapid7 InsightVM, Qualys.
- EDR (Endpoint Detection and Response): Засоби моніторингу та реагування на загрози на кінцевих пристроях, таких як комп'ютери та сервери. Приклади: CrowdStrike Falcon, Carbon Black, Microsoft Defender.
- Платформи управління конфігураціями: Інструменти, які перевіряють, чи відповідає конфігурація систем та мереж політикам безпеки та стандартам, допомагаючи виявити можливі ризики. Приклади: Tripwire, Chef InSpec.
- DLP (Data Loss Prevention): Засоби запобігання витоку даних, які допомагають виявляти та захищати конфіденційну інформацію, контролюючи її переміщення по мережі або на пристрої. Приклади: Symantec DLP, McAfee Total Protection.
- Платформи управління привілейованим доступом (PAM): Інструменти, що обмежують доступ до критично важливих ресурсів лише для авторизованих користувачів та забезпечують моніторинг їхньої активності. Приклади: CyberArk, BeyondTrust.
- SOAR (Security Orchestration, Automation, and Response): Інтегровані платформи, що об'єднують різні засоби кібербезпеки для автоматизації рутинних завдань, прискорення реагування на інциденти та покращення співпраці між

командами. Приклади: Splunk Phantom, IBM Resilient. Використання цих засобів дозволяє організаціям забезпечити комплексний підхід до управління ризиками кібербезпеки, допомагаючи виявляти, оцінювати та мінімізувати ризики ефективніше.

Крім використання програмних засобів, існують різні методики управління ризиками кібербезпеки. Ось кілька основних підходів:

- NIST Cybersecurity Framework: Структура Національного інституту стандартів і технологій США надає п'ятиступеневий підхід до управління ризиками: ідентифікувати, захищати, виявляти, реагувати та відновлювати. Він також включає глибокі рекомендації щодо кожного етапу.
- ISO/IEC 27001: Стандарт міжнародної організації з сертифікації забезпечує систему управління інформаційною безпекою (ISMS), що включає ідентифікацію, оцінку та пом'якшення ризиків.
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation): Методологія аналізу кіберризиків, яка фокусується на ідентифікації критичних активів, загроз та вразливостей. Вона складається з декількох етапів, включаючи оцінку безпеки та визначення пріоритетів ризиків.
- FAIR (Factor Analysis of Information Risk): Модель, що дозволяє оцінити фінансові наслідки кіберризиків, допомагаючи встановити пріоритети в управлінні безпекою з точки зору впливу на бізнес.
- FMEA/FMECA (Failure Modes and Effects Analysis / Failure Modes, Effects, and Criticality Analysis): Методи визначення можливих типів збоїв у системі, оцінки їх впливу та ймовірності виникнення для планування заходів з пом'якшення ризиків.
- STRIDE: Модель загроз від Microsoft для ідентифікації та категоризації потенційних загроз за типами: підміна (Spoofing), спотворення (Tampering), відмова (Repudiation), розкриття (Information Disclosure), відмова в обслуговуванні (Denial of Service) та підвищення привілеїв (Elevation of Privilege).
- Threat Modeling: Методика моделювання загроз, яка допомагає створити сценарії можливих атак на систему та розробити ефективні контрзаходи.

- Risk Register: Використання реєстру ризиків для систематичного документування та відстеження виявлених ризиків, а також пов'язаних з ними стратегій управління.

3. Удосконалено метод управління ризиками кібербезпеки, який використовує стандарт FMECA та систему індикаторів критичності (діаграми Ісікави та Парето, матриці критичності), що дозволяє пріоритезувати ризики та ідентифікувати їх першопричини, аналізувати динаміку й реагувати на зміни трендів. Цей метод відрізняється від відомих введенням базової множини систем та відповідних підмножин підсистем, компонентів, функцій, порушень безперервності роботи, їх ознак і наслідків, а також побудови тривимірної матриці критичності, діаграми Парето, причинно-наслідкової діаграми Ісікави та розрахунку додаткових вагових коефіцієнтів критичності, що дає можливість проводити оцінювання рівня важливості ОКІ, оцінювати ризики і ранжувати ОКІ як за кількісними, так і за якісними параметрами та пропонує множину коригувальних заходів для зменшення виявленого рівня критичності.

Створення спеціалізованого програмного забезпечення на основі запропонованого методу дозволить, крім якісного і кількісного оцінювання ризику, автоматизовано оцінювати важливість ОКІ в різних галузях та секторах критичної інфраструктури. У свою чергу, це дасть змогу здійснювати перерозподіл інвестицій в кібербезпеку певних ОКІ в умовах обмежених матеріальних та інших ресурсів.

Практична цінність роботи підтверджена актом впровадження, який міститься в Додатку А.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Action Plan 2010-2015 for Canada's Cyber Security Strategy, 2013 [Electronic resourse]. – Access mode: http://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf.

2. Anti-Malware [Electronic resource]. — URL : http://www.anti-malware.com/

3. Austrian Cyber Security Strategy, 2013, Vienna [Electronic resourse]. – Access mode: https://www.bka.gv.at/DocView.axd?CobId=50999.

4. Canada's Cyber Security Strategy [Electronic resource]. — URL : http://publications.gc.ca/site /eng/379746/publication.html

5. Cyber Security Strategy — A world-leading, resilient and vigorous cyberspace [Electronic resource]. — URL : http://www.nisc.go.jp/eng/pdf/CyberSecurityStrategy.pdf

6. Cyber Security Strategy [Electronic resource]. — URL : http://www.kmin.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf

7. Cyber Security Strategy for Germany [Electronic resource]. — URL : http://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1

8. Cyber Security Strategy for Germany, 2011, Berlin [Electronic resourse]. – Access mode: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile.

9. Cyber Security Strategy of Estonia, 2014 [Electronic resourse]. –Access mode: https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf.

10. Cyber Security Strategy of the Czech Republic for the 2011 – 2015 period [Electronic resource]. — URL : http://www.enisa.europa.eu/media/news-items/CZ_Cyber_Security_Strategy_20112015.PDF

11. Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space [Electronic resource]. — URL : // http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf

12. Cybersecurity Strategy for Defence of Belgium, 2014. [Electronic resourse]. – Access mode: https://ccdcoe.org/sites/default/files/strategy/Belgian%20Defence%20Cyber%20Security%20Strategy.pdf.

13. Cybersecurity Strategy, 2014, Nairobi [Electronic resourse]. – Access mode: http://www.icta.go.ke/wp-content/uploads/2014/03/GOK-national-cybersecurity-strategy.pdf.

14. Cyberspace Protection Policy of the Republic of Poland, 2013, Warsaw [Electronic resourse]. – Access mode: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/copy_of_PO_NCSS.pdf.

15. Défense et sécurité des systèmes d'information Stratégie de la France, 2011 [Electronic resourse]. – Access mode: https://www.enisa.europa.eu/media/news-items/french-cyber-security-strategy-2011.

16. Denning D.E. The Terrorism Research Center [Електронний ресурс] / D.E. Denning. — Режим доступу: http://www.washprofile.org/en/node/686

17. Gemignani, Computer Crime: The Law in '80, Indiana Law Review, Vol. 13, 1980, p. 681.

18. German Cyber Security Strategy [Electronic resource]. — URL : http://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1

19. Glossary and Acronyms (Archived) / European Commission [Electronic resource]. — URL : http://ec.europa.eu/information_society/tl/help/glossary/index_en.htm#c

20. Government Resolution on National Information Security Strategy [Electronic resource]. — URL : http://www.lvm.fi/c/document_library/get_file?folderId=57092&name=DLFE-5405.pdf&title=Valtioneuvoston%20 periaatep%C3%A4%C3%A4t%C3%B6s%20kansalliseksi%20tietoturvastra

21. Information Security Research and Development Strategy [Electronic resource]. — URL : http://www.nisc.go.jp/eng/pdf/R_and_D_Strategy_eng.pdf

22. International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World, 2011, Washington [Electronic resourse]. – Access mode: https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

23. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World [Electronic resource]. — URL : http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyber space.pdf

24. ISO/IEC 27032, Information technology — Security techniques — Guidelines for cybersecurity. — 2012. — 50 p.

25. IT Emergency and Crisis Exercises in Critical Infrastructures [Electronic resource]. — URL : http://www.bmi.bund.de/cae/servlet/contentblob/560098/publicationFile/27811/kritis_3_eng.pdf

26. Jamaica National Cyber Security Strategy, 2015 [Electronic resourse]. – Access mode: http://mstem.gov.jm/sites/default/files/Jamaica%20National%20Cyber%20Security%20Strategy.pdf.

27. Jason Brown, Executive’s Cybersecurity Program Handbook: A comprehensive guide to building and operationalizing a complete cybersecurity program , Packt Publishing, 2023.

28. Jason Edwards; Griffin Weaver, "State-level Cybersecurity Regulations," in The Cybersecurity Guide to Governance, Risk, and Compliance , Wiley, 2024, pp.287-297, doi: 10.1002/9781394250226.ch16.

29. Kerr K. Putting cyberterrorism into context [Electronic resource]. — URL : http://www.auscert.org.au/render.html?it=3552

30. Latvian cyber security strategy for the period 2014 to 2018, 2014 [Electronic resourse]. – Access mode: https://ccdcoe.org/sites/default/files/strategy/LVA_CSS_2014-2018.pdf.

31. McLaughlin, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, Vol. 2, p. 217.

32. National Cyber Security Masterplan 2018, 2013 [Electronic resourse]. – Access mode: https://www.ida.gov.sg/~/media/Files/Programmes%20and%20 Partnership/Initiatives/2014/ncsm2018/NationalCyberSecurityMasterplan202018.pdf.

33. National Cyber Security Policy, 2013, New Delphi [Electronic resourse]. – Access mode: http://deity.gov.in/content/national-cyber-security-policy-2013-1.

34. National Cyber Security Strategy 2014-2019, 2014 [Electronic resourse]. – Access mode: http://mtci.govmu.org/English/Documents/Final%20National%20 Cyber%20Security%20Strategy%20November%202014.pdf.

35. National Cyber Security Strategy of Hungary, 2013, Budapest [Electronic resourse]. – Access mode: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/HU_NCSS.pdf

36. National Cybersecurity Strategy, 2014 [Electronic resourse]. – Access mode: http://www.dpp.gov.bd/upload_file/gazettes/10041_41196.pdf.

37. National Military Strategy for Cyberspace Operations [Electronic resource]. — URL : http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf

38. National Strategy to Secure Cyberspace [Electronic resource]. — URL : http://www.dhs.gov/national-strategy-secure-cyberspace

39. On the approval of the programme for the development of electronic information security (cyber-security) for 2011–2019 [Electronic resource]. — URL : http://www.ird.lt/doc/teises_aktai_en/EIS(KS)PP_796_2011-06-29_EN_PATAIS.pdf

40. Per Concordiam, Журнал по проблемам безопасности и обороны Европы, Том 2, Выпуск 2, Garmisch-Partenkirchen, Germany, 68 с.

41. Petrov O., Korchenko O., Lakhno V. Method and model of intellectual threats detection for information and communication transport environment // Ukrainian Scientific Journal of Information Security. — 2015. — Vol. 21, Issue 1. — P. 26-34.

42. Pollitt M.M. «A Cyberterrorism Fact or Fancy?», Proceedings of the 20th National Information Systems Security Conference, 1997, pp. 285-289.

43. Qatar National Cyber Security Strategy, 2015 [Electronic resourse]. – Access mode: http://docplayer.net/2856349-National-cyber-security-strategy-2015-2017.html.

44. SecurityLab [Electronic resource]. — URL : http://www.securitylab.com

45. Strategie de la France: Défense et sécurité des systèmes d'information [Electronic resource]. — URL : http://www.enisa.europa.eu/media/news-items/french-cyber-security-strategy-2011

46. Strategie nationale en matiere de cyber securite [Electronic resource]. — URL : http://www.gouvernement.lu/salle_presse/actualite/2011/11-novembre/23-biltgen/dossier.pdf

47. Strategy on Cyber Security of Montenegro to 2017, 2013, Podgorica [Electronic resourse]. – Access mode: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/CyberSecurityStrategyforMontenegro.pdf.

48. The National Cyber Security Strategy (NCSS): Success through cooperation [Electronic resource]. — URL : http://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011

49. K. Leontiiev, I. Babeshko and V. Kharchenko, "Assumption Modes and Effect Analysis of XMECA: Expert based safety assessment," 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2020, pp. 90-94, doi: 10.1109/DESSERT50317.2020.9125008.

50. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. — К. : НАУ. — 2013. — 432 с.

51. Бутузов В.М. Протидія комп'ютерній злочинності в Україні (системно структурний аналіз): Монографія / В.М. Бутузов. — К. : КИТ, 2010. — 145 с.

52. Вильский Г. Кластерно-вероятностная методология исследования информационной безопасности движения морских судов / Г. Вильский // Безпека інформації. — 2014. — Т. 20, № 1. — С. 92-96.

53. K. Leontiiev, I. Babeshko and V. Kharchenko, "Assumption Modes and Effect Analysis of XMECA: Expert based safety assessment," 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2020, pp. 90-94, doi: 10.1109/DESSERT50317.2020.9125008.

54. Гавриш С.Б. Комп'ютерний тероризм: сучасний стан, прогнози розвитку та шляхи протидії / С.Б. Гавриш // Боротьба з організованою злочинністю і корупцією (теорія і практика) [Електронний ресурс]. — Режим доступу: http://archive.nbuv.gov.ua/portal/soc_gum/bozk/2009_20/20text/g20_01.htm

55. Гончар С.Ф. Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури : монографія / С.Ф. Гончар. – Київ : «Альфа реклама», 2019. – 176с.

56. Довгань О.Д. Кібертероризм як загроза інформаційному суверенітету держави / О.Д. Довгань, В.Г. Хлань // Інформаційна безпека людини, суспільства, держави — №3 (7), 2011. — С. 49-53.

57. Дубов Д.В. Кібербезпека: світові тенденції та виклики для України / Д.В.Дубов, М.А.Ожеван. — К. : НІСД, 2011. — 30 с.

58. Зелена книга з питань захисту критичної інфраструктури в Україні. Національний інститут стратегічних досліджень [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/public/File/2014_table/1125_zelknuga.pdf

59. Климчик О.О. Кримінально-правова кваліфікація використання комп'ютерних технологій для вчинення терористичних актів / О.О. Климчик, Р.М. Кравченко // Інформаційна безпека людини, суспільства, держави — №1 (3), 2010. — С. 26-30.

60. Компьютерная преступность и кибертерроризм / под ред. В.А. Голубева, Э.В. Рыжкова. — Запорожье : Центр исслед. компьютерной преступности, 2005. — Вып. 3. — 448 с.

61. Лахно В.А. Обеспечение защищенности автоматизированных информационных систем транспортных предприятий при интенсификации

перевозок: Монография / В.А. Лахно, А.С. Петров. — Луганск: изд-во ВНУ им. В. Даля, 2010. — 280 с.

62. Лахно В. Інформаційна безпека інтелектуальних транспортних систем / В. Лахно // Захист інформації. — 2015. — Т. 17, № 4. — С. 298-305.

63. Лахно В. Підвищення кібербезпеки інформаційно-комунікаційних систем транспорту / В. Лахно // Безпека інформації. — 2016. — Т. 22, № 1. — С. 44-50.

64. Мельник С.В. До проблеми формування понятійно-термінологічного апарату кібербезпеки / С.В. Мельник, О.О. Тихомиров // Актуальні проблеми управління інформаційною безпекою держави: зб. матер. наук.-практ. конф., 22 березня 2011. — К.: Вид-во НА СБ України, 2011. — Ч.2. — С. 43-48.

65. Мельник С.В. До проблеми формування понятійно-термінологічного апарату кібербезпеки / С.В. Мельник, О.О. Тихомиров, О.С. Лєнков // Збірник наукових праць Військового інституту КНУ ім. Тараса Шевченка. — К. : ВІКНУ, 2011. — Вип. 30. — С. 159-165.

66. Міщенко А.В. Питання інформаційної безпеки в аспекті підвищення цільової ефективності авіатранспортного комплексу / А.В. Міщенко // Вісник Чернігівського держ. технолог. університету. Серія : Технічні науки. — 2015. — № 1. — С. 47-51.

67. Міщенко А.В. Ресурсна оптимізація циклічних процесів лінійного типу функціонування авіатранспортного комплексу / А.В. Міщенко // Наукоємні технології. — 2014. — № 2. — С. 116-118.

68. O. Illiashenko, V. Kharchenko and M. Ahtyamov, "Security assessment and green issues of FPGA-based information & control systems," The International Conference on Digital Technologies 2013, Zilina, Slovakia, 2013, pp. 185-190, doi: 10.1109/DT.2013.6566309.

69. Мохор В. В. Методи оцінки сумарного ризику кібербезпеки об'єктів критичної інфраструктури / В. В. Мохор, С. Ф. Гончар, О. М. Дибач. // Ядерна та радіаційна безпека. – 2019. – №2(82). – С. 57–61.

70. Мохор В.В. Дослідження правомірності подання ризиків векторами у евклідовому просторі / Мохор В.В., Гончар С.Ф. // Електронне моделювання. – 2019. – Т.41. – №4. – С. 73-84.

71. Мохор В.В. Идея построения алгебры рисков на основе теории комплексных чисел / Мохор В.В., Гончар С.Ф. // Електронне моделювання. – 2018. – Т.40. – №4. – С. 107-111.

72. Пилипчук В.Г. Теоретичні та державно-правові аспекти протидії інформаційному тероризму в умовах глобалізації / В.Г. Пилипчук, О.П. Дзьобань // Стратегічна пріоритети. — №4 (21), 2011. — С. 12-17.

73. Погорецький М.А. Поняття кіберпростору як середовища вчинення злочину / М.А. Погорецький, В.П. Шеломенцев // Інформаційна безпека людини, суспільства, держави — №2 (2), 2009. — С. 80.

74. M. Catelani, L. Ciani, D. Galar and G. Patrizi, "Risk Assessment of a Wind Turbine: A New FMECA-Based Tool With RPN Threshold Estimation," in IEEE Access, vol. 8, pp. 20181-20190, 2020, doi: 10.1109/ACCESS.2020.2968812.

75. Словник термінів з кібербезпеки / За загальною редакцією Копана О.В., Скулиша Є.Д. — К. : ВБ «Аванпост-Прим». — 2012. — 214 с.

76. Старостина Е. Подход к выработке единого понятия «кибертерроризм» [Электронный ресурс]. — Режим доступа : http://rudocs.exdat.com/docs/index-198810.html

77. Z. Yuhui, L. Shiyu, Z. Lijing and T. Gang, "Natural Gas Pipeline Network Risk Assessment Based on FMECA-Fuzzy Comprehensive Analysis," 2018 IEEE International Conference of Safety Produce Informatization (IICSPI), Chongqing, China, 2018, pp. 11-15, doi: 10.1109/IICSPI.2018.8690464.

78. L. Ciani, G. Guidi and G. Patrizi, "Fuzzy-Based Approach to Solve Classical Risk Priority Number Drawbacks for Railway Signaling Systems," in IEEE Intelligent Transportation Systems Magazine, vol. 15, no. 1, pp. 36-47, Jan.-Feb. 2023, doi: 10.1109/MITS.2021.3121433.

79. C. Chen, Z. Yang, F. Chen and W. Chen, "Modified FMECA of Motorized Spindle Unit Based on Maintenance Cost," 2018 Annual Reliability and Maintainability

Symposium (RAMS), Reno, NV, USA, 2018, pp. 1-4, doi: 10.1109/RAM.2018.8463025.

80. Тропина Т.Л. Киберпреступность и кибертерроризм: поговорим о понятийном аппарате // Сборник научных трудов Международной конференции «Информационные технологии и безопасность». — Вып. 3. — К. : Национальная академия наук Украины, 2003. — С. 173-181.

81. Шеломенцев В.П. До концепції законопроекту про кібернетичну безпеку / В.П. Шеломенцев // Боротьба з Інтернет-злочинністю : матеріали міжнар. наук.-техн. конф. — Донецьк : ДЮІ МВС України, 2013. — С. 12-14.

82. Wilhelmsen, Cheryl A., and Lee T. Ostrom. Risk assessment: tools, techniques, and their applications. John Wiley & Sons, 2019.

83. Fagan, Michael, et al. "IoT Device Cybersecurity Guidance for the Federal Government." NIST Special Publication 800 (2021): 213.

84. Burnap, Pete. "Risk Management & Governance Knowledge Area Issue." (2021). Version 1.1.1. https://www.cybok.org/media/downloads/Risk_Management_Governance_v1.1.1.pdf

85. V. Kharchenko, Y. Ponochovniy, A. -S. M. Q. Abdulmunem and I. Shulga, "AvTA Based Assessment of Dependability Considering Recovery After Failures and Attacks on Vulnerabilities," 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Metz, France, 2019, pp. 1036-1040, doi: 10.1109/IDAACS.2019.8924251.

86. M. Catelani, L. Ciani, D. Galar, G. Guidi, S. Matucci and G. Patrizi, "FMECA Assessment for Railway Safety-Critical Systems Investigating a New Risk Threshold Method," in IEEE Access, vol. 9, pp. 86243-86253, 2021, doi: 10.1109/ACCESS.2021.3088948.

ДОДАТКИ

Додаток А

ГРОМАДСЬКА ОРГАНІЗАЦІЯ «НАУКОВА АСОЦІАЦІЯ КІБЕРБЕЗПЕКИ УКРАЇНИ» (ГО «НАКБУ»)
Код ЄДРПОУ 44833202, р/р IBAN UA613052990000026009025026546
АТ КБ «Приватбанк», МФО 305299
Україна, 03161, м. Київ, вул. Донця Михайла, буд. 2А, оф. 966
www.scsa.org.ua +38 (097) 193-44-25 s.gnatyuk@scsa.org.ua

АКТ

впровадження результатів магістерської кваліфікаційної роботи Євгенія РИЖОГО на тему «Методи оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури» у діяльність Громадської організації «Наукова асоціація кібербезпеки України»

Громадська організація «Наукова асоціація кібербезпеки України» засвідчує цим актом те, що результати кваліфікаційної роботи Євгенія Рижого «Методи оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури» використовуються у діяльності організації.

Рижим Є. було удосконалено метод управління ризиками кібербезпеки, який використовує стандарт FMECA та систему індикаторів критичності (діаграми Ісікави та Парето, матриці критичності), що дозволяє пріоритезувати ризики та ідентифікувати їх першопричини, аналізувати динаміку й реагувати на зміни трендів

Розроблене спеціалізоване програмне забезпечення на основі запропонованого методу дозволяє, крім якісного і кількісного оцінювання ризику, автоматизовано оцінювати важливість ОКІ в різних галузях та секторах критичної інфраструктури. Проведено тестування цього програмного забезпечення і перевірено його якість та придатність для використання в реальних умовах.

Отже, результати, отримані Рижим Є. під час написання кваліфікаційної роботи, дозволили провести оцінювання ризиків та оцінити важливість ОКІ в різних галузях та секторах критичної інфраструктури, у свою чергу, це дає можливість здійснювати перерозподіл інвестицій в кібербезпеку певних ОКІ в умовах обмежених матеріальних та інших ресурсів.

Президент ГО «НАКБУ» Сергій ГНАТЮК