Міністерство освіти і науки України
Харківський національний університет радіоелектроніки
Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Методика аналізу загроз та вразливостей до кібератак сучасних інформаційних систем
(тема)

Виконав:
студент 2 курсу, групи АМСЗІм-21-2
Магдаліна М.І.
(прізвище, ініціали)

Спеціальність: 125 Кібербезпека
(код і повна назва спеціальності)
Тип програми: освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма: Адміністративний менеджмент у сфері захисту інформації
(повна назва освітньої програми)

Керівник: доцент кафедри ІКІ ім. В.В. Поповського Снігуров А.В.
(посада, прізвище, ініціали)

Допускається до захисту
Зав. кафедри _____ Лемешко О.В.
(підпис) (прізвище, ініціали)

2023р.

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)
Рівень вищої освіти другий (магістерський)
Спеціальність 125 Кібербезпека
(код і повна назва)
Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма Адміністративний менеджмент у сфері захисту інформації
(повна назва)

ЗАТВЕРДЖУЮ
Зав. кафедри_____
(підпис)
«____» _____2023р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентці Магдаліні Марії Ігорівні
(прізвище, ім'я, по батькові)

1. Тема роботи: Методика аналізу загроз та вразливостей до кібератак сучасних інформаційних систем
затверджена наказом по університету від «12» травня 2023р. № 469Ст.
2. Термін подання студентом роботи до екзаменаційної комісії 25.05.2023р.
3. Вихідні дані до роботи: 1) Основні підходи до побудови моделі загроз (порушника) та вразливостей для реалізації оцінки ризиків інформаційної безпеки. 2) Найпоширеніші сучасні атаки на інформаційні системи (кібератаки та інформаційні атаки). 3) Сучасні методи оцінки ризиків: якісні і кількісні методи оцінки ризиків (методи CRAMM, CVSS v3). 4) Механізми оцінки рівня впливу на результати оцінки ризиків потенціалу порушників.
4. Перелік питань, що потрібно опрацювати в роботі:
1) Аналіз сучасних підходів до побудови моделі загроз та моделі порушника, моделі вразливостей, які існують на даний час в сфері інформаційної безпеки.
2) Механізми оцінки ризику інформаційної безпеки, удосконалення методів оцінки ризику інформаційної безпеки CRAMM, CVSSv3.1 з урахуванням моделі загроз (моделі порушника).
3) Механізми розрахунку параметрів моделі порушника з урахуванням мотивації та потенціалу порушників.

5. Перелік графічного матеріалу із зазначенням креслень, плакатів, комп'ютерних ілюстрацій: демонстраційний матеріал у вигляді ppt-презентації.

6. Консультанти розділів роботи

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		(підпис)	(дата)
Основна частина	доцент Снігуров Аркадій Владиславович		

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	23.03.2023	виконано
2	Збір матеріалів для дослідження	30.03.2023	виконано
3	Розробка 1 розділу	15.04.2023	виконано
4	Розробка 2 розділу	30.04.2023	виконано
5	Розробка 3 розділу	15.05.2023	виконано
6	Оформлення кваліфікаційної роботи	25.05.2023	виконано

Дата видачі завдання 23 березня 2023 року

Студент _____ Магдаліна М.І.
(підпис) (прізвище, ініціали)

Керівник роботи _____ доцент Снігуров А.В.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 85 с., 15 рис., 37 табл., 1 додаток, 18 джерел.

МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ВРАЗЛИВІСТЬ, РИЗИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, CRAMM, CVSS.

Об'єкт дослідження – процес розробки моделі загроз (порушника) та моделі вразливостей в інтересах оцінки ризиків інформаційної безпеки сучасним інформаційним системам.

Предметом дослідження – удосконалення механізму побудови моделі загроз (порушника), удосконалення методики оцінки ризику інформаційної безпеки CRAMM з урахуванням моделі порушника та методики оцінки вразливостей CVSS.

Методи дослідження – емпіричний аналіз, формалізація та порівняння.

Метою даної роботи є дослідження питань побудови моделі загроз (порушника) та вразливостей для удосконалення процесу оцінки ризику інформаційної безпеки. В кваліфікаційній роботі введений показник порушника – рівень небезпеки порушника, який включає мотивацію порушника, кваліфікацію порушника, технічний потенціал порушника, розроблена кількісна модель оцінки даних показників, приводяться приклади розрахунку даних показників для навчальної ситуації. В кваліфікаційній роботі запропонований механізм удосконалення методики оцінки ризику CRAMM з використанням моделі порушників та методики оцінки вразливостей CVSS. Проведені дослідження показують, що удосконалена модель порушника, використання в методиці CRAMM механізму оцінки вразливостей по методиці CVSS дає більш точні та обґрунтовані результати оцінки ризику інформаційної безпеки.

ABSTRACT

The report contains: 85 p., 15 fig., 37 tables, 1 application, 18 sources.

THREAT MODEL, VIOLATOR MODEL, VULNERABILITY, INFORMATION SECURITY RISK, CRAMM, CVSS.

The object of research is the process of developing a model of threats (offender) and a model of vulnerabilities in the interest of assessing information security risks to modern information systems.

The subject of the research is the improvement of the threat (infringer) model construction mechanism, the improvement of the CRAMM information security risk assessment methodology taking into account the offender model and the CVSS vulnerability assessment methodology.

Research methods – empirical analysis, formalization and comparison.

The purpose of this work is to study issues of building a model of threats (infringer) and vulnerabilities to improve the information security risk assessment process. In the qualification work, the indicator of the violator is introduced - the level of danger of the violator, which includes the motivation of the violator, the qualifications of the violator, the technical potential of the violator, a quantitative model for evaluating these indicators is developed, and examples of calculating these indicators for an educational situation are given. In the qualification work, a mechanism for improving the CRAMM risk assessment method using the violator model and the CVSS vulnerability assessment method is proposed. The conducted studies show that the improved model of the violator, the use of the CVSS vulnerability assessment mechanism in the CRAMM method gives more accurate and justified information security risk assessment results.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ ТА ТЕРМІНІВ

АСУ – автоматизована система управління
ІБ – інформаційна безпека
ІС – інформаційна система
ІКТ - інформаційно-комунікаційні технології
ЛАЗР – лазерний акустичний засіб розвідки
ПЕМВН – побічні електромагнітні випромінювання та наводки
СУІБ – система управління інформаційною безпекою
CCTA – Central Computer and Telecommunications Agency
CRAMM – CCTA Risk Analysis and Management Method
CVSS – Common Vulnerability Scoring System
NIST – National Snstitute of Standards and Technology

ВСТУП

Оцінка ризиків інформаційної безпеки (ІБ) є одним з ключових процесів при побудові та функціонування системи управління інформаційною безпекою (СУІБ) організації (компанії, установи). Завданням даного процесу є здійснення прогнозу відносно потенційних загроз та вразливостей організації для певних критичних інформаційних ресурсів. Оцінка ризику ІБ безпеки здійснюється з використанням різних методик. Кожна з методик має свої особливості, свій рівень деталізації параметрів. Дослідження механізмів оцінки ризику інформаційної безпеки були проведені в ряді кваліфікаційних робіт [1, 2].

Одним з складних питань при оцінці ризику є побудова моделі загроз та її складової – моделі порушника. Проблема в побудові даних моделей полягає в певній невизначеності відповідно того, хто може бути порушником для організації, яка мотивація та потенціал порушника. Також непростим завданням є визначення вразливостей, через які загрози для організації можуть реалізовуватися.

В кваліфікаційній роботі проведено дослідження моделі загроз та моделі вразливостей.

В першому розділі кваліфікаційної роботи проведений аналіз сучасних підходів, які існують у світі для побудови моделей загроз та вразливостей. Можна побачити, що порушники, як правило, поділяються на класи відповідно їх можливостей. Кількість класів в моделі може бути різним.

В другому розділі кваліфікаційної роботи приведені результати дослідження щодо розробки моделі порушника на підставі трьох параметрів: мотивація порушника, кваліфікація порушника, технічний потенціал порушника. Останні два показники об’єднуються в такий показник, як потенціал порушника. Приведена якісний та кількісний підхід для оцінки даних показників. В роботі розроблена кількісна модель оцінки даних показників порушника, приводяться приклади розрахунку даних показників для навчальної ситуації.

В моделі вразливостей як правило використовується два показника: можливість проникнення порушника до критичного активу; ступінь порушення конфіденційності, цілісності або доступності критичного активу з боку порушника при його проникненні до цього активу. Але в дані показники слабо формалізовані. Тому в кваліфікаційній роботі запропоновано використовувати для оцінки рівня

вразливостей методику CVSSv3.1. В методиці CVSSv3.1 перелік показників значно більше і становлять базові, тимчасові метрики та метрики навколишнього середовища, які описані в першому розділі кваліфікаційної роботи.

В третьому розділі кваліфікаційної роботи запропонований механізм удосконалення методики оцінки ризику CRAMM з використанням моделі порушників та методики оцінки вразливостей CVSS. Проведені дослідження показують, що удосконалена модель порушника, використання в методиці CRAMM механізму оцінки вразливостей по методиці CVSS дає більш точні та обґрунтовані результати оцінки ризику інформаційної безпеки.

Результати досліджень опубліковані в трьох тезах доповідей на Молодіжному міжнародному форумі [3 - 5].

1 СУЧАСНІ ПІДХОДИ ДО ПОБУДОВИ МОДЕЛІ ЗАГРОЗ ТА ПОРУШНИКА

1.1 Загальне поняття моделі загроз

При оцінці ризиків інформаційної безпеки одним з ключових завдань є побудова моделі загроз і її складової – моделі порушника. Оцінка ризиків інформаційної безпеки (ІБ) вимагає розуміння рівня загроз (можливості - Likelihood, ймовірності – Probability, або щорічної кількості - Annualized rate of occurrence). Ця оцінка є різною для різних компаній, різних ризикових ситуацій, різної безпекової ситуації [6, 7].

Відомо, що усі загрози поділяються відповідно джерела загрози на загрози від антропогенних джерел, загрози від природних джерел та загрози від техногенних джерел. До перших відносяться загрози від людини. Такою людиною може бути зловмисник, який реалізує або таргетовану (цільову) атаку, або нетаргетовану атаку. Такою людиною може бути зловмисник, який по необережності або халатності порушує інформаційну безпеку компанії. Зловмисники можуть бути зовнішні та внутрішні (інсайдери). До типів зовнішніх зловмисників можуть відноситися представники спеціальних служб іншої держави, кримінальні структури, потенційні злочинці і хакери, несумлінні партнери, представники аварійних служб і наглядових організацій, технічний персонал телекомунікаційних послуг. До інсайдерів можуть відноситися основний персонал компанії (програмісти, розробники, користувачі), представники служби захисту інформації, допоміжний склад (охорона, прибиральники тощо), технічний персонал (експлуатація, життєзабезпечення).

Під природними загрозами розуміються пожежі, землетруси, повені, урагани, магнітні бурі, радіоактивне випромінювання, інші форс-мажорні обставини. Під техногенними загрозами розуміються технічні проблеми з засобами зв'язку, мережами інженерних комунікацій (каналізація, водопостачання), транспортом, неякісними технічними засобами обробки інформації, неякісними програмними засобами обробки інформації, проблеми з допоміжними засобами (охоронна сигналізація, телефони) тощо.

Модель загроз та модель порушника мають дати відповідь на одне з головних питань при оцінці ризиків ІБ – який порушник реальний для конкретної компанії, яка природна або техногенна загроза реальна для компанії.

При аналізі поставленого питання необхідно зрозуміти, по – перше, що таке модель. Модель — це абстрактне представлення (опис) реальності в певній формі (наприклад, у математичній, фізичній, символічній або графічній), призначене для розвитку розуміння цієї реальності. В доповіді приводяться приклади моделі загроз ІБ, яка представлена в текстовій формі, та приклади математичної моделі таких загроз. В доповіді аналізуються проблеми адекватності та точності моделі загроз. Важливим поняттям при побудові моделі загроз є класифікація загроз. Класифікація — це система групування об'єктів дослідження або спостереження відповідно до їх загальних ознак. Класифікація загроз дозволяє їх поділити по певним класам, східним по значенням параметрів моделі. Це дає змогу виділити для кожного класу загроз східні механізми їх реалізації та побудувати механізми захисту від цих загроз.

При побудові моделі ненавмисних загроз – природних та техногенних в більшості випадків вистачає статистики реалізації цих загроз у світі, країні та регіоні компанії, історія реалізації цих загроз в самій компанії. Методи експертного аналізу загроз з використанням такої інформації дають можливість з певною якістю побудувати модель даних загроз. Складніше ситуація є з побудовою моделі зловмисника. Параметрами моделі мають бути: мотивація зловмисника та його потенціал. Під потенціалом зловмисника розуміється наявність у нього певної кваліфікації та обладнання для реалізації конкретної атаки.

Проведемо аналіз загального підходу до побудови моделі загроз, моделі порушника та моделі вразливостей представлені в [8]. Механізм деструктивного впливу на інформаційну систему можна умовно представити у виді, який показаний на рисунку 1.1 .

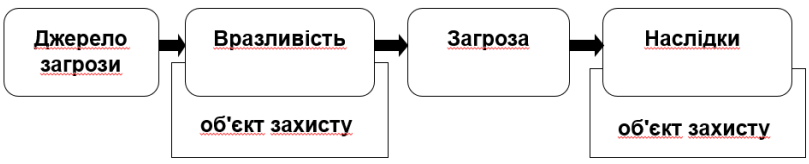

Рисунок 1.1 – Абстрактний механізм деструктивного впливу на інформаційну систему

Джерело загрози - це потенційні антропогенні, технічні або стихійні носії загрози безпеки.

Загроза – це потенційна можливість певним чином порушити інформаційну безпеку.

Уразливість – це дефект або слабке місце в системних захисних процедурах, проект, реалізації або внутрішніх регуляторах безпеки, які можуть проявитися (будучи випадково активізовані або навмисне проексплуатувати) і привести до порушення безпеки або відступу від політики безпеки.

Наслідки – можливі наслідки реалізації загрози при взаємодії джерела загрози через уразливості на інформаційну систему.

Сучасний приклад джерел загроз для сфері інформаційної безпеки представлений на рис. 1.2.

Рисунок 1.2 – Приклад джерел загроз для сфері інформаційної безпеки

Як показав світовий і вітчизняний досвід, атаки є найбільш небезпечними загрозами (що обумовлено їх ретельною підготовкою, скритністю проведення, цілеспрямованим вибором об'єктів і цілей атак).

Атаки готуються і проводяться порушником, причому можливості проведення атак обумовлені можливостями порушника. Іншими словами, конкретні можливості порушника визначають конкретні атаки, які може провести порушник.

Для більш повного аналізу потенційних загроз вводиться поняття «модель загроз». Для більш повного аналізу потенційних атак вводиться поняття «модель порушника». Модель порушника тісно пов'язана з моделлю загроз і, по суті, є її частиною. Смислові відношення між ними такі. У моделі загроз міститься максимально повний опис загроз безпеки об'єкта.

Модель порушника містить опис припущення про можливості порушника, які він може використовувати для розробки і проведення атак, а також про обмеження на ці можливості.

Первинну інформацію для розробки моделі порушника доцільно отримати у вищого менеджменту, що представляє себе положення організації на ринку, що має відомості про конкурентів і про те, яких методів впливу можна від них очікувати.

Відомості, необхідні для розробки моделі порушника, можна отримати і з спеціалізованих досліджень щодо порушень в області інформаційної безпеки в тій сфері бізнесу, для якої проводиться аналіз ризиків.

Правильно пророблена модель порушника дозволяє адекватно оцінити ризики інформаційної безпеки організації і відповідно виробити вимоги до СУІБ, розробити заходи щодо захисту, оптимально розподілити ресурси для побудови СУІБ.

Чим точніше зроблений прогноз (складені модель загроз і модель порушника), тим нижче ризики порушення ІБ в організації при мінімальних ресурсних витратах.

1.2 Сучасні підходи до побудови моделі зовнішнього порушника інформаційної безпеки

Приклад методики порушника ІБ, яка побудована на підставі його потенціалу, представлена в таблиці 1.1.

Таблиця 1.1. – Методика порушника інформаційної безпеки на основі його потенціалу

№ з/п	Потенціал порушника	Типи	Можливості реалізації загроз інформаційній безпеці
1	2	3	4
1.	Порушники з низьким потенціалом	Зовнішні суб'єкти (фізичні особи), особи, які забезпечують функціонування інформаційних систем або обслуговуючих інфраструктуру оператора, користувачі інформаційної системи, колишні працівники, особи, які залучаються для установки, налагодження, монтажу, пусконалагоджувальних та інших робіт	Мають можливість отримати інформацію про уразливість окремих компонент інформаційної системи, яка опублікована в загальнодоступних джерелах. Мають можливість отримати інформацію про методи та засоби реалізації загроз безпеці інформації , опублікованих в загальнодоступних джерелах, і (або) самостійно здійснює створення методів і засобів реалізації атак на підставі власних знань та власного досвіду
2.	Порушники з середнім потенціалом	Терористичні, екстремістські угруповання, злочинні групи (кримінальні структури), конкуруючі організації, розробники, виробники, постачальники програмних, технічних та програмно-технічних засобів, адміністратори інформаційної системи і адміністратори безпеки	Мають всі можливості порушників з низьким потенціалом. Мають обізнаність про заходи захисту інформації, що застосовуються в інформаційній системі даного типу. Мають можливість атакувати інформаційну систему з використанням наявних у вільному доступі апаратних і програмних засобів, в тому числі складних в технічному плані та вартісних

Продовження таблиці 1.1

1	2	3	4
3.	Зловмисник з високим потенціалом	Спеціальні служби іноземних держав	Мають всі можливості порушників з низьким та середнім потенціалами. Мають можливість здійснювати атаку з використанням апаратно-програмних та програмних засобів, створених в спеціалізованих лабораторіях. Використовують наукові дослідження щодо розробки та реалізації атак.

В методиці NIST CVSS v3 metrics представлений свій підхід до моделі порушника, який реалізований в метриці розрахунку рівня вразливості [9]. Окремі елементи даної моделі представлені в таблиці 1.2.

Таблиця 1.2 – Приклад метрики методики Common Vulnerability Scoring System. Вектор доступу (Attack Vector)

№ з/п	Метрика	Опис
1.	Потребується фізичний доступ	Зловмисникові потрібен безпосередній фізичний доступ до об'єкта, на якому розташована вразливість
2.	Потребується локальний доступ	Зловмисник експлуатує вразливість за допомогою локального доступу, вразливий компонент не прив'язується до стеку мережі, а шлях атакуючого – через можливості читання / запису / виконання.
3.	Можливий доступ із суміжної мережі	Атака обмежена однією спільною фізичною (наприклад, Bluetooth, IEEE 802.11) або логічною (наприклад, локальною IP-підмережею) мережею, і не може бути виконана через границю шару OSI (наприклад, маршрутизатор)
4.	Можливий доступ з будь-якої мережі	Зловмисник може атакувати віддалено через OSI layer 3 (мережевий рівень)

Таблиця 1.3 – Приклад метрики методики Common Vulnerability Scoring System. Складність атаки (Attack Complexity)

№ з/п	Метрика	Опис
1.	Низька	Немає особливих умов для доступу зловмисником до вразливості (наприклад, коли система доступна багатьом користувачам одночасно або коли вразлива конфігурація працює на безлічі вузлів мережі)
2.	Висока	Успішність атаки вимагає від злочинця здійснювати певні вимірювані зусилля для підготовки чи виконання атаки. Наприклад проведення розвідки системи захисту, підготовка цільового середовища для підвищення надійності експлуатації вразливості, вбудовування себе в логічний мережевий шлях між ціллю та ресурсом, що атакується, для перехоплення або зміни мережевих зв'язків (наприклад, атака – людина посередині).

Таблиця 1.4 – Приклад метрики методики Common Vulnerability Scoring System. Обов'язкові привілеї (Privileges Required)

№ з/п	Метрика	Опис
1.	Немає	Зловмиснику не потрібна авторизація перед атакою
2.	Висока	Зловмиснику потрібні привілеї, які надають основні можливості користувача, які, як правило, можуть впливати лише на налаштування та файли, що належать користувачеві. Крім того, зловмисник з низькими привілеями може мати можливість впливати лише на нечутливі ресурси.
3.	Низька	Зловмисник авторизований, тобто вимагає привілеїв, які забезпечують значний (наприклад, адміністративний) контроль над вразливим компонентом, який може вплинути на загальні параметри та файли.

Таблиця 1.5 – Приклад метрики методики Common Vulnerability Scoring System. Взаємодія з користувачем (User Interaction)

№ з/п	Метрика	Опис
1.	Немає	Вразливість системи може експлуатуватися зловмисником без необхідності дій будь-якого іншого (крім зловмисника) окремого користувача (або процесу, ініційованого користувачем)
2.	Потрібно	Для успішної експлуатації уразливості зловмисником будь-якому іншому користувачеві (крім зловмисника) потрібно вжити певні дії, перш ніж вразливість може бути використана.

Приклад класифікації порушників за рівнем можливостей при порушенні ІБ автоматизованої системи управління (АСУ) представлений в таблиці 1.6.

Таблиця 1.6 – Приклад моделі порушника для автоматизованої системи управління

№ з/п	Рівень порушника	Можливості порушника
1.	Перший рівень	Запуск завдань (програм) з фіксованого набору, що реалізують заздалегідь передбачені функції по обробці інформації.
2.	Другий рівень	Визначається можливістю створення і запуску власних програм з новими функціями з обробки інформації.
3.	Третій рівень	Визначається можливістю управління функціонуванням АСУ, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування.
4.	Четвертий рівень	Визначається всім обсягом можливостей осіб, які здійснюють проектування, реалізацію і ремонт технічних засобів АСУ, аж до включення до складу власних технічних засобів з новими функціями з обробки інформації.

При цьому в своєму рівні порушник вважається фахівцем вищої кваліфікації, знає все про АСУ і, зокрема, про систему і засобах її захисту.

Підхід до оцінки мотивації зовнішнього порушника щодо порушення ІБ представлений в таблиці 1.7.

Таблиця 1.7 – Приклад підходу до оцінки мотивації зовнішнього порушника щодо порушення інформаційної безпеки

№ з/п	Вид порушника	Можлива мотивація
1.	Одиночний порушник	1) Отримати матеріальну вигоду. 2) Помститися. 3) Самоствердитися. 4) Підвищити свою кваліфікацію тощо
2.	Комерційна фірма – конкурент	1) Прибрати конкурента або знизити його можливості (DDOS – атака знижує інформаційні можливості організації); 2) Отримання матеріальної вигоди через переманювання клієнтів організації (з'їм інформації про клієнтів організації з подальшим переманюванням); 3) Підвищення своїх конкурентних можливостей через бенчмаркінг тощо.
3.	Злочинні організації	1) Отримання матеріальної вигоди. 2) Виконання замовлення прибрати конкурента тощо
4.	Спеціальні служби іноземної держави	1) Отримання інформації про фундаментальні розробки, плани керівництва тощо, особливо що складають держ. таємницю. 2) Прибрати конкурента, що працює на світових ринках. 3) Дезорганізація системи управління держави (економіка, фінанси, транспорт, військове управління та інше).

Приклад підходу до класифікації зовнішнього порушника за наявними у нього ресурсами представлений в таблиці 1.8.

Таблиця 1.8 – Приклад підходу до класифікації зовнішнього порушника за наявними у нього ресурсами

№ з/п	Наявність ресурсу	Зв'язок наявності ресурсу з можливостями	Тип порушника
1.	Низька	Може використовувати: саморобні закладні пристрої; доступ через мережу	Поодинокий зловмисник
2.	Середня	Може використовувати: - недороге заводське обладнання для знімання інформації (стетоскопи, диктофони тощо) - доступ через мережу.	Поодинокий зловмисник Невелика комерційна організація
3.	Висока	Може використовувати дороге обладнання для порушення безпеки інформації (ЛАЗР, засоби знімання ПЕМВН тощо)	Середня комерційна організація, середня кримінальна структура
4.	Дуже висока	Може використовувати будь-які канали для порушення інформаційної безпеки (професійні технічні засоби розвідки тощо)	Велика комерційна організація, спецслужба іноземної держави, велика кримінальна структура

Приклад загальній класифікації зовнішнього порушника за наявними у нього знань про інформаційну систему організації представлений в таблиці 1.9.

Таблиця 1.9 – Приклад загальній класифікації зовнішнього порушника за наявними у нього знань про інформаційну систему організації

№ з/п	Наявність інформації та знань про ІС організації	Зв'язок наявності ресурсу з можливостями	Тип порушника
1.	Низька	Має загальний рівень знань про побудову інформаційну систему (ІС) організації, системи захисту ІС	Студент, випускник вузу (по ІТ технологіям або ІБ)
2.	Середня	Має теоретичні та практичні знання з системі інформаційної безпеки організації. Спеціалізується на побудові систем захисту ІС організації	Практикуючий фахівець з ІБ
3.	Висока	Має повну інформацію про побудову ІС організації, забезпечення інформаційної безпеки організації	Спеціаліст з інформаційних технологій, ІБ, який працював в даній організації. Зловмисник, який співпрацює з таким фахівцем

Приклад класифікації порушників з точки зору методу реалізації атаки (за місцем дії) приведений в таблицях 1.10 – 1.11.

Таблиця 1.10 – Приклад класифікації порушників з точки зору методу реалізації атаки (за місцем дії)

№ з/п	Шлях доступу до інформації	Особливості доступу (канали атак)
1	2	3

Продовження таблиці 1.10

1	2	3
1.	Без доступу на контрольовану територію організації	За мережі через Інтернет Через ПЕМВН
2.	З контрольованої території без доступу в будівлі і споруди	Через ПЕМВН. Необхідний фізичний доступ на контрольовану територію
3.	Усередині приміщень, але без доступу до технічних засобів	Через ПЕМВН. Необхідний фізичний доступ на контрольовану територію і в приміщення
4.	З робочих місць користувачів локальної мережі	Необхідний фізичний доступ на контрольовану територію і в приміщення. Необхідно знати логін, пароль
5.	З робочого місця системного адміністратора	Необхідний фізичний доступ на контрольовану територію і в приміщення, де знаходиться сервер. Необхідно знати логін, пароль

Таблиця 1.11 – Приклад класифікації порушників з точки зору методу реалізації атаки (за місцем дії)

№ з/п	Шлях доступу до інформації	Особливості доступу (канали атак)
1	2	3
1.	Без доступу на контрольовану територію організації	Через спрямовані мікрофони Через ЛАЗР Через акусто-електромагнітний канал

Продовження таблиці 1.11

1	2	3
2.	З контрольованої території без доступу в будівлі і споруди	Необхідний фізичний доступ на контрольовану територію. Через спрямовані мікрофони Через віброакустичний, акусто-електричний і акусто-електромагнітний канал витоку
3.	З приміщень організації, але без доступу у виділене приміщення	Необхідний фізичний доступ на контрольовану територію і в приміщення організації. Через віброакустичний, акусто-електричний і акусто-електромагнітний канал витоку
4.	З доступом у виділене приміщення	Необхідний фізичний доступ на контрольовану територію і в виділене приміщення. Через прямий акустичний канал витоку

Підхід до оцінки можливого часу і способу атаки представлений в таблиці 1.12. Може визначатися на підставі припущення про наявність у порушника інформації про режим роботи організації, її інформаційної системи, системи інформаційної безпеки організації.

Таблиця 1.12 – Підхід до оцінки можливого часу і способу атаки

№ з/п	Опис порядку вибору часу і способу атаки	Умови для вибору часу і способу атаки
1	2	3
1.	Атака здійснюється в будь-який зручний для атакуючої сторони час без урахування можливих дій ІС і СУІБ організації (рефлексія 0 рівня).	Порушник не проводить розвідку ІС, що атакується, не проводить серйозної аналітичної роботи з прогнозування дій СУІБ організації

Продовження таблиці 1.12

1	2	3
2.	Вибір часу (і способу) атаки проводиться на основі розуміння щодо режиму функціонування ІС і СУІБ, організації, можливих захисних дій організації, атакується (рефлексія 1 рівня)	Порушник проводить розвідку режиму функціонування ІС і СУІБ, визначає чи прогнозує можливі дії СУІБ при тих чи інших видах атак
3.	Вибір часу (і способу) атаки проводиться на підставі розуміння того, як СУІБ прогнозує можливі дії атакуючої сторони і будує стратегію і тактику захисту на основі такого прогнозу (рефлексія 2 рівня)	Порушник проводить ретельну розвідку структури, режиму функціонування ІС і СУІБ, а також проводить серйозну аналітичну роботу по оцінці СУІБ організації, що атакується.

1.3 Сучасні підходи до побудови моделі внутрішнього порушника (інсайдера)

На даний момент однією з розповсюджених моделей та класифікації інсайдерів є представлена на рис 1.3. Дана модель була опублікована працях країни агресора [11]. На наш погляд аналіз наукових праць країни агресора має бути обов'язковим для розуміння його намірів та можливостей.

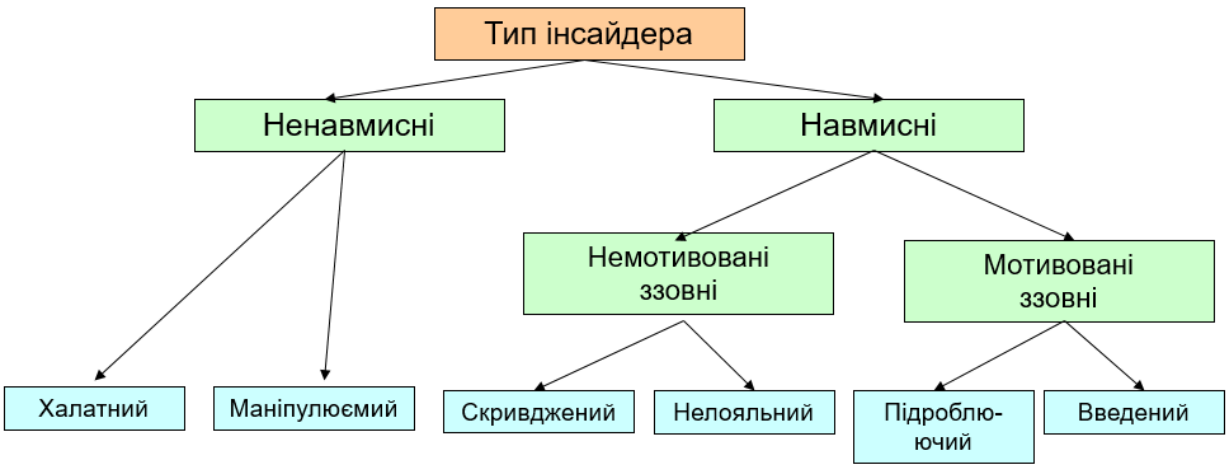

Рисунок 1.3 – Приклад класифікації внутрішніх порушників (інсайдерів)

Халатні інсайдери («необережні») є найбільш поширеним типом внутрішніх порушників. Їх порушення щодо критичної інформації носять невмотивований характер, не мають конкретних цілей, наміру, користі. Дані співробітники створюють незлонамерені, ненаправлені загрози (при цьому можуть діяти з кращих спонукань). Зіткнувшись з неможливістю скопіювати інформацію, цей тип порушника буде діяти за інструкцією – звернутися за допомогою до колег або системному адміністратору, які пояснять йому, що винесення інформації за межі офісу заборонено.

Маніпульовані інсайдери – найчастіше жертви соціальної інженерії. Можуть віддати зовнішньому зловмисникові внаслідок обману персональну інформацію – паролі, пін-коди, номери кредитних карт, конфіденційну інформацію тощо. Оскільки маніпульовані і недбалі співробітники діють зі свого розуміння «блага» компанії (виправдовуючись тим, що іноді заради цього блага потрібно порушити «дурні» інструкції, які тільки заважають ефективно працювати), два цих типу порушників іноді об'єднують в тип «незлонамеренних». Однак шкода не залежить від намірів, зате від намірів залежить поведінка порушника в разі неможливості здійснити свою дію. Як лояльні співробітники, ці порушники, зіткнувшись з технічним блокуванням їх спроб порушити регламенти зберігання і руху інформації, звернуться за допомогою до колег, технічного персоналу або керівництву, які можуть вказати їм на неприпустимість планованих дій.

Ображені порушники (по-іншому, саботажники) – це співробітники, які прагнуть завдати шкоди компанії з особистих мотивів. Найчастіше мотивом такої поведінки може бути образа, що виникла через недостатню оцінки їх ролі в компанії – недостатній розмір матеріальної компенсації, неналежне місце в корпоративній ієрархії, відсутність елементів моральної мотивації або відмову у виділенні корпоративних статусних атрибутів (ноутбука, автомобіля, секретаря). Для оцінки моделей поведінки порушника відзначаються два ключових відмінності від інших типів порушників: по-перше, співробітник не збирається залишати компанію; по-друге, він прагне завдати шкоди, а не вкрасти інформацію. Іншими словами, він прагне, щоб керівництво не дізналося, що витік стався з його вини, і, зіткнувшись з технічною неможливістю вкрасти будь-яку інформацію, він може направити свою руйнівну енергію на щось інше, наприклад на знищення або фальсифікацію доступної інформації, розкрадання матеріальних цінностей. Ображений інсайдер, виходячи з власних уявлень про цінності інформації та завдану шкоду, визначає,

яку інформацію має сенс викрасти і кому її передати. Найчастіше він передає інформацію в пресу або тіньові структури відповідно для оголошення або шантажу.

Нелояльні інсайдери – перш за все, це співробітники, що прийняли рішення змінити місце роботи, або міноритарні акціонери (акціонер, загальна частка власності якого в компанії, зареєстрованої на фондовій біржі, становить менше 50%), які вирішили відкрити власний бізнес (стало звичним, що звільняється співробітник комерційного відділу забирає з собою копію бази клієнтів, а фінансового – копію фінансової бази). По спрямованості загроза, що виходить від таких порушників, є ненаправленою - порушники намагаються забрати максимально можливу кількість доступної інформації, часто навіть не підозрюючи про її цінності і не маючи уявлення, як вони її будуть використовувати. Найчастіший спосіб отримання доступу до інформації або можливості її скопіювати – це імітація виробничої необхідності. Саме на цьому їх найчастіше і ловлять. Викравши інформацію, вони не приховують факту викрадення. Більш того, іноді викрадена інформація використовується як гарант для забезпечення комфортного звільнення - з компенсацією і рекомендаціями.

Ображені і нелояльні співробітники самі визначають об'єкт розкрадання, знищення або спотворення і місце його збуту.

Підроблюючі порушники – це співробітники, мета яких визначає замовник викрадення інформації. В цьому випадку інсайдери прагнуть якомога надійніше завуалювати свої дії (принаймні, до моменту успішного розкрадання). Нерідкі випадки інсайдерів мимоволі: шантаж, вимагання ззовні буквально не залишають їм вибору і змушують виконувати накази третіх сторін. Саме тому підроблюючі інсайдери можуть робити найрізноманітніші дії при неможливості виконання поставленого завдання. Залежно від умов вони можуть припинити спроби, імітувати виробничу необхідність, а в найбільш важких випадках піти на злам, підкуп інших співробітників, щоб отримати доступ до інформації.

Введені інсайдери – співробітники спеціально влаштовані на роботу для викрадення інформації, або завербовані, тобто спочатку лояльні, але згодом підкуплені або залякані. Небезпека, яку представляють порушники цього типу, полягає в тому, що в разі технічних обмежень на винос інформації за межі корпоративної інформаційної мережі «замовники» можуть забезпечити їх відповідними пристроями або програмами для обходу захисту і «введений» порушник піде до кінця,

щоб отримати дані. У його арсеналі будуть найвитонченіші засоби і великий професійний досвід злому.

Зведені дані по опису моделі інсайдерів приведені в таблиці 1.13.

Таблиця 1.13 – Зведені дані моделі інсайдерів

№ з/п	Тип	Умисел	Користь	Постановка задачі	Дії при неможливості вкрасти інформацію
1.	Халатний	Ні	Ні	Ні	Повідомлення
2.	Маніпульований	Ні	Ні	Ні	Повідомлення
3.	Ображений	Так	Ні	Сам	Відмова
4.	Нелояльний	Так	Ні	Сам	Імітація
5.	Підроблюючий	Так	Так	Сам/Ззовні	Відмова/імітація/злом
6.	Введений	Так	Так	Ззовні	Злом

Приклад класифікації інсайдерів за рівнем ризику (враховує посаду інсайдера в організації – рівень знання інсайда про інформаційну систему і рівень його доступу до інформаційних активів) представлений на рис. 1.4.

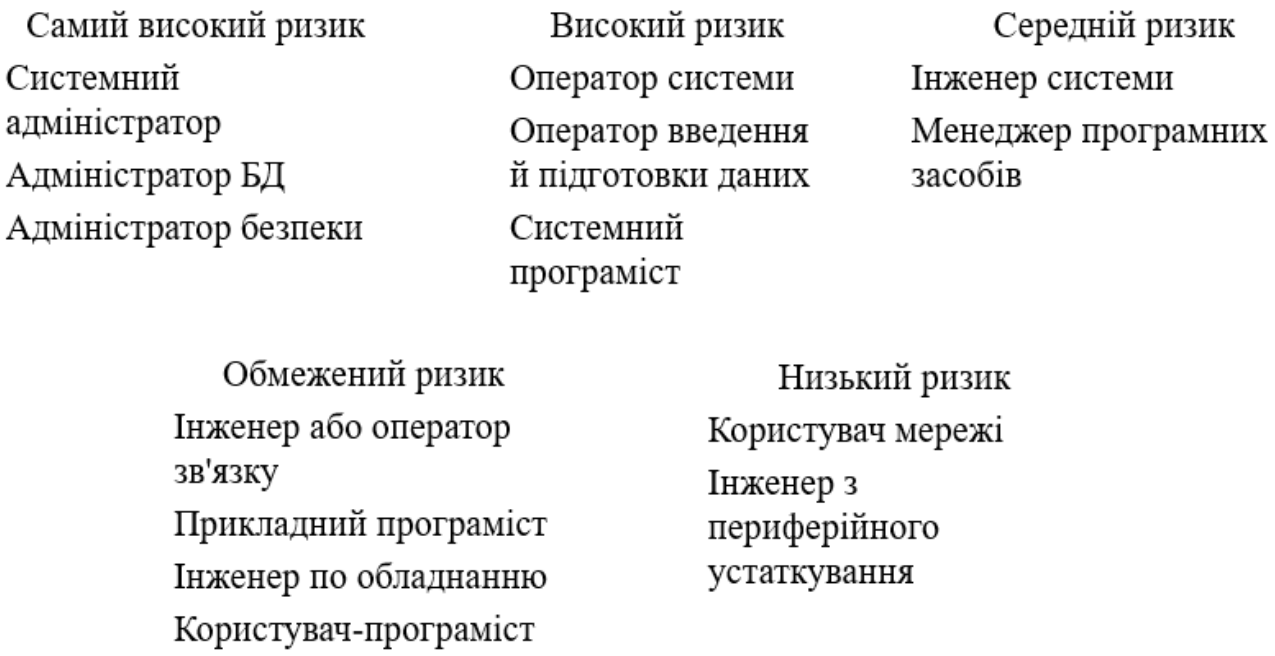

Рисунок 1.4 – Приклад класифікації інсайдерів за рівнем ризику

1.4 Приклад моделі зловмисників, представлений в стандарті ISO/IEC 27005

Дана модель представлена в додатку С стандарту. В кваліфікаційній роботі дана модель представлена в таблиці 1.14 [7].

Таблиця 1.14 – Приклад моделі зловмисників, представлений в стандарті ISO/IEC 27005

№ з/п	Джерело загрози	Мотивація	Можливі наслідки
1	2	3	4
1.	Хакер, крекер	Повстання Его Виклик Статус Гроші	Хакерство Соціальна інженерія Вторгнення в систему, порушення Несанкціонований доступ до системи

Продовження таблиці 1.14

1	2	3	4
2.	Комп'ютерний злочинець	Руйнування інформації Незаконне розкриття інформації Грошово-кредитна вигода Неправомірне чергування даних	Комп'ютерний злочин (наприклад, кібер-переслідування) Шахрайська дія (наприклад, перегравання, наслідування, перехоплення) Інформаційне хабарництво Імітація Вторгнення в систему
3.	Терорист	Помста Розвідка Руйнування Шантаж Політичні вигоди Освітлення у пресі	Бомба/Тероризм Інформаційна війна Системна атака (наприклад, розподілена відмова в обслуговування) Проникнення в систему Втручання у систему
4.	Індустріальний шпигунство (компанії, іноземні уряди, інші урядові інтереси)	Конкурентоспроможне перевага Економічний шпигунство	Економічна розвідка Інформаційний крадіжка Вторгнення в персональні дані Соціальна розробка Проникнення в систему Несанкціонований доступ до системи (доступ до секретної, приватної та/або пов'язаною з технологією інформації)

Продовження таблиці 1.14

1	2	3	4
5.	Інсайдер (погано навчені, розсерджені, зловмисні, недбалі, нечесні чи звільнені службовці)	Розвідка Его Цікавість Грошово-кредитна вигода Помста Ненавмисні помилки та упущення (наприклад, помилка введення даних, помилка програмування)	Напад на службовця Шантаж Перегляд секрету фірми Неправильне комп'ютерне звернення Шахрайство та крадіжка Інформаційне хабарництво Введення фальсифікованих даних, руйнування даних Перехоплення Шкідливий код (наприклад, вірус, логічна бомба, троянський кінь) Продаж персонального інформації Системні помилки Вторгнення в систему Системний саботаж Несанкціонований доступ до системи

1.5 Моделі вразливостей інформаційних систем

Приклад моделі вразливостей, представлений в таблиці 1.15 стандарту ISO/IEC 27005 [7].

Таблиця 1.15 дає приклади вразливостей у різних галузях безпеки, включаючи приклади загроз, які могли б експлуатувати цю вразливість. Перелік може забезпечити довідку під час оцінки загроз та уразливості, визначити відповідні інциденті сценарії.

Таблиця 1.15 – Приклад моделі вразливостей інформаційних систем

№ з/п	Тип вразливостей	Приклад вразливостей	Приклад загрози
1	2	3	4
1.	Апаратні засоби	Недостатнє обслуговування / дефектна інсталяція з носіїв даних	Пролом у ремонтопридатності інформаційної системи
		Вади схем для періодичних замін	Руйнування обладнання або носіїв
		Сприйнятливість до вологості, пилу, забруднення	Пил, корозія, зледеніння
		Чутливість до електромагнітної радіації	Електромагнітна радіація
		Вади ефективного контролю внесення змін конфігурації	Помилка використання
		Сприйнятливість до змін напруги	Втрата джерела живлення
		Сприйнятливість до температурним змінам	Метеорологічне явище
		Незахищене зберігання	Крадіжка носіїв або документів
		Недолік в обережності при знищення	Крадіжка носіїв або документів
		Неконтрольоване копіювання	Крадіжка носіїв або документів

Продовження таблиці 1.15

1	2	3	4
2.	Програмне забезпечення	Відсутність чи недостатня програмне тестування	Зловживання правами
		Відомі недоліки в програмне забезпечення	Зловживання правами
		Немає 'виходу з системи' при залишення робочої станції	Зловживання правами
		Передача чи багаторазове використання носіїв даних без належного стирання	Зловживання правами
		Невелика кількість ревізій	Зловживання правами
		Неправильний розподіл прав доступу	Зловживання правами
		Широко розповсюджене програмне забезпечення	Спотворення даних
		Застосування прикладних програм до фальшивих даних у термінах часу	Спотворення даних
		Складний користувальницький інтерфейс	Помилка використання
		Встановлено неправильний параметр	Помилка у використанні
		Некоректні дати	Помилка у використанні

Продовження таблиці 1.15

1	2	3	4
3.	Мережа	Вади ідентифікуючих та розпізнавальних механізмів для користувальницької автентифікації	Підроблення прав
		Незахищені таблиці паролів	Підроблення прав
		Поганий менеджмент паролями	Підроблення прав
		Запущено непотрібні служби	Незаконна обробка даних
		Недопрацьоване чи нове програмне забезпечення	Програмний збій
		Неясні чи неповні специфікації для розробників	Програмний збій
		Вади ефективного контролю внесення змін	Програмний збій
		Неконтрольоване завантаження та використання програмного забезпечення	Підробка програмного забезпечення
		Вади у процедурі резервного копіювання	Підробка програмного забезпечення
		Вади фізичного захисту будівлі, дверей та вікон	Крадіжка носіїв або документів
		Нестача доказу посилки або отримання повідомлення	Заперечення дій
		Незахищені лінії зв'язку	Підслуховування
		Незахищений чутливий трафік	Підслуховування
		Погане спільне проведення	Відмова телекомунікаційного обладнання
		Єдиний пункт відмови	Відмова телекомунікаційного обладнання
		Вади ідентифікації та автентифікація відправника та одержувача	Підроблення прав
		Небезпечна мережева архітектура	Віддалений шпигунство

Продовження таблиці 1.15

1	2	3	4
4.	Персонал	Відсутність персоналу	Порушення доступності персоналу
		Неадекватні процедури вербування	Знищення обладнання або носіїв
		Недостатнє навчання безпеки	Помилка використання
		Неправильне використання програмного забезпечення та обладнання	Помилка використання
		Вади розуміння безпеки	Помилка використання
		Нестача механізмів моніторингу	Незаконна обробка даних
		Неконтрольована робота зовнішнім штатом або прибираючим персоналом	Крадіжка носіїв або документів
		Вади політики для правильного використання носіїв передачі даних та обміну повідомленнями	Несанкціоноване використання обладнання
5.	Сайт організації	Неадекватне та недбале використання фізичного контролю доступу до будівлі та приміщень	Знищення обладнання або носіїв інформації
		Розташування в області, сприйнятливою до затоплення	Нестабільна потужність мережі
		Повінь	Втрата джерела живлення
		Нестача фізичного захисту створення, дверей та вікон	Крадіжка обладнання
		Вади формальної процедури для користувальницької реєстрації та де-реєстрації	Зловживання правом

Продовження таблиці 1.15

1	2	3	4
5.	Сайт організації	Вади формального процесу для перегляду права доступу (диспетчерський менеджмент)	Зловживання правом
		Дефіцит або недостатні умови (щодо безпеки) у контрактах з клієнтами та/або третіми особами	Зловживання правом
		Вади у процедурі для контролю за коштами обробки інформації	Зловживання правом
		Вади регулярних ревізій (диспетчерський менеджмент)	Зловживання правом
		Брак процедур виявлення ризику та оцінки	Зловживання правом
		Недостатність інформації в записах звітів про несправності журналах адміністратора та користувача	Зловживання правом
		Неадекватна відповідь обслуговуючого сервісу	Порушення ремонтопридатності інформаційної системи
		Вади або недостатнє угоди сервісного обслуговування	Порушення ремонтопридатності інформаційної системи
		Вади процедури контролю внесення змін	Порушення ремонтопридатності інформаційної системи
		Вади формальної процедури для менеджменту	Спотворення даних

Продовження таблиці 1.15

1	2	3	4
5.	Сайт організації	Вади формальних процедур записів для СУІБ, які робить диспетчерський менеджмент	Спотворення даних
		Вади формального дозволи для процесу загального доступу до інформації	Дані з ненадійних джерел
		Вади належного розподілу обов'язків інформаційної безпеки	Заперечення дій
		Вади планів безперервності	Відмова обладнання
		Вади політики використання пошти	Помилка використання
		Нестача процедур для того, щоб ввести програмне забезпечення в експлуатовані системи	Помилка використання
		Нестача звітів у файлах реєстрації адміністратора та оператора	Помилка використання
		Нестача процедур для обробки секретних даних	Помилка використання
		Вади обов'язків інформаційної безпеки в описах завдань	Помилка використання
		Вади або недостатні умови (щодо інформаційної безпеки) у контрактах із службовцями	Незаконна обробка даних

Продовження таблиці 1.15

1	2	3	4
		Нестача певного дисциплінарного процесу в випадку інформаційного інциденту безпеки	Крадіжка обладнання
		Нестача формальної політики з використання мобільної комп'ютерної техніки	Крадіжка обладнання
		Брак менеджменту активами дистанційного резервування	Крадіжка обладнання
5.	Сайт організації	Нестача або недостатня політика «чистого столу та чистого екрану»	Крадіжка носіїв або документів
		Нестача санкцій коштом обробки інформації	Крадіжка носіїв або документів
		Нестача встановлених контрольних механізмів у у разі порушень правил безпеки	Крадіжка носіїв або документів
		Нестача регулярних переглядів контролів	Несанкціоноване використання обладнання
		Нестача процедур для того, щоб повідомити про вразливість безпеки	Несанкціоноване використання обладнання
		Нестача процедур погодження умов з інтелектуальної власністю	Використання підробки або скопійованого програмного забезпечення

Для ідентифікації вразливості залежно від критичності інформації та інформаційно-комунікаційних технологій (ІКТ) можуть використовуватися превентивні

методи, такі як тестування інформаційної системи, системних та доступних ресурсів (наприклад, розподілені фонди, доступні технології, проведення тесту людей–експертів). Випробувальні методи включають:

– автоматизований інструмент сканування вразливостей;
– тестування безпеки та оцінку;
– тестування проникнення;
– перегляд коду.

Щоб переглянути групу головних комп'ютерів або мережу на предмет відомих уразливих служб (наприклад, систему, що дозволяє анонімний протокол передачі файлів), передачу sendmail), використовується автоматизований інструмент сканування вразливості. Однак слід зазначити, що частина потенційних уразливостей, ідентифікованих автоматизованим інструментом сканування, можливо, не є реальною вразливістю в контексті системного середовища. Наприклад, деякі з цих інструментальних засобів сканування оцінюють потенційну вразливість, не розглядаючи середовище сайту та вимоги. Частина вразливостей, позначених автоматизованим програмним забезпеченням сканування, можливо, фактично не вразлива для певного сайту, але може бути налаштована, тому що обстановка вимагає цього. Таким чином, цей випробувальний метод може зробити помилкові допуски.

Тестування безпеки та оцінка є іншою методикою, яка може використовуватися в ідентифікації вразливості системи ІКТ під час оцінки ризику.

Це включає розробку та виконання плану випробувань (наприклад, випробувальний скрипт, випробувальні процедури та очікувані результати випробувань). Мета системного тестування безпеки полягає в тому, щоб перевірити ефективність контролю безпеки системи ІСТ, оскільки вони були застосовані в експлуатованому середовищі. Ціль полягає в тому, щоб гарантувати, що менеджмент використовує схвалену специфікацію безпеки для прикладного програмного забезпечення та обладнання та здійснюють політику безпеки організації або використовує галузеві стандарти.

Може використовуватися тестування проникнення, щоб доповнити перегляд контролю безпеки та гарантувати, що забезпечені різні аспекти системи ІКТ.

Коли застосовується тестування проникнення в процесі оцінки ризику, результати цього можуть використовуватися, щоб оцінити здатність системи ІКТ протистояти навмисним спроб обійти системну безпеку. Мета полягає в тому,

щоб перевірити систему ІКТ з точки зору джерела загрози та ідентифікувати потенційні відмови у схемах системні захисту ІКТ.

Перегляд коду є найповнішим (але також найдорожчим) у шляху оцінки вразливості.

Результати цих типів тестування безпеки допоможуть ідентифікувати вразливість системи.

Важливо, що інструментальні засоби проникнення та методики можуть дати хибні результати, якщо не успішно експлуатується вразливість. Щоб експлуатувати специфічну вразливість, потрібно знати точну систему /додаток/ та встановлені виправлення на перевіреній системі. Якщо ці дані не відомі під час тестування, це не може бути можливим для успішної експлуатації специфічної вразливості (наприклад, отримуючи remote reverse shell12); проте, це все ж таки можливо, щоб зруйнувати або перезапустити процес або систему, що перевіряється. У такому разі перевірений об'єкт слід вважати вразливим.

2 МЕТОДИКА ПОБУДОВИ МОДЕЛІ ЗАГРОЗ ТА МОДЕЛІ ВРАЗЛИВОСТЕЙ

2.1 Пропозиції щодо оцінки параметрів моделі порушника та моделі вразливостей

Аналіз чинних підходів до моделі порушника показав, що параметрами цієї моделі є:

– мотивація порушника;

– кваліфікація порушника;

– технічний потенціал порушника.

Останні два показники в певних моделях порушників об’єднуються в такий показник, як потенціал порушника.

В моделі вразливостей як правило використовується два показника:

– можливість проникнення порушника до критичного активу;

– ступінь порушення конфіденційності, цілісності або доступності критичного активу з боку порушника при його проникненні до цього активу.

В методиці CVSSv3 перелік показників значно більше і становить базові, тимчасові метрики та метрики навколишнього середовища, які описані в першому розділі кваліфікаційної роботи.

Проведемо аналіз даних показників.

Дуже важливо зрозуміти особливості визначення параметрів, точність параметрів та адекватність параметрів.

1) Мотивація порушника.

Даний показник показує, чому певний порушник намагається атакувати критичні активи організації.

Відповідно до чинної статистики загрози є спрямовані та неспрямовані. Якщо загроза неспрямована, то зловмисник атакує будь які інформаційні ресурси. Така ситуація має місце, наприклад, коли шкідлива програма розповсюджується через інтернет, і та атакує будь які інформаційні ресурси, через які вона може проникнути.

Якщо загроза є спрямованою, порушник атакує організацію, яка є його ціллю. При цьому порушник може проводити аналіз системи захисту, збирати ін-

формацію про посадових осіб організації, проводити розвідувальні або імітуючі дії тощо.

Мотивація порушника може мати різні категорії:

– отримання фінансової вигоди;

– конкуренція в бізнес-середовищі;

– крадіжка ноу-хау, інтелектуальних знань;

– дезорганізація системи управління організації;

– помста тощо.

Класифікацію рівня мотивації можна зробити наступним чином:

– мотивація низька – порушник не має намірів атакувати дану організацію. Таким порушником може бути халатний або маніпульований інсайдер, або зовнішній порушник з неспрямованою загрозою;

– мотивація середня – порушник має або середню фінансову вигоду від реалізації атаки, або інсайдер, скривджений на організацію, або нелояльний інсайдер тощо;

– мотивація висока – порушник має значну фінансову вигоду від реалізації атаки, або це підроблюючий інсайдер;

– мотивація дуже висока – порушник є співробітником спеціальної служби іноземної держави та має завдання на проникнення до критичних інформаційних активів.

2) Кваліфікація порушника.

Даний показник показує, яку кваліфікацію вимагає від порушника реалізація тієї чи іншої атаки. Аналіз підходів, які були проаналізовані в 1 розділі кваліфікаційної роботи показує, що як правило кваліфікація порушника поділяється на наступні рівні:

– низький рівень кваліфікації – порушник має загальні знання в технічній сфері або не має таких. До цієї категорії можуть відноситися зовнішні порушники, такі як клієнти організації, хакери – початківці, порушники, які скривджені на організацію та інші, або внутрішні порушники, такі як допоміжний персонал організації, співробітники гуманітарних сфер (економісти, фінансисти) тощо. Кваліфікація таких порушників дозволяє застосовувати сучасні засоби атаки які можна придбати в інтернеті або на ринку;

– середній рівень кваліфікації – порушник має технічні знання для реалізації атаки, він розуміє фізичні принципи атаки, розуміє можливості щодо про-

никнення. До цієї категорії відносяться зовнішні та внутрішні порушники, які мають технічні знання, певний досвід атак;

– високий рівень кваліфікації – порушник має технічні знання, досвід реалізації атак, глибоко розуміє механізми реалізації атак, можливо знає інформаційну систему організації, систему захисту інформаційних активів організації. До цієї категорії відносяться технічні фахівці, внутрішні та зовнішні для організації, які працюють в сфері інформаційної безпеки або працювали з певними процесами інформаційної безпеки, мають досвід та можливо працювали в організації, яку будуть атакувати;

– дуже високий рівень – порушники спеціально підготовлені для здійснення атак на інформаційні ресурси. Це ті, кого в спеціальних службах готують для атакуючих дій.

3) Технічний потенціал порушника.

Технічний потенціал порушника визначає можливість використовувати певні технічні засоби для реалізації атак, складні або нескладні. Можна поділити даний показник на наступні рівні:

– низький технічний потенціал – можливість використовувати дешеві сучасні засоби та методи атак, які можна придбати через інтернет або на ринку технічних засобів, наприклад купити стетоскоп для реалізації віброакустичного каналу зйому інформації, або диктофон для реалізації прямого акустичного каналу зйому інформації, або замовити DDOS – атаку через інтернет на сайт організації;

– середній технічний потенціал – можливість виготовляти дешеві технічні засоби самостійно, користуючись технічною літературою, наприклад самому зробити радіозакладний пристрій для зйому інформації, або самому розробити нескладну шкідливу програму;

– високий технічний потенціал – можливість закупати складні технічні засоби для реалізації атак та їх використовувати, наприклад лазерний акустичний засіб розвідки;

– дуже високий технічний потенціал – можливість розробляти та використовувати складні програмні або апаратно-програмні засоби для атак, наприклад, засоби перехоплення паразитних електромагнітних випромінювань апаратури, професійні акустичні закладні пристрої, які мають акустопуск або накопичен-

ня інформації та скидання на приймач в певний час, складні шкідливі програми та інше.

Введемо такий параметр, як рівень небезпечності порушника для організації, який є функцією параметрів мотивації, кваліфікації та технічного потенціалу порушника:

$$Rп = f\ \{мотивація, кваліфікація, технічний потенціал\}\ . \qquad (2.1)$$

Оцінка даного показника можлива як по якісній шкалі, так і кількісній. В розділі 2.2 приводиться приклад оцінки даного показника по якісні шкалі, а в розділі 2.3 по кількісній.

2.2 Якісний підхід до оцінки параметрів моделі порушника

При побудові моделі порушника для реальних умов організації необхідно зрозуміти ряд певних моментів:

– які типи порушників притаманні організації;

– який рівень небезпечності кожного з цих типів порушників для організації.

Особливістю побудови моделі порушника є те, що рівень небезпечності порушників навіть в рамках одного типу можуть різнитися. Наприклад, беремо ситуацію, коли порушник – це конкуруюча організація. Кожна організація має свій рівень розвитку, фінансові ресурси, бажання атакувати тощо. І рівень небезпечності кожної конкуруючої організації буде різним. В сучасних моделях порушника це не враховується. Інший приклад, це звільнені співробітники, які можуть бути потенційними порушниками. У кожного свій рівень кваліфікації, мотивації, технічних можливостей.

В кваліфікаційній роботі пропонується механізм оцінки рівня небезпечності порушника, який дозволяє провести таку оцінку для усіх можливих порушників для конкретної організації враховуючі об’єктивну інформацію.

Для якісної оцінки ступеня небезпечності порушника будемо використовувати шкалу параметрів рівня небезпеки порушника, представлену в підрозділі 2.1. В даному підрозділі кожен параметр представлений в чотирьох рівневій шкалі: низький, середній, високий, дуже високий.

Спочатку пропонується поєднати такі параметри, як кваліфікація та технічний потенціал. В результаті такого поєднання отримуємо проміжний показник – потенціал порушника. Це не суперечить чинним підходам, представлений в 1 розділі кваліфікаційної роботи. На другому етапі здійснюється поєднання мотивації порушника та проміжного показника – потенціалу порушника. В таблиці 2.1 представлений порядок поєднання кваліфікації порушника та його технічного потенціалу.

Таблиця 2.1 – Порядок поєднання кваліфікації порушника та його технічного потенціалу

№ з/п	Потенціал порушника		Технічний потенціал порушника			
			низький	середній	високий	дуже високий
1.	Кваліфікація порушника	низький	низький	низький	середній	високий
		середній	низький	середній	високий	високий
		високий	середній	високий	високий	дуже високий
		дуже високий	високий	високий	дуже високий	дуже високий

В таблиці 2.2 представлений порядок поєднання рівня мотивації порушника та його потенціалу – проміжного параметра, представленого в таблиці 2.2.

Таблиця 2.2 – Порядок поєднання мотивації порушника та його потенціалу

№ з/п	Рівень небезпеки порушника		Потенціал порушника			
			низький	середній	високий	дуже високий
1.	Мотивація порушника	низький	низький	низький	середній	високий
		середній	низький	середній	високий	високий
		високий	середній	високий	високий	дуже високий
		дуже високий	високий	високий	дуже високий	дуже високий

Наведемо приклад оцінки рівня небезпеки порушника для ситуації, яка приведена в даному розділі. Наприклад, для організації, в якій будується СУІБ, поте-

нційним порушником є конкуруюча організація. Рівень мотивації на атаку у даній організації дуже високий, але у фінансовому плані ця організація достатньо слабка і не може виділити значні фінансові ресурси для здійснення атаки (власними силами або через певні спеціалізовані структури). Тобто технічний потенціал низький, кваліфікація людей, що будуть реалізовувати атаку – низький. Тоді потенціал даного порушника – низький, а рівень небезпеки – високий. Тобто даний порушник хоч і не має значних потужностей для атаки, все рівно може задати шкоди нашій організації використовуючи недорогі методи атак.

2.3 Кількісний підхід до оцінки параметрів моделі порушника

На даний момент є певні напрацювання в дослідженій літературі що кількісного підходу щодо оцінки параметрів моделі порушника з використанням математичних моделей [12 - 16]. Напишемо та проаналізуємо їх. В роботі будемо використовувати результати досліджень, приведених у вказаній літературі.

Так мотивацію порушника пропонується визначати через ймовірність мотивації за формулою:

$$P_t(g, D) = \frac{g - D}{g} = 1 - \frac{D}{g}, \tag{2.2}$$

де g – цінність критичного ресурсу для порушника;

D – затрати порушника на організацію та здійснення атаки.

Дана формула має сенс, тому що аналіз результатів в крайніх точках реалізації даної моделі показує адекватні результати. Так, якщо затрати порушника на реалізацію атаки мінімальні, а вигода велика, то ймовірність мотивації прагне до 1, і навпаки, якщо затрати порушника наближаються до його вигоди, то ймовірність мотивації прагне до нуля.

Ймовірність успішної атаки визначається з виразу:

$$P_v(q, c, D) = \frac{\mu \cdot q}{\mu \cdot q + s \cdot \frac{c^2}{D}}, \tag{2.3}$$

де c – загальний об’єм інвестицій в СУІБ організації;

$\mu = g/q$ – коефіцієнт асиметрії розуміння цінності інформації сторонами атаки та захисту;

s – коефіцієнт, який визначає ефективність інвестування в СУІБ і відповідно до приведених джерел залежить від рівня зрілості організації.

Аналіз формули 2.3 показує певні припущення та недоліки при побудові даної математичної моделі. Розглянемо більш детально.

1) Якщо підставити в формулу 2.3 значення коефіцієнта симетрії μ , то скорочення показника q призводить до того, що в формулі залишається тільки показник g.

2) В формулі здійснюється допущення, що затрати на захист мають перевищувати затрати порушника на організацію та здійснення атаки в корінь з 2.

3) Коефіцієнт s визначається по методиці, яка приведена в [17] і визначається зрілістю організації.

Тобто формула (2.3) має вигляд, приведений в [12]:

$$P_v(q,c,D) = \frac{q}{q + s \cdot \frac{c^2}{D}} \cdot \tag{2.4}$$

В роботі [12] приводиться підхід до побудови моделі оцінки порушників на підставі теорії рефлексивного управління.

2.4 Пропозиції щодо розробки моделі порушника

Вважаємо, що в організації є множина груп критичних інформаційних активів. Будемо об’єднувати критичні активи в групи для зменшення розрахунків. Під групою інформаційних активів будемо розуміти певні активи, об’єднані за принципом єдиного функціонування. Тобто, критичні активи однієї групи мають єдиний вид (електронний, паперовий, акустичний), знаходяться в одному місці (комп’ютері, сервері, кімнаті, озвучуються в одній кімнаті), мають єдиний доступ певних посадових осіб.

Послідовність дій в побудові моделі порушника будемо пропонувати наступне:

1) Для кожної групи критичних активів формується множина потенційних методів атаки. Кожен метод атаки має фізичний принцип, пристрої, метод їх застосування.

2) Для кожного методу атаки формується потенціал (кваліфікація та технічний потенціал), потрібний для його застосування.

3) Для кожної групи критичних активів формується множина потенційних порушників. Основним критерієм включення порушників до цієї множини є мотивація порушника, тобто прогноз, кому необхідна цю група інформаційних активів.

4) Для кожного потенційного порушника визначається як прогноз його наявний потенціал.

5) Для кожної групи критичних активів визначається перелік порушників відповідно до їх ступеню небезпечності (мотивації та потенціалу) для реалізації кожної атаки.

6) Визначається множина порушників для організації для усіх груп критичних інформаційних активів.

Проведемо формалізацію моделі порушника на підставі кількісних підходів.

1) Формування для кожного з групи критичних інформаційних активів переліку потенційних атак є за метою зрозуміти, як ці активи можна атакувати. Тобто необхідно сформувати для кожної групи інформаційних активів множини потенційних атак, які можна реалізувати на підставі фізичних принципів.

2) Для кожного методу атаки формується потенціал порушника (кваліфікація та технічний потенціал), потрібний для його застосування.

Технічний потенціал для кожної атаки формується на підставі наступних чинників:

– вартість технічних засобів для здійснення атаки (враховується вартість розробки або (та) закупівлі на ринку ІБ);

– вартість проникнення засобів для здійснення атаки (може бути, якщо це необхідно). Як приклад, можна привести ситуацію з занесенням радіозакладного пристрою в кабінет топменеджера організації, при якому порушник має заплатити співробітнику організації для рішення цього завдання.

Кваліфікація визначається наявністю осіб, які можуть реалізувати атаку.

Тому потенціал порушника визначемо з виразу:

$$П_{порушник_x} = \sum_{i=1}^{N} B_i + \sum_{j}^{K} B_{кв\,j}, \quad (2.5)$$

де B_i – вартість кожного засобу або дії для реалізації певної х-ї атаки;

$B_{кв\,j}$ – вартість дії фахівців, які мають реалізувати х–у атаку.

1) Для кожної групи критичних активів формується множина потенційних порушників. Оцінка рівня мотивації кожного з порушників можлива з використанням підходу [12]. Основним критерієм включення порушників до цієї множини є мотивація порушника, тобто прогноз, кому необхідна цю група інформаційних активів.

Формула (2.1) модифікується наступним чином:

$$Рівень\_мотивації = 1 - \frac{D^*}{g^*}, \quad (2.6)$$

де D^* – прогноз від менеджменту СУІБ щодо порушника на бачення їм потенційних його затрат на організацію та здійснення атак. Тут є певна рефлексія, тобто це прогноз менеджменту СУІБ відносно того, як порушник бачить свої затрати на реалізацію атаки;

g^* – прогноз від менеджменту СУІБ щодо порушника на бачення їм потенційної цінності критичного ресурсу організації. Тут також є певна рефлексія, тобто це прогноз менеджменту СУІБ відносно того, як порушник бачить свій потенційний виграш затрати на реалізацію атаки.

2) Для кожного порушника здійснюється прогноз його потенціалу (кваліфікація та технічний потенціал), потрібний для його застосування.

Прогноз технічного потенціалу порушника для кожної атаки формується на підставі наступних чинників:

– можливість виділення фінансових ресурсів для закупівлі технічних засобів для здійснення атаки (враховується вартість розробки або (та) закупівлі на ринку ІБ):

– можливість виділення фінансових ресурсів для оплати проникнення засобів для здійснення атаки (може бути, якщо це необхідно);

– можливість закупівлі спеціалізованих засобів атаки на ринку (необхідно зазначити, що продаж, зберігання, закупівля певних засобів для здійснення атак заборонено по закону).

Тому прогноз потенціалу порушника визначимо з виразу:

$$П^{*}_{порушник_x} = \sum_{i=1}^{N} В_i + Кс_{кв_j} \cdot \sum_{j}^{K} В_{кв\ j}, \qquad (2.7)$$

де $В_i$ – вартість кожного засобу або дії для реалізації певної х–ї атаки;

$В_{кв\ j}$ – вартість дії фахівців, які мають реалізувати х–у атаку;

$Кс_{кв_j}$ – прогноз коефіцієнту кваліфікації кожного з j-го фахівця, який залучений для реалізації х-ї атаки. Кваліфікація визначається наявністю осіб, які можуть реалізувати х-у атаку.

Оцінка кваліфікації осіб, які потрібні для реалізації атаки, або які є в доступності порушнику для реалізації атаки будемо визначати наступним чином, представленим в таблиці 2.3.

Таблиця 2.3 – Прогнозні дані щодо вагових коефіцієнтів збільшення витрат на фахівців, які мають реалізувати атаку від порушника

№ з/п	Рівень кваліфікації порушника	Ваговий коефіцієнт
1.	Низький (або фахівець вже є у порушника, або він сам)	1
2.	Середній (потрібного фахівця необхідно залучати ззовні)	1,2
3.	Високий (потрібного фахівця необхідно залучати ззовні)	1,4

Логіка таблиці 2.3 має на увазі, що якщо потрібен порушнику кваліфікований фахівець, він його або вже має і платить стільки, скільки коштує такий фахівець на ринку праці (акцентуємо увагу, що це прогноз, і якщо у службі безпеки організації є більш точна інформація про порушника, вона його реалізовує при прогнозі), або замовляє ззовні. При побудові даної моделі прийняте допущення

збільшення вартості фахівця, найнятого ззовні відповідно до вартості механізму атаки. Але це припущення має бути удосконалення проведенням додаткових досліджень.

3) Визначення переліку k порушників, відповідно до їх ступеню небезпечності (мотивації та потенціалу) для реалізації кожної х–ї атаки, х=1, Х, для кожного конкретної групи критичних активів пропонується визначати з виразу:

$$РН_x^k = Рівень\_мотивації_x \cdot \frac{К_{закуп_i} \cdot \sum_{i=1}^{N} В_i + Кс_{кв_j} \cdot \sum_{j}^{K} В_{кв\ j}}{\sum_{i=1}^{N} В_i + \sum_{j}^{K} В_{кв\ j}}, \quad (2.8)$$

де $К_{закуп_i}$ – коефіцієнт, який показує можливість закупівлі певного засобу атаки на ринку порушником. Даний коефіцієнт показує, наскільки збільшаться витрати порушника, якщо засіб атаки необхідно покупати складний способом. Пропозиції щодо даного коефіцієнта приведені в таблиці 2.4, але обґрунтування даного коефіцієнта має бути експертним дослідженням фахівців з інформаційної безпеки.

Таблиця 2.4 – Прогнозні дані щодо вагового коефіцієнта, який показує можливість закупівлі певного засобу атаки на ринку порушником

№ з/п	Коефіцієнт $К_{закуп_i}$	Ваговий коефіцієнт
1.	Низький (засіб атаки легко покупається на ринку або в інтернеті)	1
2.	Середній (засіб атаки покупається на ринку, або в інтернеті, але внаслідок певних причин, наприклад вимоги кримінального кодексу, необхідно докласти зусиль, щоб його купити)	1,2
3.	Високий (засіб атаки є таким, що не продається вільно)	1,4

4) Оцінка можливості атаки певної групи активів певним порушником з використанням усіх можливих методів атаки можна знайти з виразу:

$$РН_x = \sum_{k=1}^{K} РН_x^k \cdot \qquad (2.9)$$

5) Результат оцінки для кожної групи критичних активів переліку порушників відповідно до їх ступеню небезпечності для реалізації кожної атаки фіксується в таблиці, як це показано в таблиці 2.5.

Таблиця 2.5 – Результат оцінки для кожної групи критичних активів переліку порушників відповідно до їх ступеню небезпечності для реалізації кожної атаки

№ з/п	Групи критичних активів	Порушник №1	Порушник №2	Порушник №3	…	Порушник №Y	Сума рівня небезпеки по групам активів
1.	Гр.акт.№ 1	$РН_{11}$	$РН_{12}$	$РН_{13}$	…	$РН_{1Y}$	$РН_{гр.акт1}$
2.	Гр.акт. № 2	$РН_{21}$	$РН_{22}$	$РН_{23}$	…	$РН_{2Y}$	$РН_{гр.акт2}$
….	…						
N.	Гр.акт № N	$РН_{N1}$	$РН_{N2}$	$РН_{N3}$	…	$РН_{NY}$	$РН_{гр.актN}$
	Сума рівня небезпеки по порушникам	$РН_1$	$РН_2$	$РН_3$		$РН_Y$	

Наведемо приклад розрахунку моделі порушника на підставі кількісних підходів за приведеною пропозицією.

1) Для прикладу є дві групи інформаційних активів, які знаходяться в електронному виді на комп’ютері керівника організації та обговорюються під час нарад в його кабінеті. Основною властивістю інформації є конфіденційність. Комп’ютер керівника організації підключений до локальної мережі компанії та через неї до інтернет. В цьому прикладі не ставиться завдання виявити усі загрози для такої ситуації, тому оберемо певні типові атаки для даної ситуації.

Визначимо перелік таких типових атак. Даний перелік атак представлений в таблиці 2.6.

Таблиця 2.6 – Перелік типових атак на конфіденційну інформацію відповідно до поставленої ситуації

№ з/п	Група інформаційних активів	Типова атака
1.	Інформаційні активи, які озвучуються в кабінеті керівника організації	Використання радіозакладного пристрою
		Використання диктофону
		Підслуховування з коридору
		Використання стетоскопу (віброакустичний канал витоку інформації)
		Використання лазерного акустичного засобу розвідки
		Використання акусто-електричного каналу зйому інформації
		Використання параметричного каналу зйому інформації
2.	Інформаційні активи, які знаходяться в комп’ютері керівника організації	Проникнення шкідливої програми через мережу (відвідування інфікованих сайтів, хробак, інфікування через електронну пошту тощо)
		Фізичне інфікування комп’ютеру шкідливою програмою
		Зйом порушником інформації через побічні електромагнітні випромінювання
		Зйом порушником інформації через наводки побічних електромагнітних випромінювань

2) Формування прогнозу щодо потрібного потенціалу порушника (кваліфікація та технічний потенціал), потрібний для застосування кожної атаки.

Для прикладу будемо брати орієнтовну вартість засобів атаки. В реальних питаннях побудови СУІБ необхідно ретельно аналізувати вартість певних засобів для здійснення атаки, які є на ринку на даний момент часу. Також для оцінки рівня кваліфікації фахівця будемо припускати, що для низькокваліфікованих атак рівень фахівця або низький, або порушник має у себе такого фахівця. Для інших атак порушник залучає фахівців ззовні. Як базову вартість фахівців будемо вва-

жати 20% від вартості засобу атаки. Приклад прогнозу потрібного потенціалу порушників для здійснення атаки представлений в таблиці 2.7.

Таблиця 2.7 – Приклад прогнозу потрібного потенціалу порушників для здійснення атаки

№ з/п	Тип атаки	Технічний потенціал (вартість засобу атаки), грн	Вартість дії фахівців, які мають реалізувати атаку, грн	Потрібна кваліфікація порушника		Потрібний потенціал порушника
				Потрібний рівень	Ваговий коефіцієнт	
1	2	3	4	5	6	7
1.	Використання радіозаклад-ного пристрою	10000	2000	середній	1,2	12400
2.	Використання диктофону	1000	200	низький	1	1200
3.	Підслуховування з коридору		500 (оплата послуг)	низький	1	500
4.	Використання стетоскопу (віброакустичний канал витоку інформації)	5000	1000	середній	1,2	6200
5.	Використання лазерного акустичного засобу розвідки	100000	20000	високий	1,4	128000

Продовження таблиці 2.7

1	2	3	4	5	6	7
6.	Використання акусто-електричного каналу зйому інформації	20000	4000	високий	1,4	25600
7.	Використання параметричного каналу зйому інформації	200000	40000	високий	1,4	256000
8.	Проникнення шкідливої програми через мережу (відвідування інфікованих сайтів, хробак, інфікування через електронну пошту тощо)	10000	2000	середній	1,2	12400
9.	Фізичне інфікування комп’ютеру шкідливою програмою	1000	200	низький	1	1200
10.	Зйом порушникм інформації через побічні електромагнітні випромінювання	50000	10000	високий	1,4	64000

Продовження таблиці 2.7

1	2	3	4	5	6	7
11.	Зйом порушником інформації через наводки побічних електромагнітних випромінювань	70000	14000	високий	1,4	89600

3) Формування для кожної групи критичних активів множини потенційних порушників.

Наприклад, для визначеної ситуації мається два типи порушників – кримінальна організація та конкуруюча організація.

Приклад мотивації для кожного з типу порушників можна визначити відповідно формули (2.5). Для оцінки мотивації порушника як приклад візьмемо наступні дані, приведені в таблиці 2.8.

Прогноз потенційних затрат на отримання певної інформації є інформацією з певною ступеню невизначеності представлений в таблицях 2.9 та 2.10. Дані в таблиці умовні, так як вони мають бути прив’язані до конкретної ситуації.

Таблиця 2.8 – Вихідні дані для прогнозу мотивації порушника

№ з/п	Тип порушника	Тип інформації	D^* – прогноз щодо порушника на бачення їм потенційних його затрат на організацію та здійснення атак	g^* – прогноз потенційної цінності критичного ресурсу для порушника
1	2	3	4	5
1.	Кримінальна організація	Інформаційні активи, які озвучуються в кабінеті керівника організації	30000	100 000
		Інформаційні активи, які знаходяться	10000	40 000

		в комп’ютері керівника організації		
2.	Конкуруюча організація	Інформаційні активи, які озвучуються в кабінеті керівника організації	20000	120 000
		Інформаційні активи, які знаходяться в комп’ютері керівника організації	15000	60 000

4) Формування для кожного порушника прогнозу його потенціалу (кваліфікація та технічний потенціал), потрібного для застосування певної атаки. Враховуємо, як допущення, що порушник не може використовувати кілька атак, а буде використовувати тільки одну атаку на критичний інформаційний ресурс. Результат оцінки представлений в таблицях 2.9 та 2.10. При цьому експертна оцінка щодо прогнозу потенційних затрат на побудову та здійснення атаки порушником з таблиці 2.7 повинна враховуватися.

Результат оцінки для визначених для прикладу групи критичних активів переліку порушників відповідно до їх ступеню небезпечності для реалізації атак представлений в таблиці 2.11.

Таблиця 2.9 – Результат прикладу оцінки прогнозу потенціалу порушника – кримінальна організація, який він може мати для реалізації певної атаки

№ з/п		Потрібний потенціал порушника	Прогноз коефіцієнту кваліфікації кожного з j-го фахівця	Коефіцієнт $К_{закуп_i}$	Прогноз наявного потенціалу порушника	Коефіцієнт мотивації порушника	Рівень потенціалу порушника	Рівень небезпеки порушника	Нормований рівень небезпеки порушника
1	2	3	4	5	6	7	8	9	10
1.	Використання радіозакладного пристрою	12400	1	1,2	14880	0,85	2,016	1,716	0,028
2.	Використання диктофону	1200	1	1	1200	0,988	25	24,7	0,414
3.	Підслуховування з коридору	500	1	1	500	0,995	60	59,7	1
4.	Використання стетоскопу (вібро-акустичний канал витоку інформації)	6200	1	1	6200	0,938	4,838	4,539	0,076

Продовження таблиці 2.9

1	2	3	4	5	6	7	8	9	10
5.	Використання лазерного акустичного засобу розвідки	128000	1,2	1,4	215040	0	0,139	0	0
6.	Використання акусто-електричного каналу зйому інформації	25600	1,2	1,2	36864	0,078	0,81	0,064	0,001
7.	Використання параметричного каналу зйому інформації	256000	1,4	1,4	501760	0	0,059	0	0

Продовження таблиці 2.9

1	2	3	4	5	6	7	8	9	10
8.	Проникнення шкідливої програми через мережу (відвідування інфікованих сайтів, хробак, інфікування через електронну пошту тощо)	12400	1,2	1	14880	0,628	0,67	0,42	0,007
9.	Фізичне інфікування комп’ютеру шкідливою програмою	1200	1	1	1200	0,97	8,33	8,08	0,135

Продовження таблиці 2.9

1	2	3	4	5	6	7	8	9	10
10.	Зйом порушником інформації через побічні електромагнітні випромінювання	64000	1,2	1,4	107520	0	0,093	0	0
11.	Зйом порушником інформації через наводки побічних електро-магнітних випромінювань	89600	1,2	1,4	150528	0	0,066	0	0

Таблиця 2.10 – Результат прикладу оцінки прогнозу потенціалу порушника – конкуруюча організація, який він може мати для реалізації певної атаки

№ з/п		Потрібний потенціал порушника	Прогноз коефіцієнту кваліфікації кожного з j-го фахівця	Коефіцієнт $К_{закуп_i}$	Прогноз наявного потенціалу порушника	Коефіцієнт мотивації порушника	Рівень потенціалу порушника	Рівень небезпеки порушника	Нормо-ваний рівень небезпеки порушника
1	2	3	4	5	6	7	8	9	10
1	Використання радіозакладного пристрою	12400	1	1,2	14880	0,876	1,34	1,177	0,019
2	Використання диктофону	1200	1	1	1200	0,99	16,67	16,5	0,276
3	Підслухо-вування з коридору	500	1	1	500	0,995	40	39,83	0,667
4	Використання стетоскопу (вібро-акустичний канал витоку інформації)	6200	1	1	6200	0,948	3,226	3,059	0,051

Продовження таблиці 2.10

1	2	3	4	5	6	7	8	9	10
5	Використання лазерного акустичного засобу розвідки	128000	1,2	1,4	215040	0	0,093	0	0
6	Використання акусто-електричного каналу зйому інформації	25600	1,2	1,2	36864	0,386	0,542	0,209	0,0035
7	Використання параметричного каналу зйому інформації	256000	1,4	1,4	501760	0	0,039	0	0

Продовження таблиці 2.10

1	2	3	4	5	6	7	8	9	10
8	Проникнення шкідливої програми через мережу (відвідування інфікованих сайтів, хробак, інфікування через електронну пошту тощо)	12400	1,2	1	14880	0,752	1,008	0,758	0,0127
9	Фізичне інфікування комп’ютеру шкідливою програмою	1200	1	1	1200	0,98	12,5	12,25	0,205

Продовження таблиці 2.10

1	2	3	4	5	6	7	8	9	10
10	Зйом порушником інформації через побічні електромагнітні випромінювання	64000	1,2	1,4	107520	0	0,139	0	0
11	Зйом порушником інформації через наводки побічних електро-магнітних випромінювань	89600	1,2	1,4	150528	0	0,099	0	0

Таблиця 2.11 – Результат оцінки для визначених для прикладу групи критичних активів переліку порушників відповідно до їх ступеню небезпечності для реалізації атак

№ з/п	Групи критичних активів	Кримінальна організація	Конкуруюча організація	Сума рівня небезпеки порушника по групам активів
1.	Інформаційні активи, які озвучуються в кабінеті керівника організації	90,719	60,775	151,494
2.	Інформаційні активи, які знаходяться в комп’ютері керівника організації	8,5	13,008	21,508
3.	Сума рівня небезпеки по порушникам	99, 219	73,783	

Аналіз таблиці 2.11 дає при побудові СУІБ наступну інформацію. З точку зору рівня небезпеки порушника більш небезпечним для визначених вихідних даних для організації є кримінальна організація, тому що згідно прогнозу менеджменту дана структура може виділити більше фінансових ресурсів для атак ніж конкуруюча організація. З точки зору рівня небезпеки для інформаційних активів, інформаційні активи, які озвучуються мають більше з точки зору потенційної загрози для них, ніж активи, які знаходяться в комп’ютері керівника організації, внаслідок більших можливостей на їх атаку. При цьому враховується вартість засобів атаки, вартість фахівців для атаки та можливість знаходження на ринку цих засобів.

3 ПІДХОДИ ДЛЯ УДОСКОНАЛЕННЯ МЕТОДИКИ ОЦІНКИ РИЗИКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ З УРАХУВАННЯМ УДОСКОНАЛЕНИЙ МОДЕЛІ ЗАГРОЗ ТА МЕТОДИКИ ОЦІНКИ ВРАЗЛИВОСТЕЙ CVSS

3.1 Підхід до комбінації методу CRAMM з методом CVSS для покращення оцінки ризику інформаційної безпеки компанії

При оцінці ризиків інформаційної безпеки (ІБ) компанії виникає питання якості такої оцінки. Якість оцінки ризику ІБ, по-перше, залежить від точності вихідних даних, до яких відносяться точність описання бізнес процесів компанії, розуміння ТОП-менеджментом компанії того, які активи в компанії реально критичні, точності опису моделі загроз, розуміння своїх вразливостей. А, по друге, від точності опису параметрів ризику ІБ – рівня (частоти) загроз, рівня вразливості, вартості критичного інформаційного активу.

Одним з кращих методів оцінки ризику ІБ є метод CRAMM (CCTA Risk Analysis and Management Method). Даний метод на даний час використовується в урядових департаментах Великобританії та прийнятий багатьма комерційними організаціями та іншими державними адміністраціями по всьому світу [18].

Метод оцінки ризику інформаційної безпеки CRAMM (CCTA Risk Analysis and Management Method) використовується для визначення рівня ризику, пов'язаного з інформаційною системою, та для розробки планів дій з метою зниження цього ризику до прийнятного рівня.

Один з прикладів застосування методу CRAMM може бути пов'язаний з оцінкою ризику від хакерських атак на комп'ютерну мережу компанії.

Кроки оцінки ризику за методом CRAMM можуть включати наступне:

1) Визначення активів: ідентифікація всіх ресурсів комп'ютерної мережі, які можуть бути загрозою для безпеки інформації, таких як сервери, бази даних, додатки, периферійні пристрої, роутери тощо.

2) Визначення загроз: ідентифікація всіх потенційних загроз для цих активів, таких як хакерські атаки, віруси, фішинг, зламані паролі тощо.

3) Визначення вразливостей: оцінка можливості атакування активів, з урахуванням їх вразливостей, таких як слабкі паролі, застаріле програмне забезпечення, недостатньо захищені мережеві з'єднання тощо.

4) Визначення наслідків: оцінка наслідків успішної атаки на кожен актив, таких як втрата даних, зниження продуктивності, зниження репутації компанії тощо.

5) Оцінка ризику: на основі результатів попередніх кроків, можна визначити рівень ризику для кожного активу та загрози. Наприклад, ризик атаки хакерів на сервери може бути високим, оскільки хакерські атаки мають високий рівень загрози, а сервери мають вразливість застарілого програмного забезпечення. Таким чином, оцінка ризику може бути визначена на основі формули CRAMM: ризик = загроза х вразливість х наслідок.

Рівень загрози в методі CRAMM оцінюються за п’ятибальною шкалою: дуже низький, низький, середній, високий або дуже високий. Зміст даної оцінки має такі значення: дуже низька – очікується, що інцидент траплятиметься в середньому не частіше одного разу на 10 років; низька – очікується, що інцидент траплятиметься в середньому раз на 3 роки, середня – очікується, що інцидент траплятиметься в середньому раз на рік, висока – очікується, що інцидент траплятиметься в середньому раз на 4 місяці, дуже висока – очікується, що інцидент траплятиметься в середньому раз на місяць.

Рівні вразливості оцінюються за шкалою низький, середній або високий. Зміст даної оцінки має такі значення: низька – якщо інцидент трапиться, ймовірність реалізації найгіршого сценарію (оцінено під час оцінки активів) буде не більше 33%, середня – якщо інцидент трапиться, існуватиме від 33% до 66% шансів реалізації найгіршого сценарію (оцінено під час оцінки активів), висока – якщо інцидент трапиться, ймовірність реалізації найгіршого сценарію (оціненого під час оцінки активів) буде вище 66%.

Оцінка рівня активу здійснюється по кільком категоріям, як то «Менеджмент і бізнес–операції», «Особиста безпека», «Персональна інформація», «Юридичні та нормативні зобов'язання», «Правозастосування», «Комерційно-економічні інтереси», «Фінансові втрати/переривання діяльності». Рівень активу

для кожної з цих категорій визначається в шкалі від 1 (мінімальний вплив на бізнес-процеси компанії) до 10 (максимальний вплив на бізнес-процеси компанії).

Результат оцінки ризику відповідно методу CRAMM розраховується в шкалі від 1 до 7. Можна побачити, що точність оцінки рівня загрози середня (п’ять рівнів), точність оцінки вартості активу висока (10 рівнів), але точність оцінки рівня вразливості нижче ніж середня (3 рівня). Зрозуміло, що цю методику розробляли фахові експерти, які вирішили визначити такі рівні показників ризику ІБ.

6) Розробка планів дій: на основі оцінки ризику можна розробити план дій з метою зниження ризику до прийнятного рівня. Наприклад, для зниження ризику атаки хакерів на сервер можуть бути запропоновані такі заходи: оновлення програмного забезпечення на сервері, встановлення більш складних паролів, використання шифрування даних тощо.

Отже, на основі методу оцінки ризику інформаційної безпеки CRAMM можна оцінити рівень ризику для кожного активу та загрози і розробити плани дій для зниження ризику до прийнятного рівня.

Виникає питання, як можна підвищити точність оцінки ризику ІБ?

В методиці CRAMM рівень загрози оцінюється на підставі механізму, приведеному в таблиці 3.1

Таблиця 3.1 – Підхід до оцінки рівня загрози

Рівень загрози	Опис
дуже низька	Очікується, що інцидент траплятиметься в середньому не частіше одного разу на 10 років
низька	Очікується, що інцидент траплятиметься в середньому раз на 3 роки
середня	Очікується, що інцидент траплятиметься в середньому раз на рік
висока	Очікується, що інцидент траплятиметься в середньому раз на 4 місяці
дуже висока	Очікується, що інцидент траплятиметься в середньому раз на місяць

З урахуванням досліджень, приведених в розділі 2 кваліфікаційної роботи пропонується визначати рівень загрози наступним чином, який приведений в таблиці 3.2.

Таблиця 3.2 – Оновлений підхід до оцінки рівня загрози

Рівень загрози	Рівень небезпеки порушника по реалізації конкретної атаки
дуже низька	0 – 0,1
низька	0,11 – 1
середня	1,1 – 10
висока	10,1 – 20
дуже висока	20 і більше

Для прикладу, який описаний в 2 розділі кваліфікаційної роботи, можемо побудувати наступну реалізацію даного показника, представленого в таблиці 3.3 для порушника – кримінальна організація, та 3.4 для порушника – конкуруюча організація.

Таблиця 3.3 – Приклад перерахунку нормованого рівня небезпеки порушника в рівень загрози по методиці CRAMM для порушника – кримінальної організації

№ з/п	Тип атаки	Нормований рівень небезпеки порушника	Рівень загрози по методиці CRAMM
1	2	3	4
1	Використання радіозакладного пристрою	1,716	середній
2	Використання диктофону	24,7	дуже високий
3	Підслуховування з коридору	59,7	дуже високий
4	Використання стетоскопу (віброакустичний канал витоку інформації)	4,539	середній
5	Використання лазерного акустичного засобу розвідки	0	дуже низький

Продовження таблиці 3.3

1	2	3	4
6	Використання акусто-електричного каналу зйому інформації	0,064	дуже низький
7	Використання параметричного каналу зйому інформації	0	дуже низький
8	Проникнення шкідливої програми через мережу	0,42	низький
9	Фізичне інфікування комп'ютеру шкідливою програмою	8,08	середній
10	Зйом порушником інформації через побічні електромагнітні випромінювання	0	дуже низький
11	Зйом порушником інформації через наводки побічних електромагнітних випромінювань	0	дуже низький

Таблиця 3.4 – Приклад перерахунку нормованого рівня небезпеки порушника в рівень загрози по методиці CRAMM для порушника – конкуруючої організації

№ з/п	Тип атаки	Нормований рівень небезпеки порушника	Рівень загрози по методиці CRAMM
1	2	3	4
1	Використання радіозакладного пристрою	1,177	середній
2	Використання диктофону	16,5	дуже високий
3	Підслуховування з коридору	39,83	дуже високий
4	Використання стетоскопу (віброакустичний канал витоку інформації)	3,059	середній
5	Використання лазерного акустичного засобу розвідки	0	дуже низький

Продовження таблиці 3.4

1	2	3	4
6	Використання акусто-електричного каналу зйому інформації	0,209	низький
7	Використання параметричного каналу зйому інформації	0	дуже низький
8	Проникнення шкідливої програми через мережу	0,758	низький
9	Фізичне інфікування комп’ютеру шкідливою програмою	12,25	високий
10	Зйом порушником інформації через побічні електромагнітні випромінювання	0	дуже низький
11	Зйом порушником інформації через наводки побічних електромагнітних випромінювань	0	дуже низький

В кваліфікаційній роботі пропонується рівень вразливості оцінювати відповідно методу CVSS. В стандарті NIST CVSS v3 критичність вразливостей оцінюється на основі декількох глобальних груп метрик: базові метрики, тимчасові метрики, метрики навколишнього середовища – дозволяють деталізувати базові та тимчасові метрики та врахувати особливості середовища в якому знаходиться вразливість, що підлягає оцінці.

Якщо використовувати як оцінку рівня вразливості для методу CRAMM базові метрики методу CVSS, то вже в дану метрику входять такі параметри, як Вектор доступу (Attack Vector), Складність атаки (Attack Complexity), Обов'язкові привілеї (Privileges Required), Взаємодія з користувачем (User Interaction), рівень збитків конфіденційності, цілісності та доступності інформації. Рівень вразливості згідно методу CVSS розраховується в шкалі від 1 до 10.

В методиці CRAMM оцінка вразливості здійснюється на підставі трьохрівневої шкали, представленій в таблиці 3.5.

Таблиця 3.5 – Підхід до оцінки рівня вразливості

Рівень вразлиості	Опис
низька	Якщо інцидент трапиться, ймовірність реалізації найгіршого сценарію (оцінено під час оцінки активів) буде не більше 33%.
середня	Якщо інцидент трапиться, існуватиме від 33% до 66% шансів реалізації найгіршого сценарію (оцінено під час оцінки активів).
висока	Якщо інцидент трапиться, ймовірність реалізації найгіршого сценарію (оціненого під час оцінки активів) буде вище 66%.

Така оцінка рівня вразливості є дуже не точною і фактично залежить від експертної оцінки менеджерів СУІБ. Використання методики CVSS дозволяє значно поглибити рівень оцінки вразливості. Питання використання даної методики для оцінки рівня вразливості були досліджені в кваліфікаційних роботах [Сацюк, Слюсар]. В даній кваліфікаційній роботі розробляються пропозиції щодо удосконалення методики оцінки ризику ІБ CRAMM шляхом введення показника рівня небезпеки порушника та показника оцінки вразливості по методиці CVSS.

В методиці CVSS переведення числової шкали в якісну здійснюється на підставі наступної логіки, представленої в таблиці 3.6.

Таблиця 3.6 – Механізм переведення кількісної шкали в якісну по методиці CVSS.

№ з/п	Якісна шкала рейтингу	Кількісна шкала рейтингу
1.	Жодного	0
2.	Низький	0,1 – 3,9
3.	Середній	4,0 – 6,9
4.	Високий	7,0 – 8,9
5.	Критичний	9,0 – 10

В кваліфікаційній роботі пропонується наступне переведення шкали методики CVSS в шкалу методики оцінки вразливості CRAMM, яке представлене в таблиці 3.7.

Таблиця 3.7 – Механізм переведення шкали методики CVSS в шкалу методики оцінки вразливості CRAMM

№ з/п	Якісна шкала рівня вразливості методики CRAMM	Якісна шкала рейтингу CVSS	Кількісна шкала рейтингу CVSS
1.	Низька	Жодного	0
		Низький	0,1 – 3,9
2.	Середня	Середній	4,0 – 6,9
3.	Висока	Високий	7,0 – 8,9
		Критичний	9,0 – 10

Приведемо приклади розрахунку рівня вразливості для атак, які використовувалися в даній кваліфікаційній роботі. Результати оцінки представлені в таблицях додатку А , та рисунках 3.1 – 3.11.

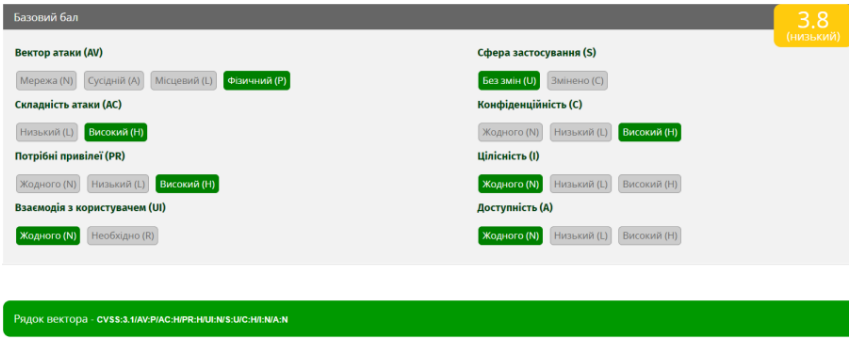

Рисунок 3.1 – Результат розрахунку рівня вразливості щодо через використання радіозакладного пристрою по базовим метрикам стандарту CVSS v3.1

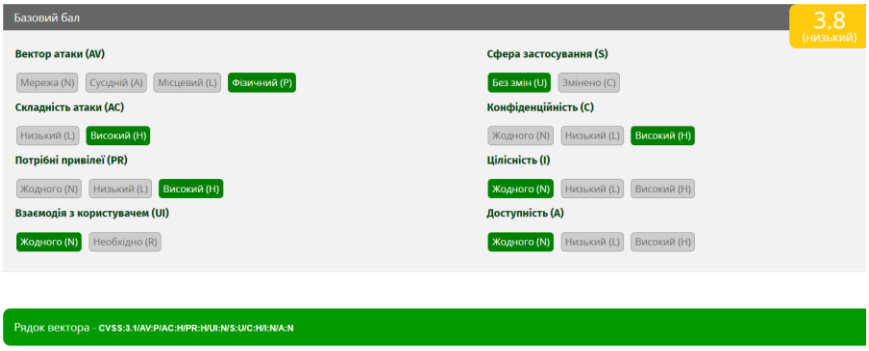

Рисунок 3.2 – Результат розрахунку рівня вразливості щодо зйому порушником інформації через використання диктофону по базовим метрикам стандарту CVSS v3.1

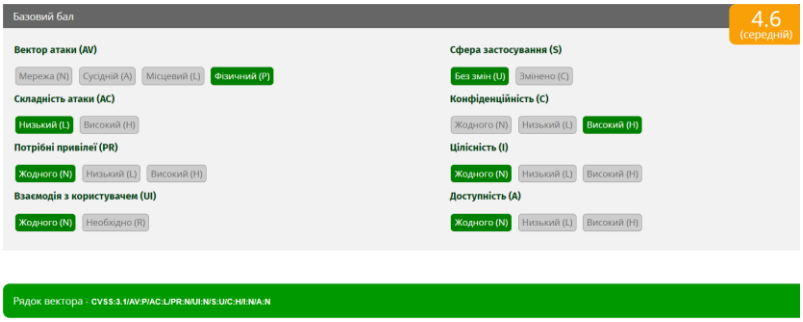

Рисунок 3.3 – Результат розрахунку рівня вразливості щодо зйому порушником інформації через підслуховування з коридору по базовим метрикам стандарту CVSS v3.1

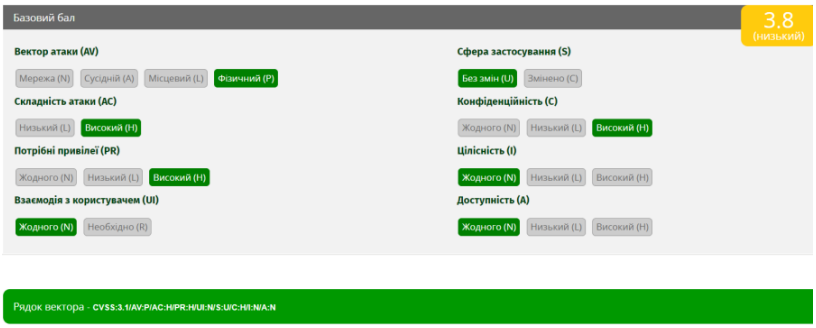

Рисунок 3.4 – Результат розрахунку рівня вразливості щодо зйому порушником інформації через використання стетоскопу (віброакустичний канал витоку інформації) по базовим метрикам стандарту CVSS v3.1

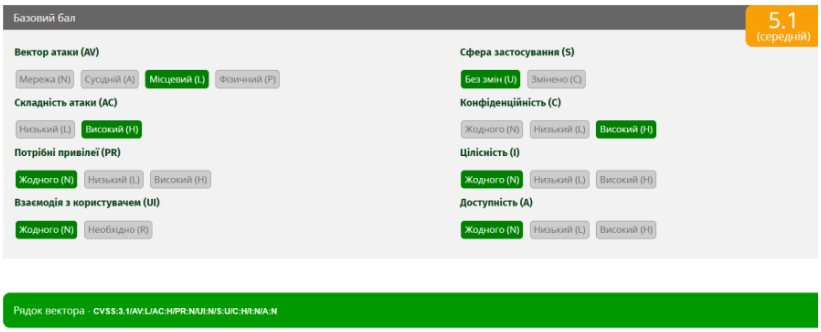

Рисунок 3.5 – Результат розрахунку рівня вразливості щодо зйому порушником інформації через лазерні акустичні засоби розвідки по базовим метрикам стандарту CVSS v3.1

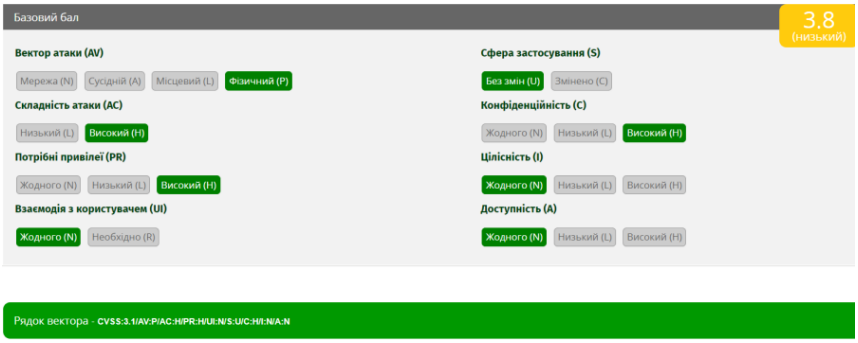

Рисунок 3.6 – Результат розрахунку рівня вразливості щодо зйому порушником інформації через фізичного інфікування комп’ютеру шкідливою програмою по базовим метрикам стандарту CVSS v3.1

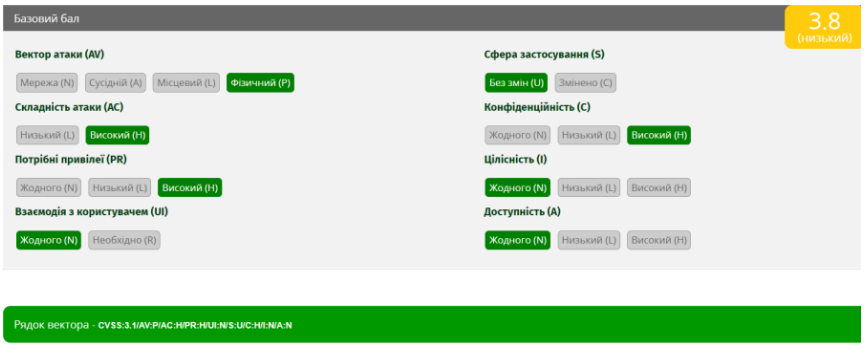

Рисунок 3.7 – Результат розрахунку рівня вразливості щодо зйому порушником інформації через акусто-електричного каналу зйому інформації по базовим метрикам стандарту CVSS v3.1

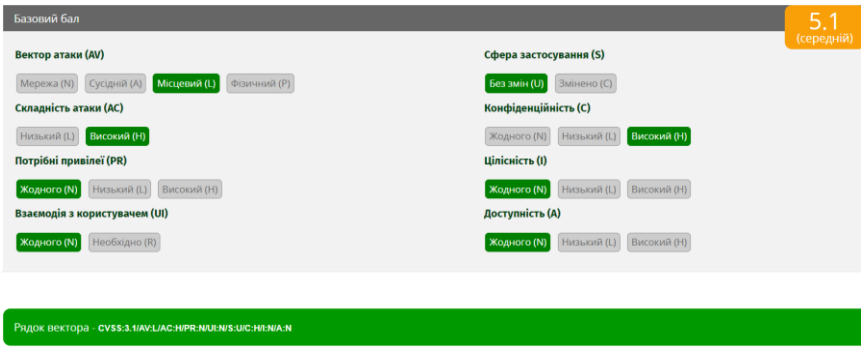

Рисунок 3.8 – Результат розрахунку рівня вразливості щодо зйому порушником інформації через параметричний акустичний канал зйому інформації по базовим метрикам стандарту CVSS v3.1

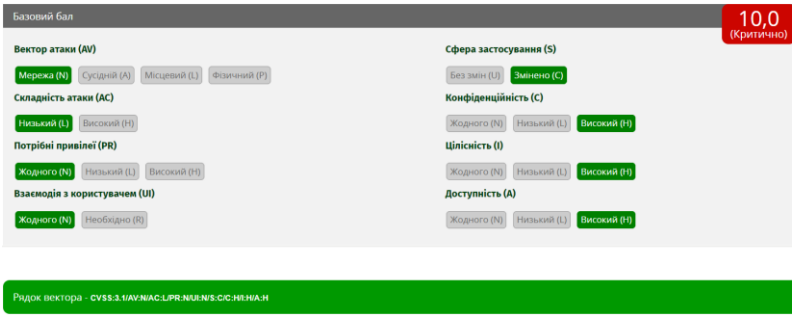

Рисунок 3.9 – Результат розрахунку рівня вразливості щодо зйому порушником інформації через проникнення шкідливої програми через мережу по базовим метрикам стандарту CVSS v3.1

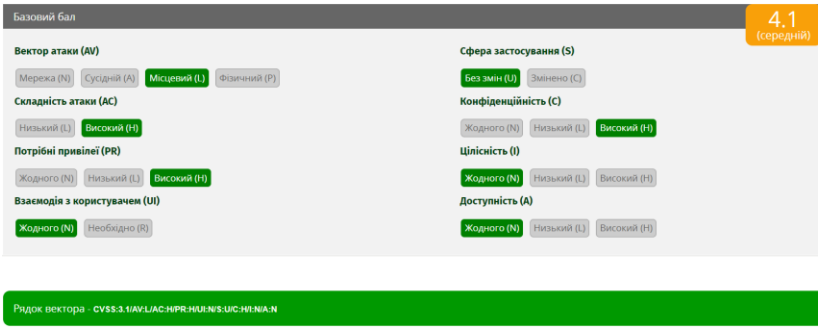

Рисунок 3.10 – Результат розрахунку рівня вразливості щодо зйому порушником інформації через побічні електромагнітні випромінювання по базовим метрикам стандарту CVSS v3.1

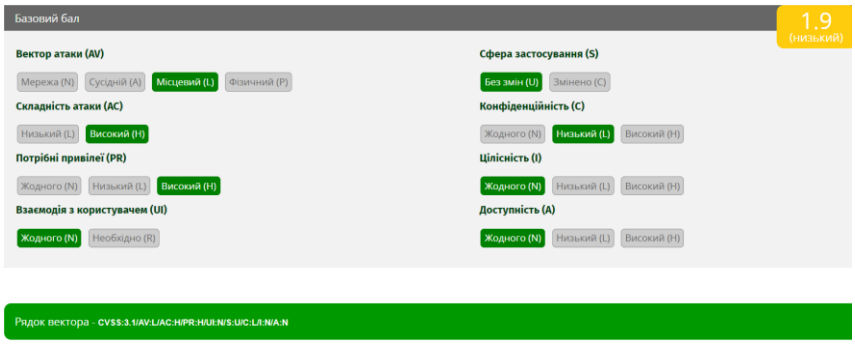

Рисунок 3.11 – Результат розрахунку рівня вразливості щодо зйому порушником інформації через наводки побічних електромагнітних випромінювань по базовим метрикам стандарту CVSS v3.1

Зведені дані по дослідженим рівням вразливостей приведені в таблиці 3.8.

Таблиця 3.8 – Зведені дані по рівням вразливостей

№ з/п	Тип атаки	Рівень вразливості по методиці CVSS	Рівень вразливості по методиці CRAMM
1	Використання радіозакладного пристрою	3,8	Низька
2	Використання диктофону	3,8	Низька
3	Підслуховування з коридору	4,6	Середня
4	Використання стетоскопу (віброакустичний канал витоку інформації)	3,8	Низька
5	Використання лазерного акустичного засобу розвідки	5,1	Середня
6	Використання акусто-електричного каналу зйому інформації	3,8	Низька
7	Використання параметричного каналу зйому інформації	5,1	Середня
8	Проникнення шкідливої програми через мережу	10	Висока
9	Фізичне інфікування комп’ютеру шкідливою програмою	3,8	Низька
10	Зйом порушникм інформації через побічні електромагнітні випромінювання	4,1	Середня
11	Зйом порушником інформації через наводки побічних електромагнітних випромінювань	1,9	Низька

Таким чином для обраної ситуації отримані значення рівня вразливості за допомогою методики CVSS для використання в методиці CRAMM.

3.2 Приклад оцінки ризику інформаційної безпеки з використанням модифікованої методики CRAMM

Матриця, по якій здійснюється оцінка ризиків по методиці CRAMM представлена в таблиці 3.20.

Також для оцінки для обраної ситуації будемо використовувати дані, наведені в таблицях 3.3, 3.4, 3.8.

Таблиця 3.9 – Матриця ризиків методу CRAMM

Threat	Very Low	Very Low	Very Low	Low	Low	Low	Medium	Medium	Medium	High	High	High	Very High	Very High	Very High
Vuln. Asset Value	LOW	MEDIUM	HIGH	LOW	MEDIUM	HIGH	LOW	MEDIUM	HIGH	LOW	MEDIUM	HIGH	LOW	MEDIUM	HIGH
1	1	1	1	1	1	1	1	1	2	1	2	2	2	2	3
2	1	1	2	1	2	2	2	2	3	2	3	3	3	3	4
3	1	2	2	2	2	3	2	3	3	3	3	4	3	4	4
4	2	2	3	2	3	3	3	3	4	3	4	4	4	4	5
5	2	3	3	3	3	4	3	4	4	4	4	5	4	5	5
6	3	3	4	3	4	4	4	4	5	4	5	5	5	5	6
7	3	4	4	4	4	5	4	5	5	5	5	6	5	6	6
8	4	4	5	4	5	5	5	5	6	5	6	6	6	6	7
9	4	5	5	5	5	6	5	6	6	6	6	7	7	7	7
10	5	5	6	5	6	6	6	6	6	6	7	7	7	7	7

Результати оцінки ризиків представлені в таблицях 3.10 та 3.11. Будемо враховувати, що оцінка йоде по критерія класу активу – Фінансові втрати/переривання діяльності. Рівень класу активу – 6.

Таблиця 3.10 – Приклад оцінки рівня ризику по методиці CRAMM для порушника – кримінальної організації

№ з/п	Тип атаки	Рівень загрози по методиці CRAMM	Рівень вразливості по методиці CRAMM	Рівень ризику по методиці CRAMM
1	2	3	4	5
1	Використання радіозакладного пристрою	середній	низька	4
2	Використання диктофону	дуже високий	низька	5
3	Підслуховування з коридору	дуже високий	середня	5

Продовження таблиці 3.10

1	2	3	4	5
4	Використання стетоскопу (віброакустичний канал витоку інформації)	середній	низька	4
5	Використання лазерного акустичного засобу розвідки	дуже низький	середня	3
6	Використання акусто-електричного каналу зйому інформації	дуже низький	низька	3
7	Використання параметричного каналу зйому інформації	дуже низький	середня	3
8	Проникнення шкідливої програми через мережу	низький	висока	4
9	Фізичне інфікування комп'ютеру шкідливою програмою	середній	низька	4
10	Зйом порушником інформації через побічні електромагнітні випромінювання	дуже низький	середня	3
11	Зйом порушником інформації через наводки побічних електромагнітних випромінювань	дуже низький	низька	3

Таблиця 3.11 – Приклад оцінки ризику по методиці CRAMM для порушника – конкуруючої організації

№ з/п	Тип атаки	Рівень загрози по методиці CRAMM	Рівень вразливості по методиці CRAMM	Рівень ризику по методиці CRAMM
1	2	3	4	5
1	Використання радіозакладного пристрою	середній	низька	4
2	Використання диктофону	дуже високий	низька	5

Продовження таблиці 3.11

1	2	3	4	5
3	Підслуховування з коридору	дуже високий	середня	5
4	Використання стетоскопу (віброакустичний канал витоку інформації)	середній	низька	4
5	Використання лазерного акустичного засобу розвідки	дуже низький	середня	3
6	Використання акусто-електричного каналу зйому інформації	низький	низька	3
7	Використання параметричного каналу зйому інформації	дуже низький	середня	3
8	Проникнення шкідливої програми через мережу	низький	висока	4
9	Фізичне інфікування комп’ютеру шкідливою програмою	високий	низька	4
10	Зйом порушником інформації через побічні електромагнітні випромінювання	дуже низький	середня	3
11	Зйом порушником інформації через наводки побічних електромагнітних випромінювань	дуже низький	низька	3

Таким чином, проведені дослідження показують, що удосконалена модель порушника, використання в методиці CRAMM механізму оцінки вразливостей по методиці CVSS дає більш точні та обґрунтовані результати оцінки ризику інформаційної безпеки.

3.3 Пропозиції щодо програмної реалізації механізму оцінки ризику інформаційної безпеки по методиці CRAMM з використанням пакету Excel

Для реалізації методу оцінки ризику інформаційної безпеки CRAMM в Excel можна скористатися таблицею, де будуть відображені всі активи, загрози, вразливості, наслідки та рівні ризику.

1) Створіть таблицю в Excel зі стовпчиками: «Актив», «Загроза», «Вразливість», «Наслідок», «Рівень ризику».

2) У стовпчику «Актив» перерахуйте всі активи, які мають відношення до інформаційної безпеки, наприклад: сервер 1, сервер 2, база даних 1, база даних 2, робоча станція 1, робоча станція 2 тощо.

3) У стовпчику «Загроза» перерахуйте всі потенційні загрози, які можуть виникнути, наприклад: хакерська атака, шкідлива програма, зйому інформації через побічні електромагнітні випромінювання та наводки, фішинг тощо.

4) У стовпчику «Вразливість» перерахуйте всі можливі вразливості для кожного активу, наприклад: застаріле програмне забезпечення, слабкі паролі, недостатньо захищені мережеві з'єднання тощо.

5) У стовпчику «Наслідок» перерахуйте всі можливі наслідки в разі успішної атаки на кожен актив, наприклад: втрата даних, зниження продуктивності, зниження репутації компанії тощо.

6) У стовпчику «Рівень ризику» використайте формулу CRAMM, щоб визначити рівень ризику для кожного активу та загрози.

7) Оцініть рівень ризику для кожного активу та загрози, використовуючи формулу CRAMM.

8) Розробіть план дій з метою зниження ризику до прийнятного рівня на основі результатів оцінки ризику. Для цього можна використати додатковий стовпчик з назвою "План дій", де будуть описані заходи з метою зниження ризику до прийнятного рівня. Наприклад, якщо ризик атаки хакерів на сервер є високим, то можна запропонувати такі заходи: оновлення програмного забезпечення на сервері, встановлення більш складних паролів, використання шифрування даних тощо.

9) Використовуйте фільтри для зручності відображення даних, щоб швидко знаходити необхідну інформацію, наприклад, загрози з високим рівнем ризику або активи з найбільшим ризиком.

10) Періодично оновлюйте таблицю, виконуючи оцінку ризику і вносячи необхідні зміни в план дій з метою забезпечення безпеки інформації.

Отже, реалізація методу оцінки ризику інформаційної безпеки CRAMM в Excel може бути корисною для компаній, які хочуть відстежувати та забезпечувати безпеку своїх інформаційних активів.

ВИСНОВКИ

Завдання на кваліфікаційну роботу виконано в повному обсязі.

В кваліфікаційні роботі проведений аналіз сучасних підходів щодо побудови моделі загроз та моделі вразливостей. Одним з таких підходів є підхід, представлений в стандарті ISO/IEC27005. Наведено, що дані моделі в основному мають описовий характер та слабо формалізовані.

В кваліфікаційній роботі пропонується формалізація моделі порушника з використанням кількісного та якісного підходів. Для більш чіткої формалізації вводить такий параметр, як рівень небезпеки порушника для реалізації конкретних атак на організацію. Основна увага робиться на кількісний підхід, який дозволяє отримати числові значення рівня небезпеки порушника, наводиться приклад розрахунку даного показника для двох типів порушників – кримінальна організація та конкуруюча організація.

Також в кваліфікаційній роботі пропонується підхід для вдосконалення методики оцінки ризику ІБ CRAMM. Аналіз даної методики показує, що показники, які в неї входять, а саме рівень загрози та рівень вразливості, не є точними. Тому для оцінки рівня вразливості даної методики пропонується використовувати показник – рівень небезпеки порушника, а для оцінки рівня вразливості підхід, який реалізований в методиці NIST CVSSv3.1. В кваліфікаційній роботі приводиться приклад розрахунку рівня ризику ІБ з урахуванням запропонованих пропозицій. Також в кваліфікаційній роботі пропонується механізм збору інформації та розрахунку рівня ризику з використанням програмного продукту Excel.

Результати досліджень опубліковані в трьох тезах доповідей на конференції та можуть використовуватися для практичної роботи при побудові системи управління інформаційною безпекою та у навчальному процесі підготовки фахівців з інформаційної безпеки.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Сацюк Д. В. Дослідження методів оцінки ризику інформаційної безпеки систем електронного документообігу : кваліфікаційна робота другого (магістерського) рівня вищої освіти : 125. Харків, ХНУРЕ, 2022. 86 с.

2. Слюсар Н.М. Дослідження методів оцінки ризику інформаційної безпеки сучасних систем електронного документообігу : кваліфікаційна робота другого (магістерського) рівня вищої освіти : 125. Харків, ХНУРЕ, 2023. 96 с.

3. Магдаліна М.І. Деякі погляди на побудову моделі загроз в інтересах оцінки ризику інформаційної безпеки компанії. *Перспективи розвитку інфокомунікацій та інформаційно-вимірювальних технологій*: матеріали 27-го Міжнародного молодіжного форум «Радіоелектроніка та молодь у XXI столітті», м. Харків, 10 – 12 травн. 2021 р. Харків: ХНУРЕ, 2023. С. 120 – 121.

4. Магдаліна М.І. Підходи до безперервного удосконалення моделі загроз в інтересах оцінки ризику інформаційної безпеки компанії *Перспективи розвитку інфокомунікацій та інформаційно-вимірювальних технологій*: матеріали 27-го Міжнародного молодіжного форум «Радіоелектроніка та молодь у XXI столітті», м. Харків, 10 – 12 травн. 2021 р. Харків: ХНУРЕ, 2023. С. 122 – 123.

5. Магдаліна М.І. Підхід до комбінації методу CRAMM з методом CVSS для покращення оцінки ризику інформаційної безпеки компанії *Перспективи розвитку інфокомунікацій та інформаційно-вимірювальних технологій*: матеріали 27-го Міжнародного молодіжного форум «Радіоелектроніка та молодь у XXI столітті», м. Харків, 10 – 12 травн. 2021 р. Харків: ХНУРЕ, 2023. С. 124 – 125.

6. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection. Information security management systems. URL: https://www.iso.org/standard/27001 (дата звернення: 15.04.2023).

7. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection. Guidance on managing information security. URL: https://www.iso.org/standard/80585.html (дата звернення: 15.04.2023).

8. Снігуров А.В. Менеджмент інформаційної безпеки: Комплекс навчально-методичного забезпечення навчальної дисципліни. Харків: ХНУРЕ, 2018. 534 с.

9. Common Vulnerability Scoring System. URL: https://www.first.org/cvss/user-guide (дата звернення: 15.04.2023).

10. Снігуров А.В., Кравченко А.Д., Ткаченко Е.А. Підхід до підвищення ефективності виявлення інсайдерів при забезпечення інформаційної безпеки організації. *Східноєвропейський журнал передових технологій*.. 2011. № 9 (50). С. 17-20.

11. Скиба В.Ю., Курбанов В.А. Руководство по защите от внутренних угроз информационной безопасности : Монографія. Спб, 2008. 320 с.

12. Архипов А. Применение рефлексивных моделей рисков для защиты информации в киберпространстве. *Захист інформації*. 2017. Том. 19. № 3. С. 204-213.

13. Архипов О. Вступ до теорії ризиків: інформаційні ризики : Монографія. Київ: Нац. Академія СБУ, 2015, 248 с.

14. Архипов А. Применение экономико-стоимостных моделей информационных рисков для оценивания предельных объемов инвестиций в безопасность информации. *Захист інформації*. 2015. Том 17. №3, С. 211-218.

15. Корченко А.Г. Построение систем защиты информации на нечетких множествах : Монографія. Київ: МК-Пресс, 2006. 320 с.

16. Архипов О.С., Муратов О.Є., Бровко В.Д. Основи теорії ризиків : Навчальний посібник. Київ: НАСБ України, 2019. 267 с.

17. Луцкий М.Г, Иванченко Е.В., Казмирчук С.В., Охрименко А.А. Современные средства управления информационными рисками. URL: https://er.nau.edu.ua/handle/NAU/9210?locale=uk (дата звернення 1.04.2023).

18. CRAMM (CCTA Risk Analysis and Management Method). URL: https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html (дата звернення 8.04.2023).