МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки

ВІВЧАР Дарія Володимирівна

Алгоритми кількісної оцінки ризиків кібербезпеки в системах критичної інфраструктури / Quantitative risk assessment algorithms for critical infrastructure systems

спеціальність: 125 – Кібербезпека
освітньо-професійна програма –Кібербезпека

Кваліфікаційна робота

Виконав студент групи КБм -21
Д.В. Вівчар

Науковий керівник
д.т.н., професор В.В.Яцків

Кваліфікаційну роботу
Допущено до захисту:

«____» _____ ___2022 р.

Завідувач кафедри
_____ **В.В.Яцків**

ТЕРНОПІЛЬ - 2022

Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки
Освітній ступінь «магістр»
спеціальність: 125 - Кібербезпека
освітньо-професійна програма –Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ В.В.Яцків
____" _____ 2021 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
Вівчар Дарія Володимирівна
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи:
Алгоритми кількісної оцінки ризиків кібербезпеки в системах критичної інфраструктури / Quantitative risk assessment algorithms for critical infrastructure systems
керівник роботи д.т.н., професор В.В. Яцків
затверджені наказом по університету від 31 грудня 2021 року № 606
2. Строк подання студентом закінченої випускної кваліфікаційної роботи 16 листопада 2022 року.

3. Вихідні дані до кваліфікаційної роботи: завдання на випускну кваліфікаційну роботу студента, наукові статті, технічна література.

4. Основні питання, які потрібно розробити:
– провести аналіз загроз у системі захисту інформації;
– визначити способи оцінки активів;
– дослідити методи управління ризиками;
– дослідити методи кількісної оцінки ризику;
– розробити алгоритм оцінки ризиків.
5. Перелік графічного матеріалу у роботі.
– основні етапи забезпечення інформаційної безпеки;
– основні загрози кібербезпеці зі звіту ENISA;
– приклад реєстру активів;
– процес аналізу ризиків інформаційної безпеки;
– алгоритм управління ризиками;

– основні етапи аналізу експертної інформації;
– схема алгоритму оцінки ризику.

6. Консультанти розділів кваліфікаційної роботи

	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 11 жовтня 2021 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строки виконання етапів кваліфікаційної роботи	Примітка
1	Аналіз предметної області	12.2021 р. – 03.2022 р.	
2	Методи та підходи до оцінки загроз кібербезпеці	03.2022 р. – 05.2022 р.	
3	Дослідження	05.2022 р. – 11.2022 р.	

Студент _____ Вівчар Д.В.
(підпис)

Керівник роботи _____ д.т.н., професор В.В. Яцків
(підпис)

АНОТАЦІЯ

Кваліфікаційна робота на тему «Алгоритми кількісної оцінки ризиків кібербезпеки в системах критичної інфраструктури» на здобуття освітнього ступеня «Магістр» зі спеціальності 125 «Кібербезпека» освітньо-професійної програми «Кібербезпека» написана обсягом 73 сторінки і містить 8 ілюстрації, 5 таблиць, 1 додаток та 25 джерел за переліком посилань.

Метою кваліфікаційної роботи є підвищення ефективності алгоритмів кількісної оцінки ризиків.

Методи досліджень. Для розв’язання поставлених задач у даній кваліфікаційній роботі використано: теорія ймовірності, методи оцінки ризиків, методи управління ризиками.

Результати дослідження. Удосконалено алгоритм оцінки ризиків кібербезпеки в системах критичної інфраструктури та кількісних підходів до оцінки ризиків.

Розроблено модель оцінки ризику з використанням експертних методів.

Результати роботи можуть успішно застосовуватися при кількісній оцінці ризиків в системах критичної інфраструктури.

Ключові слова: ІДЕНТИФИКАЦІЯ ЗАГРОЗ, АНАЛІЗ РИЗИКІВ, ОЦІНКА РИЗИКІВ, УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ.

ABSTRACT

The master's thesis on "Algorithms for the quantitative assessment of cyber security risks in critical infrastructure systems" for obtaining the Master's degree in the specialty 125 "CyberSecurity" of the educational and professional program "CyberSecurity" is written on 73 pages and contains 8 illustrations, 5 tables, 1 appendice and 25 sources according to the list of references.

The method of qualification work is to improve the effectiveness of algorithms for quantitative risk assessment.

Research methods: probability theory, risk assessment methods, risk management methods were used to solve the tasks in this qualification work.

Research results. The algorithm for assessing cyber security risks in critical infrastructure systems and several approaches to risk assessment has been improved.

A risk assessment model using expert methods has been developed.

The results of the work can successfully harm the quantitative assessment of risks in critical infrastructure systems.

Keywords: IDENTIFICATION OF THREATS, ANALYSIS OF RISKS, ASSESSMENT OF RISKS, MANAGEMENT OF INFORMATION SECURITY.

ЗМІСТ

ВСТУП 7
1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ 9
1.1 Аналіз та ідентифікація загроз 9
1.2 Визначення критичності активів 11
1.2.1 Ідентифікація людей, процедур та активів даних 19
1.2.2 Ідентифікація обладнання, програмного забезпечення та мережевих активів 20
1.3 Ідентифікація загрози. Модель загрози STRIDE 23
2 МЕТОДИ ТА ПІДХОДИ ДО ОЦІНКИ РИЗИКІВ КІБЕРБЕЗПЕКИ 26
2.1 Кількісна оцінка ризику 26
2.2 Якісна оцінка ризику 28
2.3 Факторний аналіз інформаційного ризику 37
2.4 Нормативні документи та рекомендації з оцінки ризиків 39
3 РОЗРОБКА АЛГОРИТМІВ ОЦІНКИ РИЗИКІВ 42
3.1 Процес проведення оцінки ризиків 42
3.3 Оцінка ризику 45
3.4 Обробка ризику 47
3.5 Алгоритм оцінки ризиків кібербезпеки 49
ВИСНОВОК 57
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 58
ДОДАТОК А 61

ВСТУП

Актуальність. У сучасному світі, який характеризується великою кількістю інформації та інформаційних ресурсів у розпорядженні сучасних організацій і підприємств, все більше уваги приділяється питанню захисту даних.

Основне завдання забезпечення інформаційної безпеки все більше вирішується в результаті впровадження різноманітних методів і дотримання вимог нормативно-правових актів, удосконалення процесу управління інформацією на основі застосування організаційних заходів.

Сучасні IT-системи наражаються на низку загроз, що є результатом несанкціонованого доступу, модифікації, підробки або розкриття інформації. Щоб захистити інформаційні ресурси та сервіси від потенційних загроз, необхідно застосовувати відповідні заходи з управління ризиками та безпеки.

Методологія, що використовується для визначення оцінки ризику, може бути якісною чи кількісною, або їх поєднанням. Якісні оцінки часто використовуються для отримання загального рівня ризику та визначення ключових ризиків. Крім того, може знадобитися більш кількісний або детальний аналіз значних ризиків.

Вивченню питань розробки, реагування, аналізу та дослідження загроз інформаційній безпеці присвячено низку публікацій, тому тема роботи є актуальною.

Мета і завдання дослідження. Метою роботи є підвищення ефективності алгоритмів кількісної оцінки ризиків.

Досягнення визначеної мети передбачає вирішення таких завдань:

– провести аналіз загроз у системі захисту інформації;

– визначити способи оцінки активів;

– дослідити методи управління ризиками;

– дослідити методи кількісної оцінки ризику;

– розробити модель оцінки ризику експертними методами;

– розробити модель оцінки ризику експертними методами.

Об’єкт дослідження – процес оцінки ризиків кібербезпеки.

Предмет дослідження – методи та алгоритми оцінки ризиків інформаційної безпеки.

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

Наукова новизна одержаних результатів. Удосконалено алгоритм оцінки ризиків кібербезпеки в системах критичної інфраструктури з використанням кількісних підходів.

Практичне значення отриманих результатів. Розроблено класифікацію загроз на основі моделі загрози STRIDE.

Публікації та апробація КР.

1. Яцків Н.Г., Вівчар Д.В., Черняк Т.Г. Аналіз підходів до оцінки ризиків. Матеріали проблемно-наукової міжгалузевої конференції «Автоматизація та комп’ютерно-інтегровані технології» (АКІТ - 2022), Тернопіль, 2022. – С. 104-106.

2. Яцків Н.Г., Вівчар Д.В. Аналіз підходів до оцінки ризиків. Матеріали науково-практична конференція молодих вчених, аспірантів та студентів «Кібербезпека та комп’ютерно-інтегровані технології» (КБКІТ – 2022), Тернопіль, 2022. – С. 10-12.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Аналіз та ідентифікація загроз

Джерела інформації. Інформація про екологічні загрози зазвичай доступна від різних державних і торгових груп. Загрози, пов’язані з бізнес-ресурсами, гірше задокументувати, але загалом їх можна передбачити з достатньою точністю. Важко отримати достовірну інформацію про минулі події та оцінити майбутні тенденції з ряду причин, зокрема з таких [1, 2]:

1) організації часто неохоче повідомляють про події безпеки, намагаючись зберегти корпоративний імідж, уникнути витрат на відповідальність і, у випадку відповідального керівництва та персоналу безпеки, уникнути шкоди для кар'єри;

2) деякі атаки можуть бути здійснені або, принаймні зроблені спроби без виявлення жертвою або виявлені набагато пізніше;

3) загрози продовжують розвиватися, оскільки зловмисники адаптуються до нових засобів контролю безпеки та відкривають нові методи.

Таким чином, інформування про загрози — це постійна і нескінченна проблема. Надалі розглянемо три важливі категорії джерел інформації про загрози: внутрішній досвід, служби оповіщення безпеки та глобальні опитування загроз. Важливим джерелом інформації про загрози є досвід, який організація вже має у виявленні спроб та успішних атак на її активи.

Організація може отримати цю інформацію за допомогою ефективної функції моніторингу та покращення безпеки. Тобто виявлені атаки мають спонукати до негайних дій з виправлення, а не згортати в дії на великі відстані.

Служби оповіщення безпеки спрямовані на виявлення загроз у міру їх розвитку, щоб дозволити організаціям виправляти код, змінювати методи чи

іншим чином реагувати, щоб запобігти реалізації загрози. Знову ж таки, ця категорія інформації є більш цінною для управління загрозами та інцидентами.

Велику цінність для ідентифікації загроз мають різноманітні глобальні дослідження загроз, які є легкодоступними [3].

Корисним джерелом інформації про поточні загрози є звіт ENISA Threat Landscape Report, останній опублікований у жовтні 2021 року [4]. У таблиці 1.1 наведені результати аналізу звіту.

Таблиця 1.1 – Основні загрози кібербезпеці зі звіту ENISA

Загроза	Trend (Тенденція)
1. Шкідливе програмне забезпечення	Стабільний
2. Веб-атаки	Збільшення
3. Атаки веб-додатків	Збільшення
4. Фішинг	Збільшення
5. Спам	Збільшення
6. DoS-атаки	Збільшення
7. Програми-вимагачі	Збільшення
8. Ботнети	Збільшення
9. Внутрішні погрози (зловмисні, випадкові)	Стабільний
10. Фізичні маніпуляції /пошкодження/ крадіжка/втрата	Стабільний
11. Порушення даних	Збільшення
12. Крадіжка особистих даних	Збільшення
13. Витік інформації	Збільшення
14. Комплекти експлойтів	Зниження
15. Кібершпигунство	Збільшення

Загрози ранжуються відповідно до обсягу досліджених інцидентів безпеки, а стовпець «Тенденція» стосується відносної зміни тяжкості наслідків кожної загрози.

Для кожної загрози звіт містить ланцюжок знищення , який визначає фази кібератаки.

1.2 Визначення критичності активів

Стратегія управління ризиками вимагає, щоб фахівці з інформаційної безпеки знали інформаційні активи своєї організації, тобто визначали, класифікували та визначали їх пріоритети. Після того, як активи організації були ідентифіковані, процес оцінки загроз визначає і кількісно оцінює ризики, з якими стикається кожен актив. Компоненти ідентифікації ризику показані на рисунку 1.1 [5].

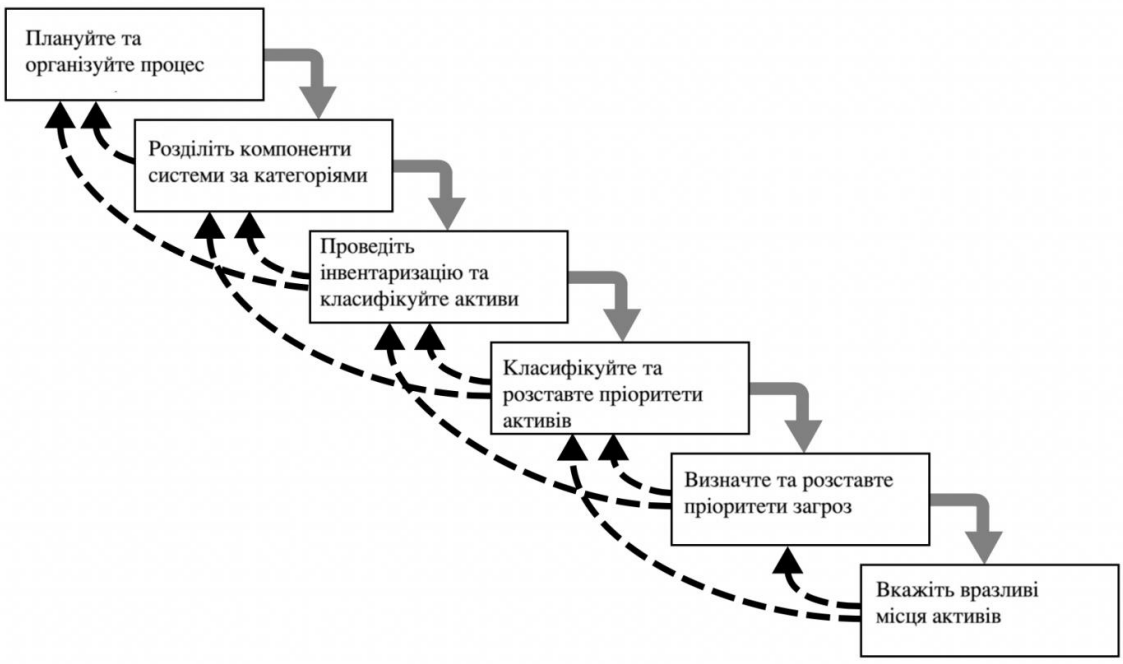


Рисунок 1.1 – Компоненти ідентифікації ризику

Ідентифікація ризиків — це ідентифікація активів, загроз, існуючих засобів контролю, вразливостей та впливів, що мають відношення до організації та слугують вхідними для аналізу ризиків. Першим кроком в оцінці ризику є документування та визначення вартості активів організації.

Актив — це все, що має цінність для бізнесу, що потребує захисту, включаючи апаратне забезпечення, програмне забезпечення, інформацію та бізнес-активи.

Можна ідентифікувати багато активів різних типів, і проблема полягає в розробці єдиного способу документування активів, наслідків для безпеки кожного та витрат, пов’язаних із інцидентами безпеки, пов’язаними з кожним.

Оцінка активів безпосередньо пов'язана з потребами бізнесу. Відповідно, вхідні дані для оцінки активів мають надавати власники та зберігачі активів, а не члени групи з оцінки ризиків.

Апаратні засоби. Апаратні засоби включають сервери, робочі станції, ноутбуки, мобільні пристрої, знімні носії, мережеве та телекомунікаційне обладнання, а також периферійне обладнання.

Основними проблемами є втрата пристрою через крадіжку або пошкодження, а також відсутність пристрою протягом тривалого періоду.

Інша проблема – несправність пристрою через навмисну дію або інші причини. Оцінка активів має враховувати вартість заміни обладнання, збитки від збоїв і витрати на відновлення.

Програмні активи. Програмні активи включають додатки, операційні системи та інше системне програмне забезпечення, програмне забезпечення віртуалізації віртуальних машин і контейнерів, програмне забезпечення для програмно-визначених мереж (SDN) і віртуалізації мережевих функцій (NFV),

системи керування базами даних, файлові системи та клієнтське та серверне програмне забезпечення.

Доступність є ключовим фактором тут, і оцінка активів повинна враховувати втрати від перебоїв і витрати на відновлення.

Інформаційні активи. Інформаційні активи включають інформацію, що зберігається в базах даних і файлових системах, як локально, так і віддалено в хмарі.

Як приклад, ITU-T X.1055 перераховує такі типи інформаційних активів у телекомунікаційному або мережевому середовищі [5, 6]:

1) дані зв'язку;
2) інформація про маршрути;
3) інформація про абонента;
4) інформація про чорний список;
5) зареєстрована службова інформація;
6) оперативна інформація;
7) інформація про несправності;
8) інформація про конфігурацію;
9) інформація про клієнта;
10) платіжна інформація;
11) зразки дзвінків клієнтів;
12) географічне розташування клієнтів;
13) статистична інформація про трафік;
14) контракти та угоди;
15) системна документація;
16) інформація про дослідження;
17) посібники користувача;
18) навчальні матеріали;

19) операційні або допоміжні процедури;

20) плани безперервності бізнесу;

21) резервні заходи щодо плану надзвичайних ситуацій;

22) аудиторські сліди та архівна інформація.

Оцінка активів має враховувати вплив загроз конфіденційності, приватності, цілісності та автентичності.

В NISTIR 7621, Інформаційна безпека малого бізнесу: пропонує наступні питання пов’язані з оцінкою інформаційних активів [7, 8]:

– що станеться з моїм бізнесом, якщо цю інформацію оприлюднити?

– що станеться з моїм бізнесом, якби ця інформація була неправильною?

– що станеться з моїм бізнесом, якщо я або мої клієнти не зможуть отримати доступ до цієї інформації?

Бізнес активи. Категорія бізнес-активів включає активи організації, які не вписуються в інші категорії, зокрема людські ресурси, бізнес-процеси та фізичне підприємство.

Ця категорія також включає нематеріальні активи, такі як контроль організації, ноу-хау, репутація та імідж організації.

Реєстр активів. Для ефективного захисту активів організація повинна забезпечити систематичний метод документування активів та їх наслідків для безпеки. Це робиться в реєстрі активів, який документує важливу інформацію, пов’язану з безпекою для кожного активу.

В таблиці 1.2 приведений робочий приклад таблиці для визначення та запису пріоритетів інформації на основі рекомендацій NISTIR 7621,

Таблиця 1.2 – Приклад таблиці визначення пріоритети типів інформації

	Приклад: контактна інформація клієнта	Тип інформації 1	Тип інформації 2	Тип інформації 3
Ціна відкриття (Конфіденційність)	Середня			
Вартість перевірки інформації (Цільність)	Висока			
Вартість втрати доступу (Доступність)	Висока			
Вартість втраченої роботи	Висока			
Штрафи, пені, сповіщення клієнтів	Середні			
Інші судові витрати	Низькі			
Витрати на репутацію/зв'язки з громадськістю	Високі			
Вартість виявлення та усунення проблеми	Висока			
Загальне значення:	Високе			

Нижче наведено приклади елементів, які можуть бути включені до кожного активу.

1. Назва/опис активу: ця інформація однозначно ідентифікує актив.

2. Тип активу: позначає тип активу, як-от фізичні/інфраструктурні активи, програмне забезпечення, інформація, послуги або людські ресурси.

3. Клас активів: для цілей оцінки ризику організація повинна групувати активи в класи, щоб ризики оцінювалися за класами активів, а не за окремими активами.

Приклади класів активів включають настільні комп'ютери/робочі станції, сервери, пристрої Payment Card Industry (PCI), обмежені/конфіденційні файли спільного доступу та обмежені принтери [9].

1. Інформаційні активи: Інформаційний актив визначає конкретно, який тип інформації обробляється, передається або зберігається активом (наприклад, персональна інформація клієнта [PII], дані PCI). Цей пункт стосується не всіх активів.

2. Власник активу: Організація повинна визначити функцію відділу/компанії, яка володіє активом і відповідає за ризики, пов'язані з активом. Його також іноді називають власником ризику або власником бізнесу.

3. Зберігач активів: це особа, відповідальна за підтримку, моніторинг та управління активом. Зазвичай це мережевий або системний адміністратор.

4. Місцезнаходження: це фізичне розташування активу.

5. Функція/бізнес-процес: це бізнес-процес або функція, яку підтримує актив (наприклад, засіб обробки інформації).

6. Тип даних/класифікація: для класифікації інформації, що передається, обробляється або зберігається активом, слід використовувати встановлену компанією політику класифікації інформації. Це допомагає пізніше оцінити ризики.

7. Класифікація вартості активів: це може бути грошова оцінка, але найчастіше це рейтинг, наприклад низький, середній або високий.

8. Пріоритет аварійного відновлення: у разі порушення безпеки, яке зачіпає кілька активів, це відносний пріоритет для виділення ресурсів на відновлення. Це може бути числова шкала (наприклад, від 1 до 10) або низька/середня/висока шкала.

9. Рівень впливу: це ступінь, до якої актив піддається загрозам. Це залежить, принаймні, від того, як актив ділиться, а також може залежати від інших факторів.

Спрощений приклад типу елементів, які повинні входити до реєстру активів приведений в таблиці 1.3.

Таблиця 1.3 – Приклад реєстру активів

Назва/опис активу	Класифікація активів	Пріоритет аварійного відновлення	Опис	Рівень експозиції
Персонал	Високий	1	Співробітники	Середній
PII клієнта	Високий	1	Особиста інформація	Низький
Виробничий веб-сервер	Середній	1	Основний веб-сайт компанії (без конфіденційних даних)	Високий

Планування та організація процесу. Як і в будь-якому великому підприємстві з інформаційної безпеки, першим кроком у процесі ідентифікації ризиків є дотримання принципів управління проектом.

Ви починаєте з організації команди, яка зазвичай складається з представників усіх постраждалих груп. Завдяки ідентифікації ризику, оскільки ризик може існувати скрізь в організації, представники будуть приходити з кожного відділу від користувачів до менеджерів, до IT та груп InfoSec.

Потім процес має бути спланований з періодичними результатами, оглядами та презентаціями керівництву. Лише тоді організація готова фактично розпочати наступний крок – визначення та класифікацію активів (табл.1.4).

Таблиця 1.4 – Класифікація компонентів інформаційної системи

Традиційні компоненти системи	Компоненти SesSDLC	Компоненти системи управління ризиками
Люди	Співробітники	Надійні співробітники Інший персонал
Клієнти	Непрацівники	Люди в перевірених організаціях Незнайомці
Процедури	Процедури	IT та стандартні процедури бізнесу Інформаційні та бізнес-чутливі процедури
Дані	Інформація	Спосіб передавання Обробка Зберігання
Програмне забезпечення	Програмне забезпечення	Додатки Операційні системи Захисні компоненти
Апаратне забезпечення	Системні пристрої та периферійні пристрої	Системи та периферійні пристрої Охоронні пристрої
	Мережеві компоненти	Компоненти інтранету Компоненти Інтернету або DMZ

1.2.1 Ідентифікація людей, процедур та активів даних

Ідентифікувати людські ресурси, документацію та активи даних складніше, ніж ідентифікувати апаратні та програмні засоби. Завдання слід доручити людям зі знаннями, досвідом і розсудливістю. Оскільки ідентифіковані люди, процедури та активи даних, вони повинні бути записані за допомогою надійного процесу обробки даних. Який би механізм ведення записів ви не використовували, переконайтеся, що він має гнучкість, щоб дозволити специфікацію атрибутів, характерних для типу активу. Деякі атрибути є унікальними для класу елементів.

Вирішуючи, які інформаційні активи відстежувати, необхідно враховувати такі атрибути активу [10]:

1. Люди. Включає назва посади/номер/ідентифікатор (уникайте імен і дотримуйтесь визначення посад, ролей або функцій); керівник; рівень безпеки; спеціальні навички.

2. Процедури. Опис; цільове призначення; зв'язок з програмним забезпеченням, апаратним забезпеченням та мережевими елементами; місце зберігання для довідки; місце зберігання для оновлення

3. Дані. Класифікація; власник, творець і менеджер; розмір структури даних; використовувана структура даних (послідовна або реляційна); онлайн або офлайн; розташування; використовувані процедури резервного копіювання.

Розробляючи процес відстеження даних, необхідно визначити, скільки даних слід відстежувати і для яких конкретних активів. Більшість великих організацій вважають, що вони можуть ефективно відстежувати лише кілька цінних фактів про найкритичніші пристрої.

Наприклад, компанія може відстежувати лише IP-адресу, назву сервера та тип пристрою для критично важливих серверів, які використовує компанія.

Вони можуть відмовитися від відстеження додаткової інформації на всіх пристроях і повністю відмовитися від відстеження настільних або портативних систем.

1.2.2 Ідентифікація обладнання, програмного забезпечення та мережевих активів

Атрибути обладнання, програмного забезпечення та мережевих активів слід відстежувати у залежності від потреб організації та її зусиль з управління ризиками, а також від уподобань і потреб спільнот інформаційної безпеки та інформаційних технологій.

Необхідно розглянути можливість включення таких атрибутів активу [11]:

1. Ім’я. Використовується найпоширеніша назву пристрою або програми. Організації можуть мати кілька назв для одного і того ж продукту.

Наприклад, програмний продукт може мати псевдонім, який компанія використовує під час його розробки, а також офіційну назву, яку використовують маркетинг і постачальники. Доцільно прийняти стандарти імен, які не передають інформацію потенційним системним зловмисникам.

Наприклад, сервер під назвою CASH5 або HQ_FIN може спонукати зловмисників скористатися ярликом до цих систем.

2. IP-адреса. Це може бути корисним ідентифікатором для мережевих пристроїв і серверів, але зазвичай не стосується програмного забезпечення. Однак можна використовувати реляційну базу даних і відстежувати екземпляри програмного забезпечення на певних серверах або мережевих пристроях.

Також багато організацій використовують протокол динамічного керування хостом (DHCP) у TCP/IP, який перепризначає IP-номери пристроям за потреби, що робить використання IP-номерів як частини процесу

ідентифікації активів проблематичним. Використання IP-адрес у інвентарі зазвичай обмежується тими пристроями, які використовують статичні IP-адреси.

3. Адреса керування доступом до медіа (MAC). MAC-адреси іноді називають електронними серійними номерами або апаратними адресами. Як частина стандарту TCP/IP, всі апаратні пристрої мережевого інтерфейсу мають унікальний номер. Номер MAC-адреси використовується мережевою операційною системою для ідентифікації конкретного мережевого пристрою. Він використовується мережевим програмним забезпеченням клієнта для розпізнавання трафіку, який він повинен обробляти.

У більшості налаштувань MAC-адреси можуть бути корисним способом відстеження з'єднання. Однак вони можуть бути підроблені деякими комбінаціями апаратного та програмного забезпечення.

4. Тип елемента. Для апаратного забезпечення ви можете розробити список типів елементів, таких як сервери, настільні комп'ютери, мережеві пристрої або тестове обладнання, з будь-яким рівнем деталізації, який вам потрібно. Для елементів програмного забезпечення ви можете розробити список типів, який включає операційні системи, спеціальні програми за типом (бухгалтерія, кадри або нарахування заробітної плати, наприклад), пакетні програми та спеціальні програми, такі як програми брандмауера. Потреби організації визначають ступінь специфічності.

Фактично типи можуть бути записані на двох або більше рівнях специфічності. Запишіть один атрибут, який класифікує актив на високому рівні, а потім додайте атрибути для більш детальної інформації. Наприклад, один сервер може бути вказаний як [12]:

– клас пристрою S (сервер);

– ОС пристрою W2K (Windows 2000);

– Device Capacity (Ємність пристрою) AS (розширений сервер).

5. Серійний номер. Для апаратних пристроїв серійний номер може однозначно ідентифікувати конкретний пристрій. Деякі постачальники програмного забезпечення також призначають серійний номер програмного забезпечення кожному екземпляру програми, ліцензованої організацією.

6. Назва виробника. Запишіть виробника пристрою або програмного компонента. Це може бути корисно під час реагування на інциденти, пов’язані з цими пристроями, або коли певні виробники оголошують про конкретні вразливості.

7. Номер моделі або номер деталі виробника. Запишіть модель або номер частини елемента. Цей запис про те, що саме являє собою елемент, може бути дуже корисним для подальшого аналізу вразливостей, оскільки деякі екземпляри вразливості застосовуються лише до конкретних моделей певних пристроїв і програмних компонентів.

8. Версія програмного забезпечення, версія оновлення або номер FCO. Якщо це можливо, задокументуйте номер версії конкретного програмного або мікропрограмного забезпечення, а для апаратних пристроїв – поточний номер порядку зміни місця (FCO). FCO – це дозвіл, виданий організацією на ремонт, модифікацію або оновлення частини обладнання. Обладнання не повертається виробнику, але зазвичай ремонтується на місці замовника, часто третьою стороною. Документування номера версії та FCO особливо важливо для мережевих пристроїв, які функціонують переважно за допомогою програмного забезпечення, що на них запущено. Наприклад, пристрої брандмауера часто мають три версії: версію операційної системи (ОС), версію програмного забезпечення та версію мікропрограми базової системи введення/виводу (BIOS). Залежно від ваших потреб, можливо, вам доведеться відстежувати всі три номери цих версій.

9. Фізичне розташування. Зверніть увагу, де фізично розташований цей елемент. Це може не поширюватися на елементи програмного забезпечення, але деякі організації мають умови ліцензії, які визначають, де можна використовувати програмне забезпечення.

10. Логічне розташування. Даний елемент можна знайти в мережі організації. Логічне розташування є найбільш корисним для мережевих пристроїв і вказує логічну мережу, до якої пристрій підключено.

11. Контролююча організація. Треба визначити, яка організаційна одиниця контролює елемент. Іноді персонал з віддаленого місця керує мережевим пристроєм, а в інших випадках команда центральних мереж керує іншими пристроями тієї ж марки та моделі. Ви повинні спробувати розрізнити, яка група чи підрозділ контролює кожен конкретний елемент, тому що ця група може захотіти сказати, який ризик може перенести цей пристрій і скільки витрат він може витримати, щоб додати елементи керування.

1.3 Ідентифікація загрози. Модель загрози STRIDE

Ідентифікація загроз – це процес виявлення джерел загроз, які можуть завдати шкоди активам системи. Джерела загроз поділяються на три категорії [13].

1. Навколишнє середовище. Прикладами є повені, землетруси, торнадо, зсуви, лавини, грози та відключення електроенергії.

2. Бізнес-ресурси. Прикладами є поломка обладнання, порушення ланцюга поставок та ненавмисна шкода заподіяна працівниками.

3. Ворожі суб'єкти. Приклади включають хакерів, активістів, інсайдерських погроз, злочинців та інші дійові особи.

Загрози як для навколишнього середовища, так і для бізнес-ресурсів повинні бути розпізнані та подолані, але основна частина зусиль щодо ідентифікації загроз, а також оцінки ризиків та управління ризиками – передбачає боротьбу із загрозами від ворожих суб’єктів. Це і є центром уваги теми, яку ми власне і розглядаємо.

Модель загрози STRIDE. STRIDE – це система класифікації загроз, розроблена компанією Microsoft, яка є корисним способом класифікації атак, які виникають внаслідок навмисних дій.

Вона включає такі категорії.

1. Підробка ідентифікаційної інформації (Spoofing identity). Прикладом підробки ідентифікаційної особи є незаконний доступ до інформації для аутентифікації іншого користувача, такої як ім'я користувача та пароль, а потім використання її. Контроль безпеки для протидії таким загрозам знаходиться в області аутентифікації.

2. Підробка даних (Tampering with data). Підробка даних передбачає зловмисне змінення даних. Приклади включають несанкціоновані зміни, внесені до постійних даних, наприклад, що зберігаються в базі даних, і зміну даних, коли вони переміщаються між двома комп’ютерами через відкриту мережу, наприклад Інтернет. Відповідні засоби контролю безпеки знаходяться в області цілісності.

3. Відмова (Repudiation). Загрози відмови пов'язані з користувачами, які заперечують виконання дії, не маючи можливості довести інше (наприклад, користувач, який виконує незаконну операцію в системі, яка не має можливості відстежувати заборонені операції).

Відповідні засоби контролю безпеки знаходяться в області невідмовності, яка відноситься до здатності системи протидіяти загрозам відмови.

Наприклад, користувачу, який купує товар, може знадобитися підписати його під час отримання. Потім постачальник може використовувати підписану квитанцію як доказ того, що користувач отримав пакет.

4. Розкриття інформації (Information disclosure). Загрози розкриття інформації передбачають розкриття інформації особам, які не повинні мати до неї доступу (наприклад, можливість користувачів читати файл, до якого їм не було надано доступ, або здатність зловмисника прочитати передані даних між двома комп'ютерами). Відповідні заходи безпеки знаходяться в зоні конфіденційності.

5. Відмова в обслуговуванні (Denial of service): атаки відмови в обслуговуванні (DoS) забороняють обслуговування дійсним користувачам, наприклад, роблячи веб-сервер тимчасово недоступним або непридатним для використання. Відповідні засоби контролю безпеки знаходяться в зоні доступності.

6. Підвищення привілеїв (Elevation of privileg). у цьому типі загроз непривілейований користувач отримує привілейований доступ і, таким чином, має достатній доступ, щоб скомпрометувати або знищити всю систему.

Загрози підвищення привілеїв включають ситуації, коли зловмисник ефективно проникає в усі захисти системи і стає частиною самої надійної системи – справді небезпечна ситуація. Відповідні засоби контролю безпеки знаходяться в зоні авторизації.

Типи загроз. На даний час зроблено багато зусиль, щоб класифікувати типи загроз, і існує значне дублювання у визначенні деяких загальних термінів. Велика категорія загроз – це шкідливе програмне забезпечення, або зловмисне програмне забезпечення, яке є загальним терміном, що охоплює багато типів програмних загроз, зокрема такі: віруси, черв'яки, програми-вимагачі, спам, логічні бомби та багато інших.

2 МЕТОДИ ТА ПІДХОДИ ДО ОЦІНКИ РИЗИКІВ КІБЕРБЕЗПЕКИ

Два фактори оцінки ризику можна розглядати як кількісно, так і якісно це вплив і ймовірність. Для впливу, якщо здається можливим призначити конкретні грошові витрати для кожної із зон впливу, тоді загальний вплив можна виразити як грошові витрати. В іншому випадку використовуються якісні терміни, такі як низький, середній, високий.

Аналогічно, ймовірність інциденту безпеки може бути визначена кількісно або якісно.

Кількісна версія ймовірності – це просто значення ймовірності, і знову ж таки якісна ймовірність може бути виражена в таких категоріях, як низька, середня та висока.

2.1 Кількісна оцінка ризику

Для кількісної оцінка рівня ризику R, при умові, що всі фактори виражені кількісно, використовують наступну формулу [14, 15]:

$$R = I * E$$

де I – ймовірність небажаної події;

E – величина впливу.

Це показник вартості порушень безпеки, виражений чисельно.

Його також можна виразити як рівень залишкового ризику (РЗР) таким чином:

$$RRV = \frac{I * E}{MF}$$

де MF – коефіцієнт пом’якшення.

У цьому рівнянні коефіцієнт пом’якшення відображає зменшення ймовірності несприятливої події через впровадження заходів безпеки. Таким чином, рівень залишкового ризику є еквівалентним очікуваній вартості порушень безпеки з впровадженням контролю.

Якщо різні фактори можна кількісно оцінити з розумним ступенем впевненості, то ці рівняння слід використовувати для прийняття рішень щодо того, скільки інвестувати в засоби контролю безпеки.

При впровадженні нових засобів контролю безпеки зменшується залишкова ймовірність несприятливої події і, відповідно, зменшується вартість порушень безпеки (рис.2.1) [15].

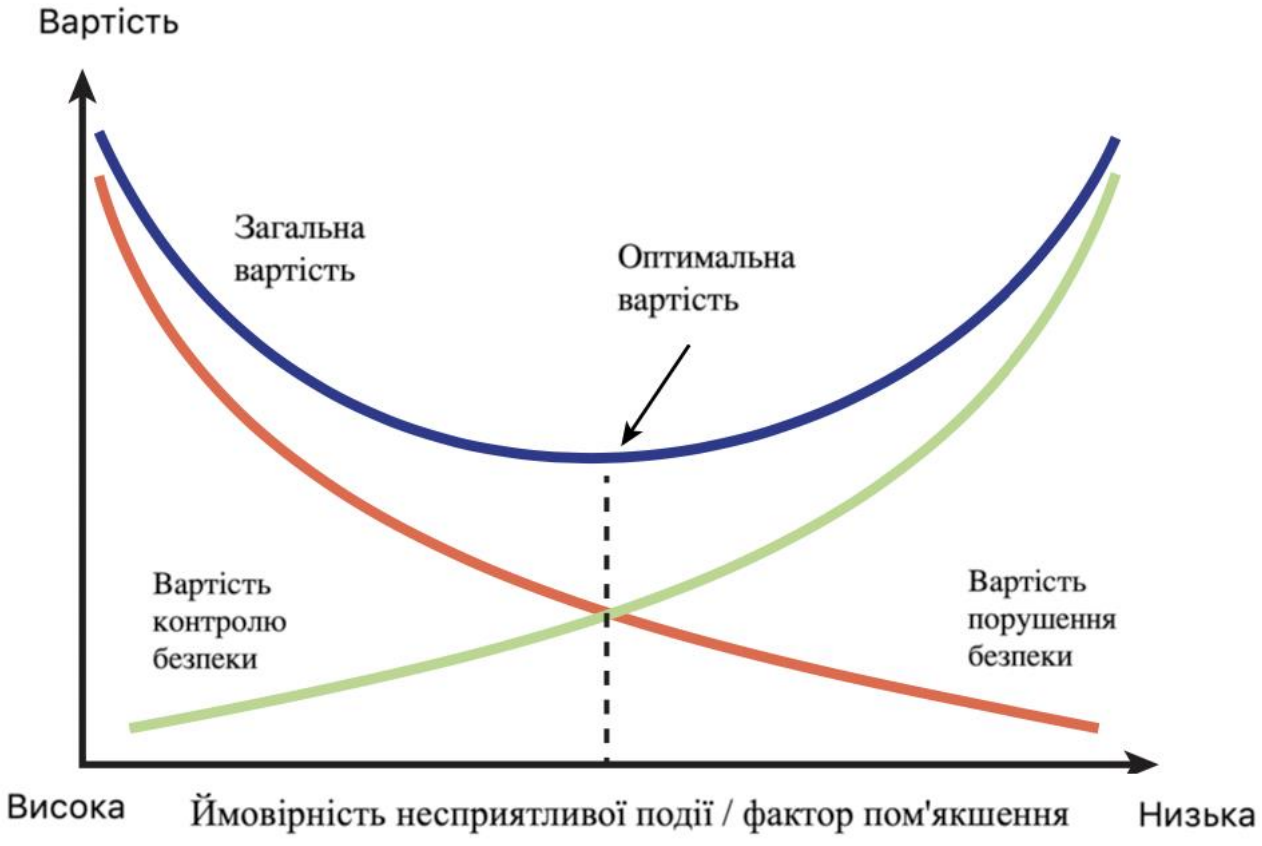


Рисунок 2.1 – Аналіз витрат для оцінки ризику

2.2 Якісна оцінка ризику

Складно припускати, що всі витрати та ймовірність впливу можна з упевненістю оцінити кількісно. Порушення безпеки трапляються рідко, і організації неохоче їх розкривають. Отже, інформація про випадки безпеки, як правило заснована на опитуваннях і не може бути використана для розробки надійних або точних значень ймовірності або частоти.

У той же час загальну вартість або потенційні втрати через порушення безпеки важко визначити кількісно. Вартість може залежати від ряду факторів, таких як тривалість простою, кількість і вплив негативної реклами, вартість відновлення та інші фактори, які важко оцінити. Проте можна, використовуючи розумне судження, ефективно використовувати якісну оцінку ризику. Якісна оцінка визначає відносний ризик, а не абсолютний ризик. Це значно спрощує аналіз, дає приблизні оцінки рівнів ризику. Якісної оцінки ризиків зазвичай достатньо для визначення найбільш значущих ризиків і дозволу керівництву встановлювати пріоритети для витрат на безпеку з розумним ступенем впевненості, що всі значні ризики пом’якшені. У таблиці 2.1 наведено порівняння кількісної та якісної оцінки ризику [16].

Таблиця 2.1 – Порівняння кількісної та якісної оцінки ризиків

	Кількісна	Якісна
Переваги	1. Пріоритет ризиків визначається фінансовим впливом; активи мають пріоритет за фінансовою цінністю. 2. Результати полегшують управління ризиками за рахунок повернення інвестицій у безпеку.	1. Це забезпечує видимість і розуміння ранжування ризиків. 2. Легше досягнути консенсусу. 3. Немає необхідності

	3. Результати можуть бути виражені в специфічній для менеджменту термінології (наприклад, грошові оцінки та ймовірність, виражені у певних відсотках). 4. Точність має тенденцію збільшуватися з часом, оскільки організація створює історичний запис даних, набуваючи досвіду.	кількісно оцінювати частоту загроз. 4. Немає необхідності визначати фінансову вартість активів. 5. Легше залучати людей, які не є експертами з питань безпеки чи комп'ютерів.
Недоліки	1. Значення впливу, присвоєні ризикам, базуються на суб'єктивних думках учасників. 2. Процес досягнення достовірних результатів і консенсусу займає дуже багато часу. 3. Розрахунки можуть бути складними та тривалими. 4. Результати представлені лише в грошовому вираженні, і для нетехнічних людей їх може бути важко інтерпретувати. 5. Процес вимагає досвіду, тому учасників нелегко навчити.	1. Існує недостатня диференціація між важливими ризиками. 2. Важко виправдати інвестиції у впровадження контролю, оскільки немає підстав для аналізу витрат/вигод. 3. Результати залежать від якості створеної групи з управління ризиками.

Необхідно зауважити, що «значення впливу, присвоєні ризикам, засновані на суб’єктивних думках учасників» зазначено як недолік кількісної

оцінки ризику (табл.2.1). Це пояснюється тим, що неможливо передбачити вартість впливу в обмежених кількісних значеннях. Залучена посадова особа або група повинні зробити суб'єктивну оцінку того, яким буде кількісне значення для певної майбутньої події. Нехтування цим обмеженням може призвести до помилкового уявлення про точність кількісної оцінки ризику. Правда також, що суб’єктивні думки використовуються для якісної оцінки впливу, але в цьому останньому випадку зрозуміло, що суб’єктивні оцінки притаманні процесу.

Організації потрібні чітко визначені категорії впливу, загрози та вразливості. FIPS 199 «Стандарти категоризації безпеки федеральних інформаційних систем» визначає три категорії безпеки на основі потенційного впливу на організацію, якщо відбудуться певні події, які поставлять під загрозу IT-активи, необхідні організації для виконання призначеної місії, захисту її активів, виконувати свої юридичні обов'язки, підтримувати свої повсякденні функції та захищати осіб [17].

Категорії 1. Низька. Очікується, що вона матиме обмежений негативний вплив на діяльність організації, організаційні активи або окремих осіб, включаючи наступне:

– спровокує погіршення спроможності місії до такої міри та тривалості, що організація може виконувати свої основні функції, але ефективність функцій помітно знижується;

– призведе до незначної шкоди активам організації;

– призведе до незначних фінансових збитків;

– завдасть незначної шкоди особам.

Категорії 2. Помірна або середня. Очікується, що вона матиме серйозний негативний вплив на діяльність організації, організаційні активи або окремих осіб, включаючи наступне:

– спровокує значну деградацію спроможності місії до такої міри та тривалості, що організація може виконувати свої основні функції, але ефективність функцій значно знижується;

– спричинить значну шкоду активам організації;

– спричинить значні фінансові втрати;

– спричинити значну шкоду особам, яка не пов'язана з втратою життя або серйозними травмами, що загрожують життю.

Категорії 1. Висока. Очікується, що вона матиме серйозний або катастрофічний негативний вплив на діяльність організації, активи організації або окремих осіб, включаючи наступне:

– спричинить серйозну деградацію або втрату можливостей місії до такої міри та тривалості, що організація не може виконувати одну або декілька своїх основних функцій;

– спричинить серйозну шкоду активам організації;

– спричинить великі фінансові втрати;

– привести до тяжкої або катастрофічної шкоди особам, включаючи втрату життя або серйозні травми, що загрожують життю.

В FIPS 199 «Стандарти категоризації безпеки федеральних та інформаційних систем» приведено ряд прикладів якісної оцінки впливу.

Наприклад, правоохоронна організація, яка керує надзвичайно чутливою слідчою інформацією, визначає, що потенційний вплив втрати конфіденційності є високим, потенційний вплив втрати цілісності є помірним, а потенційний вплив втрати доступності є помірний.

Результуюча категорія безпеки, інформація про розслідування (SC), цього типу інформації виражається як [18]:

SC = {(конфіденційність, ВИСОКА), (цілісність, ПОМІРНА), (доступність, ПОМІРНА)}.

Аналогічно, діапазони ймовірності приписуються якісним категоріям імовірності.

SP 800-100, Посібник з інформаційної безпеки:

Посібник для менеджерів, пропонує такі категорії:

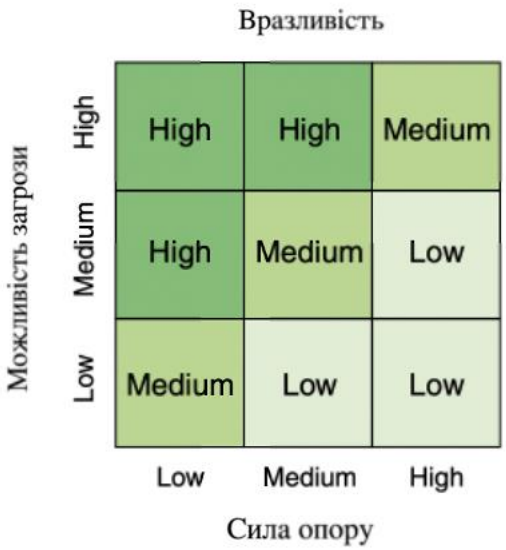
- Low: ≤0.1;
- Medium: 0.1 to 0.5;
- High: 0.5 to 1.0.

Інший тип категорій заснований на оцінці кількості подій на рік:

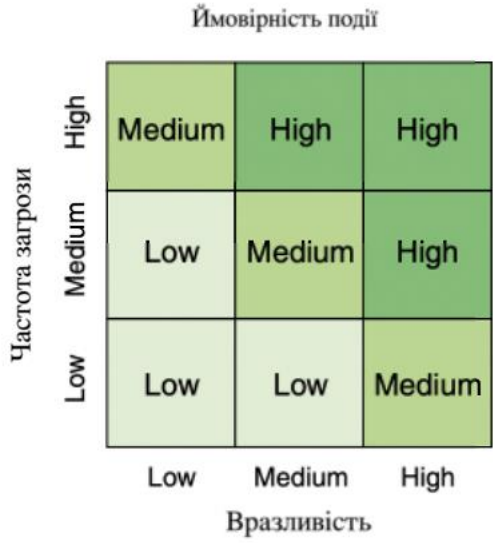
- Низький: < 1 раз на рік;
- Середній: від 1 до 11 разів на рік;
- Високий: > 12 разів на рік.

З огляду на ці категорії, часто використовують матриці для визначення ризику (рис.2.2). Вразливість до певної загрози є функцією можливостей або сили загрози та сили опору системи чи активу цій конкретній загрозі.

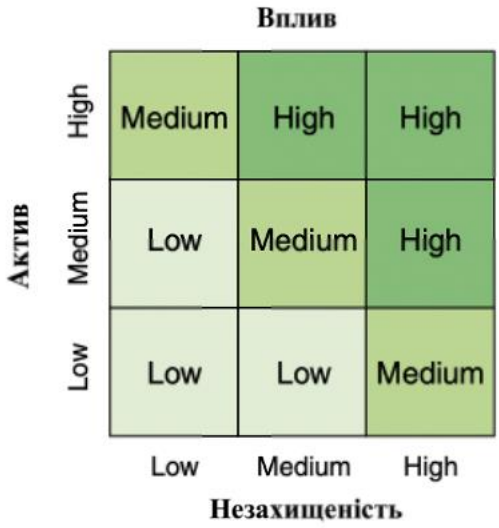
Тоді ймовірність несприятливої події безпеки, яка спричинить конкретну загрозу, залежить від частоти або ймовірності виникнення загрози та вразливості до цієї загрози.



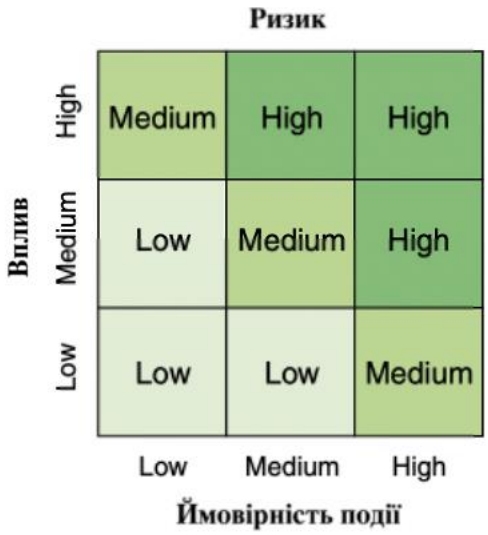
а) вразливість як функція загрози та опору



б) ймовірність як функція загрози та вразливості



в) вплив як функція активу та ризику



г) ризик як функція впливу та ймовірності

Рисунок 2.2– Якісне визначення ризику

Вплив визначається як функція класу активів і ризику збитків, які може спричинити конкретна загроза.

Наприклад, активи можна класифікувати з точки зору впливу збитків на бізнес.

Аналіз управління ризиками безпеки підприємства пропонує такі приклади класифікації:

– Низький вплив на бізнес: публічна інформація, інформація високого рівня.

– Середній вплив на бізнес: проекти мережі, списки співробітників, інформація про замовлення.

– Високий вплив на бізнес: фінансові дані, персональна інформація (PII), номери соціального страхування, інформація про медичну карту.

Аналіз управління ризиками безпеки підприємства також пропонує такі приклади ризику:

– Низький рівень ризику активів: незначні втрати або відсутність.

– Середній рівень ризику активів: обмежені або помірні втрати.

– Високий ризик активів: серйозна або повна втрата.

Отже, ризик визначається як функція впливу та ймовірності несприятливої події, яка спричиняє вплив.

Таким чином, ці матриці в поєднанні з інформованою оцінкою низьких, середніх і високих для різних факторів забезпечують розумні засоби оцінки ризику.

Однак слід мати на увазі, що результати такого грубого аналізу мають бути предметом судження.

Наприклад, на рисунку 2.2 г, порушення з низькою ймовірністю, високим рівнем впливу і з високою ймовірністю, з низьким впливом, обидва оцінені як середній ризик.

Важливим питанням при оцінці ризиків є питання: якому ризику слід надати пріоритет для дефіцитних ресурсів безпеки. У середньому можна очікувати, що кожен тип порушення принесе однакову суму річних збитків.

Чи важливіше впоратися з першим порушенням – оскільки, хоча і рідко, але якщо воно все-таки трапляється, воно може бути катастрофічним для організації – чи впоратися з останнім типом – яке може призвести до постійного потоку втрат. Цю проблему має вирішувати керівництво.

Приклад створення робочої таблиці аналізу ризиків. Простим підходом до оцінки ризику є використання робочої таблиці аналізу ризиків, яка є таблицею з одним рядком для кожної пари потенційної загрози/вразливості. Цей робочий аркуш, підготовлений групою оцінки ризиків, містить такі колонки [19, 20]:

1. Проблема безпеки: коротка інформація про кожну проблему безпеки або проблемну область. Для кожної пари загроза/вразливість має бути один рядок (а також проблеми відповідності, описані далі).

1.1. Імовірність: Оцінена ймовірність появи цієї пари загроза/вразливість. Оцінка повинна ґрунтуватися на оцінці командою вартості активів, які постраждали, та величині ризику, використовуючи матриці на рисунках 2.1 а та 2.1 б.

1.2. Вплив: передбачуваний вплив для цієї пари загроза/вразливість. Оцінка повинна ґрунтуватися на оцінці командою вартості активів, що постраждали, і величині ризику, використовуючи матрицю на рисунку 2.1 в.

1.3. Рівень ризику: рівень ризику на основі матриці на рисунку 2.1 г.

1.4. Рекомендовані засоби контролю безпеки: конкретні засоби контролю безпеки, які команда рекомендує для вирішення цієї конкретної проблеми.

1.5. Пріоритети контролю: відносний пріоритет кожного рекомендованого контролю.

1.6. Коментарі: будь-яка інша інформація, яка вважається важливою для процесу прийняття рішень щодо управління ризиками безпеки для цієї конкретної проблеми безпеки.

Проблеми з дотриманням вимог можна задокументувати на одному робочому аркуші. Вимоги до відповідності включають вимоги, встановлені політикою безпеки організації, державними постановами та відповідними стандартами акредитації.

Відповідність має бути оцінена таким чином [21:

0 = не реалізовано;

1 = частково реалізовано;

2 = реалізовано, але ще не задокументовано;

3 = впроваджено та задокументовано.

Для питань відповідності поля "Імовірність" і "Вплив" не мають значення.

Питання з оцінкою відповідності менше 3 має бути включено до робочого аркуша з високим рівнем ризику.

Інструкції з інформаційної безпеки MUSC: Управління ризиками включає низку прикладів пар загрози/вразливості, включаючи наступне:

2. Проблема безпеки: уповноважений співробітник використовує систему несанкціоновано.

2.1. Загроза: навмисне зловживання системою інсайдером.

2.2. Вразливість: недостатня підготовка (працівник не знає краще), або неналежний контроль за аудитом (працівник вважає, що його зловживання не буде виявлено), або відсутність ефективного дисциплінарного процесу (співробітник вважає, що ніяких санкцій не буде, навіть якщо його зловживання виявлено).

3. Проблема безпеки: Серйозний, постійний компроміс системи не виявлено до надто пізно, тому що ніхто не перевіряв особу, якій було доручено переглянути записи системної діяльності, які б виявили компроміс.

3.1 Загроза: навмисний несанкціонований доступ.

3.2 Уразливість: будь-яка вразливість або вразливості, які сприяли первинному вторгненню, доповненому недостатнім моніторингом та оцінкою ефективності контролю аудиту системи.

2.3 Факторний аналіз інформаційного ризику

Важливим внеском в оцінку ризику є факторний аналіз інформаційного ризику (FAIR), вперше запроваджений у 2005 році. FAIR, який був стандартизований The Open Group, отримав широке визнання [22, 23].

Його зв'язок зі стандартами ризику Міжнародної організації зі стандартизації (ISO) узагальнено таким чином:

1. ISO 27001 описує загальний процес створення системи управління інформаційною безпекою (СУІБ).

2. ISO 27005 визначає підхід до управління ризиком.

3. FAIR надає методологію для аналізу ризику.

Таким чином, FAIR надає більш конкретні вказівки, які можна використовувати в рамках, визначених ISO 27005.

Open Group опублікувала чотири стандарти, пов’язані з ризиками:

1. Таксономія ризику. Цей стандарт надає суворий набір визначень і таксономії для ризику інформаційної безпеки, а також інформацію про те, як використовувати таксономію.

2. Вимоги до методології оцінки ризиків. цей технічний посібник визначає та описує ключові характеристики, які складають будь-яку ефективну методологію оцінки ризику, таким чином забезпечуючи загальний набір критеріїв для оцінки будь-якої даної методології оцінки ризику за чітко визначеним загальним набором суттєвих вимог.

3. FAIR–ISO/IEC 27005 Cookbook. Цей технічний посібник детально описує, як застосувати методологію FAIR до системи ISO 27005.

4. Технічний стандарт Open Group Risk Analysis (O-RA). Даний документ містить набір стандартів для різних аспектів аналізу ризиків інформаційної безпеки.

FAIR надає більш детальний набір рекомендацій щодо всіх аспектів оцінки ризику. Наприклад, FAIR надає визначення ключових термінів, які є менш розмитими і більш конкретно пов’язані з процесом аналізу ризиків, ніж ISO 27005. В FAIR використовуються такі основні визначення.

Актив: будь-які дані, пристрій або інший компонент середовища, який підтримує діяльність, пов'язану з інформацією, до якої можна отримати незаконний доступ, використати, розкрити, змінити, знищити та/або вкрасти, що призведе до втрати.

Ризик: ймовірна частота та ймовірна величина майбутніх збитків.

Загроза: будь-що, що може діяти таким чином, щоб завдати шкоди активу та/або організації, наприклад, дії Бога (погода, геологічні події тощо), зловмисники, помилки та збої.

Вразливість: ймовірність того, що актив не зможе протистояти діям агента загрози.

Методологія FAIR заснована на переконанні, що суб’єктивний якісний аналіз є неадекватним у більшості ситуацій і що всі ризики, матеріальні та нематеріальні, піддаються вимірюванню та кількісній оцінці.

Фактичні результати кількісного аналізу надаються з використанням каліброваних імовірнісних оцінок, заснованих на діапазонах ймовірностей, точних порівнянь і розрахунків PERT за допомогою моделювання Монте-Карло.

2.4 Нормативні документи та рекомендації з оцінки ризиків

Ряд професійних і галузевих груп розробили документи та рекомендації з передового досвіду оцінки ризиків. Найважливішим таким документом є Стандарт належної практики інформаційної безпеки (The Standard of Good Practice for Information Security, SGP), розроблений Форумом інформаційної безпеки (Information Security Forum, ISF). Цей майже 300-сторінковий документ надає широкий спектр найкращих практик, заснованих на консенсусі галузевих і урядових організацій [23].

SGP розбиває практики в категорії оцінки інформаційних ризиків на дві області та 12 тем і надає детальні контрольні списки для кожної теми. Сфери та теми наступні.

Структура оцінки інформаційних ризиків: метою цієї галузі є проведення регулярних оцінок інформаційних ризиків для цільових середовищ (наприклад, критичних бізнес-середовища, процесів і додатків, включаючи допоміжні системи/мережі) у суворий, послідовний спосіб із застосуванням систематичного, структурована методологія.

Оцінка інформаційного ризику – підхід до управління. підсумовує завдання, щоб дати можливість особам, які відповідають за цільове середовище, визначити ключові інформаційні ризики, оцінити їх та визначити необхідне лікування, щоб утримати ці ризики в прийнятних межах.

Оцінка інформаційних ризиків – методологія: підсумовує систематичну та структуровану методологію, щоб зробити оцінку інформаційних ризиків ефективною, легкою та узгодженою в усій організації та створити чітку картину ключових інформаційних ризиків. Документ рекомендує використовувати ISO 27005 і NIST SP 800-30 для детальної інструкції.

Оцінка інформаційного ризику – допоміжний матеріал: описує допоміжний матеріал, необхідний для забезпечення правильного виконання кожного етапу оцінки ризику, оцінки дають практичні результати та можуть приймати ефективні рішення щодо ризику. Документ рекомендує використовувати BIRT і розробити набір засобів контролю безпеки на основі ISO 27002 і NIST Cybersecurity Framework.

Процес оцінки інформаційного ризику. Метою цієї галузі є прийняття методології оцінки інформаційних ризиків, яка включає важливі заходи, що охоплюють визначення обсягу, оцінку впливу на бізнес, профілювання загроз, оцінку вразливості, оцінку ризику та лікування ризиків.

Обсяг оцінки ризику: описує елементи, які визначають сферу оцінки ризику, включаючи послуги, активи та інші фактори, що впливають на рейтинги впливу (наприклад, економічні, соціальні, технологічні, правові та екологічні).

Оцінка впливу на бізнес: надає контрольні списки для визначення того, яким чином порушується конфіденційність, цілісність. та доступність інформації може мати вплив на бізнес. Ця тема містить загальні вказівки щодо використання BIRT, визначення найкращих і найгірших наслідків, а також визначення фінансових, операційних та інших впливів.

Оцінка впливу на бізнес – вимоги до конфіденційності: повторює контрольні списки із загальної оцінки впливу на бізнес.

Оцінка впливу на бізнес – вимоги цілісності: повторює контрольні списки із загальної оцінки впливу на бізнес.

Оцінка впливу на бізнес – вимоги щодо доступності: повторює контрольні списки із загальної оцінки впливу на бізнес, а також обговорює специфічні показники доступності.

Профілювання загроз: включає виявлення, характеристику та визначення пріоритету загроз. Це також включає визначення відповідних подій загроз. У центрі уваги цієї теми є характеристика ймовірності та сили кожної ідентифікованої загрози.

Оцінка вразливості: перелічує міркування для оцінки ступеня вразливості активів у сфері дії кожної загрози.

Оцінка ризику: обговорює кроки для виконання оцінки ризику на основі ISO 7005 та SP 800-30.

Обробка ризику: обговорює процес створення плану обробки ризику.

3 РОЗРОБКА АЛГОРИТМІВ ОЦІНКИ РИЗИКІВ

3.1 Процес проведення оцінки ризиків

Процес оцінки ризику складається з чотирьох кроків:

– підготуватися до оцінки;

– провести оцінку;

– повідомити результати оцінки; та (iv) підтримувати оцінку.

Основні кроки процесу оцінки ризику та конкретні завдання для проведення оцінки приведені на рисунку 3.1 [24].

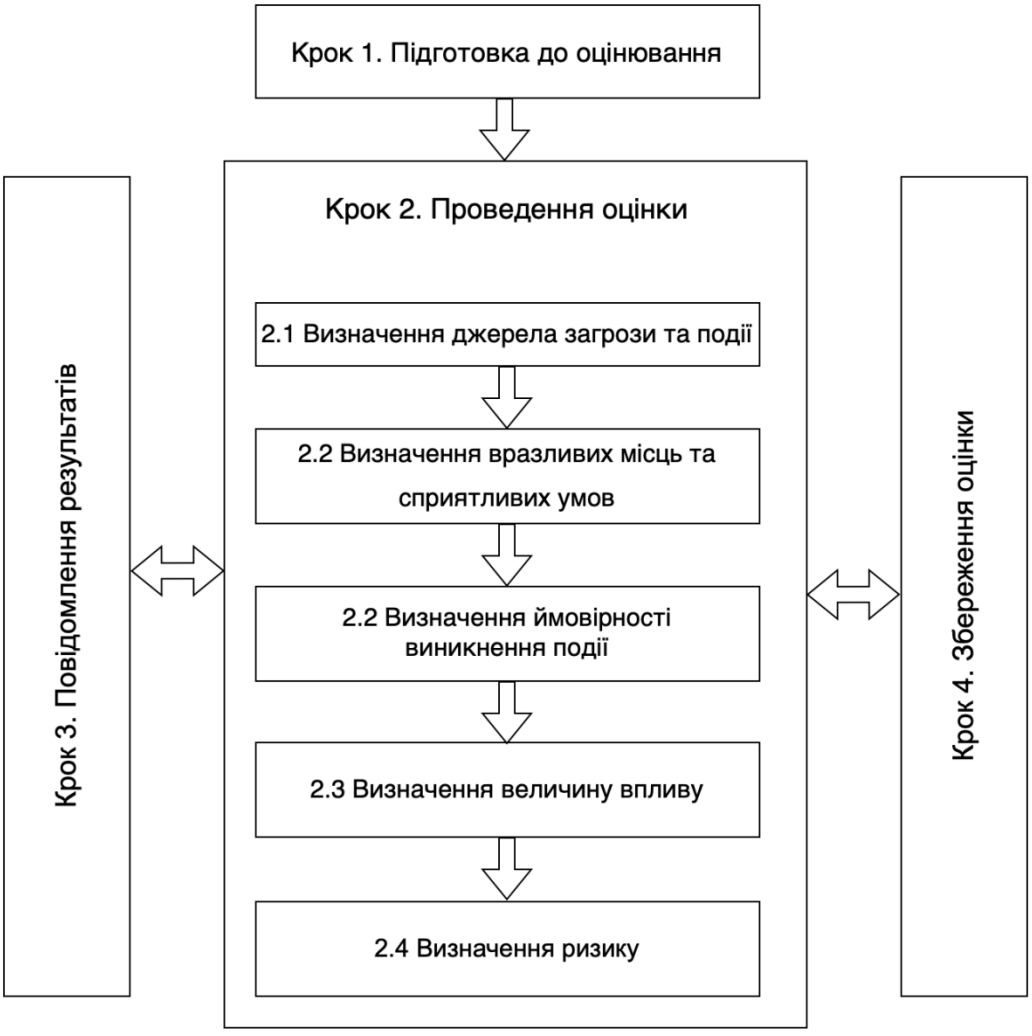


Рисунок 3.1 – Процес оцінки ризику

Важливим кроком у процесі оцінки ризику є підготовка до оцінки. Метою цього кроку є встановлення контексту для оцінки ризику. Підготовка до оцінки ризику включає такі завдання:

– визначення мети оцінювання;

– визначення обсягу оцінки;

– визначення припущення та обмеження, пов'язаних з оцінкою;

– визначення джерела інформації, які будуть використані як вхідні дані для оцінки;

– визначення моделі ризику та аналітичні підходів (тобто підходів до оцінки та аналізу), які будуть використані під час оцінки.

Кожен крок алгоритму розділений на набір завдань. Для кожного завдання керівництво надає додаткову інформацію для організацій, які проводять оцінку ризиків.

3.2 Визначення ризику

Після того, як величина збитків оцінена і частота подій збитків визначена, можна легко отримати оцінку ризику. Це робиться окремо для первинних і вторинних втрат, а потім вони об’єднуються.

Основне визначення первинного FR і вторинного SR ризику показано на рисунку 3.2 і визначається так:

FR = f3 (частота події первинної втрати, величина первинної втрати).

SR = f4 (частота події вторинної втрати, величина вторинної втрати).

Окремі значення матриці є предметом судження, яке може відрізнятися від однієї організації до іншої. Матриця f3 має відносно консервативний погляд.

Таким чином, якщо величина втрат оцінюється як дуже висока, тоді ризику присвоюється значення дуже високого, навіть якщо частота втрат лише помірна.

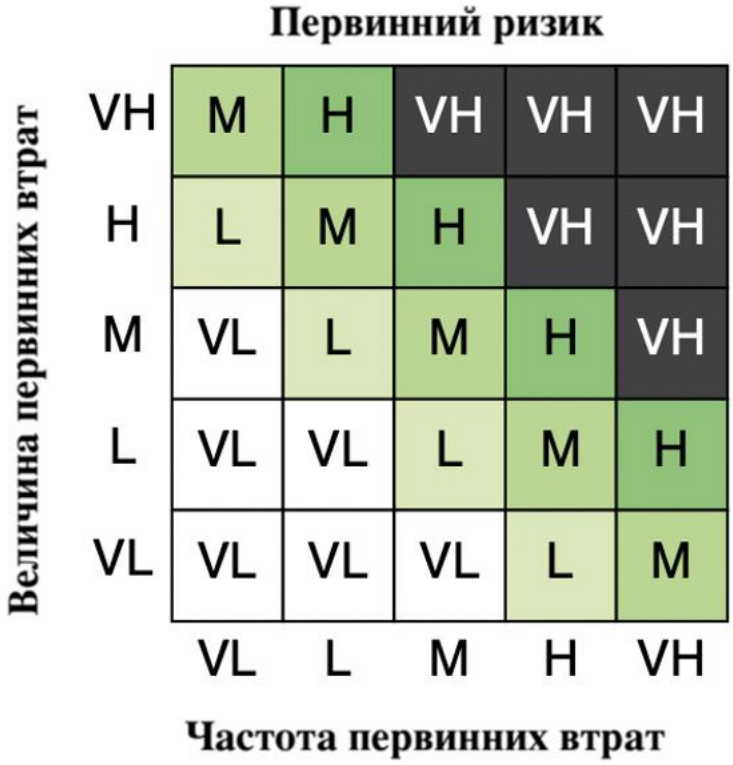


Рисунок 3.2 – Матриця визначення первинного і вторинного ризику

Аналогічно, навіть якщо величина втрат оцінюється як помірна, якщо частота подій втрат оцінюється як дуже висока, ризику присвоюється значення дуже високого.

Той самий розрахунок f3 застосовується до вторинних збитків для визначення вторинного ризику.

Потім обидва ризики об’єднуються для визначення загального ризику GR за допомогою матриці на рисунку 3.3, який визначається так:

GR = f4 (первинний ризик, вторинний ризик).

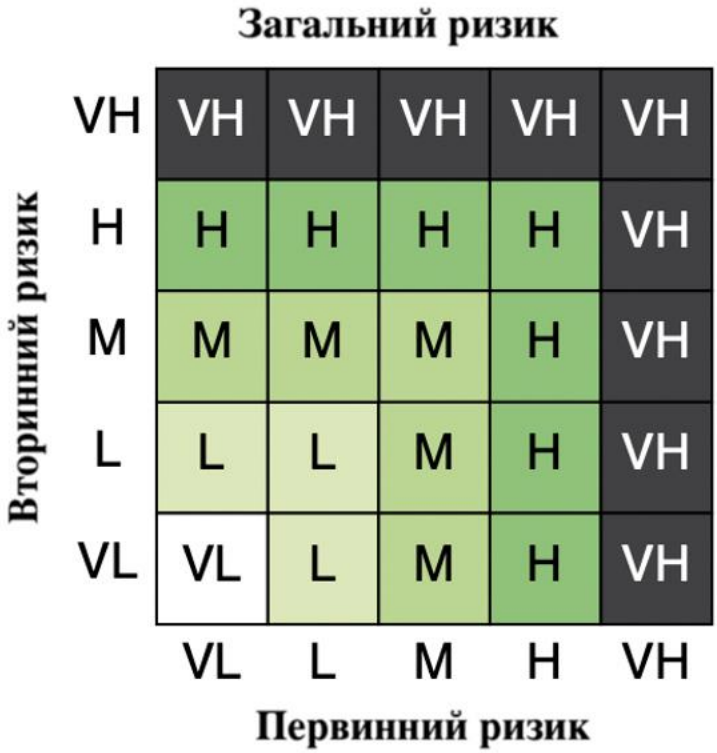


Рисунок 3.3 – Матриця визначення загального ризику

Наприклад, консервативний погляд може бути таким, що якщо первинний і вторинний ризики знаходяться на одному рівні, загальний ризик слід підняти до наступного рівня. У цьому випадку, якщо обидва ризики оцінені як високі, загальний ризик оцінюється як дуже високий. Менш консервативна стратегія вказана у функції f4.

3.3 Оцінка ризику

Після аналізу ризиків вище керівництво безпеки та керівники можуть визначити, чи приймати певний ризик, а якщо ні, то необхідно визначити пріоритет у виділенні ресурсів для пом’якшення ризику. Цей процес, відомий

як оцінка ризику, передбачає порівняння результатів аналізу ризику з критеріями оцінки ризику.

Рекомендації щодо оцінки ризиків як у ISO 27005, так і в документах FAIR є загальними, оскільки розроблені критерії значно відрізняються від однієї організації до іншої. ISO розрізняє критерії оцінки ризику та критерії прийняття ризику.

Критерії оцінки зосереджуються на важливості різних бізнес-активів і впливі, який можуть спричинити на організацію різні події безпеки. Мета полягає в тому, щоб мати можливість визначити пріоритети для обробки (лікування) ризику.

Критерії прийняття ризику стосуються того, який ризик може перенести організація, і надають вказівки щодо того, скільки бюджету можна виділити на лікування ризику.

SP 800-100 містить загальні вказівки щодо оцінки ризику та визначення пріоритетів дій на основі трирівневої моделі.

1. Високий: якщо спостереження або висновок оцінюються як високий ризик, існує гостра потреба в коригуючих заходах. Існуюча система може продовжувати функціонувати, але план коригуючих дій має бути створений якомога швидше.

2. Помірний: якщо спостереження оцінено як помірний ризик, необхідні коригувальні дії, і необхідно розробити план, щоб включати ці дії протягом розумного періоду часу.

3. Низький: якщо спостереження описується як низький ризик, уповноважена посадова особа системи повинна або визначити, чи потрібні коригувальні дії, або вирішити прийняти ризик.

3.4 Обробка ризику

Після завершення процесу оцінки ризиків керівництво повинно мати перелік усіх загроз, які становлять усі активи, з оцінкою величини кожного ризику. Крім того, оцінка ризику дає вхідні дані щодо пріоритетності та терміновості, з якою кожна загроза має бути спрямована. Реакція на набір ідентифікованих ризиків називається обробкою ризику (або реакція на ризик), як показано на рисунку 3.4.

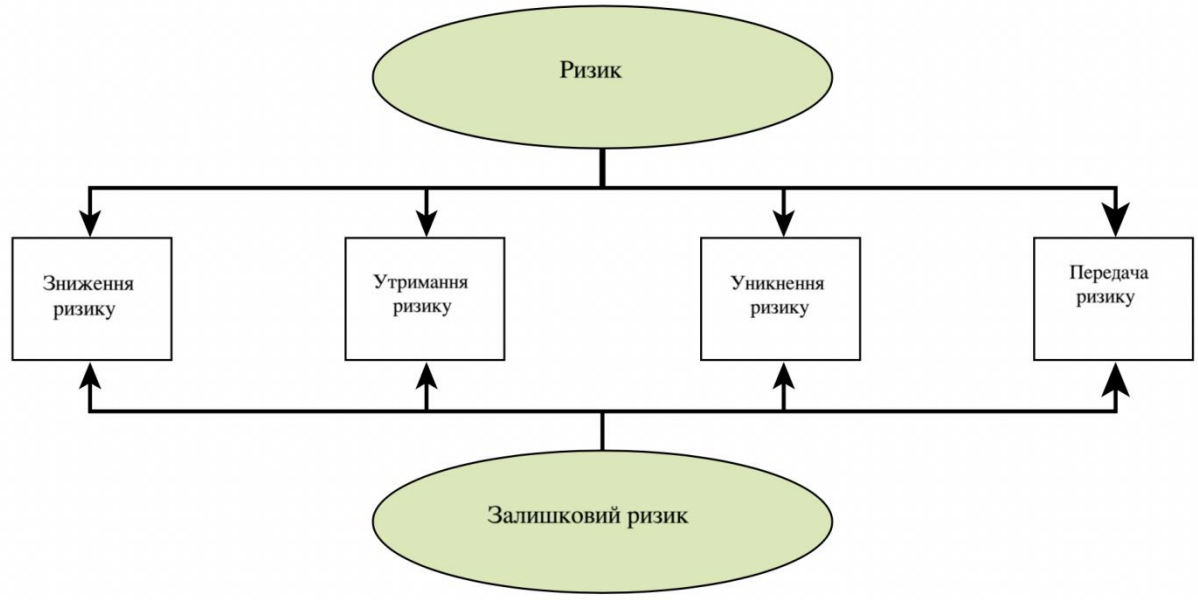


Рисунок 3.4 – Обробка ризику

В ISO 27005 використовуються такі варіанти обробки ризику.

1. Зменшення або пом'якшення ризику: дії, вжиті для зменшення ймовірності та/або негативних наслідків, пов'язаних з ризиком.

2. Утримання ризику: прийняття вартості від ризику.

3. Уникнення ризику: Рішення не втручатися в ризиковану ситуацію або діяти, щоб вийти з неї.

4. Передача або розподіл ризику: розділення з іншою стороною тягаря збитків від ризику.

Між ризиками та методами обробки існує взаємозв'язок «багато до багатьох». Одна обробка може вплинути на кілька ризиків, і кілька методів лікування можуть бути застосовані до одного ризику. Крім того, чотири варіанти не є взаємовиключними.

Як частина плану обробки ризику може бути прийнято кілька стратегій. Будь-який план обробки ризику може зменшити, але не усунути ризик. Те, що залишається, називається залишковим ризиком. На основі плану організація повинна оновити оцінку ризику та визначити, чи є залишковий ризик прийнятним, чи план потрібно оновити.

Зниження ризику. Зменшення ризику досягається шляхом впровадження контролю безпеки. Контроль безпеки може призвести до наступного:

– видалення джерела загрози;

– зміна ймовірності того, що загроза може використати вразливість;

– зміна наслідків події безпеки.

Утримання ризику. Утримання ризику, яке також називають прийняттям ризику – це свідоме рішення керівництва щодо здійснення діяльності, незважаючи на наявний ризик, або утримуватися від додавання до наявних засобів контролю, якщо такі є, для захисту активу від певної загрози.

Ця форма обробки, яка фактично не є лікуванням, є прийнятною, якщо визначена величина ризику знаходиться в межах рівня толерантності до ризику організації. В окремих випадках організація може прийняти ризик, який є більшим, ніж зазвичай прийнятний, якщо є переконливий діловий інтерес.

У будь-якому випадку ризик необхідно відстежувати і плани реагування, прийнятні для зацікавлених сторін, мають бути на місці.

Уникнення ризику. Якщо ризик у певній ситуації вважається занадто високим і витрати на пом’якшення ризику до прийнятного рівня перевищують вигоди, організація може вирішити уникнути обставин, що призводять до ризику.

Це може означати, наприклад, відмову від бізнес-можливостей, переїзд, щоб уникнути екологічної загрози чи юридичної відповідальності, або заборону використання певного апаратного чи програмного забезпечення.

Передача ризику. Розподіл або передача ризику здійснюється шляхом розподілу всієї або частини відповідальності за пом’якшення ризику або наслідків ризику іншій організації. Це може мати форму страхування, субпідряду чи партнерства з іншою юридичною особою.

3.5 Алгоритм оцінки ризиків кібербезпеки

Кожна організація стикається зі своїм власним унікальним набором ризиків безпеки, і їй необхідно використовувати свій власний підхід до оцінки ризиків кібербезпеки.

Стандарти кібербезпеки та нормативні вимоги визнають, що різні компанії повинні використовувати різні підходи для захисту своїх інформаційних систем. Щоб захистити свої дані від кіберзлочинності та підвищити загальну безпеку, потрібна комплексна програма захисту інформаційних технологій.

Початок роботи з оцінки ризиків кібербезпеки є найскладнішою частиною стратегії управління ризиками. Спочатку розглянемо, хто повинен виконувати оцінку ризиків кібербезпеки, а також переваги її проведення. Усі

організації, які використовують IT-інфраструктуру, повинні проводити оцінку ризиків кібербезпеки.

Однак деякі малі підприємства можуть мати обмежений бюджет або робочу силу, що заважає вашій здатності виконувати ретельну роботу з оцінки та зменшення ризику. З цієї причини багато організацій звертаються до програмного забезпечення для кібербезпеки, щоб допомогти їм краще оцінити, пом’якшити та контролювати свої стратегії управління ризиками. Сучасні рішення для кібербезпеки розроблені, щоб запобігти трьом основним категоріям ризиків кібербезпеки: зловмисному програмному забезпеченню, програмі-вимагачі та фішингу.

Переваги виконання оцінки ризиків безпеки. Виконання оцінки ризиків кібербезпеки та впровадження процесу управління ризиками у організації має наступні переваги [25].

1. Зменшує витрати, пов’язані з інцидентами безпеки. Ви можете зменшити довгострокові витрати, пов’язані зі збитками, спричиненими порушенням даних або крадіжкою критичних активів.

2. Забезпечує базовий рівень для організаційного ризику. Він забезпечує базову лінію для майбутніх оцінок, коли ви вирішуєте свій рівень ризику з часом.

3. Підтримує потребу в програмі кібербезпеки. Проведення оцінки ризику надає вашому CISO докази необхідності програми кібербезпеки, яку він або вона може потім показати зацікавленим сторонам.

4. Уникає злому даних. Ви можете виявити загрози, пом’якшити їх і уникнути злому даних.

5. Зменшує проблеми із дотриманням вимог. Можна уникнути проблем із дотриманням нормативних вимог, пов’язаних із даними клієнтів.

6. Зменшує втрати продуктивності. Виявивши вразливі місця та пом’якшивши їх, можна уникнути збоїв, які можуть призвести до втрати продуктивності (рисунок 3.5).

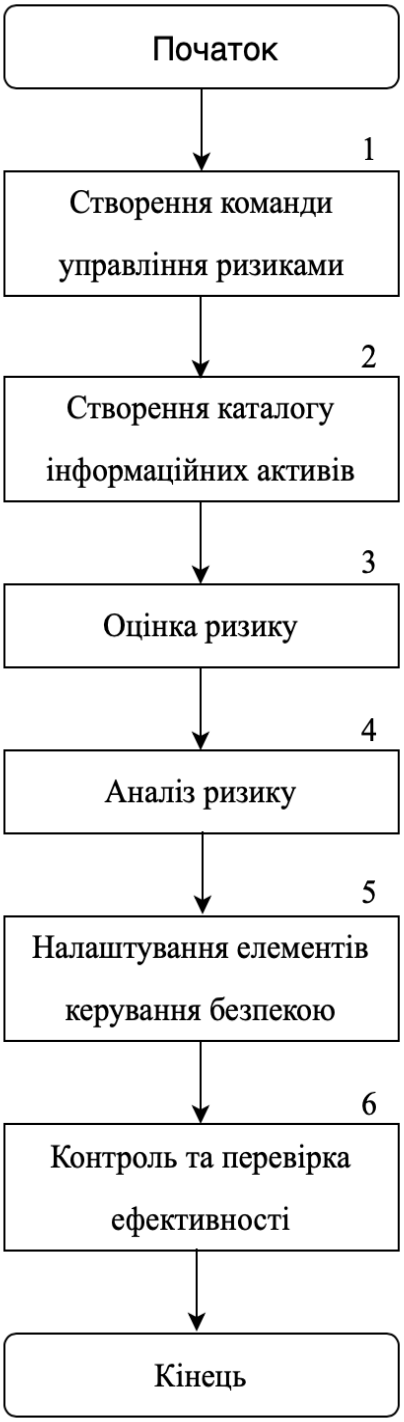


Рисунок 3.5 – Алгоритм оцінки ризиків

7. Зменшує втрати даних. Крадіжка важливих інформаційних активів може коштувати більше, ніж просто грошові збитки. Розроблений алгоритм ґрунтується на оцінці ризику, який починається з розуміння та узгодження бізнес-цілей із цілями інформаційної безпеки.

Розглянемо кроки алгоритму детальніше.

Крок 1. Створення команди управління ризиками.

Міжвідомча команда має вирішальне значення для виявлення кіберзагроз та зменшення ризиків для ваших IT-систем і даних. Команда з управління ризиками також може повідомити про ризик співробітникам і ефективніше реагувати на інциденти. Як мінімум команда повинна включати:

– вище керівництво, щоб забезпечити нагляд;

– головного спеціаліста із інформаційної безпеки, щоб переглянути архітектуру мережі;

– уповноваженого із конфіденційності, щоб знайти особисту інформацію, як того вимагає Загальний регламент ЄС про захист даних (GDPR);

– відповідального за дотримання правил, щоб забезпечити відповідність Національному інституту стандартів і технологій кібербезпеки (NIST CSF), Закону про портативність і підзвітність медичної інформації (HIPAA) та іншим стандартам безпеки;

– хтось із маркетингової команди, щоб обговорити зібрану та збережену інформацію;

– хтось із команди управління продуктом, щоб забезпечити безпеку продукту протягом усього циклу розробки;

– людські ресурси, щоб надати уявлення про особисту інформацію співробітника;

– менеджер з кожного основного напряму діяльності, щоб охопити всі дані в організації.

Крок 2. Створення каталогу інформаційних активів.

Команда з управління ризиками має працювати разом, щоб створити каталоги всіх інформаційних активів бізнесу.

Сюди входить IT-інфраструктура організації та різні рішення «Програмне забезпечення як послуга» (SaaS), «Платформа як послуга» (PaaS) та «Інфраструктура як послуга» (IaaS), які використовуються у всій компанії.

Активи, які використовуються сторонніми постачальниками, повинні бути включені у список. Сторонні постачальники залишаються значним ризиком порушення даних.

Для того щоб зрозуміти типи даних, які компанія збирає, зберігає та передає, а також місця розташування, необхідно отримати відповіді на такі запитання:

– яку інформацію збирають відділи?

– де вони зберігають цю інформацію?

– куди вони надсилають цю інформацію?

– звідки вони це збирають?

– яких постачальників використовує кожен відділ?

– який доступ мають ці постачальники?

– які методи аутентифікації, такі як багатофакторна автентифікація, ви використовуєте для доступу до інформації?

– де фізично компанія зберігає інформацію?

– які пристрої використовують працівники?

– чи мають віддалені працівники доступ до інформації? Як?

– які мережі передають інформацію?

– які бази даних зберігають інформацію?

– які сервери збирають, передають та зберігають інформацію?

Крок 3: Оцінка ризику.

Деякі відомості важливіші за інші. Не всі постачальники однаково безпечні. Коли інформаційні активи визначені, необхідно оцінити ризики для них і організації. Для цього необхідно дати відповіді на такі запитання:

– які системи, мережі та програмне забезпечення є критичними для бізнес-операцій?

– яка конфіденційна інформація потрібна для збереження доступності, конфіденційності та цілісності?

– яку особисту інформацію зберігаєте, передаєте чи збираєте, яку необхідно анонімізувати у разі збою шифрування?

– які пристрої піддаються найбільшому ризику втрати даних?

– яка ймовірність пошкодження даних?

– на які IT-системи, мережі та програмне забезпечення можуть націлюватися кіберзлочинці для порушення даних?

– яку шкоду репутації може завдати інциденту безпеки?

– які фінансові ризики несе потенційний злом даних або витік даних?

– які ризики для ведення бізнесу можуть виникнути в результаті події кібербезпеки?

– чи є у план безперервності бізнесу, який дає змогу швидко повернутися до роботи?

У процесі оцінки ризиків враховуються ризики для інформаційних активів у каталозі, а також те, яку шкоду можуть завдати підприємству порушення кожного з них. Це включає шкоду діловій репутації, фінансам, безперервності та діяльності.

Крок 4. Аналіз ризику.

Аналіз ризиків надає пріоритет визначеним ризикам. Для кожного ризику треба призначити оцінку на основі:

1. Ймовірності: ймовірність отримання доступу кіберзлочинця до активу.

2. Вплив: фінансовий, операційний та репутаційний вплив, який подія безпеки може мати на вашу організацію.

Щоб визначити рівень толерантності до ризику, треба помножити ймовірність на вплив. Також для кожного ризику необхідно визначити свою відповідь: прийняти, уникнути, передати чи пом’якшити.

Наприклад, база даних, що містить загальнодоступну інформацію, таку як визначення вимог NIST або NY DFS, може мати небагато засобів контролю, які захищають її, тому ймовірність порушення може бути високою. З іншого боку, якби зловмисники захопили лише цю інформацію чи інші загальнодоступні дані, вплив був би низьким. Таким чином, під час аналізу ризиків можна прийняти ризик інформаційної безпеки для конкретної бази даних, оскільки, незважаючи на високу ймовірність порушення, оцінка впливу є низькою. І навпаки, якщо організація збираєте фінансову інформацію від клієнтів, оцінка ймовірності порушення може бути низькою, але наслідком порушення можуть бути суворі нормативні санкції та погіршення корпоративної репутації. Тому ви можете вирішити пом’якшити цей ризик, оформивши страховий поліс кібербезпеки.

Крок 5. Налаштування елементів керування безпекою.

Даний крок передбачає визначення та впровадження засобів контролю безпеки. Контроль безпеки допоможе вам керувати потенційними ризиками, щоб вони були повністю виключені, або ймовірність їх виникнення значно зменшилася. Контроль важливий для кожного потенційного ризику. Він вимагає, щоб вся організація докладала зусиль як для його реалізації, так і для забезпечення постійного контролю. Приклади контролю включають:

1) розділення мережі;

2) шифрування в стані спокою та під час транспортування;

3) програмне забезпечення для захисту від шкідливих програм, програм-вимагачів і фішингу;

4) конфігурація брандмауера;

5) протоколи паролів;

6) багатофакторна аутентифікація;

7) навчання робочої сили;

8) програма управління ризиками постачальників.

Крок 6. Контроль та перевірка ефективності.

Для забезпечення IT-безпеки, протягом багатьох років, організації покладалися на тестування на проникнення та періодичні перевірки. Але оскільки зловмисники продовжують змінювати свої методології, щоб перешкодити контролю безпеки, організації потрібно коригувати свою політику безпеки та підтримувати програму управління ризиками, яка постійно контролює IT-середовище на предмет нових загроз. Відповідно, аналіз ризиків також має бути гнучким.

Наприклад, у рамках процесу зменшення ризику потрібно впровадити механізми реагування, щоб була можливість підтримувати надійний профіль кібербезпеки.

ВИСНОВОК

В кваліфікаційній роботі розв’язано актуальну задачу підвищення ефективності алгоритмів оцінки ризиків. При цьому отримано наступні результати.

1. Проведено аналіз загроз у системі захисту інформації та способи визначення критичності активів, зокрема: ідентифікація людей, процедур та активів даних, ідентифікація обладнання, програмного забезпечення та мережевих активів.

2. Визначено категорії загроз з використанням моделі загроз STRIDE, такі як: підробка ідентифікаційної інформації, підробка даних, відмова, розкриття інформації, відмова в обслуговуванні, підвищення привілеїв та шкідливе програмне забезпечення. Шкідливе програмне забезпечення охоплює багато типів програмних загроз, зокрема такі: віруси, черв'яки, програми-вимагачі, спам, логічні бомби та багато інших.

3. Визначено методи та підходи до оцінки ризиків кібербезпеки, зокрема кількісні, якісні та факторний аналіз інформаційного ризику.

4. Розроблено алгоритм оцінки ризиків, який складається з шести кроків та ґрунтується на розуміння та узгодження бізнес-цілей із цілями інформаційної безпеки який складається з шести кроків.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Federal Emergency Management Agency (FEMA). FEMA 452, Risk Assessment, A How-to Guide to Mitigate Potential Terrorist Attacks Against Buildings, Jan 2005.

2. Federal Emergency Management Agency (FEMA). FEMA 426, Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings, Dec 2003.

3. MHA, Guidelines on Enhancing Building Security in Singapore (GEBSS), 2010.

4. ENISA Threat Landscape 2021. [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

5. Stallings, W. Effective Cybersecurity: Understanding and Using Standards and Best Practices. Addison-Wesley. 2019. – 893 p.

6. ISO 31010 2019. Risk management – Risk assessment techniques. Management du risque -Techniques. – 268 p.

7. A. Shostack, Threat Modeling: Designing for Security, John Wiley & Sons Inc., 2014.

8. Microsoft, “Chapter 3 - Threat Modeling,” 7 July 2010. [Електронне джерело]. Режим доступу: https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648644(v=pandp.10) .

9. National Institute of Standards and Technology (NIST). “Guide for Conducting Risk Assessments,” September 2012. [Електронне джерело]. Режим доступу: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

10. Paladin Risk Management Services, “Risk Tip #5 - Hungry to Understand Risk Appetite?” 2017. [Електронне джерело]. Режим доступу: https://paladinrisk.com.au/risk-tip-5-hungryunderstand-risk-appetite.

11. Australian Government, Department of Finance, “Comcover Risk Resources - Defining Risk Appetite and Tolerance,” 2016. [Електронне джерело]. Режим доступу: https://www.finance.gov.au/sites/default/files/2019-11/case-study-defining-riskappetite-and-tolerance.PDF.

12. National Institute of Standards and Technology (NIST) “Managing Information Security Risk: Organization, Mission, and Information System View,” March 2011. [Електронне джерело]. Режим доступу: https://csrc.nist.gov/publications/detail/sp/800-39/final.

13. ISACA, CRISC Review Manual 6th Edition, ISACA, 2015.

14. Корченко А. Г. Побудова систем захисту інформації на нечітких множинах. Теорія та практичні рішення – К.: МК-прес, 2016. – 324 с.

15. Легчекова Є.В., Титов О.В. Методика розрахунку ризиків інформаційної безпеки. [Електронне джерело]. Режим доступу:

http://lib.ibteu.by/bitstream/handle/22092014/3600/Legchekova%20E.B.%2C%20Титов%20О.В.%20 Метод розрахунку.pdf

16. C. E. Bodungen, B. L. Singer, A. Shbeeb, S. Hilt and K. Wilhoit, Industrial Control Systems Hacking Exposed, McGraw-Hill Education, 2017.

17. T. Langill and E. D. Knapp, Industrial Network Security, Second Edition: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems, Elsevier, 2014.

18. Wangen, G. *Quantifying and Analyzing Information Security Risk from Incident Data*; Graphical Models for Security; Albanese, M., Horne, R., Probst, C.W., Eds.; Springer International Publishing: Cham, Switzerland, 2019, pp. 129–154.

19. Radanliev P., et al. Cyber Risk in IoT Systems. 2019.

20. Lee, In. "Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management." *Future Internet* 12.9, 2020: 157.

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

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

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

24. Яцків Н.Г., Вівчар Д.В., Черняк Т.Г. Аналіз підходів до оцінки ризиків. Матеріали проблемно-наукової міжгалузевої конференції «Автоматизація та комп'ютерно-інтегровані технології» (АКІТ - 2022), Тернопіль, 2022. – С. 104-106.

25. Яцків Н.Г., Вівчар Д.В. Аналіз підходів до оцінки ризиків. Матеріали науково-практична конференція молодих вчених, аспірантів та студентів «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ – 2022), Тернопіль, 2022. – С. 10-12.

ДОДАТОК А

Копії публікацій

ЗАХІДНОУКРАЇНСЬКИЙНАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ПРИКАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТЕФАНИКА
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВОДНОГО ГОСПОДАРСТВА ТА ПРИРОДОКОРИСТУВАННЯ
НАЦІОНАЛЬНИЙ ТРАНСПОРТНИЙ УНІВЕРСИТЕТ
НАДВІРНЯНСЬКИЙ КОЛЕДЖ НТУ
ГАЛИЦЬКИЙ КОЛЕДЖ ІМ. В. ЧОРНОВОЛА

Проблемно-наукова міжгалузева конференція

АВТОМАТИЗАЦІЯ ТА КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ

(АКІТ – 2022)

21—23 лютого 2022 року

Тернопіль

АВТОМАТИЗАЦІЯ ТА КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ

БЕЗПЕКА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Продан Т.І. Івасьєв С.В.
СУЧАСНІ МЕТОДИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ…… 62

Хомич О.В.
ДОСЛІДЖЕННЯ ПОДІЙ ФАЙЛОВОЇ СИСТЕМИ……... 65

Кулина С.В.
ВИЯВЛЕННЯ ТА ВИПРАВЛЕННЯ ПОМИЛОК У ЗАХИЩЕНИХ СИСТЕМАХ ЗБЕРІГАННЯ ДАНИХ МЕТОДОМ ОБЧИСЛЕННЯ СИНДРОМУ……... 67

Ігнатєв І.В., Кондратюк В.М.
АЛГОРИТМИ ПЕРЕВІРКИ ЧИСЛА НА ПРОСТОТУ……. 70

Олійник Н.П.
ВИКОРИСТАННЯ СИМЕТРОЧНОГО ШИФРУ AES З РЕАЛІЗАЦІЄЮ НА JAVASCRIPT…… 73

Кондіус І.С.
ОЦІНКА ЯКОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ……. 76

Ковальчук О.В., Михайлевський О.А., Глинська І.К., Шандалюк С.А.
ВИБІР МЕТОДУ ВБУДОВУВАННЯ У ЗОБРАЖЕННЯ-КОНТЕЙНЕР…. 79

Недзельський Р.В,., Архитко О.В., Бодак С.В., Тихоліз М.В., Якименко І.З.
ЕВОЛЮТИВНИЙ АЛГОРИМТ ГЕНЕРУВАННЯ ПАРАМЕТРІВ ЕЛІПТИЧНИХ КРИВИХ……... 84

Гринчук А.М., Пилипів С.І., Войтенко О.О., Черняк В.А.
СТРУКТУРА ЦЕНТРУ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЛЯ ПРОТИДІЇ ЗАГРОЗАМ……. 88

Миколишин П.П
СИСТЕМА ЗАПОБІГАННЯ ПРОНИКНЕННЮ В МЕРЕЖІ ІНТЕРНЕТ-РЕЧЕЙ……... 91

Концевич О.О., Бойко Н.З., Савіцький Т.Д.
МОДЕЛЮВАННЯ ТА ДОСЛІЖЕННЯ АТАКИ ЕНЕРГОСПОЖИВАННЯ НА ОСНОВІ ВАГИ ХЕМІНГА…….. 94

Гавриляк М.В., Цаволик Т.Г., Ігнатєв І.В.
ФУНКЦІЇ ТА ПЕРЕВАГИ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ НА БАЗІ SNORT…… 97

Терещенко О.С., Яцків В.В.
СУЧАСНІ ПЛАТФОРМИ РОЗВІДКИ КІБЕРЗАГРОЗ З ВІДКРИТИМ КОДОМ 100

Яцків Н.Г., Вівчар Д.В. Черняк Т.Г.
АНАЛІЗ ПІДХОДІВ ДО ОЦІНКИ РИЗИКІВ……... 104

Михайлишин Д.А., Цаволик Т.Г., Драпак В.І.
СИСТЕМА МОНІТОРИНГУ БЕЗПЕКИ КІНЦЕВИХ ПРИСТРОЇВ……. 107

Філіпчук М.М.
АЛГОРИТМИ ТЕСТУВАННЯ БЕЗПЕКИ ВЕБ-РЕСУРСІВ…….. 110

УДК 004.056

Яцків Н.Г.[1], Вівчар Д.В.[1], Черняк Т.Г.[1]

[1]Західноукраїнський національний університет

АНАЛІЗ ПІДХОДІВ ДО ОЦІНКИ РИЗИКІВ

Вступ. Збільшення залежності від мережевих інформаційних систем, засобів зв'язку, швидке зростання Інтернету, розвиток електронного бізнесу, ініціативи електронного уряду сприяють прогресу в інформаційних і комунікаційних технологіях, створили багато нових можливостей, але нове середовище також характеризується більшими ризиком, які необхідно аналізувати та оцінювати [1, 2].

Процес оцінки ризику оцінює ймовірність і потенційний збиток від виявлених загроз, заходи індивідуального рівня ризику кожного інформаційного активу і як вони ставляться до конфіденційності, цілісності та доступності. Наступним кроком є вимірювання ефективності існуючих заходів. Результати допомагають організації визначити, які активи є найбільш критичними, служать основою для визначення пріоритетів і рекомендують алгоритм дій для захисту активів.

Мета: провести аналіз та дослідити підходи та методи оцінки ризиків інформаційної безпеки.

1. Класифікація та аналіз методів оцінки ризиків

Оцінка ризику – це процес, який використовується для присвоєння значень наслідків, ймовірності виникнення та рівня ризику. Вона включає в себе:

1) оцінку ймовірності можливих загроз і вразливостей;

2) розрахунок впливу, який може мати загроза на кожен актив;

3) визначення кількісної (вимірні) або якісної (описуваної) вартості ризику.

Треба взяти до уваги те, що ці три змінні рідко незалежні одна від одної. В області інформаційної безпеки, є зв'язок між вартістю активів, впливом і ймовірністю. Наприклад, більш імовірно, що зловмисник буде використовувати уразливість, яка викликає більший вплив, ніж уразливість з низьким рівнем впливу. Крім того, цінний актив має більшу імовірність компрометації, ніж актив з низькою вартістю. Таким чином, в даній області необхідно приймати до уваги більше параметрів, ніж просто випадкові дії. Необхідно брати до уваги, що при наявності достатнього часу і знань, зловмисники мають можливість обійти майже всі заходи безпеки. Вони можуть бути надзвичайно творчими, коли мотивовані. Таким чином, фактор мотивації повинен також розглядатися в процесі оцінки кіберризиків.

Методи оцінку кіберризиків поділяють на кількісні, якісні та змішані (рисунок 1) [1-4].

1. Метод оцінки та моніторингу інформаційної безпеки (Information Security Assessment & Monitoring Method, ISAMM) – це методологія, яка містить ефективний і дієвий інструмент для оцінки як ризику безпеки, так і поточної відповідності вимогам ISO 27002. Крім того, вона забезпечує оптимізований план дій для усунути виявлені ризики.

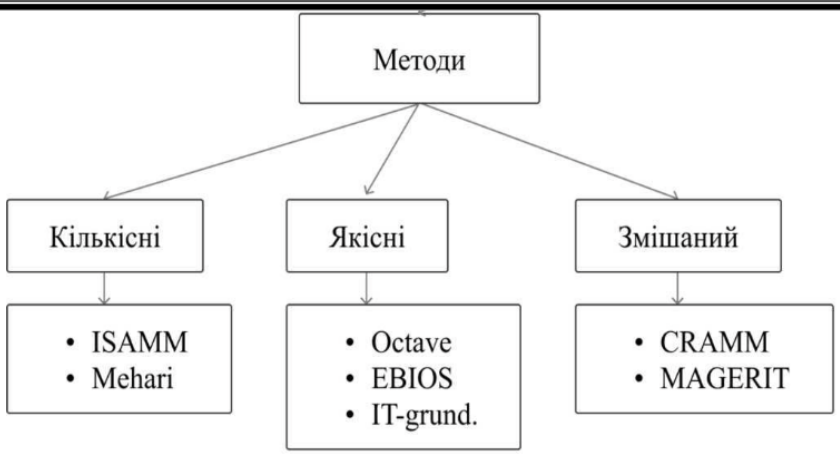


Рисунок 1 – Класифікація методів оцінки кіберризиків

2. MEHARI (Метод узгодженого аналізу ризиків) – це метод аналізу інформаційних ризиків і управління ризиками з відкритим кодом для використання фахівцями з інформаційної безпеки. MEHARI дозволяє бізнес-менеджерам, фахівцям з інформаційної безпеки/управління ризиками та іншим зацікавленим сторонам оцінювати та керувати ризиками організації, пов'язаними з інформацією, інформаційними системами та інформаційними процесами. Він розроблений для узгодження та підтримки управління ризиками інформаційної безпеки відповідно до ISO/IEC 27005, зокрема в контексті системи управління інформаційною безпекою (ISMS), сумісної з ISO/IEC 27001.

3. OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) – методологія оцінки активів та вразливостей інформаційної безпеки розроблена у Сполучених Штатах Америки в Інституті програмної інженерії при Університеті Карнегі–Меллона. Методологія OCTAVE дає змогу розробити практичні методи й рекомендації для оцінювання ризиків. Визначає стратегію оцінювання й планування дій щодо забезпечення безпеки інформації на основі оцінювання ризиків. До переваг можна віднести можливість оцінювання різних ризиків, які, за винятком технічних ризиків і ризиків порушення законодавства, безпосередньо не включені в методологію (з'ясовується в ході проведення опитування). Недоліки: не дає чітких інструкцій з організації моніторингу стану ризиків; не дає кількісної оцінки ризиків.

4. EBIOS – це метод оцінки та лікування цифрових ризиків, опублікований Національним агентством кібербезпеки Франції (ANSSI) за підтримки Club EBIOS. Він надає інструментарій, який можна адаптувати, використання якого залежить від мети проекту. EBIOS сумісний із діючими еталонними стандартами як з точки зору управління ризиками, так і з точки зору кібербезпеки.

5. CRAMM (CCTA Risk Analysis and Management Method) – це інструмент якісного аналізу та управління ризиками, розроблений Центральним агентством комп'ютерів і телекомунікацій уряду Великої Британії щоб надати урядовим департаментам метод оцінки безпеки інформаційних систем.

Цей метод передбачає комплексний підхід до оцінювання ризиків, поєднуючи кількісні та якісні оцінки. Також, він є універсальним і підходить як

для великих, так і для малих компаній. Використовується як у державному, так і в комерційному секторі. CRAMM орієнтований на різні типи організацій, що відрізняютьсяя між собою базами знань. Для комерційних організацій застосовують комерційний профіль (Commercial Profile), а для державних – державний профіль (Government profile). Перевагою цього методу є ідентифікація елементів ризику – матеріальних і нематеріальних активів та їх цінностей, загроз, заходів безпеки, величини потенційного збитку і ймовірності реалізації загрози.

Проте, недоліком є відсутність звітів з оцінених ризиків, перерахунку максимально допустимих величин ризиків. Є трудомістким і тривалим процесом з оцінювання ризиків, його застосування потребує залучення фахівців високої кваліфікації, оброблення вручну сотень сторінок звітної документації, що генеруються програмним інструментарієм CRAMM. Крім того, слід зазначити високу вартість ліцензії.

6. Magerit – це відкрита методологія для аналізу та управління ризиками, розроблена Міністерством державного управління Іспанії, яка пропонується як основа та посібник для державного управління. Враховуючи його відкритий характер, він також використовується поза адміністрацією. Magerit прагне досягти наступних цілей: повідомити осіб, відповідальних за інформаційні системи, про існування ризиків і про необхідність їх вчасного виправлення. Запропонувати систематичний метод аналізу цих ризиків. Допомогти в описі та плануванні відповідних заходів для утримання ризиків під контролем. Підготувати організацію до процесів оцінювання, аудиту, сертифікації чи акредитації.

7. Управління ризиками в системі інформаційних технологій – методологія оцінки ризиків SP800-30 (Special Publications) Національного Інституту Стандартів і Технологій (National Institute of Standards and Technology – NIST) – NIST SP800-30. Методологія NIST SP800-30 детально описує всі можливі ризики для інформаційних активів і може використовуватися для підприємств різної величини. Недоліком цієї методології є довготривалий процес аналізу і відсутність автоматизації деяких функцій [4].

Висновки. Потреба в ефективному аналізі та управлінні ризиками, що постає перед дедалі зростаючими викликами ери Інтернету та електронного бізнесу, робить використання наведених методів та інструментів незамінними. Проте організації повинні вирішити, бажано на рівні керівництва, найкращий підхід шляхом оцінки своїх потреб і вимог.

Перелік використаних джерел.

1. Stallings, W. Effective Cybersecurity: Understanding and Using Standards and Best Practices. Addison-Wesley. 2019. – 893 p.

2. Ulven, J.B.; Wangen, G. A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet,* 2021, *13*, 39. https://doi.org/ 10.3390/fi13020039

3. NIST. *Framework for Improving Critical Infrastructure Cybersecurity.* April 16, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST. CSWP.04162018.pdf

4. ISO 31010 2019. Risk management – Risk assessment techniques. Management du risque -Techniques. – 268 p.


КІБЕРБЕЗПЕКА ТА
КОМП'ЮТЕРНО-ІНТЕГРОВАНІ
ТЕХНОЛОГІЇ
КБКІТ-2022
науково-практична конференція
молодих вчених
аспірантів та студентів
м.Тернопіль

ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ПОЛІТЕХНІЧНИЙ УНІВЕРСИТЕТ
ГАЛИЦЬКИЙ ФАХОВИЙ КОЛЕДЖ ІМ. В. ЧОРНОВОЛА

КІБЕРБЕЗПЕКА ТА КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ (КБКІТ – 2022)

науково-практична конференція
молодих вчених, аспірантів та студентів

29–31 серпня 2022
Тернопіль

ЗМІСТ

СИСТЕМИ ТА ТЕХНОЛОГІЇ КІБЕРБЕЗПЕКИ

Хомич О.В.
СИСТЕМА РЕАГУВАННЯ НА ІНЦИДЕНТИ В ОС LINUX 7

Яцків Н.Г., Вівчар Д.В.
АНАЛІЗ ПІДХОДІВ ДО ОЦІНКИ РИЗИКІВ 10

Кулина С.В.
ВИЯВЛЕННЯ ТА ВИПРАВЛЕННЯ ПОМИЛОК У ЗАХИЩЕНИХ СИСТЕМАХ ЗБЕРІГАННЯ ДАНИХ МЕТОДОМ ОБЧИСЛЕННЯ ПРОЕКЦІЇ ЧИСЛА 13

Кондіус І.С.
ДОСЛІДЖЕННЯ МЕТОДИК ОЦІНКИ БЕЗПЕКИ КОМП'ЮТЕРНИХ МЕРЕЖ 17

Бовнегра Л.В., Тимошенко Л.М., Накоряков О.Г.
ДОСЛІДЖЕННЯ СИСТЕМ ОЦІНЮВАННЯ КІБЕР-СИТУАЦІЙНОЇ ОБІЗНАНОСТІ 22

Іваницький Б.О., Павловський С,. Горошко Н.М, Куць Т.І., Куць І.С
РЕЖИМИ РОБОТИ АЛГОРИТМУ AES 26

Бондарчук В.Р., Сегін А.І., Давлетова А.Я.
МЕТОДИ ЗАХИСТУ ЦИФРОВИХ ДАНИХ НА ОСНОВІ КОРЕЛЯЦІЙНИХ ФУНКЦІЙ 31

Надозірний С.В.
СУЧАСНІ ЗАГРОЗИ В СФЕРІ БЛОКЧЕЙН ПРОЕКТІВ 36

Яцків В.В., Терещенко О.С.
РОЗВІДКА КІБЕРЗАГРОЗ З ВИКОРИСТАННЯМ МОВИ ОПИСУ ПРАВИЛ YARA 40

Гринчук А.М., Лисобей Л.В., Черняк В.А.
МАТЕМАТИЧНА МОДЕЛЬ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ УСТАНОВИ 43

Бабич С.В.
ТЕХНОЛОГІЯ ОБМАНУ НА ОСНОВІ ФАЙЛІВ..... 46

БЕЗПЕКА ТА ІНТЕРНЕТ РЕЧЕЙ

Костючко С.М., Якименко І.З., Поліщук М.М., Конкевич Л.М.
СИСТЕМА ЗАХИСТУ ВІД ВНУТРІШНІХ ЗАГРОЗ ЗАСОБАМИ МАШИННОГО НАВЧАННЯ 48

Хомицький А.А.
АНАЛІЗ КО КАТЕГОРІЙ ПРИМАНОК ДЛЯ ВИЯВЛЕННЯ АТАК НА ІНТЕРНЕТ РЕЧЕЙ 51

УДК 004.056

Яцків Н.Г., Вівчар Д.В.

Західноукраїнський національний університет

АНАЛІЗ ПІДХОДІВ ДО ОЦІНКИ РИЗИКІВ

Вступ. Інформаційні загрози продовжують все більше розвиватися. Мережі критичної інфраструктури продовжують бути об'єктами глобальних нападів, як з боку зловмисників, які спонсоруюся державами, так і зловмисників, які мотивовані отриманням фінансової вигоди. У зв'язку з цим ми повинні адаптувати свої стратегії управління ризиками, щоб забезпечити належну оцінку ризиків для функціонування активів, які є критично важливими для економічного та соціального добробуту [1, 2].

Мета: Провести аналіз ефективних підходів до оцінки ризиків для критичної інфраструктури.

Визначення ризику для критичної інфраструктури

Ризик у контексті критичної інфраструктури пов'язаний із національною та соціальною стійкістю. Ризики, які мають найбільший вплив на оборону чи національну безпеку держави, соціальну чи економічну стабільність населення необхідно враховувати та включати в існуючі стратегії управління ризиками підприємств критичної інфраструктури.

Прикладом того, як ідентифікувати ризик для центру зберігання та обробки даних, є визначення можливого ризику від втрати електроенергії для центру обробки даних, щодо того, як це може порушити доступність критично важливого ресурсу для зберігання чи обробки даних та як це впливає на критично важливих споживачів активу, які залежать від роботи даного центру.

Розглянемо підхід до оцінки ризиків, який складається з шести кроків, для забезпечення важливих активів критичної інфраструктури на прикладі сектора зберігання та обробки даних [3, 4]. Розглянемо кожен з етапів детальніше (рисунок 1).

Рисунок 1 – Схематичне зображення послідовності кроків оцінки кіберризиків

Крок №1. Аналіз інформації і те, як вона відповідає критичній інфраструктурі. Визначення контексту окремої організації, як у секторі зберігання та обробки даних, так і в економіці в загальному. Формулювання бізнес-цілі,

визначення бізнес-загроз та розуміння правил безпеки та законодавчих вимог, яких вам слід дотримуватися. Немає універсального підходу до оцінки та управління ризиками. Організації повинні будуть визначитися як найкраще мінімізувати та зменшити ризик. У результаті отримаємо розуміння операційного контексту вашого бізнесу.

Крок №2. Визначення важливих активів. Організації необхідно визначити, що вона повинна захистити, які активи для неї є найбільш цінними? Порушення роботи, пошкодження чи знищення яких служб, активів і компонентів негативно вплине на те, що для організації є цінним? Це знаходяться важливі активи. Необхідно розглянути: системи, служби, мережі, людей, дані, інформацію та інші ключові активи. Визначити залежності та взаємозалежності між ключовими активами. Необхідно визначити, що потрібно для безперервної роботи активу критичної інфраструктури. Які ключові компоненти необхідні для виконання функції активу? Компоненти включають системи, послуги, мережі, інформація.

В результаті має бути визначено критично важливі об'єкти, компоненти і персонал, які необхідні для експлуатації об'єкта критичної інфраструктури.

Крок №3 – Загрози, небезпеки та вразливі місця. Необхідно проаналізувати загрози та небезпеки, які можуть завдати шкоди виявленим активам критичної інфраструктури. Провести аналіз відомих вразливостей, які можуть вплинути на активи, а також інформацію з сектора в цілому про схожі організації, які були ціллю, і як це було зроблено. Це також може включати аналіз суб'єктів загрози, їх мотивації та те, як вони можуть отримати доступ до цих активів і спробувати їх зламати (хто, чому і як).

У результаті будуть визначені найбільш актуальні загрози та небезпеки для конкретної організації.

Крок №4 – Оцінка ризику. Необхідно провести оцінку ризику, який створює кожна загроза. Оцінити ймовірність, що загроза може статися? Які можливі наслідки, якщо загроза буде реалізована? Проаналізуйте існуючі засоби контролю, які можуть зменшити ймовірність і/або наслідки інциденту безпеки. Розглянемо наміри та можливості щодо загроз, а також ймовірність і наслідки таких небезпек, як стихійні лиха.

В результаті будуть визначені ризики, пов'язані з організацією, які можуть вплинути на конфіденційність, цілісність, доступність або надійність критичних активів.

Крок №5 – Визначення заходів пом'якшення та запровадження засобів контролю. Необхідно визначити, чи початковий результат кожного ризику знаходиться в межах допустимого рівня, чи потрібно запровадити додаткові засоби контролю. Запровадити необхідні засоби контролю, а потім оновити профіль ризику (зі зміненими описами засобів контролю, ймовірністю та/або наслідками). Засоби контролю можуть включати технологічний контроль, фізичний контроль та/або діяльність у всьому спектрі запобігання, захисту, виявлення, пом'якшення, реагування та відновлення. Результат даного кроку – аналізувати та досліджувати виявлені ризики настільки, наскільки це «практично можливо».

Крок №6 – Моніторинг ризиків. Ефективне управління ризиками ніколи не

виконується на певний момент часу. Моніторинг ризиків має бути постійним, щоб слідкувати за загрозами, що постійно розвиваються, а також активи та інфраструктуру, що змінюються, які організації повинні захищати.

Доцільно використовувати показники для вимірювання прогресу та ефективності діяльності з управління ризиками безпеки, що підтримується відповідними механізмами управління. Вживати постійних заходів із вдосконалення, щоб посилити критичні вразливості активів за допомогою таких заходів, як "червона команда" (група, яка відіграє зловмисника та забезпечує зворотний зв'язок із точки зору безпеки) після інцидентів і безперервні дії з гарантії. Результати цих заходів мають використовуватися для регулярного оновлення та вдосконалення існуючого спектру методів управління ризиками. Необхідно підтримувати високий рівень обізнаності щодо безпеки та актуальних загроз. Розмір і складність організації повинні визначати, наскільки регулярно слід відстежувати та переглядати ризики, але рекомендується щонайменше щорічна перевірка процесів управління ризиками. Результат – постійний моніторинг ризиків та оновлення стратегій оцінки ризиків, якщо це необхідно.

Висновок. Розглянутий підхід до оцінки ризиків аналізує загрозу (ймовірність виникнення), вразливість (слабкість об'єкта або активу проти загроз) і вплив (наслідки події), коли такі загрози виникають, щоб визначити рівень ризику для кожного активу проти кожної відповідної загрози. Він надає розробникам безпеки, інженерам і архітекторам відносний профіль ризику, який визначає активи, які піддаються найбільшому ризику щодо конкретних загроз. Дотримуючись заходів пом'якшення, можна вивчити, щоб зменшити ризик для цінних активів із високим ризиком. Оскільки повністю усунути ризик неможливо, а кожен проект має обмежені ресурси, розробники безпеки повинні отримати розуміння власниками об'єктів, архітекторами та інженерами того, як заходи пом'якшення впливають на ризик; таким чином, щоб рішення щодо найкращих і найбільш економічно ефективних заходів, які необхідно впровадити, могли бути забезпечені для досягнення бажаного рівня захисту (управління ризиками) для об'єкта. Розглянутий підхід до оцінки ризиків допоможе зацікавленим сторонам адаптувати існуючі практики оцінки ризиків а також зрозуміти ризики в контексті критичної інфраструктури.

Перелік використаних джерел.

1. ISO 31010 2019. Risk management – Risk assessment techniques. Management du risque – Techniques. – 268 p.

2. Akinrolabu O., Nurse J.R., Martin A., New, S.. Cyber risk assessment in cloud provider environments: Current models and future needs. *Computers & Security,* 2019, *87*, 101600.

3. Ahmed, M., Panda S., Xenakis C., Panaousis, E.. MITRE ATT&CK-driven cyber risk assessment. In Proceedings of the 17th International Conference on Availability, Reliability and Security, 2022. – Pp. 1-10.

4. Lyu X., Ding, Y., Yang S. H. Safety and security risk assessment in cyber-physical systems. IET Cyber-Physical Systems: Theory & Applications, 4(3), 2019. – pp. 221-232.