ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ МОДЕЛЮВАННЯ ОЦІКИ РИЗИКІВ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ»

Виконала студентка 6 курсу, групи БСДМ-62
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Барсукова К.І.
(прізвище та ініціали)
Керівник Кожухівська О.А.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ - 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
“___”_____ 2022 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ
СТУДЕНТУ

Барсуковій Катерині Ігорівні
(прізвище, ім’я, по батькові)

1. Тема магістерської роботи: «Технологія моделювання оцінки ризиків кібербезпеки інформаційної системи організації»

керівник магістерської роботи Кожухівська Ольга Андріївна, д. т. н.
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «12» жовтня 2022 року №122.

2. Строк подання студентом магістерської роботи 15.12.2022 р.

3. Вихідні дані до магістерської роботи
корпоративна інформаційна система;
програмні комплекси управління захистом системи;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз сучасних методів та можливостей інформаційної безпеки.
2. Дослідження методик моделювання та оцінки інформаційних ризиків.
3. Побудова системи управління інформаційними ризиками.
4. Побудова алгоритму аналізу ризику.
5. Перелік графічного матеріалу
1. Тема магістерської роботи.
2. Об’єкт, предмет, мета та наукові завдання дослідження.

3. Актуальність роботи.

4. Результати аналізу основних загроз інформаційної безпеки.

5. Результати аналізу основних елементів оцінки ризиків інформаційної безепеки.

6. Область дії системи управління інформаційною безпекою.

7. Етапи розробки системи управління інформаційними ризиками.

8. Загальна схема завдання.

9. Алгоритм аналізу ризиків інформаційної безпеки.

10. Алгоритм визначення інформаційних активів організації.

11. Алгоритм визначення негативних чинників, визначення втрат та ймовірності реалізації ризику.

12-13. Реалізація алгоритму оцінки ризиків інформаційної безпеки.

14. Висновки за результатами роботи.

6. Дата видачі завдання 26.09.2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
1.	Визначення актуальності проблеми захисту кінцевих точок корпоративних інформаційних систем.	26.09.2022 р.	
2.	Аналіз наукової та технічної літератури з питань теми магістерської роботи.	20.10.2022 р.	
3.	Аналіз методик моделювання та оцінки інформаційних ризиків.	1.11.2022 р.	
4.	Розроблення варіанту реалізація алгоритму оцінки ризиків інформаційної безпеки.	20.11.2022 р.	
5.	Розроблення рекомендацій щодо застосування технології моделювання оцінки ризиків кібербезпеки інформаційної системи організації.	1.12.2022 р.	
6.	Оформлення результатів дослідження. Проходження плагіату	12.12.2022 р.	
7.	Підготовка доповіді до захисту.	15.12.2022 р.	

Студент Барсукова К.І.
(підпис) прізвище та ініціали

Керівник магістерської роботи Кожухівська О.А.
(підпис) прізвище та ініціали

РЕФЕРАТ

Текстова частина магістерської роботи: 82 сторінки, 14 рисунків, 6 таблиць, 30 джерел.

Об'єкт дослідження – процес забезпечення захисту інформаційної системи організації від ризиків кібербезпеки.

Предмет дослідження – технологія моделювання оцінки ризиків інформаційної системи організації.

Мета роботи – дослідити методики моделювання та оцінки інформаційних ризиків та розробити модель оцінювання ризиків інформаційної безпеки для корпоративних мереж.

Методи дослідження – опрацювання різних джерел за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання системи оцінки ризиків інформаційної системи.

В роботі розглянуто можливості інформаційної безпеки, які загрози постають перед інформаційною безпекою, сутність ризиків інформаційної безпеки. Проаналізовано існуючі методики моделювання оцінки ризиків, основні ризики та заходи управління ризиками та які існують методи оцінювання ризиків.

Досліджено існуючі підходи до управління ризиками, політика інформаційних ризиків, етапи побудови СУІБ. Визначено призначення, основні функції та склад системи управління інформаційними ризиками.

На основі досліджень проведених в роботі експериментально досліджено ризики, а саме: побудовано алгоритм виявлення ризиків, оцінка ризиків, знешкодження ризиків та приведено приклад реалізації цього алгоритму. Вирішено актуальне завдання щодо потреби точного та правильного аналізу можливих інформаційних ризиків. Розроблено універсальний алгоритм аналізу ризиків, який є прийнятним для будь якої організації або підприємства.

Галузь використання – кібербезпека інформаційної системи організації.

СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РИЗИКАМИ, ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФОРМАЦІЙНІ РИЗИКИ, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІФНОЮ БЕЗПЕКОЮ, АЛГОРИТМ АНАЛІЗУ РИЗИКІВ

ABSTRACT

Master’s thesis: 82 pages, 14 figures, 6 tables, 30 sources.

Object of research – the process of ensuring the protection of the organization's information system from cyber security risks.

Subject of research – the technology for modeling risk assessment of the organization`s information system.

The aim of research – to investigate methods of modeling and assessment of information risks and to develop a model of assessment of information security risks for corporate networks.

Research methods – processing of various sources on this topic, analysis of operational documentation, international standards and their comparison, modeling of the information system risk assessment system.

The paper examines the possibilities of information security, the threats facing information security, the essence of information security risks. Existing methods of risk assessment modeling, main risks and risk management measures and existing risk assessment methods are analyzed.

The existing approaches to risk management, the policy of information risks, the stages of ISMS construction were studied. The purpose, main functions and composition of the information risk management system are determined.

On the basis of the research carried out in the work, risks were experimentally investigated, namely: an algorithm for risk detection, risk assessment, risk neutralization was built, and an example of the implementation of this algorithm was given. The urgent task regarding the need for accurate and correct analysis of possible information risks has been solved. A universal risk analysis algorithm has been developed, which is acceptable for any organization or enterprise.

Field of use – cybersecurity of organization`s information system.

INFORMATION RISKS MANAGEMENT SYSTEM, INFORMATION SECURITY, INFORMATION RISKS, INFORMATION SECURITY MANAGEMENT SYSTEM, RISK ANALYSIS ALGORITHM

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІБ – інформаційна безпека

УІБ - управління інформаційною безпекою

СУІР – система управління інформаційними ризиками

СУІБ – система управління інформаційною безпекою

АСУ – автоматизована система управління

ІСУ – інформаційна система управління

ПЗ – програмне забезпечення

ІС – інформаційна система

НКК – нечіткі когнітивні карти

HRA – Human Reliability Assessment

СІБ – система інформаційної безпеки

ВСТУП

Актуальність дослідження. На даний час, одним з важливих напрямків державної політики являється покращення інформаційного суспільства в Україні, а також введення нових інформаційно-комунікаційних технологій у різні сфери суспільного життя і, звісно, безпосередньо у діяльність органів влади держави та місцевого самоврядування. Продуктивність діяльності всіх державних органів дуже сильно залежить від повноти та якості наявного інформаційного забезпечення, використання якого дозволяє знизити фінансові, часові та матеріальні ресурси.

До чинників, що стримують процес покращення державного управління з використанням інформаційно-технологічних інновацій можна віднести наявність інформаційних ризиків та загроз інформаційної безпеки. Щоб вирішувати завдання у сфері захисту інформації існує нормативно-правова база, яка включає в себе закони, укази президента, державні стандарти, за допомогою яких регулюються процеси по забезпеченню інформаційної безпеки.

Таким чином, з огляду на наявні проблеми, актуальність роботи обумовлена залежністю державних установ та приватних організацій від надійної роботи інформаційних систем, а також обумовлена наростаючою швидкістю створення нових та модифікації старих загроз інформаційної безпеки.

Об'єкт дослідження – процес забезпечення захисту інформаційної системи організації від ризиків кібербезпеки.

Предмет дослідження – технологія моделювання оцінки ризиків інформаційної системи організації.

Мета роботи – дослідити методики моделювання та оцінки інформаційних ризиків та розробити модель оцінювання ризиків інформаційної безпеки для корпоративних мереж.

Наукові завдання:

1. Проаналізувати сучасні методи та можливості інформаційної безпеки;

2. Дослідити методики моделювання та оцінки інформаційних ризиків;

3. Побудувати систему управління інформаційними ризиками;

4. Реалізувати алгоритм життєвого циклу ризику;

Методи дослідження – дослідження різноманітних джерел по даній темі, аналіз наявної документації, міжнародних стандартів та їх порівняння, моделювання системи оцінки ризиків інформаційної системи.

Практичне значення одержаних результатів. Розроблений алгоритм може бути використаний керівниками організацій та фахівцями інформаційної безпеки телекомунікаційних підприємств, державних установ та інших відомств для ефективного управління ризиками інформаційної безпеки.

Апробація результатів магістерської роботи було оприлюднено на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2022 року в Державному університеті телекомунікацій, м. Київ.

1 СУЧАСНІ МЕТОДИ ТА МОЖЛИВОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Так як в інформаційну безпеку в інформаційній системі входить широке коло проблем, пов’язане з її управлінням, виникає необхідність в забезпеченні трьох основних завдань, які складають основу безпеки інформації, що дозволить коректно функціонувати системі. Отже, необхідно забезпечити цілісність, конфіденційність та доступність інформаційних ресурсів системи.

Таким чином, першим завданням являється забезпечення цілісності ресурсів. В зв’язку з розвитком інформаційних систем, на даний час більшість комерційної інформації, фінансової звітності, а також клієнтські бази, договори, новаторські ідеї співробітників фірми, плани та стратегія її розвитку зберігаються в локальній інформаційно-комп'ютерній мережі [4, 15, 18].

Не всі документи і не в повному обсязі продубльовуються в паперовому вигляді, так як об’єм інформації часто буває досить великий. За таких умов в інформаційній безпеці передбачено систему заходів, що спрямовані на забезпечення надійного захисту від збоїв та помилок серверів та робочих станцій, які можуть призвести до повної або часткової втрати інформації. При серйозному підході до цього питання необхідним являється базування інформаційної безпеки на професійному аудиті IT-інфраструктури фірми. За допомогою IT-аудиту можна проводити оцінку стану мережі та обладнання, аналіз потенційних загроз, виявляти та відразу усувати вразливі місця кабельної системи, серверних та робочих станцій, дискових систем та порушень у конфігурації обладнання.

Завдяки цьому зменшуються технічні ризики можливої втрати інформації. Ще однією причиною пошкодження даних являється некоректна робота систем архівації, а також мережного та прикладного програмного забезпечення. Конфіденційність інформації безпосередньо пов’язана з захистом комерційних секретів [9, 11, 36], і має прямий вплив на конкурентоспроможність фірми та її стійкість на ринку. На даному етапі інформаційна безпека та захист мереж перетинається із внутрішніми та зовнішніми навмисними загрозами, метою яких

є розкрадання даних. Найбільшу загрозу становлять хакери, промислове шпигунство та витік інформації по вині співробітників.

Таким чином заходи боротьби з несанкціонованим доступом повинні концентруватись в напрямку досягнення двох основних цілей:

– створення таких умов, при яких стають неможливими випадкові чи навмисні дії, які можуть призвести до витіку даних. Для вирішення цієї проблеми використовується введення системи аутентифікації та авторизації для користувачів, а також за допомогою поділу прав та контролю доступу до інформації.

– необхідно запровадити систему, що дозволить відслідкувати дії співробітників чи зловмисників. Це можна забезпечити за рахунок використання системи контролю подій безпеки, аудиту доступу до файлів та папок.

Досить дієвими методами захисту від зовнішніх та внутрішніх загроз також являються[12]: впровадження системи паролів для користувачів, використання криптографії(шифрування) для особливо важливої інформації, обмеження доступу до приміщень, використання індивідуальних цифрових ключів, застосування мережевих екранів, встановлення систем захисту від витоків інформації через електронну пошту, FTP-сервери та Інтернет-месенджери, використання захисту інформації від копіювання.

Зараз використання для злому мереж поширення шкідливих комп'ютерних програм, які займаються збором та передачою інформації (троянські програми), а також програм-шпигунів стає все більш розповсюдженим явищем [13, 17]. Використання потужного антивірусного програмного забезпечення та серверного захисту дозволяє запобігти таким видам зовнішніх ризиків.

В інформаційній безпеці мережі також передбачено захист від зовнішніх атак, які націлені на порушення роботи серверів, комп'ютерів чи компонентів мережі, тобто від DDos-атак та спроб підбору паролів (bruteforce-атаки). Щоб захиститись від цих загроз необхідним є використання міжмережевих екранів та систем проактивного захисту, що дозволить унеможливити проведення вище названих атак.

Створення умов для безпечного і постійного доступу до інформації для користувачів, які є її власниками, являється одним із основних завдань системних адміністраторів. Прості системи, в результаті порушення доступності, часто призводять до фінансових та юридичних наслідків, втрати репутації та довіри партнерів та клієнтів.

1.1. Основні загрози інформаційної безпеки

Згідно зі звітами за 2020 рік, опублікованими лабораторією Касперського, Dr. WEB та CERT UA (Computer Emergency Response Team of Ukraine – команда реагування на комп'ютерні надзвичайні події України) було виявлено таке [16]:

– у 2020 році на 58% корпоративних комп'ютерів було відображено хоча б одна атака шкідливого ПЗ, що на 3 п.п. більше, ніж торік;

– 29% комп'ютерів, тобто. майже кожен третій комп'ютер у бізнес-середовищі зазнали хоча б однієї атаки через інтернет;

– при атаках на бізнес експлойти до офісних програм використовуються втричі частіше, ніж в атаках на домашніх користувачів;

– файловий антивірус спрацював на 41% комп'ютерів корпоративних користувачів (детектувалися об'єкти, виявлені на комп'ютерах або на знімних носіях, підключених до комп'ютерів - флешках, картах пам'яті, телефонах, зовнішніх жорстких дисках, мережевих дисках).

Основними цілями атак було отримання фінансової вигоди, як, наприклад, операція Carbanak – APT-атака, при якій зловмисники проникали у мережу банку-жертви та шукали критично важливу систему, за допомогою якої з атакованої фінансової організації виводили кошти та витік інформації з державних установ. Усього у світі налічується понад 100 жертв цієї атаки, а сумарні збитки постраждалих організацій (переважно це були банки) можуть сягати мільярда доларів. Також метою зловмисників була конфіденційна інформація. Серед постраждалих – юридичні фірми, інвестиційні компанії, організації, що працюють із криптовалютою Bitcoin, групи компаній та підприємства, залучені до операцій злиття та поглинання, IT-компанії, заклади охорони здоров'я, ріелторські компанії, а також індивідуальні користувачі.

Також зазначено, що загальна статистика щодо корпоративних користувачів (географія атак, рейтинг об'єктів, що детектуються) в цілому збігається зі статистикою домашніх користувачів. Це обумовлюється тим, що бізнес-користувачі не існують в ізольованому середовищі, їх комп'ютери стають об'єктами атак зловмисників, які розповсюджують шкідливі програми без урахування специфіки атакованого. Таких атак/шкідників більшість, і дані щодо атак, націлених саме на бізнес-користувачів, мало впливають на загальну статистику.

На основі аналізу статистики ми можемо виділити основні напрямки розвитку діяльності кіберкримінал:

– частина людей, які займалися кібер-кримінальною діяльністю, прагне мінімізувати ризики кримінального переслідування та переключається з атак шкідливих програм на агресивне розповсюдження рекламного ПЗ;

– у ПЗ, що використовується в масових атаках, зростає частка щодо нескладних програм. Це дає можливість зловмисникам підвищувати ефективність атак за рахунок модернізації шкідливого ПЗ в короткі терміни;

– кібер-кримінал постійно застосовує новітні методи анонімізації, такі як Tor, що дозволяє замаскувати командні сервери, та біткоіни для транзакцій.

У зв’язку зі стрімким розвитком інформаційних технологій, очікується продовження тенденції шифрувальників, націлених на не тільки Windows платформи: збільшення частки Android та поява шифрувальників, націлених на MacOS. Враховуючи те, що Android активно використовується і в побутовій електроніці, можуть відбуватися і атаки крипторів на "розумні" пристрої.

Відповідно до стандартів з менеджменту ризиків та інформаційної безпеки, загрозою є можливість настання інциденту безпеки в інформаційній системі [15]. Під цим терміном розуміються деякі події та джерела їх виникнення. Однак, при описі та моделюванні даних подій, рідко приділяється належна увага опису та визначенню умов, за яких дані події здатні виникнути та розвиватися. Виходячи з цього, доцільно розділити це поняття на два – погрози та сценарії загроз. Перший визначає джерело подій та умови його виникнення, другий, власне, ті дії, які цим джерелом викликаються.

Існує безліч класифікацій загроз інформаційній безпеці, які поділяють загрози за такими ознаками як джерело загрози, тип загрози, тип впливу та багато інших [16]. Однак існує кілька типів класифікації, які є основними у сучасних стандартах з інформаційної безпеки та найчастіше використовуються в науковій літератури.

За розташуванням джерела загрози ділять на внутрішні та зовнішні загрози. Внутрішні небезпеки передбачають знаходження джерела небезпеки всередині інформаційної системи або її комунікаційної структури. Основними загрозами, що підходять під цю класифікацію, є:

– користувачі системи. Неправильні дії, спричинені необережністю чи незнанням, можуть призвести до виникнення вразливості системи;

– обслуговуючий персонал системи. Адміністратори, інжинери, програмісти та інші технічні співробітники, внаслідок недостатньої кваліфікації чи помилки, можуть залишити вразливі місця в системі або створити нові;

– інсайдери. Будь-який із співробітників підприємства, який має в тій чи іншого ступеня доступ до системи, може навмисно здійснювати шкідливу діяльність з причини невдоволення, образи, підкупу чи іншої мотивації;

– інформаційна система. Нечастий випадок, коли алгоритми роботи Системи сприяють виникненню вразливих місць або інцидентів, що призводять до порушення безпеки.

Зовнішні загрози передбачають вплив на інформаційну систему ззовні. Для здійснення зовнішньої загрози необхідні певні передумови – наявність уразливості [15, 16, 14, 20] в інформаційній системі, мотивація до порушення безпеки та інші.

Зовнішні небезпеки:

– віруси. Спеціальні програми, дії яких здійснюються в трьох основних напрямках: створення умов, що перешкоджають нормальній роботі інформаційної системи, повне блокування роботи інформаційної системи, пошук та використання вразливих місць системи для відкриття віддаленого доступу до неї;

– зловмисники (хакери) – людина чи група людей, які впливають на систему з метою отримання матеріальної чи іншої вигоди;

– техногенні, природні та інші катаклізми. Вплив зовнішніх систем, довкілля та інших чинників, які призводять до порушення працездатності системи.

Цей перелік не претендує на повноту опису всіх можливих загроз, проте дає уявлення про найпоширеніші з них.

За характером виникнення загрози поділяються на ненавмисні та навмисні небезпеки. Під ненавмисними загрозами розуміються ті, які виникають в результаті збігу деяких подій, і призводять до порушення безпеки системи. Якщо проводити паралель із попередньою класифікацією, випадковими загрозами можна назвати всієї користувачів системи та різні катаклізми, а також, іноді, віруси.

Навмисні загрози передбачають вплив на систему з певною метою, яка усвідомлена та чітко розуміється. Як правило, дані погрози описують певний намір у діях, такий як фінансова вигода, блокування чи знищення системи, помста тощо.

Навмисні загрози, в більшості випадків, можна спрогнозувати, спираючись на відповідні статистичні дані, характер діяльності підприємства, конкурентні очікування та ін. Ненавмисні загрози, силу випадкового характеру їх виникнення, навпаки, досить складно визначити повною мірою, так як вони описують можливість помилки, збою та інші поодинокі випадки, що не піддаються систематизації.

1.2. Сутність ризиків інформаційної безпеки

У зв’язку з удосконаленням інформаційних технологій та загальною комп’ютеризацією, в даний час інформаційна безпека стала не просто необхідною вимогою для систем, а ще й основною їх характеристикою. Фактор безпеки являється основним в значному ряді систем, що виконують обробку інформації.

Необхідність в створення новітніх підходів до формування системи захисту та покращення інформаційного простору обумовлена комплексним характером сучасних загроз, що існують в інформаційній сфері [24].

Зараз інформація входить до переліку ресурсів(факторів) майже будь-якого виробництва. Захист і поводження з інформаційними ресурсами на підприємстві відображає ефективність управління фінансовими та соціально-економічними процесами з застосуванням інформаційних технологій.

В зв'язку з розвитком інформаційної безпеки, проблеми з її забезпечення стають все складнішими і важливішими, а інформація щодо різних напрямів діяльності організації – її найдорожчим та найціннішим ресурсом. Тому зараз одною з найважливіших складових економічної безпеки стала саме інформаційна безпека, що характеризує собою загальну захищеність організації.

Забезпечення інформаційної безпеки зараз вважається першочерговим питанням, що зумовлено глобальною інформатизацією суспільства у всьому світі, активне залучення інформаційних технологій та їх роль у кожній сфері розвитку різних держав. У нинішньому устрою світу, від якості впровадження інформаційної безпеки значною мірою залежить соціальна та економічна стабільність, а також правопорядок та дотримання прав громадян кожної країни.

Далі, проведемо аналіз термінології інформаційної безпеки, основні визначення якої продекаровано численними нормативно-правовими актами.

В Законі України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 рр.» цей термін трактується наступним чином: «інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» [10].

Інформаційна безпека (ІБ) являється характеристикою системи з огляду на її стабільність та стійкість при появі внутрішніх та зовнішніх загроз.

Інформаційно захищена система повинна зберігати свій стан та працездатність при впливу будь-якого виду загроз.

Існує три загальновизнані поняття, що характеризують інформаційну безпеку, а саме:

– доступність – можливість за визначений час отримати потрібний інформаційний ресурс суб’єктом, для якого він призначений;

– цілісність – незмінність та незнищенність інформації при її зберіганні, перегляді чи пересиланні;

– конфіденційність – захищеність інформації від перегляду користувачами, які не мають до неї доступу.

З огляду на це, при вирішенні проблем інформаційної безпеки слід починати саме з визначення суб’єктів інформаційних відносин та їх інтересів, що будуть пов’язані з користуванням ІС. Такий підхід буде найбільш правильним з методологічної точки зору.

Загрозами ІБ являються можливі негативні наслідки використання інформаційних технологій. Таким чином, можна зробити два важливих висновки:

– в залежності від категорії суб’єкта, трактування проблем з ІБ буде відрізнятись;

– ІБ це досить широке поняття, що не обмежується лише захистом інформації від небажаного доступу. Нанести моральну чи матеріальну шкоду суб'єкту інформаційних відносин можна не тільки порушивши конфіденційність, а й пошкодивши саму систему, що призведе до перерви або повного припинення роботи. Як приклад можна зазначити, що для більшості відкритих організацій, таких як навчальних чи соціальних, захист від несанкціонованого доступу знаходить далеко не на першому пріоритеті по важливості.

Неможливо досягти необхідного рівня захисту не реалізуючи заходи по підвищенню рівня ІБ системно і в повному обсязі. Тому, для класифікації заходів по підвищенню рівня безпеки в залежності від пріоритетності загрози для системи, потрібно створити систему управління ризиками ІБ. Це дасть

можливість направити всі сили на захист від найнебезпечніших загроз і дозволить мінімізувати витрати [19].

Ризик – це випадкова подія, в якій можливий або ймовірний негативний кінцевий результат пов’язаний з прийняттям певних рішень чи виконанням певних дій [20].

Випадковість ризику пов’язана, зазвичай, з неповнотою якісної інформації про подію. Через недостатню кількість необхідних засобів, обмеженість часу на збір і аналіз даних, вплив зовнішніх факторів та недостачу повноти в наукових знаннях щодо сутності ризикових процесів чи явищ, отримання всього об’єму потрібної інформації є обмеженим.

У всіх сферах людського життя наявний ризик. Це обумовлено значним об’ємом факторів і умов, які несуть вплив на кінцевий результат рішень, що приймає людина щодня. Оцінювання ризиків набуло широкого використання в багатьох сферах діяльності, в першу чергу в економічній, військові та політичній.

Завдяки швидкому розвитку обчислювальної техніки і значному приросту об’ємів інформації, що обробляється і передається, вже в кінці XX століття питання ризиків в сфері ІБ стало досить серйозним і обговорюваним. Не дивлячись на те, що більшість положень теорії ризиків інформаційної безпеки основуються на положеннях загальної теорії ризиків, тут все ж наявні певні специфічні особливості.

В подальшому, під визначенням «ризик» буде розумітись саме ризик ІБ, який являє собою поєднання імовірності настання ризикової події і спричинених цією подією збитків.

Під оцінкою ризиків мається на увазі ідентифікація ресурсів ІС і їх загроз та можливих збитків, що базується на аналізі частоти виникнення подій та об’ємах втрат. За рахунок використання кількісної оцінки ризику ІБ, розподіл наявних ресурсів для запобігання загрозам та планування майбутніх заходів щодо забезпечення ІБ є більш оптимальним. Оцінка ризиків як процес потрібно адаптувати до особливостей системи, а також, при цьому, погоджувати з найбільш дієвими та новітніми заходами.

Після закінчення процесу оцінювання ризиків, потрібно обрати один з наступних варіантів подальших дій:

– прийняти ризик, тобто з повним усвідомленням можливих наслідків, змиритись з ймовірністю його настання та нічого не змінювати. Це відноситься до ризиків, що несуть за собою незначні збитки і мають низьку імовірність настання;

– знизити ризик, тобто запровадити додаткові засоби для зниження імовірності настання та розміру збитку від загрози, провести додатковий інструктаж для працівників. В той же час, потрібно провести кількісну оцінку введення додаткових заходів по захисту, так як витрати організації на впровадження нових заходів і засобів не повинні бути більшими за можливі втрати від настання загрози;

– перенести ризик, тобто за допомогою різних засобів перенести можливі збитки від настання ризику на третю особу.

1.3. Існуючі підходи оцінювання ризиків ІБ

Не дивлячись на те, що немає чіткої класифікації методів оцінки ризиків, проте підходи до дослідження, способи розглядання окремих елементів, функціональні можливості певним чином відрізняють різні методи аналізу. Базуючись на цих відмінних рисах, методи поділяють на три загальні групи: лінгвістичні, графічні та математичні.

Графічними називаються методи, що базуються на візуалізації об’єктів, що аналізуються, та взаємодії, що наявна між ними. Здебільшого, такі методи використовуються щоб ідентифікувати всі наявні елементи ризику, процеси їх взаємодії, за рахунок побудови графів та діаграм, які дають можливість відобразити наявні дані про об’єкти дослідження.

Математичними вважаються методи, що дозволяють аналізувати поведінку, зміну властивостей та вплив елементів ризику на інші елементи за допомогою використання певних мов опису, які описують закони поведінки і зміни елементів, для окреслення особливостей та взаємодії об’єктів.

Лінгвістичними методами називаються ті, які не потребують яких-небудь інструментів, програм чи інших засобів, а лиш відповідальної за аналіз ризику команди персоналу. Це найпопулярніший та найпростіший в реалізації метод, тим не менш він не завжди є ефективним, так як всі стадії аналізу ризику потребують лише усне обговорення серед персоналу команди, результатом якого являється ідентифікація елементів, твердження про їх поводження і досить приблизна оцінка ймовірності реалізації ризику та можливі втрати.

Недоліки у використанні методів оцінки ризиків зумовлені необхідністю в оцінці інформаційних ризиків з високою точністю, робота з ними, а також потреба в певному рівні індивідуалізації рішень через різноманітні умови та фактори, що впливають на ІБ в залежності від типу об’єкта ІБ.

Далі будуть описані приклади з використання методів з оцінки ризиків для формування більш чіткого уявлення про можливості практичного використання методів оцінки ризиків в сфері ІБ.

Проблема оцінювання та дослідження інформаційних ризиків звичайно асоціюється з британським стандартом BS 7799, насамперед з його двома частинами: першою – BS 7799-1 «Звід правил з менеджменту безпеки інформації» та другою – BS 7799-2 «Системи менеджменту безпекою інформації», в яких вперше питання аналізу стану безпеки інформації та формування її захисту були напряму пов’язані з інформаційними ризиками. Однак безпосередньо аспекти оцінювання та управління ризиками, гармонізовані із змістом двох перших частин, було докладно розглянуто у третій частині стандарту BS 7799-3 «Настанови з менеджменту ризиками безпеки інформації» [3]. Проте першим міжнародним стандартом з менеджменту ризиками став стандарт ISO/IEC TR 13335-3 «Настанови з менеджменту безпеки інформаційних технологій»(1998 р.), який, як і інші стандарти серії ISO/IEC 13335, є національним стандартом України. Через десять років, у 2008 р. було видано стандарт ISO/IEC 27005 «Менеджмент ризиками безпеки інформації»[7], який наразі став одним з провідних нормативних документів у сфері управління інформаційними ризиками.

У міжнародній практиці склався загальний спільний підхід до організації управління ризиками, що відображається в більшості стандартів в сфері ІБ, які існують на даний час. В той же час слід зазначити, що управління ризиками стала однією з основних складових системи менеджменту якості організації. За рахунок більш концептуального характеру стандартів, експерти з ІБ мають можливість застосовувати всі способи, засоби і методи оцінки, аналізу та усунення ризиків.

Загалом, методи експертних оцінок являються комплексом логічних і математичних процесів обробки результатів опитування групи експертів, які являються єдиним джерелом інформації. За таких умов з'являється змога застосувати такі засоби, як інтуїцію, життєвий і професійний досвід учасників опитування [22].

Ці методи історично були першими, що виникли, за рахунок такої їх переваги як можливість використання цих методів навіть при обмеженій кількості чи майже повній відсутності інформації. Запорукою успішності проведення експертної оцінки являється унеможливлення спільного впливу учасників один на одного. Проте ці методи мають і свої недоліки, що часто можуть призводити до неточності результатів. Експерти та їх думка сильно залежить від певних зовнішніх факторів, що впливають на їх рішення, особливо при незначному об'ємі інформації про об'єкт дослідження

Найбільш поширений метод експертної оцінки базується на задумці про дискусію над проблемою серед кількох експертів в даній сфері. Недолік такого методу в тому, що процесі затвердження рішення знижується ймовірність вірної оцінки. Зазвичай судження експертів-аналітиків не сходиться з судженнями експертів-практиків, але цю відмінність можна скомпенсувати за рахунок використання коефіцієнта розбіжності.

Зараз використовується багато різноманітних методів та підходів для оцінювання ризиків, представлені багатьма компаніями, далі будуть наведені найпопулярніші з них.

Запропонована компанією Peltier and Associates методика "Facilitated Risk Analysis Process"[12] дає можливість збалансувати витрати відносно до

отримуваного результату від засобів захисту, що потрібні компанії. Матриця ризиків, яка формує правила оцінки, поділяє ризики на чотири рівні: A, B, C, D. Якщо ризик відноситься до першого рівня, то потрібно терміново виконати дії по його усуненню, це є обов'язковим. Якщо ризик відноситься до рівню B, то потрібно виконати дії по його усуненню, але це вже не терміново. Рівень C означає попередження про необхідність моніторингу за ситуацією відносно даного ризику. Ризик рівню D означає, що немає необхідності застосовувати якісь дії.

Модель «Матриці системи управління інформаційною безпекою (СУІБ)» розроблена і використовується для аналізу вже працюючих ІС для підвищення рівня захисту інформаційних ресурсів та удосконалення системи.

Модель оцінки ризиків інформаційної безпеки на основі нечітких множин створюється на основі впровадження нечітких когнітивих карт (НКК), які являють собою простий граф, що складається з вузлів, в якості яких виступають якості предметно області, наприклад поява ризику взлому системи, та зважених дуг, які виступають в ролі причинно-наслідкових зв'язків між вузлами, наприклад ймовірності появи певних подій.

Методу CRAMM [15] заснований на комплексному підході до оцінювання ризиків за допомогою поєднання кількісних і якісних методів оцінки. Він складається з трьох стадій, виконується побудова схеми зв'язків ресурсів, що використовуються для кожного з інформаційних процесів, що дає можливість обозначити критичні елементи. В якості цінності ресурсів в даному методі береться вартість відновлення даних ресурсів в випадку їх знищення, по цим значенням складається оцінка можливих збитків за школою від 1 до 10. При оцінці нижче значення 4 приймається рішення, що розглянута система не вимагає рівня захисту не вище базового і детальна оцінка ризиків ІБ не проводиться. Для кожної групи ресурсів дане ПЗ формує перелік питань з однозначною відповіддю.

Основною відмінністю наступного методу OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) [5] являється активна співпраця з власниками інформації під час пошуку критичних інформаційних ресурсів та

ризиків, що можуть їм загрожувати. Цей метод є досить гнучким за рахунок підбору критерії в залежності від потреб і вимог організації. Через своє широке поширення серед великих організацій, була створена версія OCTAVE-S для застосування на невеликих організаціях.

Таблиця 1.1.

Існуючі моделі оцінювання ризиків ІБ та їх основні переваги та недоліки

Підходи	Переваги	Недоліки
Модель на основі побудови «Матриці СУІБ»	- повнота опису інформаційної системи, її ресурсів і вразливостей; - можливість виділити найбільш уразливі ресурси; - можливість оцінки існуючої системи захисту інформації.	- наявність суб'єктивної думки щодо визначення важливості активів і частоти реалізації загроз.
Модель оцінювання ризиків інформаційної безпеки на основі нечітких множин	- застосування апарату нечіткої логіки; - можливість розрахувати ймовірність реалізації загрози; - визначає ризики реалізації відповідної загрози.	- неможливо розрахувати час, що витрачається зловмисником на реалізацію загрози, а також час виявлення атаки.
Пробіт-аналіз	- забезпечує єдину методологічну базу обліку особливостей пар загроза/наслідок; - основа для вирішення завдання кількісної оцінки у сфері безпеки інформації.	- замало практичних прикладів.
Кількісний аналіз ризиків інформаційної безпеки	- відносна простота впровадження; - зрозумілість для менеджерів; - є приклади успішного застосування	- відносно дорогий; - краще застосовується до існуючих інформаційних активів.
Методологія RiskWatch	- відносна простота впровадження; - зрозумілість для менеджерів; - можливість створення своїх профілів захищеності.	- відносно дорогий; - краще застосовується до існуючих інформаційних активів.
Методологія "Facilitated Risk Analysis Process (FRAP)"	- надає кількісний аналіз ризиків; - забезпечує симуляційну модель системи.	- занадто “науковий” метод; - тільки для відносно великих підприємств.

Продовження таблиці 1.1.

Існуючі моделі оцінювання ризиків ІБ та їх основні переваги та недоліки

Підходи	Переваги	Недоліки
Стандарти ISO	- спільний підхід до організації управління ризиками.	-концептуальний характер стандартів.
Методи експертних оцінок	- відносна простота; - можливість якісні оцінювання	- суб'єктивність думок експертів; - обмеженість суджень
Методологія CRAMM	- є універсальною і підходить для організацій як державного, так та комерційного сектору; - використовує кількісні і якісні способи оцінки ризиків; - розроблені комерційні програмні продукти, що реалізовують положення CRAMM.	-використання методики потребує спеціальної підготовки і високої кваліфікації спеціаліста; -довготривалий процес аналізу; - програмний інструментарій генерує велику кількість паперової документації, яка не завжди виявляється корисною практиці; - не дає змоги створювати власні шаблони звітів або модифікувати наявні.
Методологія OCTAVE	- швидко впроваджується; - можливе застосування для організацій різного розміру та галузей зайнятості; - є комерційні програмні продукти, що реалізовують положення методики; - високий рівень гнучкості.	- не дає кількісної оцінки ризиків; - припускає використання як способів зниження ризиків лише його зниження і прийняття; - важкість реалізації окремих етапів.
Методологія CORAS	- простота у використанні ; - підходить для нових проектів; - прийнятна вартість.	- проводиться тільки разова оцінку рівня ризику

З огляду на наведені методології, можна підсумувати, що немає такої, яка б містила в собі чіткі правила на рахунок формування розкладу наступних майбутніх оцінок ризиків, а також, в жодній з них не приділяється увага оновленню величин ризиків. Також, можна зазначити, що для разової комплексної оцінки ризиків організації є сенс використовувати саме метод CORAS, а от для постійних систематичних перевірок більш доцільним буде використовувати метод CRAMM. В той же час, для великих організацій, які

хочуть запровадити якісне управління ризиками на основі систематичних перевірок на рівні не нижче організаційного і є необхідність у створені продуманого плану по зниженню рівня ризиків кращим буде використання методу OCTAVE.

Не дивлячись на те, що в проаналізованих джерелах були наведені деякі новітні цікаві ідеї, їх реалізація часто призводить до зниження прозорості кінцевої оцінки та буде вимагати від експерта досить високої наукової підготовки в сфері математики. Таким чином, надмірна математична складність відноситься скоріше до недоліків при виборі методу оцінки ІБ.

Тому, проаналізувавши всі переваги та недоліки різних методів та моделей, було прийнято рішення обрати як базу саме факторний аналіз, основою якого буде виявлення факторів, що призводять до реалізації ризиків чи негативних наслідків з певною імовірністю. За допомогою методів факторного аналізу можна вирішити такі групи проблем, як пошук передбачуваних неявних закономірностей, які визначені впливом зовнішніх або внутрішніх факторів на ІБ, пошук та дослідження зв’язку ознак з чинниками або основними компонентами та зменшення об’єму інформації через проведення процесу оцінки з використанням узагальнених чинників або головних компонентів.

Висновок до розділу 1

В даному розділі описані основні загрози інформаційної безпеки, наведено ряд зовнішніх небезпек ІБ.

Описано сутність інформаційних ризиків, надано терміни характеристики ІБ.

Виділені підходи оцінювання ризиків ІБ. Описано основні переваги та недоліки існуючих моделей оцінювання ризиків ІБ.

2 МЕТОДИКИ МОДЕЛЮВАННЯ ТА ОЦІНКИ ІНФОРМАЦІЙНИХ РИЗИКІВ

Основним завданням при аналізі ризиків є оцінити рівень ризику, який визначається виходячи з ймовірності виникнення інциденту і наслідків від цього інциденту. У загальному випадку процес аналізу ризиків складається з наступних етапів:

1. Встановити розмір цінності інформаційних ресурсів і провести відповідне ранжування.

2. Оцінити потенційні втрати при здійсненні кожної з загроз щодо всіх інформаційних ресурсів.

3. Оцінити можливу імовірність виникнення кожної загрози для ІБ.

4. Оцінити сумарні імовірні втрати від кожної припустимої загрози відповідно до всіх ресурсів за контрольний період (за один рік).

5. Проаналізувати отримані дані по втратам для кожної загрози.

6. Для кожної з загрозі потрібно обрати з доцільних рішень:

– прийняти ризик, тобто з повним усвідомленням можливих наслідків, змиритись з ймовірністю його настання та нічого не змінювати. Це відноситься до ризиків, що несуть за собою незначні збитки і мають низьку імовірність настання;

– знизити ризик, тобто запровадити додаткові засоби для зниження імовірності настання та розміру збитку від загрози, провести додатковий інструктаж для працівників. В той же час, потрібно провести кількісну оцінку введення додаткових заходів по захисту, так як витрати організації на впровадження нових заходів і засобів не повинні бути більшими за можливі втрати від настання загрози;

– перенести ризик, тобто за допомогою різних засобів перенести можливі збитки від настання ризику на третю особу.

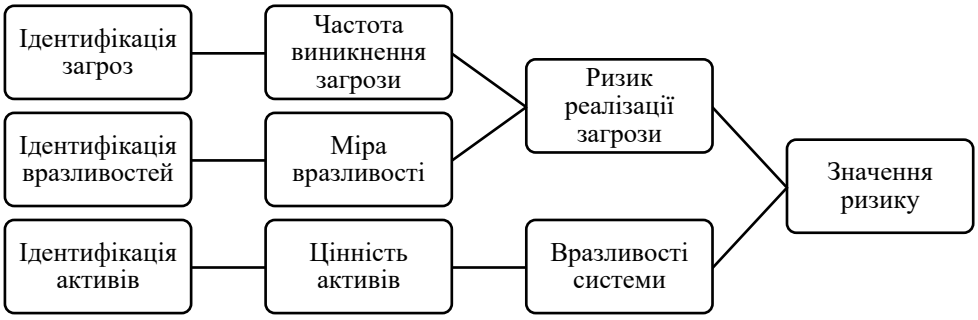


Рис. 2.1. Елементи оцінки ризиків ІБ

Ризик може бути оцінений двома способами: якісно та/або кількісно.

В підсумку проведення кількісної оцінки, необхідно щоб були визначені:

– вартість ресурсів у грошовому або іншому еквіваленті;

– перелік всіх можливих загроз ІБ з порахованими втратами при разовій реалізації для кожної з загроз;

– частота появи для всіх загроз;

– імовірні втрати при реалізації кожної загрози;

– необхідні способи уникнення та протидії для кожної загрози.

При використанні якісного підходу об’єкт не оцінюється в грошовому чи кількісному еквіваленті. Замість цього об’єкт оцінюється показником, що ранжується за певною лінгвістичною або баловою шкалою. При такій оцінці збір даних проводиться через опитування цільових груп, тобто безпосередньо з інформації отриманої від певних компетентних та досвідчених співробітників галузі, для якої розглядаються загрози.

Необхідно:

1. Встановити вартість інформаційних ресурсів. Цінність ресурсу (активу) визначається за допомогою використання рівня критичності (наслідків) у випадку порушення характеристик безпеки інформаційного ресурсу або його важливості.

2. Оцінити імовірність виникнення загрози відповідно до інформаційного ресурсу. Для такої оцінки може бути використана трирівнева якісна шкала (низька, середня, висока).

3. Оцінити рівень можливості вдалої реалізації загрози враховуючи поточний стан ІБ, застосованих заходів і засобів захисту. Також, для визначення рівня можливості реалізації загрози використовується трирівнева якісна шкала (низька, середня, висока). Показник можливості реалізації загрози відображає, наскільки потенційно виконуваною може бути загроза.

4. Підготувати заключення на рахунок рівню ризику, проаналізувавши цінність інформаційного ресурсу, імовірності виникнення загрози, можливості виникнення загрози. При оцінюванні рівня ризику може бути використана п'ятибальна або десятибальна шкала, а також еталонні таблиці для розуміння залежності рівня ризику від комбінацій показників (цінність, ймовірність, можливість).

5. Проаналізувати отримані дані по кожній загрозі і отриманому для неї рівню ризику. Досить часто трапляються випадки, коли сформована в організації група аналізу ризиків використовує поняття «прийнятний рівень ризику», яке означає той рівень ризику, який сама організація готова прийняти, тобто у випадку коли рівень ризику загрози нижчий або дорівнює прийнятному - вона вважається не актуальною. Загальне завдання якісної оцінки ризиків зводиться до зниження ризиків до прийнятного рівня.

6. Створити необхідні способи уникнення та протидії для кожної актуальної загрози.

Обидва способи мають свої позитивні і негативні сторони, і на практиці більш адекватним є комбінована оцінка елементів ризику. При цьому можна використовувати лінгвістичні змінні з термами, що відображають якісну оцінку елемента, а завдяки семантичним правилам мати і можливість перетворити терм в кількісне значення.

2.1. Методології моделювання інформаційних ризиків

Для виявлення вразливостей системи зазвичай користуються різними способами, основними з яких є використання фіктивних атак, статичний аналіз всіх елементів, надання даних про вразливості розробником ПЗ, моделювання ризиків.

Серед цих методів нас цікавить саме останній, моделювання ризиків, який являється безперервним процесом, що дає можливість виявляти, знижувати кількість загроз в системі через прийняття дій, щодо впровадження методів захисту безпосередньо під час проектування системи.

Основною перевагою цього методу являється те, що він дає можливість отримати уявлення про реальні атаки, точно окреслити зв'язок між компонентами системи, отримати шляхи реалізації та імовірності використання вразливостей і маємо уявлення про вплив можливих атак на систему.

В даний час є значна кількість різноманітних методів моделювання інформаційних ризиків. Серед них виділяють наступні: STRIDE, PASTA, Trike, VAST, OCTAVE. Про кожен метод буде окремо описано далі.

STRIDE

Розроблена корпорацією Microsoft методологія STRIDE зазвичай застосовується для описання та групування різних ризиків за їх спільними суттєвими ознаками, такими як: мета атаки, метод реалізації атаки, вразливості, які були використані для реалізації даної атаки, тощо.

Саме слово STRIDE являється абревіатурою з слів Spoofing, Tampering, Repudation, Information disclosure, DoS, Elevation of Privilege. Розгорнуте розшифрування цього слова наведене в Таблиці 2.1.

Таблиця 2.1.

Розшифрування абревіатури STRIDE

Назва	Ціль атаки	Визначення
Spoofing	Автентифікація	Видання атакуючого за іншого користувача
Tampering	Цілісність	Модифікування абовидалення інформації
Repudation	Аудит	Проведення шкідливих дій без загрози розкриття
Information Disclosure	Конфіденційність	Доступ до конфіденційних даних
DoS	Доступність	Повне або часткове знищення інформації

Продовження таблиці 2.1.

Розшифрування абревіатури STRIDE

Назва	Ціль атаки	Визначення
Elevation of Privilege	Авторизація	Викрадення або підміна даних особи для отримання повноважень

PASTA

Методологія PASTA являється доволі новою, має сім рівнів та спрямована на ризик. Загалом ця абревіатура розшифровується як «процес моделювання атаки і аналізу загроз». Його ціллю є врахувати аналіз впливу бізнесу і вимог та надати забезпечення рівноваги між бізнес-цілями та технічними вимогами з використанням процесу з семи етапів. Він має на меті надавати швидку оцінку загрозі, проводити підрахунок очок, і по завершенню моделювання загроз, експерти мають виконувати детальний їх аналіз. PASTA розроблена для надання погляду зі сторони зловмисника на систему і вразливості, що дозволить експертам покращувати свою стратегію дій.

Trike

Методологія Trike заснована на ідеї застосування моделі загроз у якості інструменту з управління ризиками, тобто використовувати моделі загроз для проведення аудиту безпеки. Самі моделі загроз базуються на «моделі вимог», яка закріплює обговорений залученими сторонами «прийнятний» рівень ризику, який надається для кожного класу активів. Результатом аналізу цієї моделі являється модель загрози в якій наявний перелік загроз з присвоєними значеннями ризику.

VAST

Головною особливістю методології VAST (Visual, Agile і Simple Threat modeling) є те, процес моделювання загроз потрібно масштабувати по всій інфраструктурі і проводити інтегрування в методологію Agile. Її ціллю являється отримання дієвих результатів для вирішення виняткових потреб різноманітних можливих зацікавлених сторін, таких як архітектори і розробники програм, співробітники сфери ІІ і керівники вищих ланок.

OCTAVE

Однією з найперших методологій, що створювались саме для моделювання загроз кібербезпеки була OCTAVE (The Operationally Critical Threat, Asset, and Vulnerability Evaluation methodology). Вона направлена на оцінювання організаційних ризиків, що виникають в випадку пошкодження даних. За допомогою використання цієї методологію можна провести ідентифікацію інформаційних ресурсів організації. Метою методології є надання конкретних даних на рахунок масштабів моделі загрози і зниження зайвої документації для активів, які погано ідентифіковані чи не входять в сферу дії системи. OCTAVE є найбільш ефективним у разі використання його при побудові корпоративної системи захисту, яка буде орієнтована на ризик. Він легко підлаштовується під цілі безпеки та середовища ризику наявні в організації, тому є доволі універсальним та корисним.

2.2. Основні ризики та заходи управління ризиками

Ризики, пов'язані з інформаційними технологіями та безпекою

Будь-яке підприємство і державна установа можуть бути схильні до ризиків, пов'язаних з інформаційними технологіями та безпекою. Таким чином, кожне з них допускає ймовірність втрати даних з наступними фінансовими або іншими ризиками, які можуть виникнути внаслідок збоїв в роботі програмного забезпечення і устаткування, неавторизованого видалення інформації, крадіжки обладнання а також кібератак[2].

Заходи управління:

– використання системи резервного копіювання, елементів резервної інфраструктури: резервний офіс і резервний центр обробки даних. Резервний офіс розрахований для розміщення необхідного персоналу установ і здатний забезпечити виконання ключових бізнес-процесів;

– для забезпечення безперебійної подачі електроенергії в аварійних ситуаціях в системі електропостачання офісів підприємств задіяні джерела автономного безперебійного живлення і дизель-генераторні установки;

– навантаження на системи, сервіси, канали зв’язку та обладнання контролюється спеціалізованою системою моніторингу;

– використовуються системи захисту.

– розроблені і впроваджені процедури та плани забезпечення безперервності й відновлення діяльності;

– основні ресурс-провайдери та канали зв'язку задубльовано.

– інфраструктури установ мають бути побудовані таким чином, що дозволяють в найкоротшій термін її масштабувати задля збільшення потужності.

2.3. Методи оцінки інформаційних ризиків

Не дивлячись на те, що немає чіткої класифікації методів оцінки ризиків, проте підходи до дослідження, способи розглядання окремих елементів, функціональні можливості певним чином відрізняють різні методи аналізу. Базуючись на цих відмінних рисах, методи поділяють на три загальні групи: лінгвістичні, графічні та математичні.

Графічними називаються методи, що базуються на візуалізації об’єктів, що аналізуються, та взаємодії, що наявна між ними. Здебільшого, такі методи використовуються щоб ідентифікувати всі наявні елементи ризику, процеси їх взаємодії, за рахунок побудови графів та діаграм, які дають можливість відобразити наявні дані про об’єкти дослідження.

Математичними вважаються методи, що дозволяють аналізувати поведінку, зміну властивостей та вплив елементів ризику на інші елементи за допомогою використання певних мов опису, які описують закони поведінки і зміни елементів, для окреслення особливостей та взаємодії об’єктів.

Лінгвістичними методами називаються ті, які не потребують яких-небудь інструментів, програм чи інших засобів, а лиш відповідальної за аналіз ризику команди персоналу. Це найпопулярніший та найпростіший в реалізації метод, тим не менш він не завжди є ефективним, так як всі стадії аналізу ризику потребують лише усне обговорення серед персоналу команди, результатом якого являється ідентифікація елементів, твердження про їх поводження і досить приблизна оцінка ймовірності реалізації ризику та можливі втрати.

Кількість методів, які здатні забезпечити весь цикл аналізу ризиків є досить малою і такі методи, як правило, дорогі в застосуванні. Інші методи вимагають залучення значної кількості експертів у різних галузях, таких як інформаційні технології, економіка, право, що також значно збільшує вартість проведення аналізу ризиків.

Графічні методи аналізу

Аналіз дерева подій (Event-tree-analysis, ETA) – є логічним методом моделювання як успіхів, так і невдач, досліджує відповідь через подію і ініціює генерацію шляху для оцінки ймовірностей результатів і загального системного аналізу. Загальна мета аналізу у вигляді дерева подій – визначення ймовірності виникнення можливих негативних наслідків, які можуть завдати шкоди системі з обраної вихідної події. Для цього необхідно використати докладну інформацію про систему, щоб зрозуміти проміжні події, сценарії аварій, та використовуючи вихідні події побудувати діаграму подій. Дерево подій починається з події, що ініціює, де наслідки цієї події йдуть двійковим чином. Кожна подія створює шлях, для якого може бути розрахована загальна ймовірність настання цього шляху[28].

Аналіз видів і наслідків відмов (Failure mode and effects analysis, FMEA). Спочатку розроблений і опублікований військово-промисловим комплексом США (у формі стандарту MIL-STD-1629), аналіз видів і наслідків відмов є сьогодні популярним, оскільки в деяких галузях промисловості розроблені і опубліковані спеціалізовані стандарти, присвячені FMEA. Перш за все, повинні бути чітко визначені межі даної системи. Система може являти собою технічний пристрій, процес або будь-що інше, що піддається FMEA-аналізу. Далі ідентифікуються види можливих відмов, їх наслідки і можливі причини виникнення. Залежно від розміру, природи і складності системи, визначення видів можливих відмов може бути виконано для всієї системи в цілому або для кожної її підсистеми індивідуально. В останньому випадку наслідки відмов на рівні підсистеми будуть проявлятися як види відмов на рівень вище. Ідентифікація видів і наслідків відмов повинна бути виконана методом «знизу-вгору», до досягнення верхнього рівня системи. Для характеристики видів і

наслідків відмов, визначених на верхньому рівні системи, використовуються такі параметри: інтенсивність, критичність відмов, ймовірність виникнення і т. п. Ці параметри можуть бути або розраховані «знизу-верх» з нижніх рівнів системи, або явно задані на її верхньому рівні. Ці параметри можуть мати як кількісний, і якісний характер. В результаті для кожного елемента системи верхнього рівня розраховується своя унікальна міра, що обчислюється з цих параметрів за відповідним алгоритмом. У більшості випадків цю міру називають «коефіцієнтом пріоритетності ризику», «критичністю», «рівнем ризику» або іншим способом[6].

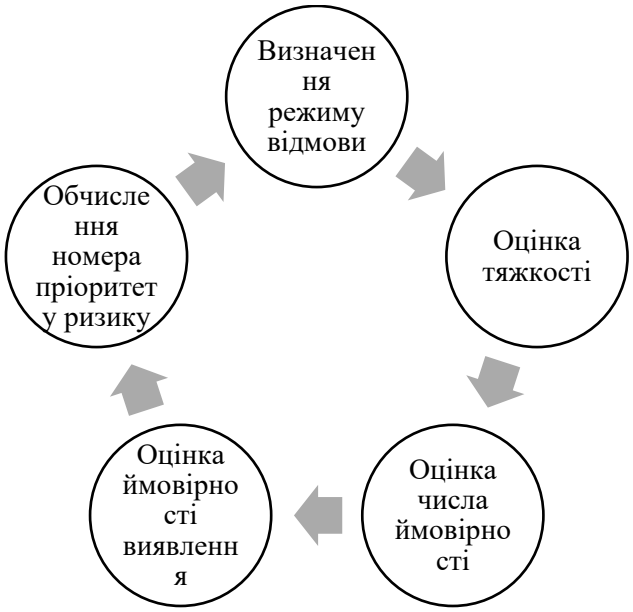


Рис. 2.3.1. Аналіз видів і наслідків відмов

Метод аналізу дерева рішень дає можливість по порядку представити альтернативні варіанти рішень, враховуючи їх вихідні дані та невизначеності. Так як і в першому методі, слід починати розробку з першої події чи прийнятого рішення, наприклад з рішення про відновлення проекту 1 чи проекту 2. Потім потрібно побудувати напрямки розвитку подій, окреслити результати, які можливо виникнуть у випадку реалізації подій, та рішення, що можливо будуть ухвалені. Можливість настання подій оцінюється на основі оцінки витрат та/або ефективності кінцевого результату вибраного напрямку розвитку подій.

Математичні методи аналізу

Метод аналізу впливу людського фактора(HRA) використовують для оцінювання впливу дій та рішень людини, особливо помилок оператора, на

загальну роботу системи. Так як майже у всіх процесах наявна можливість скоєння помилки оператором, потрібно мінімізувати можливість такого розвитку подій, який призведе до серйозних проблем. Тим не менш, за певних обставин дії оператора можуть бути єдиним захистом від катастрофічних наслідків відмови. Існування випадків, коли помили оператора стали початком розвитку подій, що привів до катастрофи, підтверджує необхідність системи оцінки дій оператора. Тобто, це свідчить про неправильність врахування лиш технічних характеристик системи при оцінюванні ризику.

На додаток слід відмітити, що врахування дій оператора при оцінюванні ризиків дає можливість знайти помилки, що негативно впливають на продуктивність, і окреслити шляхи знешкодження таких помилок і інших несправностей.

Метод Марковського аналізу використовують у випадку, коли поточний стан системи це єдине що впливає на її майбутній стан. В більшості випадків його застосовують при аналізі ремонтопридатних систем, що мають можливість працювати в кількох режимах, та якщо є недоцільним використання аналізу надійності окремих блоків. Він може використовуватись для складніших систем в разі використання вищих порядків процесу Маркова. Цей метод являється кількісним, буває дискретним та безперервним. Метод Марковського аналізу можна провести вручну, але його особливості дають можливість завтосовувати комп’ютерні програми для полегшення та пришвидшення роботи з використанням цього методу.

Метод Монте-Карло можна використовувати в тяжких ситуаціях, які складні для розуміння і вирішення з використанням аналітичних методів. Можна створити моделі систем застосувавши таблиці або інших прості методи, але наявні сучасніші програмні засоби, в яких можна працювати при складних вимогах, більшість з таких програмних засобів мають прийнятну ціну. При першій розробці і застосуванні моделі, через доволі велику кількість необхідних для методу ітерацій, отримання результатів можливо буде довгим і трудомістким. Проте сучасні програмні застосунки у багатьох випадках дозволяють пришвидшити обробку даних.

Лінгвістичні методи

Метод мозкового штурму представляє собою дискусію серед групи фахівців з метою виявлення можливих видів відмов і небезпек, ризику, заходів безпеки та способів боротьби з ризиками. Хоч термін «мозковий штурм» широко використовується як назва будь-якого обговорення групою осіб, проте в класичному варіанті наявні певні методи генерації нових ідей серед учасників обговорення за рахунок висловлювання своїх думок іншими учасниками. В даному методі передбачається направлення обговорення на періодичній основі в потрібні області та обговорення проблем, що були виявлені в результаті дискусії.

Контрольні листи представляють з себе список небезпек, ризиків або відмов засобів управління, що розробляються з огляду на отриманий раніше досвід, наявних результатів оцінки ризиків чи відмов, що вже реалізувались раніше. Необхідними пунктами процедури є:

– окреслення області використання;

– написання контрольного листа з охопленням всієї області використання. Для досягнення визначеної цілі дуже важливий ретельний підхід до цього етапу, і не допускається використання попередніх контрольних листів;

– необхідно щоб відповідальна особа використала контрольний лист по черзі до всіх елементів процесу або системи щоб визначити чи точно описаний кожен елемент.

Структурований аналіз сценаріїв методом «що, якщо?» (SWIFT). Цей метод від початку розроблявся як простіша альтернатива дослідження HAZOP. Він базується на командній роботі, наявності ведучого та використання певного набору слів або фраз-підказок, що є додатковою допомогою при ідентифікації небезпечних ситуацій та узгодження сценарію їх розвитку. Даний метод прийнято використовувати для дослідження більших систем з вищим рівнем деталізації, ніж в тих, до яких можна використовувати дослідження HAZOP.

Метод експертної оцінки

За основу для цього методу взята здатність людей використовувати свій інтелект для ефективного вирішення погано формалізовані задачі. Є два варіанта

використання методу: заочне анкетування (без особистої зустрічі фахівців) та метод «круглого столу» (живе обговорення між всіма експертами).

Метод експертних оцінок являється комплексом логічних і математичних процесів обробки результатів опитування групи експертів, які являються єдиним джерелом інформації. За таких умов з'являється змога застосувати такі засоби, як інтуїцію, життєвий і професійний досвід учасників опитування.

Ці методи історично були першими, що виникли, за рахунок такої їх переваги як можливість використання цих методів навіть при обмеженій кількості чи майже повній відсутності інформації. Запорукою успішності проведення експертної оцінки являється унеможливлення спільного впливу учасників один на одного. Проте ці методи мають і свої недоліки, що часто можуть призводити до неточності результатів. Експерти та їх думка сильно залежить від певних зовнішніх факторів, що впливають на їх рішення, особливо при незначному об'ємі інформації про об'єкт дослідження

Найбільш поширений метод експертної оцінки базується на задумці про дискусію над проблемою серед кількох експертів в даній сфері. Недолік такого методу в тому, що процесі затвердження рішення знижується ймовірність вірної оцінки. Зазвичай судження експертів-аналітиків не сходиться з судженнями експертів-практиків, але цю відмінність можна скомпенсувати за рахунок використання коефіцієнта розбіжності.

До переваг методу можна віднести оцінювання видів ризику які не можливо оцінити іншими методами та простота виконання.

В той же час наявні такі недоліки, як суб'єктивність отриманих результатів та не дуже висока точність оцінки.[9]

Метод оцінки DREAD

Метод DREAD входить до системи оцінки ризиків комп'ютерної безпеки, що використовується Microsoft, і зараз застосовується багатьма компаніями як складова методів моделювання таких як STRIDE та OWASP. Цей метод має мнемоніку, яка може оцінити ризик загроз безпеці за п'ятьма категоріями.

Переваги цього методу: можна не тільки суб'єктивно оцінити його складові, але й статистику, точність оцінки досить висока.

Недоліки цього методу: він вимагає досить точної моделі загрози та чіткої вартості ресурсу.

Висновок до розділу 2

Дослідивши та проаналізувавши наявні методи аналізу ризиків, можемо зробити висновок про те, що головними недоліками їх використання являється:

– великі фінансові вкладення для проведення аналізу ризиків;

– потреба в доволі великій групі експертів;

– відсутність у багатьох методів можливості обліку випадкових і неповних подій.

Беручи до уваги дані проблеми, можна сформулювати наступні вимоги до сучасних методів аналізу ризиків:

1. мінімізація кількості задіяних експертів у процесі аналізу ризиків;
2. використання моделей і методів, які дозволяють враховувати неповноту або відсутність частини інформації про функціонування системи.

3 ПОБУДОВА СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РИЗИКАМИ

3.1. Існуючі підходи до управління ризиками

Система управління інформаційними ризиками (СУІР) є фундаментом, на якому будуються СУІБ організації. Це найважливіша і, разом з тим, найскладніша для впровадження з усіх підсистем, що входять до складу СУІБ. Всі стратегічні рішення щодо механізмів контролю та виділенню необхідних ресурсів для СУІБ повинні прийматися на основі оцінки ризиків.

Фундаментом СУІБ служить система управління інформаційними ризиками, що являє собою:

1) Сукупність взаємопов'язаних формалізованих процесів, що забезпечують аналіз і планування, реалізацію та експлуатацію, моніторинг і аудит, коригування та вдосконалення механізмів управління ризиками;

2) Стандарти і технології управління ризиками, представлені у вигляді нормативної та робочої документації СУІР, що включає в себе політику управління ризиками та методологію оцінки ризиків, а також ще близько 20 робочих документів, з яких найважливішими є Реєстр інформаційних ризиків і План обробки ризиків;

3) Організаційну структуру управління ризиками і відповідним чином підготовлений персонал. Ролі та відповідальність за функціонування процесів управління ризиками розподіляються між керівництвом організації, керуючим комітетом з інформаційної безпеки, робочою групою з оцінки ризиків, власниками активів, користувачами і обслуговуючим персоналом інформаційних систем, менеджером інформаційної безпеки, ризик-менеджером і аудиторами.

Практика впровадження та сертифікації СУІБ різних компаній показує, що оцінка ризиків - це вразливе місце сучасних організацій, зазвичай викликає найбільші труднощі. У багатьох випадках ситуація така, що керівництво організації не має необхідної і своєчасної інформацією про ризики інформаційної безпеки для прийняття адекватних рішень в цій галузі, контролю

реалізації та оцінки ефективності прийнятих рішень. У багатьох організаціях відсутні система збору та аналізу інформації про інформаційні ризики, механізми обробки та перегляду ризиків, механізми комунікації ризиків і інші необхідні елементи, без яких система управління ризиками не працює[29].

Три необхідних складових СУІР:

1. формалізовані взаємодіючі процеси;
2. стандарти, технології, внутрішній документообіг;
3. організаційна структура і кадри.

Не може СУІР функціонувати і без чітко визначених і узгоджених з усіма учасниками процесу критеріїв оцінки та прийняття ризиків, області оцінки та інших елементів, що визначаються політикою управління ризиками.

Не варто також забувати і про цілі управління ризиками, способи оцінки досягнення цих цілей, методи вимірювання ефективності механізмів контролю та системі заохочення персоналу, яка повинна бути пов'язана з досягненням цілей СУІР і ефективністю реалізованих механізмів контролю[13].

Розробка і впровадження СУІР - процес досить трудомісткий, що вимагає високого професіоналізму і великого досвіду в управлінні ризиками. Теоретично кожна організація, що починає усвідомлювати свої потреби в забезпеченні інформаційної безпеки, в змозі рухатися по шляху створення СУІР самостійно, однак на практиці багато заходять в глухий кут на цьому шляху. Це відбувається не тільки через нестачу досвіду, професійної кваліфікації та глибини усвідомлення інформаційних ризиків.

Справа в тому, що впровадження СУІР часто пов'язано з досить істотними змінами існуючої системи управління організацією та переглядом прийнятих підходів до прийняття рішень. Це особливо складно зробити, якщо в організації досі взагалі була відсутня будь-яка система управління ризиками (ERM-система) і відповідних елементів такої системи просто не існує. В цьому випадку змінити систему управління зсередини вкрай складно. Адже будь-яка система прагне до стабільності і збереженню свого колишнього стану.

Тому в багатьох випадках допомога з боку зовнішніх консультантів, які мають достатній досвід впровадження СУІР і володіють відповідними

технологіями, є виправданою. Досвідчені консультанти зможуть провести навчання персоналу, формалізувати процеси і розробити систему внутрішньої документації для управління ризиками, провести первинну оцінку ризиків і розібратися з проблемами, які виникнуть по ходу цієї оцінки, а також «підштовхнути» керівництво організації з метою якнайшвидшого розгляду та прийняття рішень по ризиках.

Для організацій, в яких інформаційні ризики не є основними, існує варіант віддачі процесу управління ризиками на аутсорсинг спеціалізованої організації. Теоретично аутсорсинг повинен забезпечити скорочення витрат при збереженні достатнього рівня контролю над процесами управління ризиками.

3.2. Політика і контекс управління ризиками

Політика управління ризиками – внутрішній нормативний документ організації, що регламентує питання управління ризиками і базується на політиці СУІБ, стандартах і нормативних документах. Вона визначає контекст для управління ризиками; використовувану термінологію СУІР як систему взаємопов'язаних процесів, які виконуються в певній послідовності і взаємодіють один з одним певним чином; інформаційні потоки СУІР, включаючи надання звітності, комунікацію ризиків і отримання зворотного зв'язку; а також відповідальність за управління ризиками[14].

Область дії СУІР (область управління ризиками) в ідеалі повинна збігатися з областю дії СУІБ і охоплювати всю організацію. Однак оцінити відразу всі ризики для всіх активів і впровадити СУІР відразу у всій організації досить складно. Тому найчастіше застосовується стратегія поетапного впровадження. В цьому випадку область дії СУІР може охоплювати тільки частину організації.

Область управління ризиками, так само як і область дії СУІБ, може бути представлена схематично, наприклад, як показано на рисунку 3.1.

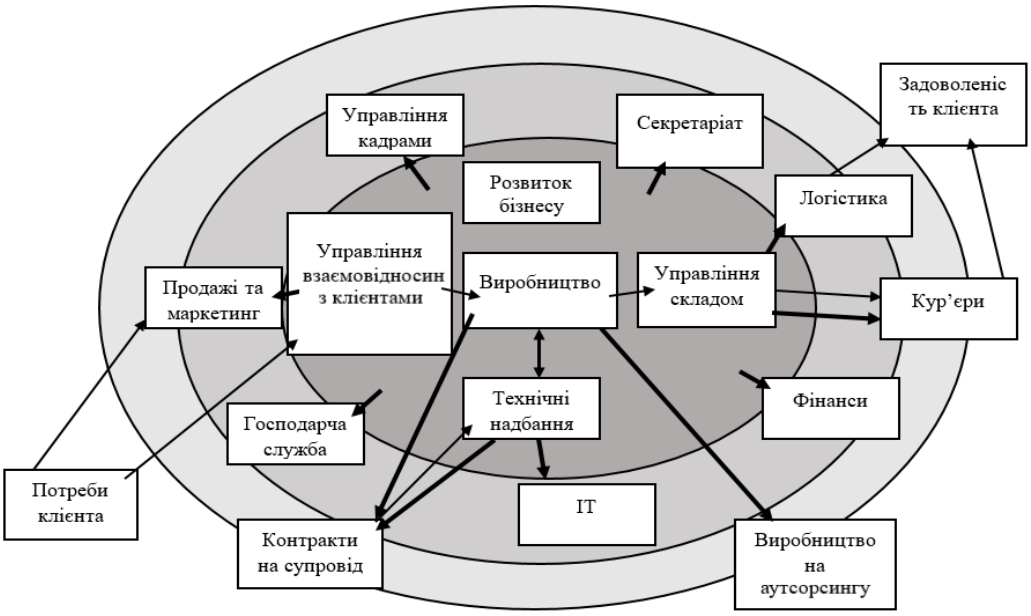


Рис.3.1. Область дії СУІБ

На даній схемі внутрішня область включає в себе структурні підрозділи організації в області дії СУІР. Ця область знаходиться всередині ширшої області, що включає в себе всі структурні підрозділи організації. Ці підрозділи (структурні одиниці) безпосереднім чином входять в зону контролю керівництва організації. Зовнішня область, крім самої організації, включає в себе також зовнішні сторони, які пов'язані з організацією договірних відносин і від яких залежить її діяльність[25].

Взаємодія між підрозділом в області дії СУІР регламентується внутрішніми процедурами і регламентами; взаємодія з зовнішніми сторонами, що не входять в зону дії СУІР, регламентується договорами та угодами про рівень сервісу (SLA) [15].

Як можна більш повне і точне визначення області дії СУІР є вкрай важливим для управління ризиками, як з точки зору ідентифікації та обмеження кількості розглянутих ризиків, так і з точки зору передачі певних ризиків зовнішнім сторонам, шляхом укладення з ними відповідних договірних відносин, що визначають їх відповідальність за забезпечення інформаційної безпеки.

Структура системи управління ризиками

Оскільки процеси управління ризиками є складовою частиною загальної системи управління організації, для їх опису використовується та ж процесна

модель, що і в інших стандартах систем управління. Ця модель зображена на рисунку 3.2. та визначає чотири групи процесів: Планування - Реалізація - Перевірка - Дія (ПРПД), що відображає стандартний цикл управління, вперше описаний в роботах Демінга. У той час як ISO 27001 описує загальний безперервний цикл управління безпекою, в стандартах BS 7799-3 і ISO 27005 міститься його проекція на процеси управління ризиками[33].

Рис. 3.2. Модель Демінга стосовно до процесів управління ризиками

Розглянемо проекцію процесів управління ризиками на процесну модель ПРПД більш детально по кожній групі процесів.

Планування

На етапі планування визначаються політика, контекст і методологія управління ризиками, інвентаризуются (ідентифікуються) активи і визначається їх цінність, формулюються профілі загроз і вразливостей, оцінюється ефективність контрзаходів і проводиться обробка ризиків. Керівництво організації приймає відповідні рішення і затверджує план обробки ризиків.

Вона включає в себе наступні заходи:

— ідентифікація активів;

— ідентифікація вимог законодавства і бізнесу, які можна застосувати до ідентифікованим активам;

— оцінювання активів з урахуванням ідентифікованих вимог законодавства і бізнесу, а також наслідків порушення конфіденційності, цілісності та доступності;

— ідентифікація значущих загроз і вразливостей для активів;

— оцінка ймовірності виникнення загроз і величини вразливостей;

— обчислення ризиків;

— оцінювання ризиків за заздалегідь визначеною шкалою ризику.

Реалізація

На етапі реалізації проводиться впровадження необхідних механізмів безпеки та інші дії по реалізації плану обробки ризиків, які можуть включати в себе, наприклад, укладення договорів страхування, угод про рівень сервісу і навіть коригування планів розвитку бізнесу з метою уникнення певних ризиків.

Перевірка

Після прийняття рішень по обробці ризиків і впровадження обраних механізмів контролю повинні починатися безперервні дії з управління ризиками. Ці дії включають в себе процес моніторингу ризиків і ефективності СУІБ, що дозволяє гарантувати, що впроваджені механізми контролю функціонують належним чином.

На етапі перевірки відстежується функціонування реалізованих механізмів безпеки, контролюється зміна факторів ризику (активів, погроз, вразливостей), проводяться аудити і виконуються різні контролюючі процедури.

Дія

На етапі дії здійснюється вдосконалення процесів управління ризиками за результатами моніторингу та аудиту, в разі необхідності переглядаються певні ризики, які використовуються підходи і методи їх оцінки, вносяться зміни в нормативну і операційну документацію організації, уточнюється контекст управління ризиками. Постійне вдосконалення є суттєвою частиною безперервних дій з управління ризиками, що вживаються з метою підвищення

ефективності впроваджених механізмів контролю для досягнення цілей, які були встановлені для СУІБ.

Далі описаний цикл управління ризиками переходить на новий виток, знову проходячи стадії Планування, Реалізації, Моніторингу та Вдосконалення. Процес функціонування, розвитку і вдосконалення СУІР реалізується по спіралі. В кінцевому підсумку всі чотири групи процесів виконуються паралельно і безперервно. Вихідні дані одних процесів надходять на вхід інших [16].

Діяльність з управління ризиками

Після початку реалізації плану обробки ризиків необхідно здійснювати безперервну діяльність з управління ризиками, яка включає в себе наступні процеси:

- супровід і моніторинг;
- аналіз з боку керівництва;
- аудит;
- управління документами;
- коригувальні та запобіжні заходи;

Супровід і моніторинг механізмів безпеки

Більшість механізмів безпеки вимагають супроводу і адміністрування протягом усього періоду їх існування. Впроваджені механізми контролю повинні регулярно відслідковуватися і аналізуватися для того, щоб гарантувати їх коректне та ефективне функціонування, а також те, що зміни середовища функціонування не знижують їх ефективності. Існує тенденція до погіршення, з часом, продуктивності будь-якого сервісу або механізму. Моніторинг призначений для виявлення цих погіршень і ініціювання коригувальних дій.

Дії з моніторингу та супроводу повинні плануватися і виконуватися на регулярній основі, відповідно до розкладу. Таким чином можуть бути мінімізовані накладні витрати і збережена ефективність механізмів безпеки.

Взаємозв’язок процесів аудиту та управління ризиками

Повинен бути розроблений графік проведення незалежної стороною регулярних внутрішніх аудитів. Незалежна сторона не обов'язково повинна бути зовнішньої по відношенню до організації. Аудити, що проводяться зовнішнім

органом, є обов'язковими для проходження сертифікації по ISO 27001, а також для акціонерних товариств, фінансових організацій та інших організацій згідно з вимогами законодавства. Внутрішні аудитори не повинні бути підконтрольні тим, хто несе відповідальність за повсякденне управління СУІБ. У разі, коли при внутрішніх аудитів виявляється необхідність у вживанні заходів по коригуванню СУІБ, ці заходи повинні бути задокументовані в повному обсязі, а також повинна бути визначена відповідальність і встановлені терміни[9].

Управління документами та записами

Для експлуатації та супроводу СУІБ необхідна повна, доступна і коректна документація, а також контрольований процес управління документами, область дії і рівень деталізації для різних організацій може варіюватися. Відповідальність за здійснення нагляду над процесом управління документацією повинна бути чітко визначена й узгоджена.

Управління документами та записами включає в себе:

1) контроль і захист документів і записів;
2) твердження, аналіз і коригування документів;
3) ідентифікація змін і статусу поточних версій;
4) забезпечення доступності, передачі, зберігання і знищення документів і записів;
5) ідентифікація застарілих документів і документів, що мають зовнішнє походження;
6) контроль над розповсюдженням документів;
7) запобігти ненавмисному використанню застарілих документів.

3.3. Етапи побудови СУІБ

Методологія аналізу ризиків

Метою процесу оцінки ризиків є визначення їх характеристик в інформаційній системі і її ресурсах. На підставі таких даних вибираються необхідні засоби управління інформаційною безпекою.

Перед тим як вносити пропозиції щодо якихось технічних рішень для системи ІБ, необхідно розробити політику безпеки для нього.

Саме політика безпеки організації описує процедуру надання та користування правами доступу для користувачів та правила щодо звітності про дії користувачів в плані безпеки.

Ефективність системи ІБ об'єкта досягається у випадку, якщо вона тісно співпрацює з правилами політики безпеки, і навпаки. Кроки для побудови політики безпеки організації:

1. впровадження автоматизації структури вартості та аналізу ризиків в опис об'єкта;

2. визначення правил будь-якого процесу використання цього типу доступу до ресурсів об'єкта автоматизації, які мають таку ступінь цінності.

3. організаційна політика безпеки формується у вигляді документа, який узгоджується з замовником, затверджується.

3.3.1. Етапи розробки системи управління ІР

1. Розробка концепції інформаційної безпеки. Визначено основні цілі, завдання та вимоги, а також загальна стратегія побудови системи ІВ. Критичні інформаційні ресурси визначені. Розроблено вимоги до системи управління ІР і визначені основні підходи до їх реалізації.

2. Створення / розвиток політики СУІР.

3. Побудова моделі системи управління ІР (на основі процесно-рольової моделі).

4. Підготовка технічного завдання на створення системи інформаційної безпеки.

5. Створення моделі системи управління ІР.

6. Розробка технічно-робочого проекту (ТРП) створення СУІР і архітектури системи управління ІР. ТРП зі створення системи управління ІР включає наступні документи:

— Пояснювальну записку, що має включати в себе опис основних технічних рішень для створення системи ІБ і організаційних заходів щодо попередньої підготовки СІБ до експлуатації.

— Обґрунтування обраних елементів системи управління ІР і вибір місця їх розположення.

— Специфікацію на комплекс технічних засобів СУІР.

— Специфікацію на комплекс програмних засобів СУІР.

— Встановлення параметрів та режиму роботи складових СУІР.

7. Тестування на стенді спроектованої системи управління ІР.

8. Створення організаційно-розпорядчих документів СУІР (політик забезпечення ІБ, процедур, регламентів і ін.).

9. Розробка робочого проекту (включаючи документацію на використовувані засоби захисту і порядок адміністрування, план введення системи управління ІР в експлуатацію та ін.), Планування навчання користувачів і обслуговуючого персоналу інформаційної системи [18].

Рис.3.2. Етапи розробки системи управління ризиками

Впровадження СУІР

Після проведення повного тестування спроектованої системи управління ІР, можна приступати до її впровадження. Роботи по впровадженню системи включають виконання наступних завдань:

— поставку програмних і технічних засобів захисту інформації;

— інсталяцію програмних компонентів;

— настройку всіх компонентів і підсистем;

— проведення приймально-здавальних випробувань;
— впровадження системи управління ІР;
— навчання користувачів;
— введення СУІР в промислову експлуатацію.

3.4. Принципи створення системи управління інформаційними ризиками

До процесу впровадження СУІР входять такі пункти, як оцінка нинішнього стану інформаційного забезпечення захисту інформації, складання переліку заходів підтримання оптимального рівня ІБ базуючись на оцінюванні ризиків. Наступним кроком після виявлення всіх вимог ІБ потрібно обрати й використовувати заходи управління так, щоб забезпечити зниження рівня ризиків від реалізації несанкціонованого доступу. Засоби управління можна обирати використовуючи стандарти чи інші документи та заходи управління, які визначені для цього класу систем, або можна самостійно розробити, щоб закрити потреби організації відповідно до обраної політики ІБ.

3.4.1. Оцінка та оброблення ризиків

При оцінці ризиків обов’язково повинен бути наявний системний підхід до аналізування ризику та порівняння кількісної оцінки ризиків з критеріями ризику для визначення ризику. Для врахування мінливості вимог ІБ і швидкості утворення нових ризиків, потрібно періодично проводити оцінку ризиків. Сама процедура оцінки ризиків повинна бути системною та однакою, щоб мати можливість однаково кількісно оцінити отримані результати за різний період, провести їх порівняння та відзначити позитивну чи негативну динаміку в використанні засобів захисту ІС.

Загалом, сама суть оцінки ризику базується на визначенні рівня цього ризику шляхом призначення йому за обраним методом певного значення та порівняння цього значення з встановленим максимально допустимим. Методика оцінки ІР в ІС буде базуватись на описаній методиці, проте для оцінки СУІБ будемо використовувати оцінні вимоги, що визначені стандартом ISO/IEC 27001

(табл. 3.1) [9]. Безпосередньо саму модель загроз та вразливостей будемо будувати базуючусь на типових вразливостях ІБ згідно з ISO/IEC 27002 (табл. 3.2) [10].

Таблиця 3.1.

Вимоги до інформаційної безпеки

№	Розділ основних вимог до ІБ	Вимоги до ІБ
1.	Загальні вимоги до СУІБ	1.1. СУІБ створена
		1.2. СУІБ впроваджена
		1.3. СУІБ знаходиться в експлуатації
		1.4. Здійснюється моніторинг СУІБ
		1.5. СУІБ аналізується
		1.6. СУІБ удосконалюється
2.	Створення й управління СУІБ	2.1. Визначені сфери дії та межі СУІБ
		2.2.Визначення дій СУІБ у виняткових ситуаціях
3.	Політика безпеки	3.1. Містить у собі основу для визначення її цілей
		3.2. Встановлює загальні напрямки та принципи діяльності
		3.3. Враховує вимоги підрозділу
		3.4. Враховує вимоги законодавства та нормативної бази
		3.5. Враховує конкретні обов’язки в сфері безпеки
		3.6. Поєднується зі стратегічним контекстом управління ризиками в організації, у якій буде створюватися СУІБ
		3.7. Встановлює критерії для оцінювання ризиків
		3.8. Затверджена керівництвом
4.	Активи	4.1. Наявні реєстри інформаційних активів
		4.2. Власники активів правильно ідентифіковані

Продовження таблиці 3.1.

Вимоги до інформаційної безпеки

№	Розділ основних вимог до ІБ	Вимоги до ІБ
4.	Активи	4.3. Наявні правила маркування конфіденційних документів
		4.4. Наявні правила поведінки з конфіденційними документами
		4.5. Наявна схема класифікації документів

Таблиця 3.2.

Модель загроз та вразливостей

Галузь безпеки	Вразливість	Загроза, що використовує дану вразливість
Безпека кадрових ресурсів (ISO/IEC 27002:2005, розділ 8)	1.1.Недостатній рівень навчання персоналу щодо безпеки	1.1.Помилка персоналу технічної підтримки
	1.2. Неосвіченість користувачів у питаннях безпеки	1.2.Помилка користувачів
	1.3.Відсутність політики безпеки в сфері коректного використання засобів телекомунікацій та передачі повідомлень	1.3.Відсутність політики безпеки в сфері коректного використання засобів телекомунікацій та передачі повідомлень
	1.4.Права доступу залишаються в працівника навіть після звільнення	1.4. Несанкціонований доступ
	1.5. Невмотивований та незадоволений персонал	1.5. Зловживання засобами обробки інформації
Фізична безпека і безпека навколишнього середовища (ISO/IEC 27002:2005, розділ 9)	2.1.Відсутність фізичного захисту будівлі, дверей та вікон	2.1. Грабіж
	2.2.Розміщення обладнання в зоні, якій загрожує затоплення	2.2. Затоплення
	2.3.Незахищене зберігання інформації	2.3. Грабіж

Продовження таблиці 3.2.

Модель загроз та вразливостей

Галузь безпеки	Вразливість	Загроза, що використовує дану вразливість
Фізична безпека безпека навколишнього середовища (ISO/IEC 27002:2005, розділ 9)	2.4.Відсутність схеми періодичної заміни обладнання	2.4. Закінчення терміну експлуатації засобів зберігання інформації
	2.5. Стрибки напруги	2.5.Флуктуація електроживлення
	2.6.Нестабільне електроживлення (подача електроенергії)	2.6.Флуктуація електроживлення
Управління комунікаціями та операціями (ISO/IEC 27002:2005, розділ 10)	3.1.Складний користувацький інтерфейс	3.1.Помилка персоналу
	3.2. Передача або повторне використання засобів зберігання інформації без потрібного очищення	3.2.Несанкціонований доступ
	3.3.Неадекватний контроль змін	3.3.Збій системи безпеки
	3.4.Неадекватне керування мережею	3.4.Перенавантаження трафіка
	3.5. Відсутність розподілу обов’язків	3.5. Зловживання системою (випадкове чи навмисне)
	3.6. Відсутність процедур резервного копіювання	3.6. Відсутність процедур резервного копіювання
	3.7.Відсутність оновлень програмного забезпечення.	3.7. Вірусне ураження
	3.8. Неконтрольоване копіювання	3.8. Грабіж
Контроль доступу (ISO/IEC 27002:2005, розділ 11)	4.1.Некоректне розмежування доступу в мережах	4.1.Несанкціоноване під’єднання до мережі
	4.2.Відсутність механізмів ідентифікації та аутентифікації	4.2. Присвоєння чужого користувацького ідентифікатора

Продовження таблиці 3.2.

Модель загроз та вразливостей

Галузь безпеки	Вразливість	Загроза, що використовує дану вразливість
Контроль доступу (ISO/IEC 27002:2005, розділ 11)	4.3. Відсутня чи некоректна політика контролю доступу	4.3.Несанкціонований доступ до інформації, системи чи програмного забезпечення
	4.4.Відсутність чи недостатнє тестування програмного забезпечення	4.4.Використання програмного забезпечення неавторизованими користувачами
	4.5.Незадовільне керування паролями	4.5.Присвоєння чужого користувацького ідентифікатора
	4.6.Відсутність захисту мобільного комп’ютерного устаткування	4.6.Відсутність захисту мобільного комп’ютерного устаткування
	4.7.Відсутність “виходу із системи”, коли залишають робоче місце	4.7.Відсутність “виходу із системи”, коли залишають
	4.8.Відсутність контролю прав доступу користувачів	4.8. Доступ зі сторони користувачів, які звільнились
	4.9.Відсутність відключення та зміни стандартних попередньо встановлених облікових записів та паролів	4.9.Несанкціонований доступ до інформації, системи чи програмного забезпечення
	4.10.Неконтрольоване використання системних утиліт	4.10.Обхід механізмів контролю системи чи додатка

Також, розглянемо особливості представлення оцінок ризиків інформаційної безпеки картами ризику. На практиці така карта відображається координатною площино. Її осями позначено параметри ризику інформаційної безпеки. Це ймовірність реалізації загрози та величина втрат. Завдяки цьому

визначається прийнятність окремого або групи ризиків інформаційної безпеки. Вона встановлюється шляхом вибору шкали оцінювання (якісної, кількісної або якісно-кількісної); розмірності карти ризику (рівнорозмірна, різнорозмірна). При використанні як рівнорозмірних, так і різнорозмірних карт ризиків інформаційної безпеки здебільшого використовуються лінгвістичні шкали оцінювання (наприклад, “дуже низька”, “низька”, “середня”, “висока”, “дуже висока”). Такий підхід обмежується складністю зіставлення вірогідних оцінок параметрів ймовірності реалізації загрози та величини втрат.

3.4.2. Рівнорозмірні карти ризиків типу nxn. Приклад застосування лінгвістичних значень ризиків.

Розглянуто як приклад тільки якісне завдання імовірної реалізації загрози та вартості втрат. Надано наступні лінгвістичні значення за зростанням величини: “Дуже низька”, “Низька”, “Середня”, “Висока”, “Дуже висока” (див. рис. 3.3). Комбінаційні значення виникають на перетині мовних і лінгвістичних стовпців, наприклад: “Дуже низька·/ Дуже висока”, “Дуже висока·/ Дуже висока”. Отримання добутку лінгвістичних змінних ризику потребує застосування теорії нечітких множин що, за відсутності відповідної статистики ускладнено. Перехід до чітких визначень оцінок імовірності, або ступеню впливу здійснюється якщо при застосуванню лінгвістичної шкали оцінок до кожного логічного терму відповідає класична чітка оцінка (1, 2, 3, ...), яка і буде визначати одну з меж (ліву або праву) інтервалу оцінювання у випадку нечітких знань експертів. При цьому, якщо знання (оцінки) є чіткими, то права границя буде співпадати з лівою [7] - [10].

Ймовірність інцидентного сценарію / Ступень впливу	Дуже низька	Низька	Середня	Висока	Дуже висока
Дуже висока	ДНхДВ	НхДВ	Сх	Вх	ДВх
Висока	ДНхВ	НхВ	СхВ	ВхВ	ДВхВ
Середня	ДНхС	НхС	СхС	ВхС	ДВхС
Низька	ДНхН	НхН	СхН	ВхН	ДВхН
Дуже низька	ДНхДН	НхДН	СхДН	ВхДН	ДВхДН

Рис.3.3 Вигляд “Карти ризиків” при задаванні лінгвістичних критеріїв

В такому випадку на перетині кожного стовпчика та кожного рядку записується добуток значень, які надані відповідному стовпчику, і відповідному рядку виходячи з визначення ризику. Для візуального поділу множини ризиків на підмножини прийнятних та неприйнятних ризиків, використовуються такі кольорові позначення: зеленим визначаються прийнятні ризики, червоним – неприйнятні. Таким чином, цей спосіб залежним від знань, навичок, рівня підготовки та досвіду експертів[7].

Висновок до розділу 3

Розроблено методологію щодо покращення побудови системи управління інформаційною безпекою. Особливу увагу треба виділити знаходженню та оцінки ризиків, загроз та можливих матеріальних та репутаційних втрат організації, щоб правильно оцінити економічну доцільність побудови СУІР. Для управління будь-якої складної системи необхідно створити жорсткий, але простий регламент обслуговування цієї системи і забезпечити контроль за тим, щоб настройки системи змінювалися відповідно до цього регламенту, застосовності до забезпечення безпеки інформаційної системи, це можна уявити так:

1) Мати в наявності політику безпеки, в якій повинно бути чітко описано, хто і на якій підставі повинен мати доступ до ресурсів інформаційної системи.

2) Мати єдину точку взаємодії співробітників організації з інформаційною системою, через яку вони зможуть формулювати свої побажання на надання доступу до тих чи інших ресурсів інформаційної системи.

3) Мати інструменти контролю основних показників функціонування інформаційної системи.

4 АЛГОРИТМ АНАЛІЗУ РИЗИКІВ

В даному розділі запропоновано алгоритм управління ризиками, який складається з декількох послідовних етапів, таких як виявлення ризиків, їх мінімізація та прийняття.

4.1. Алгоритм виявлення ризиків

В час розвитку та впровадження сучасних інформаційних технологій та засобів більшість організацій та підприємств, як державних так і комерційних, потребують більшого захисту від загроз інформаційній безпеці, які можуть призвести до деструктивного впливу як на саму організацію, так і на державу в цілому. Менеджмент інформаційної безпеки є ключовою частиною будь-якої організації, яка свідомо ставиться до своєї діяльності. Основою менеджменту інформаційної безпеки є декілька ключових понять, таких як управління інформаційними ризиками та управління доступом. Тому визначення чітких етапів дій в ході менеджменту інформаційної безпеки є дуже актуальним питанням.

Основним завданням, яке було поставлене на виконання даної магістерської роботи, було розробити універсальний алгоритм аналізу ризиків, який був би прийнятний для будь якої організації або підприємства.

На рисунку 4.1 представлена схема основного завдання даної магістерської роботи.

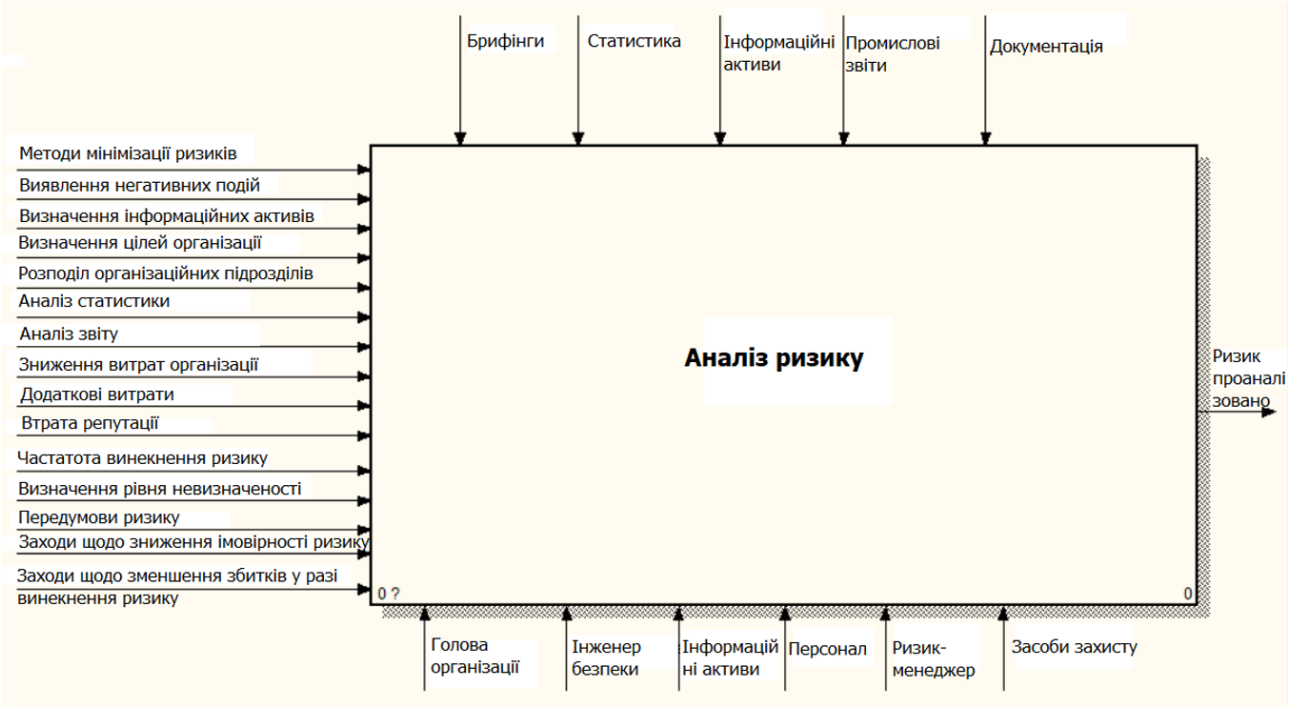


Рис. 4.1. Загальна схема задачі

На даній схемі ми можемо побачити основний блок, який являє собою аналіз ризиків. Зліва стрілками показано основні дії, які необхідно виконати в ході кожного з запропонованих етапів розробленого алгоритму аналізу ризиків. Знизу було визначено виконавців, які приймають участь у процесі аналізу ризиків. Стрілки зверху являються матеріальними потоками які використовуються в ході виконання алгоритму. І в заключенні на виході даної системи ми маємо проаналізовані ризики.

На рисунку 4.2 представлена схему розробленого алгоритму реагування на ризики інформаційної безпеки.

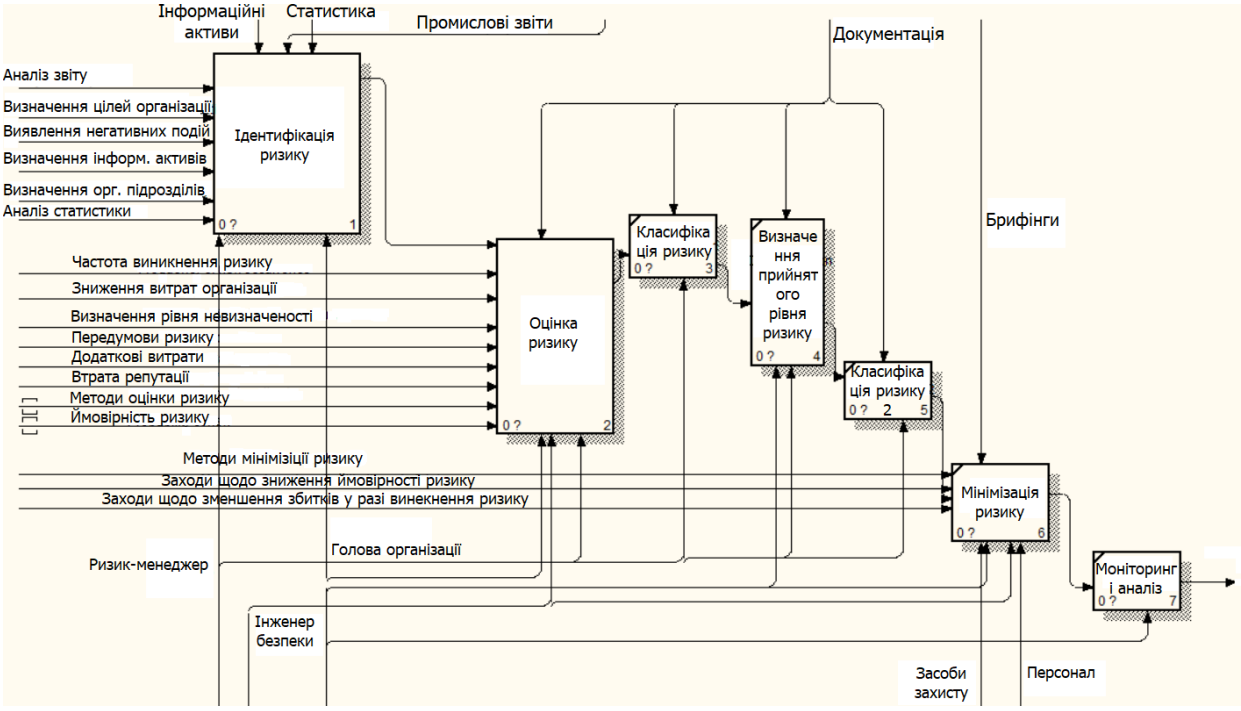


Рис. 4.2. Алгоритм аналізу ризиків інформаційної безпеки

За основу розробленого алгоритму було взято поняття з ISO 27000 та 31010, структуровано ці поняття та визначено порядок дій аналізу ризиків організації/підприємства.

Першим етапом аналізу ризиків мною було визначено виявлення ризиків. Цей етап є дуже суттєвим та важливим, оскільки правильне, точне та повне визначення ризиків є ключем для своєчасної реакції та реагування на можливі ризики інформаційної безпеки, які можуть виникнути. Після кожного з етапів необхідно перевірити чи виконана основна мета даного етапу і тільки тоді переходити до наступного етапу.

Якщо даний етап проведено не точно, неправильно і неповністю, то існує велика ймовірність того, що організація/підприємство зазнає подальших втрат.

Після виявлення та визначення ризику ключовим моментом є його оцінка. На даному етапі чітко визначаються можливі втрати та ймовірність виникнення ризику. Суттєво важливим є правильний підхід до виконання цього етапу. Адже точна оцінка ризику дає у майбутньому можливість правильно мінімізувати та визначити прийнятні для організації/підприємства ризики.

Наступним етапом в запропонованому алгоритмі є класифікація ризиків за чинниками, для більш згрупованої їх мінімізації на наступних етапах. Тут ризики поділяються на виникнення від зовнішніх і внутрішніх чинники.

Внутрішні чинники напряму залежать від організації/підприємства. Як приклад, некваліфіковані співробітники, неправильне обладнання засобами захисту, тощо.

Зовнішні чинники це чинники, які напряму не залежать від організації/підприємства. До цих чинників належать стихійні лиха, вплив конкурентів, тощо.

Після визначення, оцінки та класифікації ризиків організація визначає прийнятний рівень ризику. Прийнятний ризик – це ризик, рівень якого допустимий і обґрунтований виходячи з соціально-економічних міркувань.

Наступним етапом після визначення прийнятного рівня ризику було визначено етап класифікації ризику за критерієм прийнятний/неприйнятний. Далі робота піде з неприйнятними ризиками, на які необхідно реагувати. Реагування на ризики можливе декількома шляхами.

Після того, як спеціалісти відреагували на ризик, а саме було максимально мінімізовано вплив і ймовірність ризику, необхідно знову його класифікувати на прийнятний і неприйнятний. Якщо навіть після мінімізації ризику будь-яким з відомих методів він все ще являється для організації таким, який несе високу загрозу, то такий ризик вважається умовно прийнятним, тобто організація/підприємство умовно приймає даний ризик як такий, від якого неможливо позбутися, або зменшити його. Умовно прийнятні ризи у майбутньому обробляються на сьомому етапі запропоновано алгоритму. Тобто за ними йде спостереження та аналіз їх у майбутньому відповідальною особою, з метою попередження їх появи.

4.2. Виявлення та оцінка ризиків

Першим етапом в аналізі ризиків є його виявлення. Виявлення ризиків досить складний процес, адже потребує правильного визначення інформаційних активів та аналізу багатьох компонентів побудови організації/підприємства.

Виявлення ризиків пропонується ділити на два етапи. Перший етап являє собою визначення інформаційних активів організації (рис.4.3).

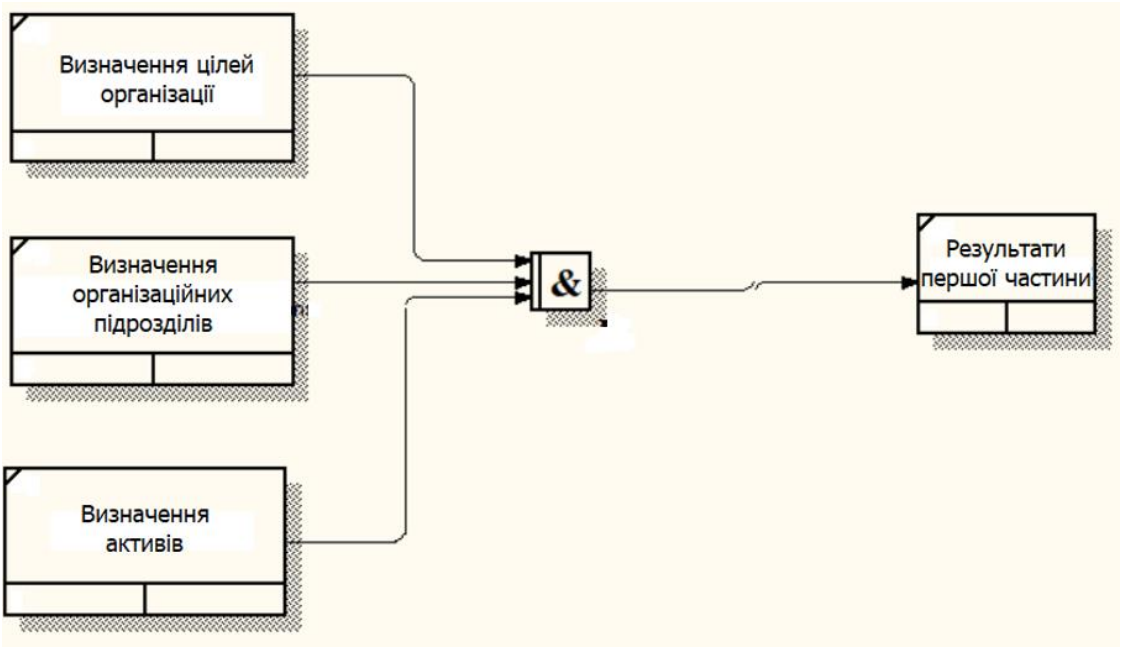


Рис. 4.3. Алгоритм визначення інформаційних активів організації

На першому етапі спеціалістами визначається основна мета організації, відповідно до якої компанія розділяється на логічні компоненти – відділи та підрозділи. Кожен відділ і підрозділ мають свої інформаційні активи. Спеціалісти виділяють ці активи відповідно до виконання завдань компанії. Після визначення інформаційних активів до кожного активу застосовується етап визначення негативних чинників, які можуть на нього впливати (рис.4.4).

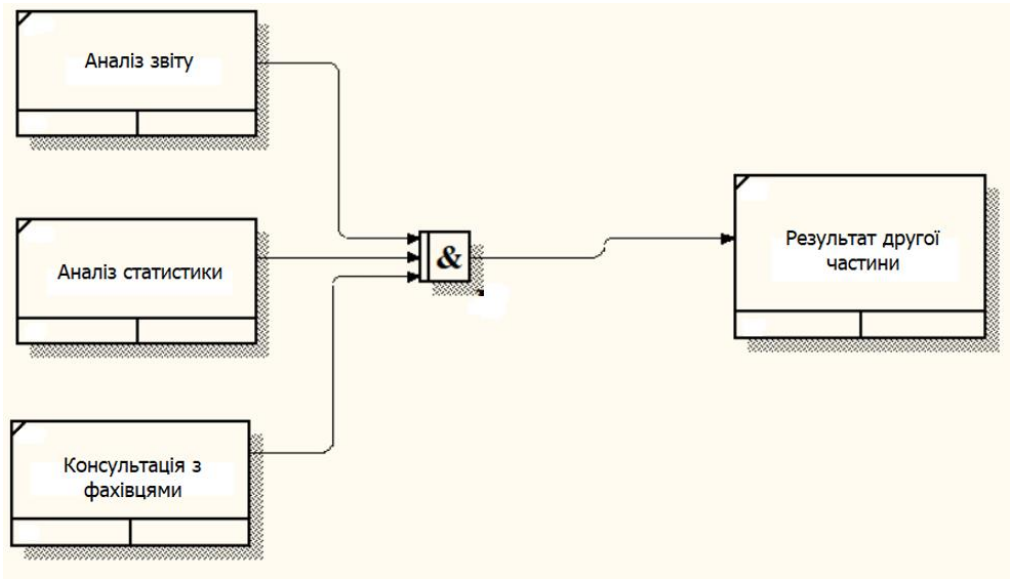


Рис. 4.4. Алгоритм визначення негативних чинників, що впливають на інформаційні активи

Негативні чинники визначаються шляхом аналізу статистичних даних та аналізу галузевих звітів підрозділів – ці два етапи виконуються всередині компанії керівником, або відповідним підрозділом. Незайвим буде обговорення можливих ризиків з галузевими спеціалістами.

Після того, як ризик було визначено, він потребує точної оцінки для визначення подальших дій. Оцінювати ризик також пропонується в два етапи. Першим етапом є визначення можливих втрат (рис 4.5).

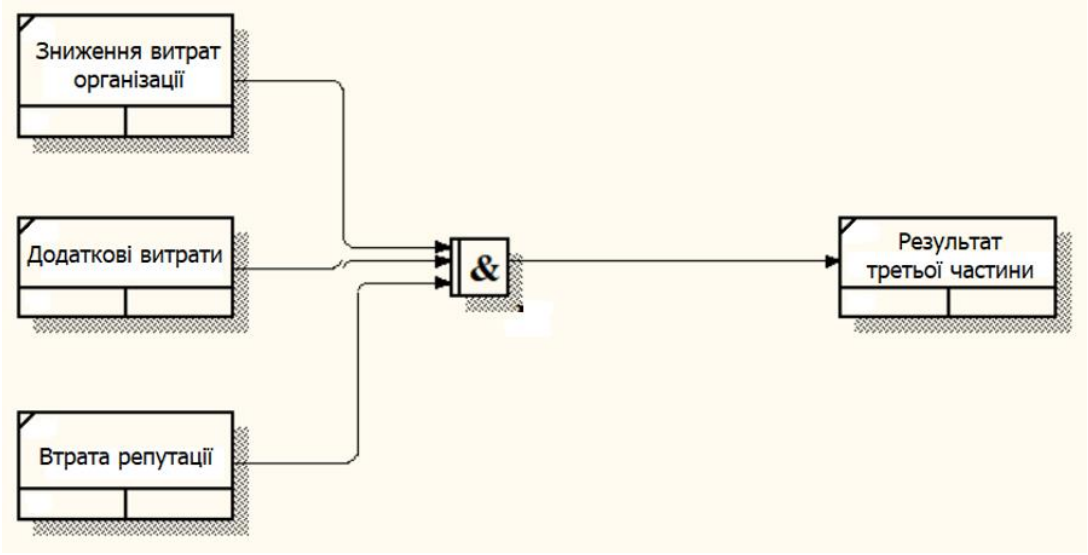


Рис. 4.5. Визначення втрат

В залежності від сфери діяльності підприємство може мати різні втрати після можливої реалізації ризику. До таких втрат належать зниження вартості підприємства, додаткова витрата коштів на поновлення роботи та, як варіант збиток репутації. В державних установах, або установах, які є об’єктами критичної інфраструктури втрати можуть бути набагато більшими і тягти за собою більші наслідки, як приклад порушення державної таємниці.

Другим етапом оцінки ризику є оцінка ймовірності того, що ризик буде реалізовано (рис.4.6).

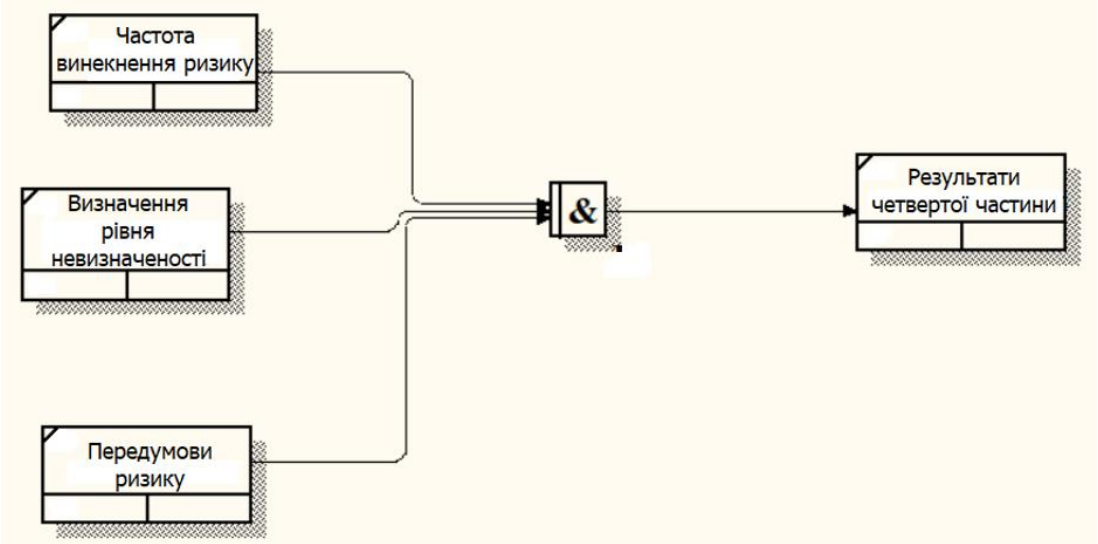


Рис. 4.6. Ймовірність реалізації ризику

До другого етапу можна віднести визначення частоти реалізації ризику. Тобто підрахування числової кількості реалізації визначеного ризику. Наступним визначається ступінь невизначеності. Чим більша невизначеність під час прийняття рішення керівником, тим більший ступінь ризику. І останнім визначаються передумови настання ризику, які в подальшому можна буде змінювати в етапі мінімізації[33].

Аналіз ризиків можливий за допомогою достатньо великого переліку методів, які наведені у (ДСТУ IEC/ISO 31010:2013).

4.3. Знешкодження ризиків

Плануючи реагування на ризики, важливо зіставляти вартість наслідків їх матеріалізації та вартість заходів щодо реагування. Економічна суть управління ризиками зводиться до вибору антиризикових заходів, які стоять менше, ніж наслідки ризику, але при цьому зводять ймовірність або вплив ризику на проект до мінімального значення (в ідеалі – до нуля). Тому ми повинні опрацювати кілька варіантів антиризикових заходів та вибрати оптимальні.

У літературі з управління проектами найчастіше описуються чотири стратегії роботи з ризиками: стратегія ухилення, стратегія передачі, стратегія зниження (або мінімізації) та прийняття ризику.

Стратегія ухилення передбачає повне виключення ризику із проекту. Ми повинні вигадати реагування, яке дозволить бути впевненими, що ризик не

матеріалізується. Це «найдорожча» стратегія, так як для деяких ризиків вона змушує відмовлятися від певних робіт, змінювати цілі проекту або, в самому радикальному випадку, відмовлятися від проекту.

Стратегія передачі перекладає наслідки матеріалізації ризику та відповідальність за реагування на третю сторону, причому сам ризик не усувається. Ця стратегія практично завжди передбачає фінансові витрати на передачу та отримання фінансової компенсації у разі матеріалізації ризику.

Стратегія зниження найпоширенішою може застосовуватися до будь-якого ризику, так як передбачає зменшення ймовірності або впливу ризику на проект. Ну і четверта стратегія - це прийняття ризику.

В даній роботі управління ризиками полягає в їх мінімізації, а саме: зменшення ймовірності виникнення ризику та зменшення втрат в разі реалізації ризику.

Мінімізація ризиків має бути рентабельною, тобто на її реалізацію має витрачатись менше коштів ніж можливий збиток від даного ризику.

4.4. Приклад реалізації алгоритму аналізу ризиків

Для прикладу реалізації запропонованого алгоритму, організацією було обрано НТУУ КПІ імені Ігоря Сікорського. Для наглядного представлення було обрано один інформаційний актив, а саме сервери навчального ситуаційного центру з кібербезпеки.

Приклад буде реалізований за схемою представленою на рисунку 4.7 – 4.8.

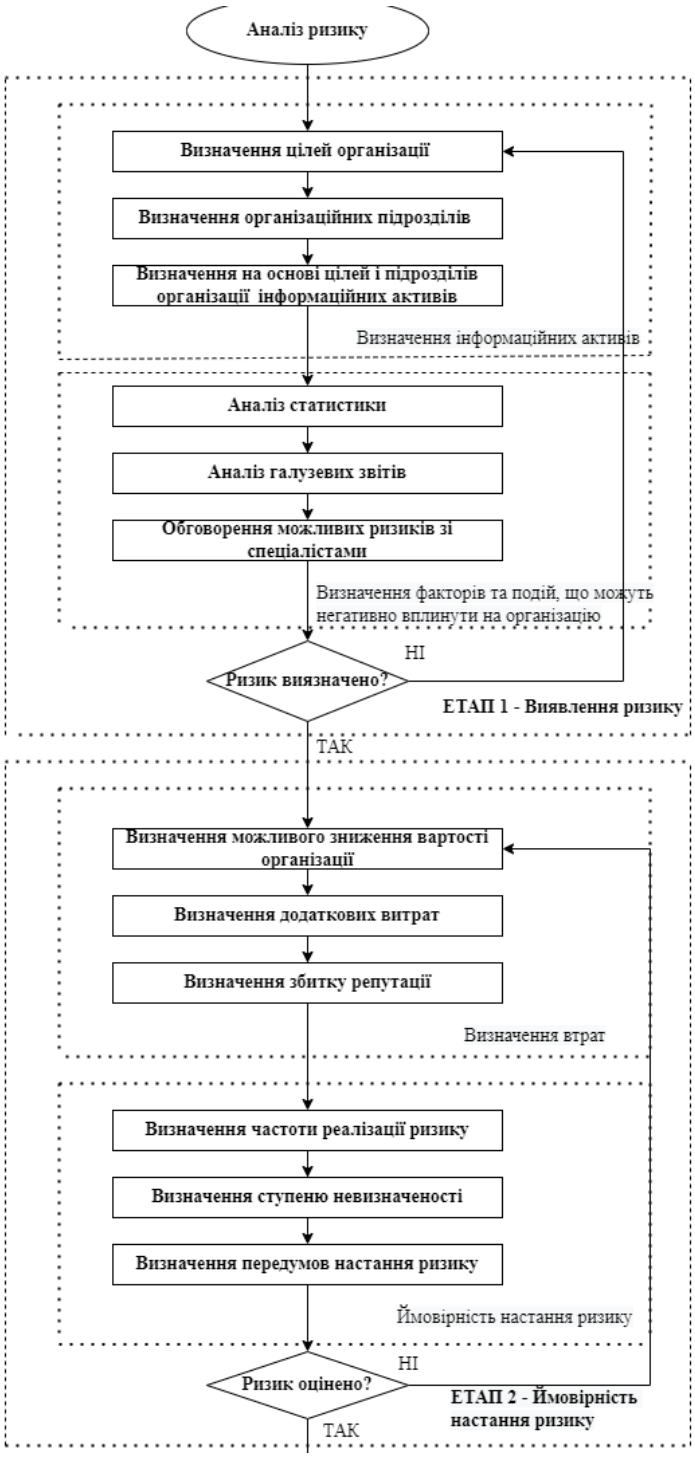


Рис. 4.7. Схема реалізації прикладу (частина перша)

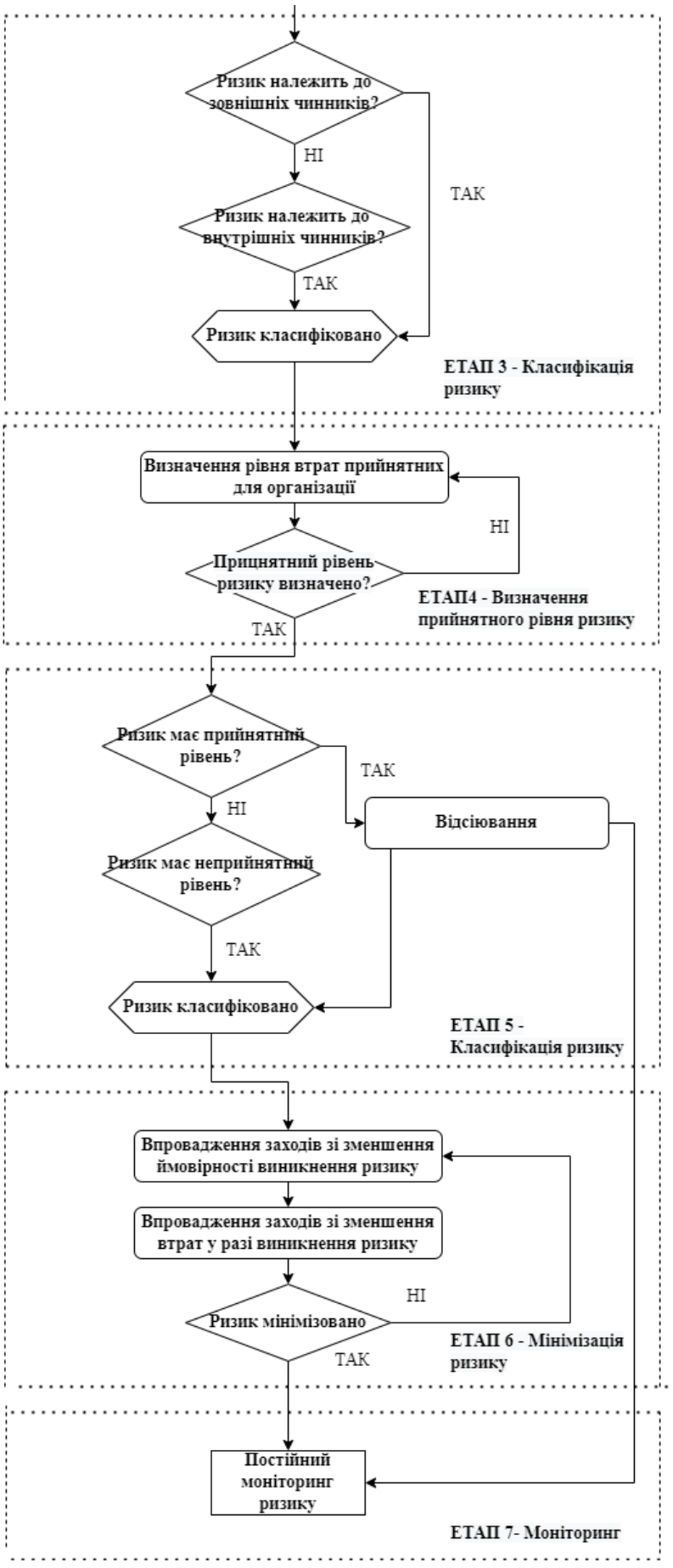


Рис. 4.8. Схема реалізації прикладу (друга перша)

І ЕТАП. Виявлення ризику:

1.1. Ідентифікування Інформаційного активу: сервери навчального ситуаційного центру з кібербезпеки.

1.2. За статистикою визначено, що основними видами небезпеки, які властиві даному інформаційному активу, є неспроможність протистояти вогню, воді та помилкам конфігурування.

1.3. Ідентифікування загроз:

- Інсайдери в підрозділі;
- Коротке замикання ;
- Пожежа;
- Неправильне використання серверів;
- Проникнення сторонніх осіб;
- Затоплення;
- Стихійне лихо.

ІІ ЕТАП. Оцінка ризику:

2.1. Ідентифікування наслідків(втрат):

- Зупинка функціонування Кіберцентру;
- Витрачання коштів на відновлення функціонування серверів;
- Втрата статусу перед керівництвом.

2.2. Ідентифікування ймовірності реалізації ризику:

- Інсайдери в підрозділі – дуже низька ймовірність;
- Коротке замикання – середня ймовірність ;
- Пожежа – низька ймовірність;
- Неправильне використання серверів – середня ймовірність;
- Проникнення сторонніх осіб – низька ймовірність;
- Затоплення – низька ймовірність;
- Стихійне лихо – низька ймовірність.

Оцінка ризику вираховується за формулою: R=YP.

Y – втрати нанесені в результаті настання ризику.

P– ймовірність настання ризику.

Таблиця 4.1.

Оцінка ризиків

РИЗИК	ОЦІНКА РИЗИКУ
Інсайдери в підрозділі	7
Коротке замикання	35
Пожежа	16
Неправильне використання серверів	48
Проникнення сторонніх осіб	8
Затоплення	14
Стихійне лихо	8

Числові показники оцінки ризиків взяті з розрахунку на те, що максимальний рівень небезпеки і ймовірність реалізації ризику рівні 8. До уваги брались вже існуючі системи захисту (протипожежна система, замок у дверях, тощо).

III ЕТАП. Класифікація ризику:

Всі ризики окрім стихійного лиха є внутрішніми і потребують мінімізації всередині організації.

IV ЕТАП. Визначення рівня прийнятного ризику:

Прийнятний ризик визначено як середній, або той, що має числові показники оцінки нижче 30.

V ЕТАП. Класифікація ризику:

Таблиця 4.2– Класифікація ризиків

РИЗИК	ОЦІНКА РИЗИКУ
Інсайдери в підрозділі	7
Проникнення сторонніх осіб	8
Стихійне лихо	8
Затоплення	14
Пожежа	16
Коротке замикання	35
Неправильне використання серверів	48

Ризики виділені жовтим кольором являються неприйнятними і потребують подальшої роботи з ними.

VI ЕТАП. Мінімізація ризику:

Для мінімізації ризику виникнення короткого замикання і можливості неправильного використання серверів необхідно:

1. Проведення навчань з особовим складом стосовно використання обладнання.

2. Проведення інструктажів керівниками підрозділів.

3. Проведення іспитів з особовим складом з питань використання обладнання.

4. Проведення технічної перевірки прокладених кабелів.

5. Встановлення автоматів вимкнення живлення.

6. Встановлення запобіжників.

7. Встановлення надійної протипожежної системи.

VII ЕТАП. Моніторинг ризику:

Після проведення мінімізації ризиків ті ризики, які залишились неприйнятними, потребують постійного моніторингу, а ті ризики, які є прийнятними потребують періодичного контролю.

Висновок до розділу 4

У зв’язку з постійною модернізацією і зростанням загроз інформаційній безпеці необхідним постає питання точного та правильного аналізу можливих ризиків. Для реалізації даного завдання в цьому розділі було представлено розроблений алгоритм аналізу ризиків з чітким визначенням етапів дій в ході проведення менеджменту інформаційної безпеки.

До основних етапів аналізу ризиків було віднесено виявлення ризиків, як перший і важливий етап, так як у майбутньому саме від цього етапу залежить подальший аналіз ризиків. Наступним етапом було визначено надання оцінки ризику, для майбутньої класифікації ризиків на прийнятні і неприйнятні.

На прикладі реалізації даного алгоритму було показано, що він є ефективним і всі етапи, які використовуються в даному алгоритмі є актуальними.

Основним завданням, яке було поставлене на виконання даної магістерської роботи, було розробити універсальний алгоритм аналізу ризиків, який був би прийнятний для будь якої організації або підприємства.

ВИСНОВКИ

В ході виконання магістерської роботи, було розглянуто сутність оцінювання ризиків інформаційної безпеки, наслідком яких, телекомунікаційні підприємства, організації, можуть понести як фінансові так і іміджеві збитки, а ще більшою загрозою виступає саме витік інформації. Тому основним завданням, яке було поставлене на виконання даної магістерської роботи, було розробити універсальний алгоритм аналізу ризиків, який був би прийнятний для будь якої організації або підприємства.

Для досягнення поставленої мети в першому розділі було проаналізовано сучасні методи та можливості інформаційної безпеки, виділені підходи оцінювання ризиків інформаційної безпеки. Описано основні переваги та недоліки існуючих моделей оцінювання ризиків інформаційної безпеки.

У другому розділі розглянуто методики моделювання та оцінки інформаційних ризиків, виявлено, що основним способом забезпечення безпеки є аналіз інформаційної системи на наявність ризиків нанесення шкоди інформаційним ресурсам, розглянуто найбільш поширені методи аналізу ризиків.

У третьому розділі побудована система управління інформаційними ризиками, надано рекомендації щодо управління будь-якої складної системи необхідно створити жорсткий, але простий регламент обслуговування цієї системи і забезпечити контроль за тим, щоб настройки змінювалися відповідно до цього регламенту.

У четвертому розділі було представлено розроблений алгоритм аналізу ризиків з чітким визначенням етапів дій в ході проведення менеджменту інформаційної безпеки. На прикладі реалізації даного алгоритму було показано, що він є ефективним і всі етапи, які використовуються в даному алгоритмі є актуальними.

Отже мета дипломної роботи щодо побудови алгоритму аналізу ризиків, який був би прийнятний для будь якої організації або підприємства досягнута в повному обсязі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Bliss C. I. The Method of Probits / C. I. Bliss // Science. – 1934. – Vol. 79. – № 2053. – P. 409–410.
2. Information technology — Security techniques — Information security management systems — Overview and vocabulary: ISO/IEC 27000:2009. — [Чинний від 01-05-2009]. — Женева: [б.в.], 2009. — 26 с. — (Міжнародні стандарти ISO/IEC).
3. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process / Richard A. Caralli, James F. Stevens, Lisa R. Young, William R. Wilson. − Carnegie Mellon University, 2008. – 154 p.
4. ISO / IEC 27005 - Information security risk management.
5. James J. Cebula A Taxonomy of Operational Cyber Security Risks / James J. Cebula, Lisa R. Young. – Hanscom AFB, MA: Carnegie Mellon University. – 47 p.
6. Maria Garnaeva. Kaspersky Security Bulletin 2015. Overall statistics for2015 / [Maria Garnaeva, Jornt van der Wiel, Denis Markushin and etc.]. – Kaspersky Lab, 2015. – 86p.
7. В. Мохор, О. Бакалинський, та В. Цуркан, “Аналіз способів представлення оцінок ризиків інформаційної безпеки”, Information Technology and Technology, vol. 6, iss. 1, 2018. doi: 10.20535/2411-1031.2018.6.1.153189.
8. С. А. Петренко, и С. В. Симонов, Управление информационными рисками. Экономически оправданная безопасность. Москва, Российская Федерация: Компания АйТи; ДМК Пресс, 2004.
9. Я. Д. Вишняков, и Н. Н. Радаев, Общая теория рисков. Москва, Российская Федерация: Издательский центр “Академия”, 2007.
10. А. М. Астахов, Исскуство управления информационными рисками. Москва, Российская Федерация: ДМК Пресс, 2010.
11. Wayne Jansen. Directions in Security Metrics Research , NISTIR 7564, April 2009 [Електронний ресурс] // NIST.gov - Computer Security Division - Computer Security Resource Center [сайт] / Wayne Jansen ; Computer Security Division , Information Technology Laboratory , National Institute of Standards and

Technology — Режим доступу: http://csrc.nist.gov/publications/nistir/ir7564/nistir7564_metrics-research.pdf

12. A Qualitative Risk Analysis and Management Tool – CRAMM. – Bethesda, Maryland: SANS Institute, 2012. – 15 p.

13. Авраменко, В.С. Модель для количественной оценки защищенности информации от несанкционированного доступа в автоматизированных системах по комплексному показателю [Текст] / В.С. Авраменко, А.В. Козленко // Труды СПИИРАН. – 2010. – Вып. 13. – С. 172-181.

14. Архипов А.Е. Особенности анализа рисков в информационно-коммуникационных системах // Захист інформації – 2012. – №4 (57) – С.18- 27.

15. Архипов А.Е. Применение экономикомотивационных соотношений для оценивания вероятностных параметров информационных рисков // Захист інформації – 2011. – №2 (51) – С.69-76.

16. Архипов А.Є., Архипова С.А. Применения мотивационностоимостных моделей для описания вероятностных соотношений в системе «атака-защита» //Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 1(16) вип., 2008р.

17. Богуш В. Інформаційна безпека держави/ В. Богуш, О. Юдін; [Гол. ред. Ю.О. Шпак]. – К.: «МК-Прес», 2005. – 432 с. 74

18. Велигодский, С.С. Показатели количественной оценки уязвимости корпоративного портала [Текст] / С.С. Велигодский, Н.Г. Милославская // Безопасность информационных технологий. – 2009. – №1. – С. 69-74.

19. Война О.А. Економічний ризик. Математичні моделі та методи керування: Навч. посібник / Київський національний ун-т ім. Тараса Шевченка. – К.: ВПЦ “Київський університет”, 2001. – 98 с.

20. Гончарова Л.Л., Возненко А.Д., Стасюк О.І., Коваль Ю.О. Основи захисту інформації в телекомунікаційних та комп’ютерних мережах. – К., 2013. – 435 с., іл.160.

21. Домарев В.В. Управління інформаційною безпекою в банківських установах (Теорія і практика впровадження стандартів серії ISO 27k) / В.В. Домарев, Д.В. Домарев – Донецьк: Велстар, 2012. – 146 с.

22. Домарев В.В. Управління інформаційною безпекою в банківських установах (Теорія і практика впровадження стандартів серії ISO 27k) / В.В. Домарев, Д.В. Домарев – Донецьк: Велстар, 2012. – 146 с.

23. Корниенко М.А. Модель оценки рисков информационной безопасности на основе теории нечетких множеств / М.А. Корниенко, Е.А. Островерхова // Материалы XVIII международного молодежного форума «Радиоэлектроника и молодежь в XXI веке». Т. 4 – Х.: ХНУРЭ, 2014. – 279 с.

24. Кучер, В.А. Использование методов теории вероятностей и математической статистики для оценки вероятностей обнаружения уязвимостей в информационных автоматизированных системах [Текст] / В.А. Кучер, В.С. Агранович // Информационное противодействие угрозам терроризма. – 2005. – №5. – С. 187-191.

25. Погребняк А.В. Технології комп'ютерної безпеки. Монографія. МЕГУ, Рівне, 2011.-117 с. Pogrebnyak A.V. Technologies ofcomputer safety. Monograph. IEGU, Rivne, 2011.-117 p.

26. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі: НД ТЗІ 3.7-003-05. — [Чинний від 08-11-2005]. — К.: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 2008. — 25 с. — (Нормативні документи системи технічного захисту інформації).

27. Про інформацію: [закон України: офіц. текст: за станом на 2 жовтня 1992 р., із змінами, внесеними Законом України від 10 січня 2012р.]: [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/2657-12.

28. Про основи національної безпеки України: [закон України: офіц. текст: за станом на 19 червня 2003р., із змінами, внесеними Законом України від 13 жовтня 2012 р.] // Відомості Верховної Ради України (ВВР). – 2012. – № 7. – ст. 53. 76

29. Ропаєва А. Г. Сучасний стан інформаційної безпеки підприємств та організацій в Україні / А. Г. Ропаєва // Теорія і практика розвитку наукових знань

(ч. ІІ): матеріали ІІ Міжнародної науково-практичної конференції м. Київ, 28-29 грудня 2017 року. – Київ. : МЦНД, 2017. – С. 22-23.

30. ДСТУ IEC/ISO 31010:2013. Керування ризиком. Методи загального оцінювання ризику. – Чинний з 11.12.2013 №1469 (Національний стандарт України).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Магістерська робота
на тему:

«ТЕХНОЛОГІЯ МОДЕЛЮВАННЯ ОЦІКИ РИЗИКІВ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ»

Виконала: БАРСУКОВА Катерина Ігорівна

Керівник: КОЖУХІВСЬКА Ольга Андріївна, д.т.н.

Об'єкт дослідження - процес забезпечення захисту інформаційної системи організації від ризиків кібербезпеки.

Предмет дослідження - технологія моделювання оцінки ризиків інформаційної системи організації.

Мета роботи - дослідити методики моделювання та оцінки інформаційних ризиків та розробити модель оцінювання ризиків інформаційної безпеки для корпоративних мереж.

НАУКОВІ ЗАВДАННЯ МАГІСТЕРСЬКОЇ РОБОТИ

1. Проаналізувати сучасні загрози інформаційної безпеки.
2. Дослідити методики моделювання та оцінки інформаційних ризиків.
3. Побудова системи управління інформаційними ризиками
4. Реалізувати алгоритм життєвого циклу ризику

АКТУАЛЬНІСТЬ РОБОТИ

- Інформація є найціннішим глобальним ресурсом.
- Недостовірність, несвоєчасне надходження, промислове шпигунство, комп'ютерна злочинність
- Необхідність в забезпеченні інформаційною безпекою
- Аналіз та оцінка ризиків
- Створення алгоритму аналізу ризиків

ОСНОВНІ ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ (ЗА ХАРАКТЕРОМ)

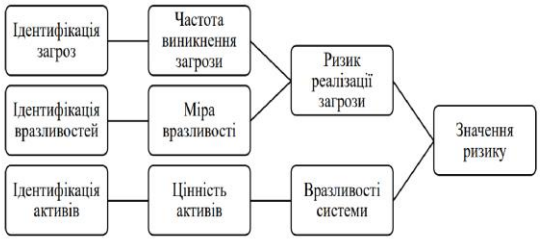
Навмисні *Ненавмисні*

ОСНОВНІ ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ (ЗА ДЖЕРЕЛОМ РОЗТАШУВАННЯ)

Внутрішні
- користувачі системи
- обслуговуючий персонал системи
- інсайдери
- інформаційна система

Зовнішні
- віруси
- зловмисники (хакери)
- техногенні, природні та інші катаклізми

ОСНОВНІ ЕЛЕМЕНТИ ОЦІНКИ ІНФОРМАЦІЙНИХ РИЗИКІВ



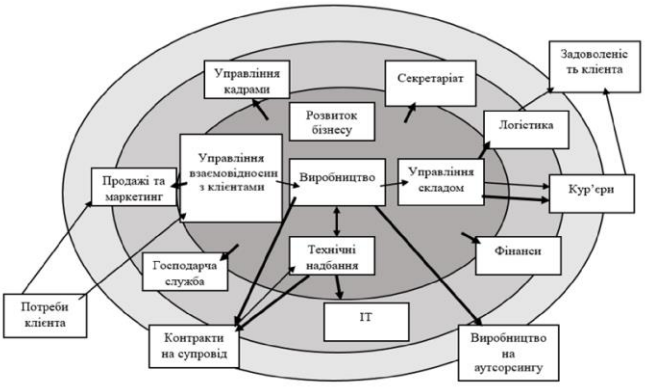
Ризик може бути оцінений двома способами: якісно та/або кількісно.

В результаті кількісної оцінки ризиків повинні бути визначені:
- цінність активів у грошовому або іншому вираженні;
- повний список всіх загроз інформаційній безпеці зі збитком від разового інциденту по кожній загрозі;
- частота реалізації кожної загрози;
- потенційний збиток від кожної загрози;
- рекомендовані заходи безпеки, контрзаходи і дії по кожній загрозі.

При якісному підході не використовуються кількісні чи грошові вираження об'єкта оцінки. Натомість об'єкту присвоюється показник, проранжований за певною лінгвістичною або баловою шкалою. Для збору даних при якісній оцінці ризиків використовуються опитування цільових груп, інтерв'ювання, анкетування, особисті зустрічі.

Обидва способи мають свої позитивні і негативні сторони, і на практиці більш адекватним є комбінована оцінка елементів ризику.

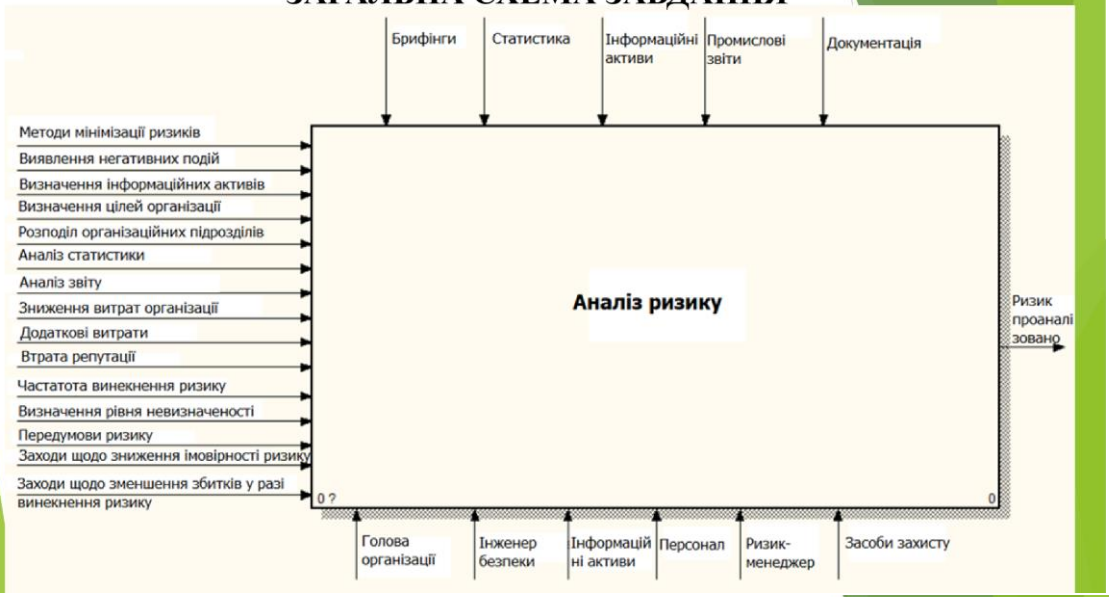
ОБЛАСТЬ ДІЇ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ (СУІБ)



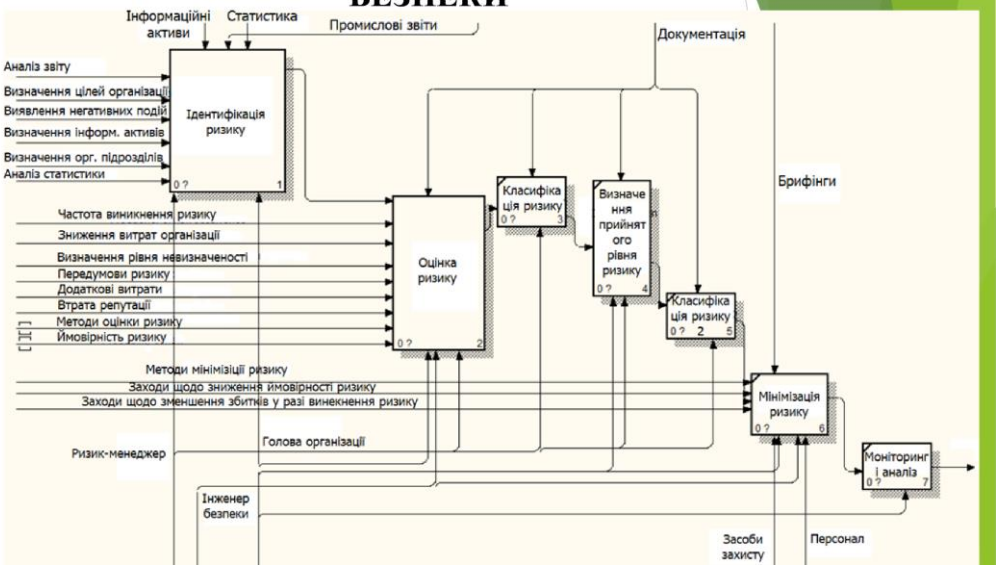
Для визначення меж управління ризиками потрібно описати інтерфейси організації та її інформаційних систем із зовнішніми системами, а також її контракти із зовнішніми сторонами, визначивши крім контактної інформації та способів зв'язку, також процедури взаємодії, контрактні зобов'язання та інші питання, що стосуються будь-яких зовнішніх взаємодій.

ЕТАПИ РОЗРОБКИ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РИЗИКАМИ(СУІР)

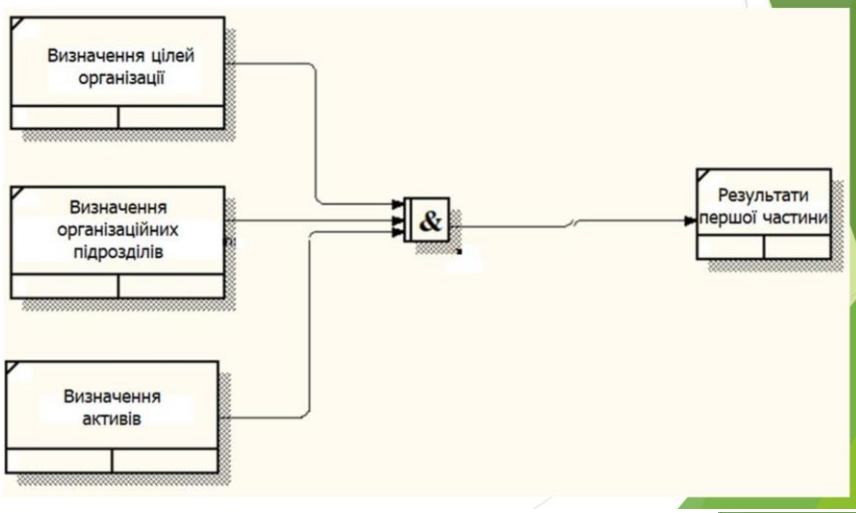
ЗАГАЛЬНА СХЕМА ЗАВДАННЯ



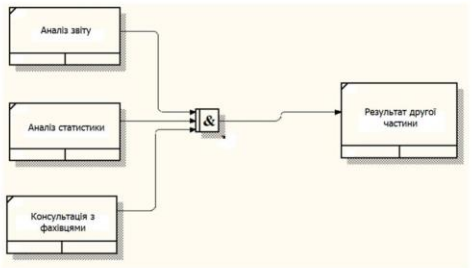
АЛГОРИТМ АНАЛІЗУ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ



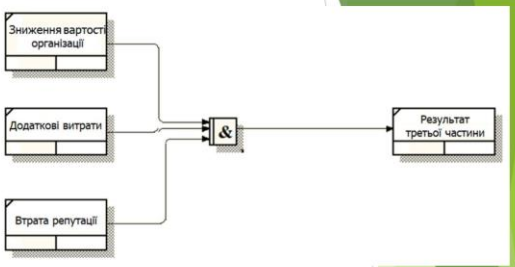
АЛГОРИТМ ВИЗНАЧЕННЯ ІНФОРМАЦІЙНИХ АКТИВІВ ОРГАНІЗАЦІЇ



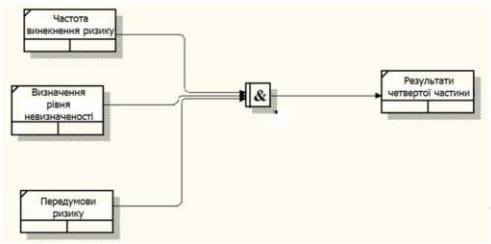
АЛГОРИТМ ВИЗНАЧЕННЯ НЕГАТИВНИХ ЧИННИКІВ



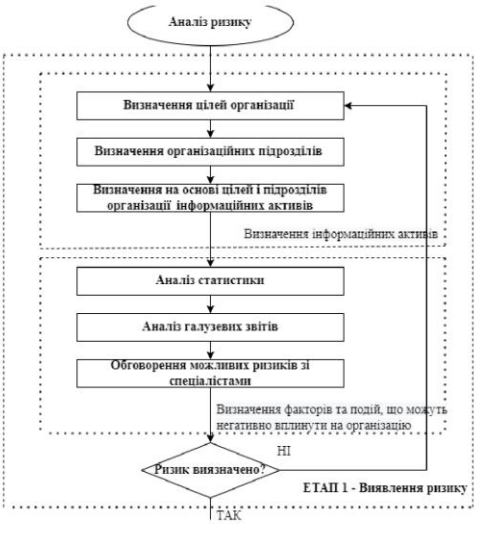
ВИЗНАЧЕННЯ ВТРАТ

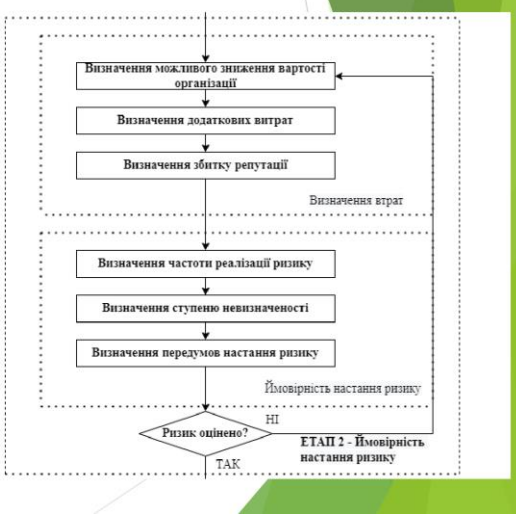


ЙМОВІРНІСТЬ РЕАЛІЗАЦІЇ РИЗИКУ

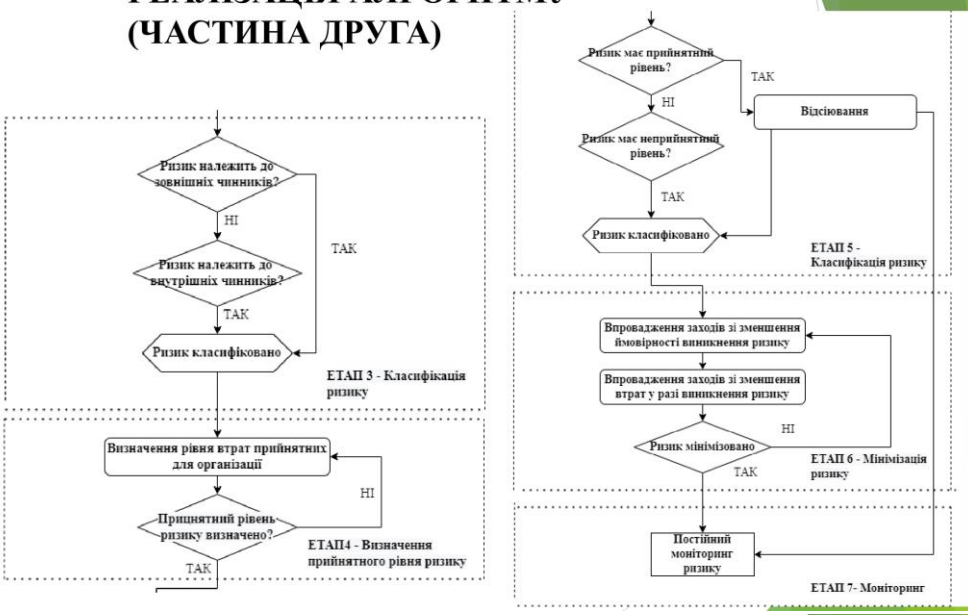


РЕАЛІЗАЦІЯ АЛГОРИТМУ(ЧАСТИНА ПЕРША)





РЕАЛІЗАЦІЯ АЛГОРИТМУ (ЧАСТИНА ДРУГА)



ВИСНОВКИ

У зв'язку з постійною модернізацією і зростанням загроз інформаційній безпеці необхідним постає питання точного та правильного аналізу можливих ризиків. Для реалізації даного завдання і представлено розроблений алгоритм аналізу ризиків з чітким визначенням етапів дій в ході проведення менеджменту інформаційної безпеки.

На прикладі реалізації даного алгоритму було показано, що він є ефективним і всі етапи, які використовуються в даному алгоритмі є актуальними.

Завдання які ставилися в роботі:

- ✓ Проаналізувати сучасні загрози інформаційної безпеки.
- ✓ Дослідити методики моделювання та оцінки інформаційних ризиків.
- ✓ Побудова системи управління інформаційними ризиками
- ✓ Реалізувати алгоритм життєвого циклу ризику

Вирішені, отже мета щодо побудови алгоритму аналізу ризиків досягнута.

Дякую за увагу!
Доповідь закінчено