МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

О. В. Коломійцев, В. І. Панченко

МЕТОДИЧНІ ВКАЗІВКИ

до виконання практичних робіт
з навчальної дисципліни «Теорія ризиків»
для студентів денної та заочної форми навчання
за спеціальністю «Комп'ютерна інженерія»

Затверджено
редакційно-видавничою
радою НТУ «ХПІ»,
протокол № 3 від 24.10.2024 р.

Харків
НТУ «ХПІ»
2024

Методичні вказівки до виконання практичних робіт з навчальної дисципліни «Теорія ризиків» для студентів денної та заочної форми навчання за спеціальністю «Комп'ютерна інженерія» / О. В. Коломійцев, В. І. Панченко. – Харків: НТУ «ХПІ», 2024. – 152 с.

Автори: *Олексій КОЛОМІЙЦЕВ,* д-р техн. наук, професор, Заслужений винахідник України, проф. каф. комп'ютерної інженерії та програмування НТУ «ХПІ»,
Володимир ПАНЧЕНКО, ст. викл. каф. комп'ютерної інженерії та програмування НТУ «ХПІ»

Рецензент: *Андрій ПАШНЄВ*, канд. техн. наук, с.н.с., доц. каф. інформаційних систем та технологій НТУ «ХПІ»

Кафедра комп'ютерної інженерії та програмування

ЗМІСТ

ВСТУП

Методичні вказівки до виконання практичних робіт з навчальної дисципліни «Теорія ризиків» призначені для набуття студентами практичних навичок у використанні методів та інструментів для оцінки і зниження ризиків у різноманітних ситуаціях, що можуть виникнути в процесі розробки та експлуатації інформаційних комп'ютерних систем.

Ризик є невід'ємною складовою сучасної технологічної діяльності, особливо в умовах швидкого розвитку інформаційних технологій та впровадження складних програмних і апаратних рішень у всіх сферах життєдіяльності людини. Оцінка і управління ризиками є важливими складовими прийняття рішень, тому знання основ теорії ризиків є необхідним для професійної діяльності інженерів, програмістів, системних адміністраторів та інших фахівців, що працюють у галузі комп'ютерних технологій.

Методичні вказівки містять опис основних тем практичних робіт, необхідні теоретичні дані, приклади вирішення задач та переліки індивідуальних варіантів завдань для закріплення матеріалів.

Матеріали методичних вказівок будуть корисними не тільки для вивчення дисципліни «Теорія ризиків», але й при виконанні дипломного проєктування магістрів, для аспірантів та фахівців з комп'ютерної інженерії.

1. ІНФОРМАЦІЙНІ РИЗИКИ ТА ЇХ ОСОБЛИВОСТІ. МЕТОДИ АНАЛІЗУ ТА ОЦІНКИ РИЗИКІВ

Мета заняття: ознайомитись з поняттям інформаційних ризиків, їх особливостями, а також навчитись виконувати аналіз та оцінку інформаційних ризиків за методом CRAMM.

1.1. Інформаційні ризики

Інформаційні технології стали невід'ємною частиною сучасного суспільства, проникаючи в усі його сфери й значно полегшуючи багато аспектів життя. Однак, разом із розвитком нових технологій виникають і нові ризики, пов'язані з їх використанням. Ці ризики умовно можна поділити на дві основні категорії: ризики інформаційної безпеки та ризики інформаційних систем.

Ризик інформаційної безпеки полягає в загрозах для конфіденційності, цілісності та доступності інформації, що виникають через недоліки в організації процесів захисту інформації. Ці загрози можуть включати використання шкідливого програмного забезпечення, зловмисні атаки на інформаційні ресурси організації, а також застосування шпигунського обладнання. Деякі приклади ризиків інформаційної безпеки:

- зупинка чи збій інформаційних систем внаслідок атак зловмисників;
- втрати або спотворення інформації через зараження комп'ютерних систем вірусами або шкідливим програмним забезпеченням;
- витік інформації через використання шпигунських пристроїв;
- людський фактор: недобросовісні співробітники або соціальна інженерія.

Мінімізація цих ризиків є завданням підрозділів інформаційної безпеки, і для цього застосовуються такі заходи, як сканери для виявлення вразливостей, антивірусні системи, файрволи, системи управління доступом і фізична безпека. Важливо також розробити відповідні політики та процедури

безпеки на всіх етапах життєвого циклу IT-систем, включаючи тестування на вразливості та моніторинг інцидентів.

Ризик інформаційних систем полягає в потенційних відмовах або порушеннях функціонування самих систем. Це може включати недосконалу інтеграцію між різними системами, технічні збої, а також недостатній процес резервного копіювання або підтримки користувачів. Ризики інформаційних систем можуть бути такими:

- збої або зупинка інформаційних систем через недостатні ресурси або помилки в системах;

- спотворення даних внаслідок неправильної інтеграції між різними IT-системами;

- втрати даних через відсутність належного резервного копіювання;

- несвоєчасне реагування на IT-інциденти через недосконаліть процесу підтримки користувачів.

Щоб зменшити ці ризики, рекомендується призначати відповідальних осіб за кожну систему, що здійснюють регулярну оцінку ризиків і визначають заходи для їх мінімізації.

Інформаційний ризик можна трактувати по-різному залежно від підходу. Одні фахівці визначають його як події, які безпосередньо впливають на інформацію (її видалення, спотворення, порушення конфіденційності чи доступності). Інші обмежують поняття інформаційного ризику лише комп'ютерними системами. Однак важливим аспектом є також ризики, пов'язані з обробкою інформації людьми, що вводять її в систему та перевіряють її достовірність на етапі збору даних.

Часто не враховуються й ризики, пов'язані з неполадками в алгоритмах обробки даних або в програмах, які використовуються для прийняття управлінських рішень. Деякі фахівці підходять до поняття «інформаційний ризик» з економічної точки зору, вважаючи це загрозою виникнення збитків через застосування IT-технологій.

Інформаційні ризики можна класифікувати за кількома критеріями:

- за джерелами: внутрішні та зовнішні ризики;

- за характером: навмисні або ненавмисні;

- за видом: прямі чи непрямі;

- за результатом: порушення достовірності, актуальності, повноти або конфіденційності інформації;

- за механізмом впливу: стихійні лиха, аварії, помилки фахівців.

Таким чином, інформаційні ризики є багатогранним явищем, що охоплює як загрози безпеці інформації, так і ризики, пов'язані з функціонуванням самих інформаційних систем. Їх мінімізація вимагає комплексного підходу та постійного моніторингу для забезпечення стабільної та безпечної роботи організаційних IT-ресурсів.

Як заходи для мінімізації зазначених ризиків можна запропонувати:

1. Покращення управління потужностями. В організації має бути призначена особа, яка відповідає за управління ресурсами. Цей фахівець збирає інформацію про плановане збільшення потужностей і на основі цього складає план для закупівлі нового обладнання та програмного забезпечення.

2. Стандартизація архітектурних та інтеграційних принципів. Необхідно визначити та задокументувати архітектурні й інтеграційні схеми, розробити стандарти взаємодії між системами та визначити вимоги до ухвалення рішень щодо введення нових систем в експлуатацію на спеціалізованому комітеті.

3. Розробка правил резервного копіювання. Процес резервного копіювання має бути регламентований, з визначенням періодичності копіювання в залежності від важливості системи, відповідальних осіб та обов'язковим періодичним тестуванням відновлення даних із резервних копій.

4. Автоматизація процесу реагування на IT-інциденти. Для ефективного реагування необхідно автоматизувати роботу служби підтримки користувачів, класифікувати звернення за рівнем критичності та визначити чіткі терміни для вирішення проблем.

5. Мотивація кваліфікованих кадрів. Одним із варіантів може бути запровадження гнучкого графіка роботи, орієнтуючись на результат, а не на відпрацьований час, або надання можливості працювати віддалено, що дозволяє залучати висококваліфікованих фахівців не лише у великих містах, а й у віддалених регіонах.

Хоча витрати на IT та інформаційну безпеку можуть бути значними, інвестиції в заходи, спрямовані на мінімізацію ризиків, є необхідними, оскільки можливі наслідки від реалізації цих ризиків можуть бути дуже серйозними і навіть незворотними.

1.2. Аналіз та оцінка інформаційних ризиків

Аналіз інформаційних ризиків – це процес комплексної оцінки рівня захищеності інформаційної системи, що передбачає визначення як кількісних (у вигляді фінансових витрат), так і якісних (рівні ризику: високий, середній, низький) показників ризику. Цей аналіз проводиться за допомогою різних інструментів і методів, які застосовуються для формування процесів захисту інформації. У результаті аналізу визначаються найбільш критичні ризики, які становлять серйозну загрозу і вимагають негайного вжиття додаткових заходів безпеки.

На сьогоднішній день не існує єдиної методики для точного визначення кількісної величини ризику. Це зумовлено двома основними причинами. По-перше, бракує достатньої кількості статистичних даних, щоб оцінити ймовірність виникнення конкретної загрози. По-друге, визначити вартість конкретного інформаційного ресурсу дуже складно. Наприклад, власник інформаційного ресурсу може точно вказати вартість обладнання та носіїв, але оцінити точну цінність даних, що зберігаються на цих пристроях, часто неможливо. Тому найпоширенішим підходом є якісна оцінка інформаційних ризиків, яка має на меті виявити фактори ризику, визначити можливі вразливі зони та оцінити вплив кожного виду ризику.

Одним з найбільш відомих методів для кількісної оцінки інформаційних ризиків є британський метод CRAMM (CCTA Risk Analysis and Management Method). Основними цілями цього методу є автоматизація управління ризиками, оптимізація витрат на управління ними, скорочення часу, необхідного для супроводження систем безпеки організації, а також забезпечення безперервності бізнес-процесів. Цей метод дозволяє створити ефективну систему управління ризиками, знижуючи ймовірність виникнення серйозних загроз та мінімізуючи можливі фінансові витрати на заходи захисту.

При проведенні розрахунків інформаційних ризиків (їх якісної оцінки) під час аналізу експертним шляхом враховуються такі фактори:

Вартість ресурсу (Asset Value, AV) – цей параметр відображає цінність конкретного інформаційного ресурсу для організації. При якісній оцінці ризиків ресурсам зазвичай присвоюється ранг у діапазоні від 1 до 3, де 1 – мінімальна вартість ресурсу, 2 – середня вартість, і 3 – максимальна вартість. Наприклад, для інформаційної банківської системи автоматизований сервер буде мати ранг $AV = 3$, оскільки це критично важливий компонент для роботи системи, а окремий інформаційний термінал – $AV = 1$, тому що його вартість значно нижча. Це дозволяє визначити важливість ресурсу для організації та зрозуміти, які з них є найбільш критичними для безпеки.

Ступінь уразливості ресурсу від загрози (Exposure Factor, EF) – цей параметр демонструє, наскільки ресурс вразливий до конкретної загрози. Наприклад, у банківській установі сервер автоматизованої системи буде мати високу доступність і стане найбільш уразливим при атаці. При якісній оцінці ризику EF зазвичай знаходиться в діапазоні від 1 до 3, де 1 – низька ступінь уразливості (мінімальний вплив), 2 – середня (існує ймовірність відновлення ресурсу), і 3 – висока ступінь уразливості (після атаки ресурс потрібно повністю замінити). Оцінка цього показника дозволяє зрозуміти, наскільки великий буде вплив загрози на ресурс, якщо вона стане реальністю.

Оцінка ймовірності виникнення загрози (Annual Rate of Occurrence, ARO) – цей показник визначає ймовірність того, що конкретна загроза здійсниться за певний період часу (найчастіше – за один рік). Оцінка ARO також може бути в діапазоні від 1 до 3, де 1 означає низьку ймовірність, 2 – середню, а 3 – високу ймовірність того, що загроза може реалізуватися. Це дозволяє прогнозувати, як часто конкретні загрози можуть мати місце і як це може вплинути на організацію.

На основі отриманих даних проводиться розрахунок Annual Loss Exposure (ALE) – це очікувані втрати, які організація може понести внаслідок реалізації конкретної загрози за визначений час. Розрахунок здійснюється за формулою:

$$ALE = (AV \times EF \times ARO).$$

Ця формула допомагає оцінити фінансові втрати, що можуть виникнути від певної загрози, беручи до уваги вартість ресурсу, ступінь його уразливості та ймовірність виникнення загрози.

Після виконання первинної оцінки ризиків отримані показники необхідно ранжирувати відповідно до їхньої важливості для організації. Це дозволяє визначити рівень ризику – низький, середній або високий, що дає змогу прийняти правильні управлінські рішення для мінімізації загроз і налаштування ефективної стратегії захисту інформаційних ресурсів.

Методика управління ризиками передбачає кілька варіантів дій у разі виникнення ризиків.

Ризик можна:

- прийняти – погодитися з ризиком і зазнати збитків, пов’язаних з ним;

- зменшити – застосувати ряд заходів, спрямованих на мінімізацію ризику;

- передати – передати витрати на покриття збитків страховій компанії або трансформувати ризик у менш небезпечний, застосовуючи спеціальні механізми.

Після цього ризики розподіляються за рівнем, і визначаються ті, які потребують першочергової уваги. Основний метод управління ризиками – це їх зменшення, хоча іноді застосовується передача ризику. Ризики середнього рівня небезпеки можна як передавати, так і зменшувати разом з ризиками високого рівня. Ризики низького рівня, як правило, приймаються і не підлягають подальшому аналізу.

Очевидно, що інтервал ранжирування ризиків визначається на основі обчислених значень їх якісних характеристик. Наприклад, якщо обчислені значення ризиків варіюються від 1 до 18, то:

- низькі ризики розташовуються в діапазоні від 1 до 7,

- середні ризики – від 8 до 13,

- високі ризики – від 14 до 18.

Таким чином, управління ризиками полягає у зменшенні значень високих і середніх ризиків до рівня низьких інформаційних ризиків, що дозволяє їх прийняти. Зниження рівня ризику досягається шляхом зменшення однієї або кількох складових формули (вартість ресурсу AV, рівень вразливості ресурсу від загрози EF, ймовірність виникнення загрози ARO) за допомогою певних заходів. Зазвичай це реалізується через зменшення рівня вразливості ресурсу та оцінки ймовірності виникнення загрози, оскільки вартість ресурсу, як правило, є досить стабільним параметром.

Приклад застосування розрахунків інформаційних ризиків для освітньої установи, наприклад, для університетської інформаційної системи, яка включає сервери для зберігання студентських даних, електронних бібліотек та навчальних матеріалів, а також комп'ютери для доступу студентів та викладачів.

1. Вартість ресурсу AV:

- сервер з даними студентів та навчальними матеріалами: $AV = 3$, оскільки цей сервер містить критичну інформацію про студентів, курси та інші важливі дані університету. Його вартість є високою як з точки зору обладнання, так і з точки зору важливості даних;

- комп’ютери в лабораторіях для студентів: $AV = 1$, оскільки хоча комп’ютери використовуються для доступу до системи, їх вартість значно нижча, а відновлення даних з них не є критичним.

2. Ступінь уразливості ресурсу від загрози EF:

- сервер з даними студентів та навчальними матеріалами: цей сервер є критичним для функціонування університетської системи, і якщо на нього буде здійснено напад або він буде пошкоджений, це може призвести до серйозних наслідків, таких як втрата важливих даних або переривання доступу до навчальних матеріалів. Тому для сервера $EF = 3$ (найвища уразливість);

- комп’ютери в лабораторіях: втрата або пошкодження комп’ютерів не є катастрофічним для університету, оскільки дані на них зазвичай не є критичними і можуть бути відновлені. Отже, для комп’ютерів $EF = 2$ (середня уразливість).

3. Оцінка ймовірності виникнення загрози ARO:

- сервер з даними студентів та навчальними матеріалами: оскільки сервер містить важливі дані, ймовірність того, що на нього буде здійснено атаку (наприклад, зловмисники можуть намагатися вкрасти особисті дані або зламати систему для отримання доступу до ресурсів), є високою. Тому для сервера $ARO = 3$ (висока ймовірність загрози);

- комп’ютери в лабораторіях: враховуючи, що комп’ютери можуть бути вразливими до вірусів чи маловідомих атак, але такі загрози виникають рідше порівняно з сервером, для лабораторних комп’ютерів $ARO = 2$ (середня ймовірність загрози).

4. Розрахунок ALE:

- для сервера $ALE = (3 \times 3 \times 3) = 27$ – це вказує на високі потенційні втрати, якщо сервер буде пошкоджений або атакований;

- для комп’ютерів у лабораторіях $ALE = (1 \times 2 \times 2) = 4$ – це вказує на значно менші потенційні втрати порівняно з сервером.

5. Ранжирування ризиків:

- сервер має високий ризик ($ALE = 27$), тому потребує негайного впровадження заходів безпеки, серед яких можуть бути регулярне резервне копіювання, шифрування даних, посилена аутентифікація, моніторинг тощо;

- комп'ютери в лабораторіях мають помірний ризик ($ALE = 4$), тому заходи безпеки можуть включати антивірусне програмне забезпечення, регулярне оновлення програмного забезпечення та навчання студентів щодо безпеки.

Завдяки цій оцінці можна зрозуміти, що найбільші зусилля слід спрямувати на захист серверів, що містять критичні дані студентів та навчальні матеріали, і забезпечити їх безперервність роботи та захист від загроз. Для лабораторних комп'ютерів заходи безпеки можна спростити, але також забезпечити базовий рівень захисту.

При кількісному розрахунку ALE для визначення можливих фінансових втрат оцінка ймовірності загрози ARO виражається значенням ймовірності в діапазоні від 0 до 1.

Приклад визначення можливих втрат для інформаційної системи управління даними університету.

Вартість інформаційного ресурсу, який знаходиться під захистом – сервер, що зберігає важливі студентські дані, складає 10000 $.

Ідентифікація активів AV – основним активом є сервер, який зберігає критичні дані ($AV = 3$). Ступінь уразливості ресурсу EF – сервер має високий рівень уразливості до кібератак ($EF = 3$). Оцінка ймовірності виникнення загрози ARO – ймовірність атаки на сервер може бути 30 % на рік (30 % ймовірності того, що загроза матеріалізується протягом року): $ARO = 0.30$.

Розрахунок ALE:

$$ALE = 3 \times 3 \times 0.30 = 2.7.$$

Оцінка фінансових втрат:

Тоді річні очікувані втрати в разі атаки (ALE) можна розрахувати так:

$$\text{Фінансові втрати} = ALE \times \text{Вартість ресурсу},$$

$$\text{Фінансові втрати} = 2.7 \times 10000\ \$ = 27000\ \$.$$

Таким чином, річні очікувані втрати від хакерської атаки на сервер можуть скласти $27000\ \$$. Це допомагає зрозуміти, скільки коштуватимуть потенційні збитки, якщо загроза стане реальністю, і прийняти відповідні заходи для зменшення цих ризиків.

Метод CRAMM має кілька важливих переваг з практичного застосування:

- надійність і досвід. Цей метод є перевіреним і широко застосовуваним, що дозволяє накопичити значний досвід і розвинути необхідні професійні навички;

- формалізованість процесів. Чітка структура та формалізований підхід знижують ризик помилок під час реалізації аналізу та управління ризиками;

- автоматизація. Наявність інструментів для автоматизації аналізу ризиків дозволяє значно зменшити час і ресурси, необхідні для проведення цих заходів;

- каталоги загроз та вразливостей. Наявність готових каталогів допомагає спростити вимоги до спеціалізованих знань та досвіду виконавців, що відповідають за аналіз і управління ризиками.

Проте метод CRAMM також має низку недоліків:

- складність збору даних. Процес збору початкової інформації є трудомістким і потребує значних ресурсів як всередині організації, так і ззовні;

- великі витрати часу і ресурсів. Виконання процесів аналізу і управління ризиками займає чимало часу та потребує значних фінансових і людських ресурсів;

- необхідність залучення великої кількості людей. Організація роботи великої команди та комунікацій між її членами вимагає значних зусиль і витрат;

- складність в оцінці ризиків у грошовому еквіваленті. Неможливість точно оцінити ризики в термінах фінансових витрат ускладнює їх використання при розробці техніко-економічних обґрунтувань для інвестицій у систему захисту інформації.

Метод CRAMM активно використовується як в урядових, так і в комерційних установах, і вважається фактично стандартом для управління ризиками інформаційної безпеки у Великобританії. Цей метод підходить для організацій, що працюють у міжнародному контексті та відповідають вимогам міжнародних стандартів управління ризиками. Водночас його впровадження вимагає значних ресурсів і часу, особливо на етапі початкового запровадження.

1.3. Перелік деяких інформаційних ризиків згідно з методом CRAMM

Перелік ризиків, які оцінюються методом CRAMM, можна поділити на кілька категорій: загрози для доступності, цілісності, конфіденційності інформації, а також для фізичної безпеки, відповідності нормативам та людського фактору.

1. Загрози для доступності (Availability Risks). Ці загрози пов’язані з недоступністю інформаційних ресурсів та систем, що перешкоджає або зупиняє роботу користувачів та організаційних процесів.

- Відмова апаратного забезпечення:
  - вихід з ладу серверів, збої в роботі мережевих пристроїв (маршрутизаторів, комутаторів), комп’ютерних систем;
  - пошкодження або вихід з ладу пристроїв зберігання інформації (жорстких дисків, SSD).
- Відмова програмного забезпечення:
  - збої в роботі операційних систем (наприклад, Windows, Linux);
  - проблеми з базами даних (наприклад, MySQL, PostgreSQL), втрата доступу через відмову БД.

- Перерви в роботі системи через несанкціоновані дії:
    - атаки типу DDoS (Distributed Denial of Service), які «забивають» сервери або мережу, блокуючи доступ до ресурсів;
    - помилки адміністраторів або неправильно налаштовані сервери/мережі, що ведуть до втрати доступу.
- Помилки резервного копіювання:
    - невиконання регулярного резервного копіювання або пошкодження копій, що призводить до втрати критичних даних.
- Фізична недоступність серверів або робочих місць:
    - пошкодження серверів через стихійні лиха, пожежі, повені, землетруси.

2. Загрози для конфіденційності (Confidentiality Risks). Ці ризики пов’язані з порушенням або витоком конфіденційної інформації, несанкціонованим доступом до даних, що знижує рівень безпеки та порушує законодавчі вимоги.

- Неавторизований доступ до даних:
    - несанкціонований доступ до персональних даних, фінансової або комерційної інформації;
    - використання вразливостей програмного забезпечення або слабких паролів для проникнення в систему.
- Витік даних через людський фактор:
    - перехоплення даних через небезпечні канали зв’язку (нешифровані електронні листи, незахищені Wi-Fi мережі);
    - витік інформації через віддалену роботу співробітників або через пристрої BYOD (Bring Your Own Device).
- Атаки соціальної інженерії:
    - фішинг, скам або інші методи маніпуляції співробітниками з метою отримання доступу до конфіденційних даних.
- Зловживання правами доступу:

- інсайдерські загрози, коли співробітники з доступом до чутливої інформації зловживають своїми правами (наприклад, передача паролів стороннім особам).

- Крадіжка даних:
  - викрадення фізичних носіїв інформації (жорстких дисків, флеш-накопичувачів, ноутбуків).
- Злочинне перехоплення даних:
  - використання технологій для перехоплення трафіку в мережі (наприклад, атаки Man-in-the-Middle).

3. Загрози для цілісності (Integrity Risks). Ці ризики включають будь-які ситуації, які можуть призвести до зміни або пошкодження даних, що знижує їх точність та достовірність.

- Некоректне оновлення програмного забезпечення:
  - встановлення неперевірених патчів або оновлень, що можуть порушити стабільність або цілісність даних.
- Шкідливе програмне забезпечення (Malware):
  - віруси, трояни, руткіти, програмне забезпечення, яке змінює або пошкоджує файли даних.
- Помилки в програмуванні та інтеграції:
  - неправильна інтеграція компонентів інформаційної системи або помилки в алгоритмах, що призводять до зміни даних.
- Інтеграція даних з ненадійних джерел:
  - використання зовнішніх джерел даних, що можуть містити помилкову або спотворену інформацію.
- Несанкціоновані зміни в коді програм:
  - модифікація програмного коду або бази даних без дозволу адміністратора.

4. Загрози для відповідності нормативним вимогам (Compliance Risks). Ці ризики пов’язані з порушенням вимог законодавства та внутрішніх політик організації в області безпеки інформації.

- Невиконання вимог законодавства:
    - порушення правил захисту персональних даних (GDPR, HIPAA тощо) та інших нормативно-правових актів.
- Порушення внутрішніх політик безпеки:
    - недотримання політик з управління доступом, політик резервного копіювання, використання слабких паролів або недостатнього шифрування.
- Втрата ліцензій або сертифікацій:
    - втрати, що виникають через порушення стандартів безпеки, необхідних для сертифікації (наприклад, ISO 27001).

5. Загрози людського фактору (Human Factor Risks). Ці ризики пов’язані з помилками або навмисними діями людей, які призводять до загроз для безпеки інформаційних систем.

- Невірне використання системи:
    - помилки користувачів, які можуть призвести до неправильного введення даних, неправильно налаштованого програмного забезпечення, втрати важливої інформації.
- Невиправдане розкриття паролів або ключів доступу:
    - використання слабких паролів, передача паролів через небезпечні канали зв’язку, зберігання паролів у відкритому вигляді.
- Інсайдерські загрози:
    - співробітники, які можуть цілеспрямовано викрасти дані або навмисно пошкодити систему, використовуючи свій доступ.
- Недотримання політик безпеки:
    - співробітники, які не дотримуються правил використання інформаційних ресурсів, наприклад, не зашифровують конфіденційну інформацію або використовують застарілі системи.

6. Загрози для фізичної безпеки (Physical Security Risks). Ці ризики стосуються безпеки фізичних ресурсів, які підтримують інформаційні технології (сервери, мережеве обладнання, сховища даних, робочі станції).

- Неадекватна фізична безпека серверних приміщень:
    - відсутність належних заходів для контролю доступу до серверних приміщень або технічних зон, що може призвести до несанкціонованого фізичного доступу до обладнання.
- Необмежений доступ до обладнання:
    - відсутність ефективних заходів контролю фізичного доступу, таких як використання карток доступу, відеоспостереження, замків на дверях, що дозволяє стороннім особам мати доступ до критичних компонентів системи.
- Пошкодження або крадіжка обладнання:
    - фізична крадіжка або пошкодження серверів, комп'ютерних систем або носіїв даних, що містять конфіденційну інформацію.
- Стихійні лиха та їх вплив на інфраструктуру:
    - пошкодження серверів, мережевого обладнання чи інфраструктури через стихійні лиха: повені, пожежі, землетруси тощо.
- Втрата обладнання або його пошкодження:
    - втрата важливого обладнання або його пошкодження через людські помилки, неправильне транспортування чи неналежне зберігання.

7. Загрози для підтримки безперервності бізнесу (Business Continuity Risks). Ці ризики пов'язані з порушеннями, що можуть призвести до зупинки або зниження ефективності бізнес-процесів.

- Відсутність плану відновлення після катастроф:
    - невизначеність щодо того, як відновити систему або бізнес-процеси після серйозного інциденту, наприклад, у випадку атаки або стихійного лиха.

- Неадекватні резервні копії та архіви:
    - відсутність або недостатня кількість копій даних для відновлення системи в разі втрати або пошкодження.
- Збої в роботі критичної інфраструктури:
    - втрата функціональності важливих систем, які забезпечують основні бізнес-процеси (наприклад, бухгалтерія, фінансові операції).

8. Загрози для управління змінами (Change Management Risks). Ці ризики виникають у зв’язку з процесами зміни компонентів інформаційної системи, такими як програмне або апаратне забезпечення, налаштування конфігурацій або операційні процеси.

- Невірне впровадження змін:
    - помилки, пов’язані з оновленням програмного забезпечення або апаратної частини без належного тестування;
    - несанкціоновані або неповні зміни в конфігураціях, які порушують нормальну роботу системи або створюють вразливості.
- Відсутність тестування змін:
    - впровадження нових версій програм або апаратних пристроїв без попереднього тестування на тестовому середовищі.
- Невиконання процедур відкату змін:
    - відсутність чітких і протестованих процедур для відкату змін, якщо вони спричиняють проблеми з продуктивністю або безпекою.
- Недосконале управління версіями:
    - невідповідність між версіями програмного забезпечення, що використовуються на різних системах, або між середовищами (розробка, тестування, виробництво).
- Несанкціонований доступ до інструментів зміни:

- зловживання доступом до системних налаштувань або інструментів адміністрування для внесення змін, які порушують політики безпеки або призводять до збоїв.

9. Загрози для технологічної інфраструктури (Infrastructure Risks). Ці ризики пов’язані з фізичною та віртуальною інфраструктурою організації, яка підтримує інформаційні системи.

- Невірна конфігурація мережі:
  - неправильне налаштування мережевих компонентів (файрволів, маршрутизаторів, проксі-серверів), що дозволяє несанкціонований доступ або порушення цілісності даних.
- Вразливості в програмному забезпеченні:
  - наявність відомих вразливостей у використовуваних програмах чи платформах, які можуть бути використані для атак (наприклад, SQL ін’єкції, крос-сайт скриптинг).
- Фізичні пошкодження інфраструктури:
  - пошкодження серверів, комутаторів, сховищ даних або інших критичних інфраструктурних компонентів через зовнішні або внутрішні чинники (наприклад, падіння напруги, пошкодження кабелів).
- Неадекватне резервне копіювання інфраструктури:
  - втрата конфігураційних файлів або важливих налаштувань серверів через відсутність належного резервного копіювання.
- Проблеми з моніторингом інфраструктури:
  - відсутність або недостатня кількість інструментів для моніторингу стану інфраструктури, що може призвести до виявлення проблем лише після того, як вони спричинили серйозні наслідки.

10. Загрози для моніторингу та управління інцидентами (Incident Management Risks). Ці ризики пов’язані з відсутністю або недостатньою

ефективністю механізмів виявлення, аналізу та реагування на інциденти, що можуть призвести до серйозних порушень безпеки.

- Невчасне виявлення інцидентів:
    - недостатня увага до збору логів, моніторингу аномалій або недосконаліть інструментів для своєчасного виявлення загроз, таких як вторгнення в мережу, спроби зламів або несанкціонованих змін.
- Недостатнє реагування на інциденти:
    - відсутність чіткої стратегії реагування на інциденти, що призводить до затримок у розслідуванні або відновленні після інцидентів безпеки.
- Необґрунтоване ігнорування ризиків:
    - систематичне ігнорування дрібних інцидентів або незначних порушень, які, у кінцевому підсумку, можуть привести до великих атак або витоків даних.
- Недостатній аналіз інцидентів:
    - невідповідний або поверхневий аналіз інцидентів без ретельного вивчення причин і застосування коригувальних дій для запобігання повторенню.
- Невиправдане розкриття інцидентів:
    - втрата контролю над інцидентами через неправильне управління інформуванням внутрішніх або зовнішніх зацікавлених сторін про загрози безпеці.

11. Загрози для управління доступом (Access Control Risks). Ці ризики пов’язані з управлінням правами доступу користувачів та систем до різних ресурсів і даних в організації.

- Неналежне управління правами доступу:
    - неправильне або недостатнє управління правами доступу до критичної інформації та ресурсів, що дозволяє неавторизованим користувачам отримати доступ до чутливої інформації.

- Відсутність принципу найменших привілеїв:
    - надання користувачам більших прав доступу, ніж це необхідно для виконання їх роботи, що збільшує ризик витоку або модифікації даних.
- Невірне управління паролями та аутентифікацією:
    - використання слабких паролів, недостатня складність паролів або їх часта зміна; відсутність двофакторної аутентифікації (2FA).
- Відсутність аудитів доступу:
    - відсутність регулярних перевірок і аудитів прав доступу, що призводить до несанкціонованого доступу до чутливої інформації.
- Необмежений доступ до адміністративних прав:
    - нехтування контролем над адміністративними правами в системах, що дозволяє адміністраторам або іншим користувачам з високими правами викрадати, змінювати або видаляти дані.

1.4. Індивідуальні завдання

Оцінити ризики для вказаної ситуації. Сформулювати не менше чотирьох загроз, які можуть виникнути. Провести оцінку ризиків за методом CRAMM, враховуючи можливі загрози та вразливості. Виконати ідентифікацію активів, ступінь уразливості ресурсів, оцінку ймовірності виникнення загроз та вартість ресурсів згідно сучасних даних, отриманих з довідкових ресурсів у мережі Інтернет. Оцінити Annual Loss Exposure (ALE) для кожної загрози. Визначити, які загрози потребують першочергової уваги. Розробити рекомендації щодо зниження ризиків для найбільш небезпечних загроз (наприклад, як зменшити ймовірність відмови жорсткого диска або покращити захист від несанкціонованого доступу).

1. Атака на вебсайт електронної комерції, на якому зберігаються особисті дані клієнтів та фінансова інформація.

2. Втрата даних через помилки користувачів у корпоративній системі, яка використовується для управління проєктами, і працівники іноді випадково видаляють важливі дані.

3. Кібератака на базу даних, що містить конфіденційну інформацію про клієнтів. Вразливість до атак через SQL-ін’єкцію є реальним ризиком.

4. Втрата даних через збій системи резервного копіювання – періодичні збої можуть призвести до неповного відновлення даних.

5. Кібератака на систему управління підприємством (ERP-система), яка використовується для управління фінансами, запасами і персоналом. Система містить конфіденційну інформацію, що може бути скомпрометована через кібератаку.

6. Втрата даних через помилку користувача в CRM-системі, яка використовується для управління взаємовідносинами з клієнтами, в якій зберігається історія взаємодії, контактні дані та угоди.

7. Збитки через вірус у мережі підприємства, яка піддається ризику зараження вірусами, що може призвести до втрати даних або збоїв у роботі систем.

8. Збої в серверному обладнанні, яке використовується для зберігання і обробки даних, і збої в його роботі можуть призвести до тимчасового припинення доступу до важливих даних.

9. Атака через шкідливе програмне забезпечення на файловий сервер, який компанія використовує для зберігання та обміну важливими документами між співробітниками.

10. Втрата даних через відмову жорсткого диска на сервері бази даних з інформацією про клієнтів, замовлення та фінансові транзакції.

11. Втрата доступу до хмарного сховища через атаку на постачальника послуг, яке використовується для збереження всіх своїх документів і файлів.

12. Збої в роботі системи моніторингу та контролю доступу до фізичних і інформаційних ресурсів, яка включає камери спостереження, контроль доступу через картки і моніторинг фізичного доступу до серверів.

1.5. Контрольні запитання

1. Що таке ризик?

2. Що таке ризик інформаційної безпеки?

3. Як можна класифікувати інформаційні ризики?

4. Які є засоби мінімізації інформаційних ризиків?

5. Що лежить в основі методу CRAMM?

6. Як розраховуються очікувані втрати?

7. Наведіть приклади основних інформаційних ризиків.

8. Що таке ступінь уразливості ресурсу від загрози?

9. Як розраховуються значення параметру Вартість ресурсу в методі CRAMM?

10. Які існують рівні ризику?

2. КЛАСИФІКАЦІЯ РИЗИКІВ ТА ЇХ НЕВИЗНАЧЕНІСТЬ

Мета заняття: ознайомитись з основними типами інформаційних ризиків, їх класифікацією, а також навчитись застосовувати отримані знання для оцінки та управління ризиками в організації.

2.1. Класифікація інформаційних ризиків

Інформаційні ризики – це загрози, що виникають у результаті використання інформаційних технологій і систем для збереження, обробки та передачі даних. Вони мають значний вплив на безпеку інформації, цілісність даних, доступність систем і можуть призвести до фінансових або репутаційних збитків. Визначення і класифікація інформаційних ризиків допомагають організаціям ефективно ними управляти. Ризики можна класифікувати за різними критеріями залежно від їх типу, джерела, ймовірності виникнення і ступеня невизначеності. Кожен тип ризику має свій рівень невизначеності, що визначається ймовірністю виникнення події та наслідками для організації.

Класифікація інформаційних ризиків є підкатегорією загальної класифікації ризиків і має вузьку спеціалізацію, орієнтуючись на ризики, пов’язані з інформаційними технологіями та даними. Загальна класифікація ризиків охоплює значно ширший спектр аспектів, включаючи економічні, політичні та соціальні фактори, що не завжди мають пряме відношення до інформаційних систем, але можуть мати вплив на організацію.

Один з варіантів класифікації інформаційних ризиків дозволяє виділити такі категорії:

1. За типом впливу на інформацію:

- конфіденційність: ризики, пов’язані з витоком або несанкціонованим доступом до інформації;
- доступність: ризики, пов’язані з недоступністю інформації або систем;

- цілісність: ризики, пов’язані з пошкодженням, зміною або порушенням точності даних.

2. За типом джерела загрози:

- внутрішні загрози: дії або помилки працівників організації; необережне поводження з конфіденційною інформацією; порушення безпеки на рівні внутрішніх систем;

- зовнішні загрози: атаки з боку хакерів або інших організацій; втручання державних органів або конкурентів; шпигунство або саботаж з боку зовнішніх осіб.

3. За рівнем уразливості:

- високий рівень ризику: зміна стратегічних або критичних даних, які можуть суттєво вплинути на діяльність організації;

- середній рівень ризику: втрата або несанкціоноване використання менш критичних даних;

- низький рівень ризику: доступ або втрата інформації, що не є критично важливою для організації.

4. За наслідками для організації:

- фінансові ризики: втрата фінансових ресурсів через витік даних або відновлення після кіберінцидентів; пошкодження репутації організації, що може призвести до фінансових збитків;

- операційні ризики: збої в роботі критичних інформаційних систем; втручання в операційну діяльність підприємства;

- юридичні та нормативні ризики: невиконання вимог законодавства щодо захисту персональних даних; штрафи та санкції через порушення нормативних актів;

- репутаційні ризики: втрата довіри клієнтів через порушення безпеки або витік даних; публічні скандали, пов’язані з недбалим ставленням до захисту інформації.

5. За типом загрози:

- технічні ризики: програмні помилки, збої систем; вразливості в програмному забезпеченні; втрата або пошкодження даних; невідповідність стандартам безпеки інформаційних технологій;

- людські помилки (гуманітарні ризики): ненавмисне порушення політик безпеки; невміння правильно реагувати на інциденти; недосконаліть навичок персоналу;

- загрози з боку кіберзлочинців (кіберзлочинність, кіберзагрози): атаки з використанням шкідливих програм (віруси, трояни, руткіти); фішинг, соціальна інженерія; дистрибуція шкідливих файлів, блокування доступу до систем (ransomware);

- фізичні загрози: пожежі, повені, стихійні лиха; крадіжка фізичних носіїв інформації; доступ до серверних приміщень без авторизації;

- організаційні ризики: недосконала політика безпеки; невиконання або часткове виконання політик і процедур захисту інформації.

2.2. Невизначеність ризиків

Невизначеність інформаційних ризиків – це невизначеність або відсутність точності щодо ймовірності виникнення ризику та його можливих наслідків. Вона є важливим аспектом при оцінці та управлінні інформаційними ризиками, оскільки в багатьох випадках організації важко точно передбачити, чи і коли виникне певна загроза, а також оцінити масштаби її впливу на інформаційні системи та дані.

Існують такі типи невизначеності інформаційних ризиків:

1. Невизначеність щодо ймовірності. Це невизначеність, що стосується того, як часто може виникнути конкретна загроза. Наприклад, може бути важко передбачити, скільки часу пройде до того, як відбудеться кібератака на інформаційну систему.

2. Невизначеність щодо наслідків. Це невизначеність стосується того, які конкретно наслідки буде мати конкретна загроза для інформаційної системи, компанії або користувачів. Наприклад, кібератака може призвести

до різного ступеня шкоди – від тимчасового збою в роботі системи до серйозних фінансових і репутаційних втрат.

3. Невизначеність щодо вразливостей. Іноді неможливо точно передбачити, чи організація має незахищені уразливості в своїх інформаційних системах, які можуть стати об’єктом атаки. Це може бути через постійно змінювані технології та методи злому.

У табл. 2.1 наведено рівні невизначеності для деяких видів ризиків.

Таблиця 2.1 – Рівні невизначеності ризиків

Ризик	Невизначеність	Пояснення
Витік даних	Середня	Хоча організації можуть впроваджувати політики безпеки, атаки часто мають непередбачуваний характер
Незаконний доступ до інформації	Висока	Ризик може виникнути в будь-який момент, якщо механізми безпеки не відповідають новим загрозам.
Зміна або модифікація даних	Низька	Модифікацію даних часто можна виявити через регулярні перевірки систем або аудит.
Пошкодження даних	Середня	Системи резервного копіювання можуть зменшити ризик, але технічні проблеми можуть виникати непередбачувано.
Атака типу DDoS	Висока	Атаки DDoS мають низьку ймовірність, але можуть мати серйозні наслідки, особливо якщо організація не підготовлена.
Несправність системи або обладнання	Середня	Технічні несправності можуть бути передбачені, якщо проводяться регулярні технічні перевірки.
Комп’ютерні віруси	Середня	За допомогою антивірусних систем можна знизити ймовірність зараження, але нові види вірусів можуть бути складні для виявлення.
Атаки через фішинг	Висока	Складно передбачити, коли саме зловмисники запустять таку атаку, особливо коли вона спрямована на окремих користувачів.
Необережність співробітників	Середня	Ризик можна зменшити завдяки регулярному навчанню та перевіркам.
Зловживання правами доступу	Низька	Можна контролювати через обмеження прав доступу та моніторинг діяльності співробітників.
Кіберзлочинці	Висока	Злочинці постійно вдосконалюють свої методи атак, що ускладнює їх прогнозування.
Природні катастрофи	Висока	Природні катастрофи важко прогнозувати, однак вони можуть мати руйнівні наслідки.

Причини невизначеності інформаційних ризиків визначаються через кілька факторів:

1. Швидкий розвиток технологій: Технології безпеки постійно змінюються, і нові методи атак з’являються швидше, ніж їх можна виявити та запобігти.

2. Зміни в загрозах і вразливостях: Постійні зміни в кіберзагрозах, нові вразливості в програмному забезпеченні та апаратному забезпеченні, нові методи соціальної інженерії тощо ускладнюють прогнозування інформаційних ризиків.

3. Людський фактор. Людський фактор є основним джерелом невизначеності. Помилки співробітників, порушення політик безпеки або навіть умисні дії можуть викликати труднощі в прогнозуванні та оцінці ризиків.

4. Складність оцінки впливу. Оцінка впливу загрози на інформаційні системи і дані може бути дуже складною, оскільки різні організації можуть мати різні рівні захисту і різні види даних, які потребують різного рівня захисту.

Для зменшення невизначеності та управління інформаційними ризиками використовуються кілька підходів:

1. Аудит і тестування безпеки. Регулярне проведення аудитів інформаційної безпеки, виявлення вразливостей і тестування систем допомагає зменшити невизначеність щодо можливих загроз та вразливих місць у системах.

2. Використання моделювання ризиків. Моделювання ризиків дозволяє передбачити ймовірні сценарії розвитку загроз і оцінити можливі наслідки різних варіантів ситуацій, що зменшує невизначеність при прийнятті рішень.

3. Застосування стандартів і протоколів безпеки: Впровадження міжнародних стандартів (наприклад, ISO/IEC 27001) дозволяє знизити невизначеність, адже вони надають структуровані підходи до управління інформаційною безпекою.

4. Планування реагування на інциденти. Розробка і впровадження планів реагування на інциденти допомагає організаціям швидко і ефективно

реагувати на непередбачувані ситуації, що виникають у разі реалізації інформаційного ризику.

5. Навчання і підвищення обізнаності співробітників. Зниження ризиків, пов'язаних з людським фактором (наприклад, фішинг, несанкціоноване поширення даних), можна досягти через підвищення обізнаності співробітників і навчання їх методам кібербезпеки.

2.3. Шкала тяжкості наслідків ризику

Шкала тяжкості наслідків ризику – це інструмент, який використовується для оцінки потенційного впливу ризику на організацію, її діяльність, ресурси та репутацію в разі його реалізації. Вона допомагає визначити пріоритети в управлінні ризиками та сприяє ухваленню рішень про заходи для зменшення цього ризику.

Зазвичай шкала тяжкості наслідків ризику представлена у вигляді бальних оцінок (від 1 до 5 або від 1 до 10), де 1 – це мінімальний вплив, а максимальне значення – найбільш серйозні наслідки.

Приклад шкали тяжкості наслідків ризику:

1. Мінімальний вплив (1-2 бали).

Наслідки: несуттєві або тимчасові проблеми, що не мають значного впливу на операційну діяльність або репутацію компанії.

Приклад: легке порушення роботи внутрішньої мережі, що не призводить до втрат даних або зниження ефективності роботи. Можлива затримка в доступі до певних систем.

Можливі заходи: невеликий обсяг дій для відновлення роботи. Може бути достатньо мінімальних коригувальних дій.

2. Низький вплив (3-4 бали).

Наслідки: проблеми, які впливають на певні процеси або відділи, але не мають значного ефекту на загальну діяльність організації. Можливо, виникають незначні фінансові втрати.

Приклад: втрата незначної кількості даних або тимчасовий доступ до обмеженої частини інформації (наприклад, не критичної для бізнесу).

Можливі заходи: необхідно вжити певні заходи для виправлення ситуації, але загальний вплив на бізнес обмежений.

3. Середній вплив (5-6 балів).

Наслідки: вплив на операційну діяльність організації або фінансові результати. Збої в роботі можуть вплинути на певні департаменти, але не призводять до серйозних втрат. Може виникнути тимчасова втрата репутації.

Приклад: витік конфіденційної, але не критичної інформації (наприклад, втрата даних про співробітників або нетехнічних аспектів бізнесу). Можлива затримка у виконанні важливих завдань або проєктів.

Можливі заходи: потрібно вжити певних коригувальних дій для відновлення нормальної діяльності. Може знадобитися внутрішнє розслідування або інші адекватні дії.

4. Високий вплив (7-8 балів).

Наслідки: суттєвий вплив на функціонування компанії, великий фінансовий збиток або серйозні репутаційні втрати. Можливе порушення виконання основних бізнес-процесів, що впливають на клієнтів чи постачальників.

Приклад: перехоплення важливої корпоративної інформації, фінансових даних або інтелектуальної власності. Серйозні наслідки для бренду і репутації. Можлива втрата великих клієнтів.

Можливі заходи: потрібно вжити оперативних і серйозних заходів для виправлення ситуації, включаючи юридичні дії. Можливе залучення зовнішніх експертів для відновлення бізнесу.

5. Критичний вплив (9-10 балів).

Наслідки: критичні наслідки для організації, можливе призупинення її діяльності або банкрутство. Значні фінансові втрати, серйозне порушення безпеки, репутаційні катастрофи.

Приклад: витік або крадіжка важливих даних (фінансових, клієнтських або технічних), що призводить до серйозних юридичних наслідків, втрата цінних клієнтів або великі штрафи за порушення норм захисту даних.

Можливі заходи: потрібно негайно вжити всі доступні заходи для мінімізації шкоди, включаючи співпрацю з правоохоронними органами, судові позови та відновлення репутації через публічні заяви.

Приклад застосування шкали тяжкості для інформаційного ризику:

Сценарій: порушення безпеки на корпоративному сервері, у результаті якого відбувся витік особистих даних клієнтів.

Мінімальний вплив (1-2 бали): витік незначної кількості даних, що не впливає на безпеку клієнтів і не веде до фінансових втрат або репутаційних збитків.

Низький вплив (3-4 бали): витік даних, що може вплинути на деякі сегменти клієнтів, але без серйозних фінансових або юридичних наслідків для організації.

Середній вплив (5-6 балів): витік важливих, але не критичних даних, які можуть призвести до невеликих фінансових втрат або пошкодження репутації.

Високий вплив (7-8 балів): витік важливих особистих даних клієнтів, що веде до значних фінансових збитків або потенційних судових позовів від клієнтів.

Критичний вплив (9-10 балів): витік великих обсягів критичних даних, що веде до масштабних фінансових втрат, серйозних юридичних наслідків та загрози для існування компанії.

2.4. Приклад вирішення задачі

Задача: організація використовує відкриту бездротову мережу для підключення своїх співробітників. Мережа не має належного шифрування та паролів, що створює ризик перехоплення даних. Необхідно класифікувати

ризик. Оцінити ймовірність виникнення та вплив цього ризику. Запропонувати заходи для зменшення цього ризику.

Рішення:

1. Класифікація ризику:

- Тип ризику: кіберризик, пов’язаний з безпекою інформаційних систем, оскільки ризик стосується захисту даних, що передаються через бездротову мережу.

- Тип загрози: загроза перехоплення даних, оскільки відсутність належного шифрування дозволяє стороннім особам (наприклад, хакерам) перехоплювати і зчитувати дані, що передаються через мережу.

- Тип уразливості: відкрите підключення без паролів та шифрування. Відсутність базових засобів захисту, таких як WPA2 (шифрування) або паролі, створює велику ймовірність для несанкціонованого доступу.

- Тип інформації, що піддається ризику: конфіденційна інформація компанії, наприклад, електронна пошта, особисті дані співробітників або корпоративні документи, які можуть бути зловмисно зчитані через відкриту мережу.

- Тип впливу: витік конфіденційної інформації може призвести до порушення конфіденційності і навіть до фінансових і репутаційних втрат для компанії.

2. Оцінка ймовірності та впливу ризику:

- Ймовірність виникнення ризику: у разі використання відкритої бездротової мережі без належного захисту ймовірність перехоплення даних є високою. Зловмисники можуть використовувати різні методи, такі як моніторинг трафіку (наприклад, через Wi-Fi зловмисника або програмне забезпечення для перехоплення даних), для того щоб побачити та зібрати незахищену інформацію. Враховуючи, що мережа не має паролів і не шифрує передану інформацію, ймовірність того, що зловмисники можуть зчитати трафік, становить 80-90 % у випадку використання стандартних інструментів для прослуховування бездротового сигналу.

- Вплив ризику: якщо зловмисники отримають доступ до конфіденційних даних (наприклад, паролів, фінансової інформації, робочих документів), це може спричинити:

- фінансові втрати через зловживання інформацією;

- пошкодження репутації компанії (наприклад, втрата довіри клієнтів, співробітників);

- юридичні наслідки: порушення стандартів захисту даних (наприклад, GDPR, якщо йдеться про особисті дані клієнтів або співробітників).

Враховуючи, що йдеться про відкриту мережу, і якщо зловмисники зможуть перехопити критично важливу інформацію, вплив буде критичним. Його оцінка може становити 7-9 балів із 10 за шкалою тяжкості.

3. Заходи для зменшення цього ризику:

- Впровадження шифрування (WPA2 або WPA3): найперше, що необхідно зробити – це встановити на маршрутизаторі належне шифрування для бездротової мережі. Використання WPA2 (Wi-Fi Protected Access 2) або WPA3 (новіший стандарт, який забезпечує кращу безпеку) є найефективнішим способом запобігання перехопленню даних.

- Використання паролів для доступу до мережі: відкрита мережа є дуже вразливою, тому потрібно обов’язково встановити паролі для підключення. Важливо, щоб паролі були достатньо складними та часто змінювались. Впровадження політики складних паролів для доступу до мережі значно підвищить рівень безпеки.

- VPN (Virtual Private Network): всі співробітники, які підключаються до відкритої бездротової мережі, повинні використовувати VPN. VPN шифрує весь інтернет-трафік, що значно знижує ризик перехоплення даних.

- Моніторинг трафіку: для своєчасного виявлення спроб несанкціонованого доступу та перехоплення даних, можна впровадити системи моніторингу трафіку, які будуть фіксувати підозрілі дії в мережі (наприклад, несанкціоновані підключення).

- Інструктаж для співробітників: важливо провести навчання співробітників щодо небезпек використання відкритих мереж і переконатися, що вони розуміють необхідність використання шифрування, паролів та VPN під час підключення до мережі.

- Оновлення програмного забезпечення: переконатися, що програмне забезпечення на маршрутизаторах, ноутбуках та інших пристроях актуальне, оскільки старі версії можуть мати відомі вразливості.

- Аудит безпеки: регулярно проводити аудит безпеки бездротових мереж і перевіряти, чи виконуються вимоги щодо шифрування та захисту мережі.

2.5. Індивідуальні завдання

Для вказаної ситуації виконати класифікацію ризика: визначити його тип, тип загрози, тип уразливості, тип інформації, яка піддається ризику, тип впливу. Оцінити ймовірність виникнення ризику та його вплив. Запропонувати заходи для зменшення ризику.

1. Оцінка ризику атаки через фішинг. Співробітник компанії отримав електронний лист, який виглядав як офіційне повідомлення від банку, із запитом на оновлення даних для доступу до корпоративного рахунку. Лист мав на меті отримати конфіденційні дані через фальшивий вебсайт.

2. Оцінка ризику конфіденційності. В організації працює кілька департаментів, і один із них має доступ до чутливих даних клієнтів, таких як адреси, номери телефонів і фінансові реквізити. Через недостатній контроль за доступом до системи, один із співробітників випадково надсилає лист з цією інформацією неправомірному адресату через електронну пошту.

3. Оцінка ризику доступності даних. Компанія використовує хмарне сховище для зберігання важливої документації, включаючи фінансові звіти та контракти. У зв’язку з відсутністю плану відновлення після катастрофи,

під час перебоїв в інтернет-з’єднанні важливі файли стали недоступні на кілька годин, що вплинуло на роботу всіх департаментів.

4. Оцінка ризику шкідливих програм. У компанії співробітники часто використовують корпоративні ноутбуки для роботи вдома. Останнім часом спостерігається велика кількість повідомлень про фішинг-атаки через електронну пошту, і один із співробітників випадково завантажив шкідливу програму, яка зашифрувала важливі корпоративні файли.

5. Оцінка ризику несанкціонованого доступу. В організації є внутрішня база даних з фінансовою інформацією. Один із співробітників, маючи доступ до бази, навмисно змінює суми транзакцій, що викликає фінансові втрати. Після цього, коли інші співробітники звертаються до системи, вони помічають ці зміни.

6. Оцінка ризику фішингу. Співробітники компанії отримали електронні листи, що виглядали як повідомлення від служби підтримки їхнього банку. Листи містили посилання для оновлення банківських реквізитів. Один із співробітників, не звернувши увагу на підозрілість листа, перейшов за посиланням і ввів свої облікові дані.

7. Оцінка ризику помилок у програмному забезпеченні. В організації використовується програмне забезпечення для обробки замовлень. У результаті недавнього оновлення програми з’явилась помилка, через яку деякі замовлення не потрапляли до обробки, що спричинило втрату потенційних клієнтів.

8. Оцінка ризику несанкціонованого доступу до системи. Співробітники можуть входити в систему за допомогою пароля. Однак є підозра, що один із співробітників передав свої облікові дані колезі, і той отримав несанкціонований доступ до чутливої інформації.

9. Оцінка ризику фізичної втрати даних. Під час відрядження один із співробітників втратив ноутбук, на якому зберігалася важлива корпоративна інформація без шифрування.

10. Оцінка ризику атаки типу DDoS. Компанія виявила, що вебсайт часто стає недоступним через величезну кількість запитів, які надходять одночасно, що перешкоджає користувачам доступу до сайту.

11. Оцінка ризику невдачі системи резервного копіювання. Під час спроби відновлення даних компанія з'ясувала, що система резервного копіювання не працює належним чином, через що важливі файли не були відновлені після збоїв в основній системі.

12. Оцінка ризику помилок під час інтеграції систем. Під час інтеграції нової системи для автоматизації бухгалтерії виникли проблеми з синхронізацією даних, через що деякі транзакції не потрапили в фінансові звіти.

13. Оцінка ризику витоку конфіденційної інформації через соціальні мережі. Один з працівників компанії в особистих соціальних мережах випадково опублікував скріншоти внутрішніх документів організації, які містили чутливу фінансову інформацію. Через кілька днів ця інформація стала доступною для широкої аудиторії.

14. Оцінка ризику недостатньої захищеності хмарного сховища. Компанія зберігає важливі дані в хмарному сховищі стороннього постачальника послуг. Після проведення аудиту виявлено, що в налаштуваннях доступу до сховища були дозволені недостатньо жорсткі правила безпеки, і доступ до даних був можливий за допомогою простих паролів.

2.6. Контрольні запитання

1. За якими категоріями можна класифікувати інформаційні ризики?
2. Що таке невизначеність інформаційних ризиків?
3. Які типи невизначеності ризиків існують?
4. Поясніть для кількох інформаційних ризиків рівні їх невизначеності.
5. Які фактори впливають на рівень невизначеності інформаційних ризиків?

6. Яким чином можна зменшити рівень невизначеності ризику?

7. Перерахуйте ключові властивості ризик-менеджменту.

8. Що таке шкала тяжкості наслідків ризику?

9. Чим визначається рівень впливу по шкалі тяжкості?

10. Наведіть приклади оцінювання кількох інформаційних ризиків за шкалою тяжкості.

3. УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РИЗИКАМИ

Мета заняття: ознайомитись з основними етапами та методиками управління інформаційними ризиками, а також навчитись застосовувати методику NIST для оцінки та управління інформаційними ризиками в організації.

3.1. Етапи та заходи управління інформаційними ризиками

Управління інформаційними ризиками – це процес виявлення, оцінки, контролю та зменшення ризиків, що можуть вплинути на інформаційні ресурси та інформаційні технології організації. Це важливий компонент стратегії забезпечення кібербезпеки, який дозволяє знизити ймовірність і вплив можливих загроз на конфіденційність, цілісність та доступність даних.

Основні етапи управління інформаційними ризиками:

1. Ідентифікація ризиків. На цьому етапі проводиться виявлення всіх можливих загроз і вразливостей, що можуть вплинути на інформаційні ресурси організації.

2. Оцінка ризиків. Оцінка ймовірності того, що конкретний ризик здійсниться, а також визначення його потенційного впливу на організацію.

3. Аналіз і пріоритизація ризиків. Ризики оцінюються на основі їх ймовірності та серйозності наслідків. Ризики, які мають високу ймовірність і значний вплив, отримують вищий пріоритет.

4. Розробка стратегії управління ризиками. Розробка плану для мінімізації або уникнення ризиків. Стратегії можуть включати:

- прийняття ризику (коли вплив є незначним або організація готова його прийняти);

- зменшення ризику (впровадження заходів для зменшення ймовірності чи впливу);

- уникнення ризику (зміна умов або діяльності, щоб уникнути ризику);

- передача ризику (перенесення частини ризику на сторонніх партнерів, наприклад, через страхування чи аутсорсинг).

5. Впровадження заходів для управління ризиками. На цьому етапі реалізуються практичні заходи для контролю ризиків.

6. Моніторинг і аудит. Постійний моніторинг стану безпеки інформаційних систем і перевірка ефективності заходів, вжитих для зменшення ризиків.

7. Відповідь на інциденти. Планування та виконання дій у разі реалізації інформаційного ризику або інциденту безпеки. Включає оперативне реагування, розслідування інциденту, відновлення та мінімізацію наслідків.

8. Навчання і підвищення обізнаності. Проведення тренінгів для співробітників, щоб вони розуміли ризики та методи їх уникнення, особливо в контексті захисту інформаційної безпеки.

Заходи для управління інформаційними ризиками:

1. Впровадження політики безпеки. Розробка внутрішніх нормативних документів, які регулюють доступ до інформаційних ресурсів, обробку даних, їх збереження та передачу.

2. Шифрування даних. Використання технологій шифрування для захисту даних, що зберігаються або передаються в мережі.

3. Аутентифікація та авторизація. Впровадження багаторівневої автентифікації (наприклад, по паролю, відбитку пальця та смарт-картці) для забезпечення безпеки доступу до інформаційних систем.

4. Інформаційне навчання та обізнаність персоналу. Організація регулярних тренінгів і тестувань для співробітників, щоб знизити ризик людських помилок (наприклад, натискання на фішингові посилання).

5. Оновлення програмного забезпечення та систем. Регулярне оновлення програмного забезпечення для виправлення вразливостей і зниження ймовірності використання їх зловмисниками.

6. Резервне копіювання даних. Регулярне створення резервних копій критичних даних для захисту від їх втрати через атаки чи технічні збої.

3.2. Методики управління інформаційними ризиками

Методики управління інформаційними ризиками допомагають організаціям ефективно і системно підходити до виявлення, оцінки, управління та зниження ризиків, що виникають у процесі обробки інформації. Існує кілька різних підходів і методик для управління інформаційними ризиками, серед яких найбільш відомими є:

1. Методика NIST (National Institute of Standards and Technology). NIST розробив низку стандартів і керівництв, які визначають підходи до управління інформаційними ризиками, зокрема для забезпечення кібербезпеки. Підхід включає ідентифікацію активів, оцінку загроз і вразливостей, визначення контролів безпеки, моніторинг і реагування на інциденти безпеки. Основні документи:

- NIST Cybersecurity Framework (CSF) – набір стандартів, кращих практик і керівних принципів, що допомагають організаціям визначити, запобігти, виявити, реагувати та відновлюватися після інцидентів безпеки;

- NIST SP 800-53 – рекомендації щодо контролю безпеки для інформаційних систем та організацій;

- NIST SP 800-30 – методика оцінки ризиків, яка дозволяє організаціям оцінювати ймовірність та наслідки ризиків.

2. Методика ISO 27001 (International Organization for Standardization) – міжнародний стандарт для систем управління безпекою інформації (ISMS), що охоплює створення політик безпеки, оцінку ризиків і визначення управлінських заходів для мінімізації ризиків. Підхід включає регулярні оцінки ризиків, використання політик і процедур для контролю безпеки, а також постійний моніторинг і вдосконалення системи управління. Основні принципи:

- визначення контексту та масштабів ISMS;

- оцінка і управління ризиками за допомогою оцінки вразливостей, загроз та впливу на активи;

- визначення заходів для зменшення або контролю ризиків;

- моніторинг і перегляд ефективності системи управління.

3. Методика COBIT (Control Objectives for Information and Related Technologies) – набір найкращих практик для управління IT, зокрема управління ризиками та безпекою інформаційних систем. Підхід полягає в чіткому розмежуванню між керівництвом, технічними і операційними аспектами IT-безпеки, зокрема через управління активами, ризиками та перевірки виконання. Основні принципи:

- визначення стратегічних цілей IT та відповідних процесів управління безпекою;

- управління ризиками через стандартизацію та моніторинг процесів;

- визначення та управління IT-активами для забезпечення їх безпеки;

- перевірка результатів і впровадження покращень на основі аналізу.

4. Методика FAIR (Factor Analysis of Information Risk) – методика для кількісної оцінки ризиків, яка допомагає організаціям визначати ймовірність і вплив інцидентів безпеки, використовуючи математичні моделі. Методика базується на кількісних оцінках, що дозволяє точно прогнозувати ймовірність і вплив різних типів інцидентів безпеки та визначити відповідні фінансові ризики. Основні принципи:

- аналіз загроз і вразливостей;

- визначення факторів ризику (ймовірність, рівень загрози, потенційні наслідки);

- розрахунок потенційного фінансового впливу на організацію.

5. Методика OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) – методика, орієнтована на управління ризиками інформаційної безпеки, що зосереджена на оцінці критичних активів організації, загрозах та вразливостях. OCTAVE фокусується на практичному

впровадженні управління ризиками з урахуванням організаційної стратегії та потреб у безпеці. Основні принципи:

- ідентифікація та аналіз критичних активів;

- визначення потенційних загроз і вразливостей;

- визначення рівня впливу на організацію та можливі заходи для їх зменшення.

6. Методика IRAM (Information Risk Assessment Methodology) є методикою оцінки та управління інформаційними ризиками, що надає конкретні кроки для виявлення та оцінки ризиків в інформаційних системах. IRAM дозволяє організаціям зібрати необхідну інформацію для того, щоб сформувати адекватну стратегію безпеки та забезпечити відповідне управління ризиками. Основні принципи:

- ідентифікація інформаційних активів і систем;

- оцінка загроз, вразливостей і впливу на організацію;

- пріоритизація ризиків для визначення найбільш критичних загроз.

7. Методика Risk IT – методика, розроблена ISACA (Information Systems Audit and Control Association, міжнародна професійна асоціація, орієнтована на IT-управління), яка зосереджена на управлінні ризиками IT та їх впливі на бізнес. Вона допомагає організаціям ефективно керувати IT-ризиками через управління безпекою, захистом даних і управління проєктами. Risk IT забезпечує системний підхід до управління ризиками, з урахуванням специфіки IT-інфраструктури та її інтеграції в загальні бізнес-процеси. Основні принципи:

- визначення ризиків IT і їх інтеграція в загальний процес управління бізнесом;

- оцінка та управління ризиками в контексті IT-стратегій;

- визначення та мінімізація впливу IT-інцидентів на організацію.

3.3. Використання методики NIST

Детальний приклад використання методики NIST для управління інформаційними ризиками на прикладі організації, яка зберігає конфіденційні фінансові дані клієнтів через онлайн-платформу.

Опис організації: організація є великою фінансовою компанією, яка обробляє та зберігає конфіденційні фінансові дані своїх клієнтів. Операції проводяться через онлайн-платформу, і компанія повинна забезпечити захист цих даних від внутрішніх і зовнішніх загроз.

Для вирішення використовуються такі документи NIST:

1. NIST SP 800-30 (Guide for Conducting Risk Assessments) – забезпечує керівництво щодо проведення оцінки ризиків, визначаючи, як ідентифікувати загрози та вразливості, а також оцінювати ймовірність та наслідки потенційних інцидентів.

2. NIST SP 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations) – визначає набір безпекових контролів, яких повинна дотримуватися організація для захисту своїх інформаційних систем. Він включає в себе контроль доступу, захист даних, моніторинг безпеки тощо.

3. NIST SP 800-39 (Managing Information Security Risk: Organization, Mission, and Information System View) – описує підходи для управління інформаційними ризиками на різних рівнях організації, включаючи рівень інформаційних систем, рівень бізнес-процесів і організаційний рівень.

4. NIST SP 800-61 (Computer Security Incident Handling Guide) – визначає кроки та процедури для реагування на інциденти безпеки, що включає в себе ідентифікацію інциденту, його оцінку та відновлення.

5. NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment) – пропонує методології для тестування безпеки систем та оцінки їх вразливостей, що є важливим кроком для виявлення слабких місць у системах.

Кроки використання методики NIST для управління ризиками:

1. Ідентифікація активів і загроз (NIST SP 800-30):

1.1. Початковий етап включає визначення активів організації, які потребують захисту. Для фінансової компанії це можуть бути:

- фінансові дані клієнтів;

- персональна інформація клієнтів;

- онлайн-платформа для обробки транзакцій.

1.2. Після ідентифікації активів, наступним кроком є виявлення загроз, які можуть вплинути на ці активи. Це можуть бути:

- зовнішні кіберзагрози, такі як хакерські атаки або фішинг;

- внутрішні загрози, зокрема, співробітники з ненадійним доступом до даних;

- технічні вразливості в програмному забезпеченні або мережах.

2. Оцінка ймовірності та впливу (NIST SP 800-30). Оцінка ймовірності виникнення кожної загрози та її потенційного впливу дозволяє визначити, які ризики є найважливішими. Наприклад, для фішингових атак ймовірність може бути високою, але вплив може бути значно меншим, якщо організація застосовує двофакторну аутентифікацію для користувачів. Для DDoS-атак ймовірність може бути середньою, але вплив буде високим, оскільки атакована система може стати недоступною, що призведе до втрати доходів.

3. Визначення контролів безпеки та впровадження (NIST SP 800-53). Оскільки оцінено, які ризики є найбільшими, наступний крок – впровадження контролів безпеки. Відповідно до NIST SP 800-53, організація має застосувати такі заходи:

- контроль доступу – використовувати багаторівневу аутентифікацію для доступу до критичних даних;

- шифрування – шифрувати дані як при зберіганні, так і при передачі, використовуючи протокол TLS;

- аудит і моніторинг – впровадити системи моніторингу для виявлення аномальних дій, що можуть свідчити про порушення безпеки;

- регулярне оновлення – проводити регулярні оновлення програмного забезпечення, щоб усувати вразливості;

- фізичний захист – забезпечити фізичний захист серверів, на яких зберігаються дані.

4. Моніторинг та управління ризиками (NIST SP 800-39). Управління ризиками повинно бути постійним процесом. Важливо регулярно переглядати ефективність впроваджених заходів та вносити необхідні корективи. Проводити регулярні аудити та перевірки відповідності контрольним стандартам, таким як ISO 27001, та тестування на вразливості (тест на проникнення або пентестинг, penetration test, pentesting – метод оцінювання захищеності комп'ютерної системи чи мережі шляхом часткового моделювання дій зовнішніх зловмисників з проникнення у неї).

5. Реагування на інциденти та відновлення (NIST SP 800-61). У випадку виявлення інциденту безпеки, таких як витік даних або компрометація системи, компанія повинна мати чіткий план дій. Згідно з NIST SP 800-61:

- визначити тип інциденту;

- ізолювати пошкоджену систему для запобігання подальшому поширенню атаки;

- оцінити обсяг пошкоджень та відновити систему з резервних копій;

- сповістити відповідні органи (якщо це необхідно за законом) і клієнтів про інцидент.

6. Тестування та вдосконалення заходів безпеки (NIST SP 800-115). Після впровадження заходів безпеки, організація повинна регулярно тестувати їхню ефективність. Це включає:

- тестування на проникнення (pentesting) для виявлення вразливих місць;

- оцінка вразливостей у програмному забезпеченні та мережах, що можуть бути експлуатовані атакувальниками;

- оцінка ефективності засобів моніторингу та реагування.

Другий приклад описує оцінку ризиків, пов’язаних з оновленням критичних програмних компонентів у системі.

Формулювання задачі: оцінити ризики, пов’язані з оновленням критичних програмних компонентів у системі. Для цього необхідно використовувати методику NIST SP 800-40 для управління оновленнями програмного забезпечення.

Рекомендується застосовувати автоматизовані засоби для виявлення необхідних оновлень, тестувати оновлення в окремому середовищі перед їхнім впровадженням у виробниче середовище. Важливо також створити план оновлень, щоб уникнути потенційних проблем з сумісністю або безпекою.

Кроки використання методики NIST для управління ризиками:

1. Оцінка ризиків. На першому кроці важливо проаналізувати основні ризики, пов’язані з оновленням програмного забезпечення. Ключові ризики можуть включати:

- несумісність оновлень з існуючою інфраструктурою. Програмні оновлення можуть призвести до неполадок або несумісності з іншими компонентами системи, що може призвести до втрати функціональності чи навіть до падіння системи;

- відсутність належного тестування оновлень. Оновлення можуть містити баги чи уразливості, які, не протестовані в середовищі, подібному до виробничого, можуть спричинити збої в роботі або збільшити уразливість системи до атак;

- невірно налаштовані права доступу після оновлення. Відновлення або зміна конфігурації програмних компонентів під час оновлення може призвести до проблем із правами доступу, що створює можливість для несанкціонованого доступу;

- безпека оновлень. Відсутність перевірки цілісності і автентичності оновлень може дозволити зловмисникам використовувати їх як канал для

впровадження шкідливого коду (наприклад, через атаки типу Man-in-the-Middle або використання шкідливих оновлень);

- проблеми з резервним копіюванням і відновленням. Якщо система має помилки після оновлення, і не було проведено достатнього резервного копіювання даних чи належного плану відновлення, то можуть виникнути серйозні проблеми у відновленні інформації або функціональності системи.

2. Застосування NIST SP 800-40 для управління оновленнями. NIST SP 800-40 – це стандарт, який надає рекомендації щодо управління оновленнями програмного забезпечення для мінімізації ризиків безпеки.

Кроки для управління оновленнями:

2.1. Ідентифікація оновлень, що потребують впровадження:

- регулярно перевіряти наявність нових оновлень для всіх програмних компонентів, які мають критичне значення для безпеки та функціонування системи;

- оновлення повинні бути класифіковані на основі їхньої важливості (критичні оновлення, виправлення безпеки, виправлення багів тощо).

2.2. Тестування оновлень:

- перед тим як оновлення будуть впроваджені в основну систему, потрібно проводити їх тестування в контрольованому середовищі, яке максимально відображає виробничі умови.

- тестування повинно включати перевірку на сумісність з іншими програмними компонентами та перевірку наявності потенційних вразливостей або проблем.

2.3. Розробка плану впровадження оновлень: створення детального плану оновлення, який включає чіткі процедури для кожного етапу оновлення:

- попередження користувачів і адміністраторів про заплановані оновлення;

- проведення оновлення в години мінімальної активності користувачів (якщо можливо);

- моніторинг системи після оновлення для виявлення можливих проблем або неполадок.

2.4. Контроль за безпекою оновлень:

- перевірка джерела оновлень для впевненості в їхній легітимності та цілісності;

- використання цифрових підписів або хеш-сум для перевірки, що оновлення не було змінено під час завантаження;

- якщо можливо, здійснення шифрування файлів оновлень для запобігання маніпуляціям з ними під час передачі через мережу.

2.5. Резервне копіювання та відновлення після оновлення:

- перед впровадженням оновлення необхідно створити повну резервну копію всіх важливих даних та конфігурацій;

- у випадку невдачі оновлення повинна бути готова стратегія відновлення (rollback) до попередньої робочої версії програмного забезпечення.

2.6. Моніторинг та аудит:

- після впровадження оновлення організація повинна здійснювати моніторинг на наявність будь-яких аномальних подій, які можуть бути пов’язані з оновленням;

- проведення аудиту дозволяє виявити і оцінити будь-які проблеми безпеки, що можуть виникнути після оновлення.

3. Зниження ризиків за допомогою NIST SP 800-40.

3.1. Впровадження багаторівневого тестування оновлень. Застосування середовищ для тестування, включаючи середовище розробки, середовище для тестування та проміжне середовище, яке може бути аналогічним до виробничого, дозволяє виявляти потенційні проблеми до застосування оновлення в основній системі.

3.2. Використання автоматизованих систем для моніторингу оновлень. Інструменти для автоматичного відслідковування оновлень забезпечують

своєчасне реагування на нові версії програмного забезпечення, що можуть виправляти вразливості.

3.3. Документування і стандартизація процесів оновлення. Створення чітких інструкцій для адміністраторів з впровадження оновлень та налаштування автоматизованих процесів допомагає знизити ризик помилок через людський фактор.

3.4. Інтеграція з політиками безпеки організації. Усі оновлення повинні бути частиною загальної стратегії з управління інформаційними ризиками в організації. Це дозволить забезпечити узгодженість із політиками безпеки та додатковими заходами захисту.

4. Реалізація та контроль.

4.1. Проведення оновлення. Після тестування та перевірки всіх компонентів, оновлення можна провести у виробничому середовищі. Важливо це зробити в період низької активності користувачів (якщо це можливо) для мінімізації можливих збоїв.

4.2. Моніторинг результатів оновлення. Після виконання оновлення необхідно уважно моніторити систему на предмет неполадок або аномальних подій. Одразу реагувати на будь-які проблеми, що виникають, і при необхідності відкотити оновлення до попереднього стану.

4.3. Завершення процесу оновлення та звітність. Після успішного впровадження оновлень, провести підсумковий аудит і звітування. Переконатися, що всі компоненти працюють без порушень, і надати звіт керівництву або зацікавленим сторонам.

3.4. Індивідуальні завдання

Для вказаної ситуації за допомогою методики NIST розробити основні етапи управління інформаційними ризиками. Необхідні документи NIST можна отримати за посиланням: https://csrc.nist.gov/publications/sp800

1. **Ідентифікація ризиків для корпоративної мережі.** Визначити всі можливі ризики для мережі організації, яка використовує складну інфраструктуру серверів та клієнтських пристроїв. При вирішенні використовувати NIST SP 800-30 для ідентифікації загроз і вразливостей, здійснивши аналіз мережі та інфраструктури. Оцінити ймовірність і вплив кожної загрози для визначення рівня ризику.

2. **Аналіз ймовірності та впливу кіберзагроз.** Оцінити ймовірність і вплив різних типів кіберзагроз (наприклад, фішинг, DDoS-атаки) для компанії, яка здійснює онлайн-продажі. При вирішенні використовувати NIST SP 800-39 для визначення ймовірності загроз і оцінки їх впливу на бізнес-процеси. Для кожної кіберзагрози оцінити ймовірність виникнення та їх вплив. Також визначити пріоритетність заходів безпеки.

3. **Оцінка безпеки хмарних сервісів.** Оцінити ризики, пов’язані з використанням хмарних сервісів для зберігання даних і обробки транзакцій. При вирішенні використовувати рекомендації NIST SP 800-53 для аналізу ризиків безпеки хмарних рішень.

4. **Моніторинг внутрішніх загроз.** Виявити внутрішні загрози, наприклад, зловживання доступом співробітників до конфіденційних даних. При вирішенні використовувати NIST SP 800-53 для визначення заходів контролю доступу та моніторингу активності співробітників.

5. **Розробка плану відновлення після катастроф.** Розробити план відновлення після природної катастрофи (наприклад, повені чи землетрусу), що може пошкодити фізичну інфраструктуру. При вирішенні використовувати NIST SP 800-34 для створення плану відновлення бізнесу та забезпечення безперервності роботи.

6. **Аналіз захисту даних при передачі через незахищені мережі.** Оцінити ризики, пов’язані з передачею чутливих даних через незахищені мережі, наприклад, через відкриту Wi-Fi мережу. При вирішенні використовувати NIST SP 800-53 для визначення вимог до шифрування та захисту даних при передачі.

7. Аналіз загроз для інтернет-магазину. Оцінити потенційні ризики для інтернет-магазину, зокрема можливість витоку фінансових даних або компрометації платіжних систем. При вирішенні використовувати NIST SP 800-30 для ідентифікації загроз для електронної комерції та оцінки їх ймовірності та впливу.

8. Оцінка впливу вразливостей програмного забезпечення. Оцінити ризики, пов'язані з використанням вразливих програмних компонентів в організації. При вирішенні використовувати NIST SP 800-53 для визначення вразливостей та розробки стратегій для їх усунення.

9. Ідентифікація фізичних загроз для серверів. Оцінити фізичні ризики для серверів, які зберігають критично важливі дані компанії. При вирішенні використовувати NIST SP 800-53 для оцінки фізичних загроз і визначення контролів безпеки, таких як доступ до серверних кімнат.

10. Ризики від зовнішніх постачальників. Оцінити ризики, які виникають через співпрацю з зовнішніми постачальниками, зокрема щодо доступу до систем і даних компанії. При вирішенні використовувати NIST SP 800-161 для управління ризиками постачальників та визначення контролів для забезпечення безпеки.

11. Оцінка ризиків для мережевої інфраструктури. Оцінити безпеку корпоративної мережевої інфраструктури (мережі, маршрутизатори, брандмауери). При вирішенні використовувати NIST SP 800-115 для тестування мережі на вразливості і визначення контролів захисту.

12. Управління ризиками, пов'язаними з мобільними пристроями. Оцінити ризики, пов'язані з використанням мобільних пристроїв у корпоративній мережі (наприклад, смартфонів та планшетів). При вирішенні використовувати NIST SP 800-124 для визначення політик безпеки та контролю доступу до мобільних пристроїв.

13. Проведення аудиту безпеки інформаційної системи. Провести аудит безпеки інформаційної системи організації, яка обробляє медичні дані пацієнтів, для виявлення вразливостей і недостатніх заходів захисту. При

вирішенні використовувати NIST SP 800-53 для визначення необхідних контролів безпеки та оцінки їхньої ефективності. Оцінити ризики і запропонувати контрзаходи для мінімізації загроз.

3.5. Контрольні запитання

1. Що означає управління інформаційними ризиками?
2. Які основні етапи управління інформаційними ризиками?
3. Які заходи можуть вживатися для управління інформаційними ризиками?
4. Яка основна ідея методики NIST?
5. У чому полягає головна ідея методики ISO 27001?
6. На чому основана методика COBIT?
7. Наведіть короткі властивості методики FAIR.
8. На чому зосереджена методика OCTAVE?
9. Які основні принципи методики IRAM?
10. Що дозволяє робити методика Risk IT?

4. АНАЛІЗ ПРИЧИН ТА НАСЛІДКІВ РИЗИКУ

Мета заняття: ознайомитись з методами визначення причинно-наслідкових зв'язків інформаційних ризиків, а також навчитись застосовувати методи «риб'ячого скелету» та «краватка-метелик» для аналізу інформаційних ризиків в організації.

4.1. Аналіз причин та наслідків

Аналіз причин і наслідків ризику є важливою частиною управління інформаційною безпекою, оскільки дозволяє з'ясувати основні фактори, які призводять до ризиків, і розглянути наслідки цих ризиків для організації.

Цей процес дозволяє детально зрозуміти, чому виникають певні загрози для інформаційних систем та якими можуть бути наслідки для бізнесу, репутації, фінансів або інших важливих аспектів діяльності компанії. Знати джерела ризиків і чітко визначити, до яких наслідків вони можуть призвести, допомагає розробити ефективну стратегію для зменшення ймовірності їхнього виникнення або мінімізації їхнього впливу.

Роль аналізу причин та наслідків:

- ідентифікація основних джерел ризику. За допомогою такого аналізу організація може визначити, які конкретно фактори (внутрішні чи зовнішні) створюють найбільші загрози для її інформаційних систем. Це можуть бути як технічні проблеми (вразливості в програмному забезпеченні або застарілі системи безпеки), так і людські фактори (недостатньо кваліфіковані співробітники, помилки користувачів).

- прогнозування наслідків. Після ідентифікації можливих джерел ризику потрібно з'ясувати, які негативні наслідки можуть виникнути, якщо ці ризики реалізуються. Наприклад, витік конфіденційної інформації може призвести до фінансових втрат, втрати репутації, юридичних наслідків або навіть зупинки діяльності на певний час.

- оцінка впливу на організацію. Визначення, як саме кожен ризик може вплинути на бізнес-процеси, фінансовий стан, дотримання нормативних вимог або репутацію, дозволяє встановити пріоритети в управлінні цими ризиками. Цей етап необхідний для того, щоб знати, які ризики вимагають найбільш термінових і ефективних заходів.

Завдяки такому підходу організація може не лише знижувати ймовірність виникнення певних ризиків, але й підготуватися до можливих наслідків, створивши відповідні плани дій у разі їх реалізації. Оцінка причин і наслідків ризиків є ключовим етапом у плануванні заходів з управління ризиками та забезпечення стабільної і безпечної роботи інформаційних систем.

4.2. Діаграма Ісікава

Діаграма Ісікава (Ishikawa) або метод «Риб'ячого скелету» є популярним методом, що допомагає виявити потенційні причини ризику за допомогою побудови дерева причин. Цей метод застосовується для виявлення основних факторів, які можуть призвести до інциденту або проблеми в інформаційних системах.

Для інформаційних систем діаграма Ісікава може бути побудована на основі певних принципів, які допомагають класифікувати причини проблем залежно від аспектів інформаційної системи. Основні принципи, які часто використовуються для побудови діаграми Ісікава саме в контексті інформаційних систем:

1. Принцип **5M** (Methods, Machines, Materials, Man, Measurement). Цей принцип є класичним і охоплює п'ять основних категорій причин:

- Methods (методи): процеси, методики, технічні рішення, що використовуються в розробці та підтримці інформаційної системи. Сюди входять налаштування сервісів, структура коду, алгоритми чи програмування тощо. Наприклад, погано налаштована система моніторингу, що веде до

затримок у виявленні помилок у системі або неправильне налаштування протоколів зв’язку між компонентами;

- Machines (машини): технічне обладнання, сервери, мережеві пристрої, комп’ютери, використовувані для забезпечення функціонування інформаційної системи. Наприклад, недостатня потужність серверів або мережеве обладнання, яке не відповідає вимогам швидкості або обсягу даних;

- Materials (Матеріали): програмне забезпечення, інструменти, фреймворки та бібліотеки, які використовуються для розробки та підтримки системи. Наприклад: застаріле програмне забезпечення або некоректно налаштовані бібліотеки безпеки;

- Man (Людина): фактори, пов’язані з людьми, які працюють із системою, включаючи технічних фахівців, адміністраторів і кінцевих користувачів. Наприклад: некваліфіковані спеціалісти, які не мають достатнього досвіду для налаштування або підтримки системи, що може призвести до помилок в її роботі;

- Measurement (Вимірювання): інструменти, які використовуються для моніторингу, аналізу та оцінки ефективності та безпеки інформаційної системи. Приклад: відсутність або неправильне використання інструментів для моніторингу роботи серверів, що призводить до невчасного виявлення проблем.

2. Принцип **4P** (People, Processes, Products, Policies). Цей принцип спеціально адаптований для бізнесу та інформаційних систем і охоплює чотири основні аспекти:

- People (Люди): персонал, який працює з системами та забезпечує їхню функціональність, включаючи розробників, адміністраторів, користувачів, технічну підтримку. Наприклад: недостатня підготовка персоналу або відсутність кваліфікації у роботі з новими технологіями;

- Processes (Процеси): процеси, пов’язані з розробкою, впровадженням, підтримкою та експлуатацією інформаційних систем. Це можуть бути робочі

процедури, стандарти, політики. Наприклад: відсутність чітко встановлених стандартів для розробки коду або випробування програмного забезпечення;

- Products (Продукти): програмне забезпечення, апаратне забезпечення та інші компоненти, які забезпечують функціонування інформаційної системи. Наприклад: використання некоректно розроблених чи застарілих продуктів, що мають дефекти або не відповідають вимогам.

- Policies (Політики): управлінські, безпекові, операційні політики, які визначають правила взаємодії з інформаційною системою. Наприклад: слабкі політики безпеки даних, що можуть призвести до вразливостей або витоків інформації.

3. Принцип **6M** (Methods, Machines, Materials, Man, Measurement, Management). Цей принцип є доповненням до **5M**, де додається додатковий елемент:

- Management (Управління): стратегії, організаційна структура, а також ухвалення рішень на рівні управління, що може впливати на всю інформаційну систему. Наприклад: неправильне управління проєктами, недостатній контроль за розподілом ресурсів або негнучка організаційна структура, що може призвести до затримок у розвитку системи.

4. Принцип **7M** (Man, Machines, Methods, Materials, Measurement, Management, Environment). Цей принцип містить ще один важливий елемент – Mother Nature або Environment (Навколишнє середовище), який стосується фізичних та інформаційних умов, у яких функціонує система:

- Mother Nature, Environment (Навколишнє середовище): технічні та організаційні умови, в яких функціонує система, інфраструктура, середовище для розробки, умови для тестування тощо. Наприклад: несприятливі умови для розробки або тестування програмного забезпечення, що може призвести до виникнення помилок.

5. Принцип **4S** (Systems, Software, Security, Support). Цей принцип більше підходить для інформаційних систем, де акцент робиться на чотири основні сфери:

- Systems (Системи): технологічна інфраструктура та програмне забезпечення, що складають систему. Наприклад: неправильне налаштування операційних систем, що може призвести до збою в роботі сервісів;

- Software (Програмне забезпечення): конкретні програми та застосунки, що використовуються для виконання завдань системи. Наприклад: помилки в коді програмного забезпечення або використання старих версій програм;

- Security (Безпека): політики та заходи щодо захисту інформації та ресурсів від несанкціонованого доступу. Наприклад: вразливості в системі безпеки, які можуть призвести до кібератак або витоку даних;

- Support (Підтримка): процеси, інструменти та кадри, що забезпечують підтримку та обслуговування системи. Наприклад: недостатня підтримка від технічної команди, що може призвести до проблем у роботі системи.

6. Принцип **3C** (Customer, Company, Competitors). Цей принцип застосовується до бізнес-аналізу інформаційних систем:

- Customer (Клієнт): потреби та вимоги кінцевих користувачів. Наприклад: відсутність аналізу потреб клієнтів, що призводить до розробки незручного або непотрібного функціоналу;

- Company (Компанія): стратегія та внутрішні процеси компанії, що використовує інформаційну систему. Наприклад: неправильне управління проєктом або ресурсами компанії, що може призвести до затримок або помилок у розробці;

- Competitors (Конкуренти): конкурентне середовище і вплив інших компаній на ефективність інформаційної системи. Наприклад: відставання від конкурентів у впровадженні нових технологій.

Для діаграм Ісікава також існує ще ціла низка принципів їх побудови відповідно до сфер застосування. Наприклад:

- принцип 4M (5M мінус вимірювання) – цей принцип використовується для більш простих ситуацій, де достатньо лише чотирьох категорій причин у випадках, коли немає потреби у вимірюванні для

розв’язання проблеми: Методи (Methods), Машини (Machines), Матеріали (Materials), Людина (Man);

- принцип 3P (People, Process, Product) – зменшується кількість категорій до трьох. Корисний у ситуаціях, коли потрібно зосередитися на людському факторі та процесах, але продукт або послуга теж можуть бути важливими для аналізу;

- принцип 5S (Sort, Set in Order, Shine, Standardize, Sustain). Застосовується в контексті поліпшення ефективності та якості, зокрема в японському підході до покращення виробничих процесів, де важливо зрозуміти, на яких етапах відбуваються збої або відхилення від стандартів. Діаграма Ісікава використовується для ідентифікації проблем на кожному етапі: Sort – сортування, Set in Order – організація процесу, Shine – підтримка чистоти, Standardize – стандартизація, Sustain – підтримка поліпшень;

- принцип 3B (Bottleneck, Barrier, and Bridge). Застосовується для ідентифікації вузьких місць у процесах або системах, де існують конкретні обмеження або перепони, що призводять до проблем у виконанні процесів або досягненні мети. У діаграмі Ісікава категорії виглядають так: Bottleneck – вузьке місце, яке обмежує ефективність системи, Barrier – бар’єр або перешкода на шляху до досягнення мети, Bridge – міст або спосіб подолати ці перешкоди та вузькі місця;

- принцип 5W1H (What, Why, When, Where, Who, How). Принцип, орієнтований на вивчення основних питань про проблему, який дозволяє зібрати важливу інформацію для глибокого розуміння: What – «що відбувається?», Why – «чому це відбувається?», When – «коли це відбувається?», Where – «де це відбувається?», Who – «хто відповідальний за це?», How – «як можна виправити ситуацію?».

Переваги діаграми Ісікава:

1. Систематичний підхід до аналізу проблем. Діаграма Ісікава дозволяє структуровано виявити всі можливі причини, що можуть впливати на певну

проблему. Це допомагає забезпечити більш глибоке розуміння причинного зв’язку.

2. Візуалізація. Діаграма має наочну форму, що дозволяє легко побачити всі фактори, що призводять до проблеми. Це спрощує аналіз і допомагає групі краще зорієнтуватися.

3. Можливість для командної роботи. Діаграма Ісікава часто використовується під час колективних сесій «мозкового штурму». Це сприяє залученню всіх учасників до процесу аналізу і допомагає знайти різноманітні причини проблеми.

4. Ідентифікація основних причин. За допомогою діаграми можна швидко зрозуміти, що є основними причинами проблеми, і відокремити їх від менш значущих.

5. Гнучкість. Діаграма Ісікава може бути адаптована під різні сфери діяльності, від виробництва до інформаційних систем і бізнесу. Це робить її універсальним інструментом для вирішення проблем.

6. Допомога в пошуку рішень. Завдяки виявленим основним і другорядним причинам можна вибудовувати стратегії для усунення дефектів і покращення системи чи процесу.

Недоліки діаграми Ісікава:

1. Складність у разі великої кількості факторі. Якщо проблема дуже складна, то діаграма може стати надто громіздкою і важко читабельною. У такому випадку може бути важко виділити головні причини серед численних можливих варіантів.

2. Не завжди показує пріоритети. Діаграма Ісікава фокусується на зборі всіх можливих причин, але не завжди дозволяє однозначно визначити, які з них є найбільш критичними для вирішення проблеми. Для цього потрібно додатково використовувати інші методи аналізу.

3. Потребує значної кількості часу. Процес побудови діаграми може зайняти багато часу, особливо при великих і складних системах. Це може

бути непродуктивно, якщо проблема проста або має обмежену кількість причин.

4. Може бути суб'єктивною. Оскільки діаграма Ісікава побудована на основі інтерпретації учасників процесу, може виникати суб'єктивність у визначенні причин, що не завжди дозволяє отримати об'єктивні результати.

5. Не дає конкретних рішень. Хоча діаграма Ісікава допомагає виявити основні причини проблеми, вона не надає конкретних рекомендацій або рішень. Для цього потрібні додаткові аналітичні інструменти або експертні оцінки.

6. Обмеження в комплексному аналізі. Діаграма не дає глибокої статистичної оцінки та не враховує взаємозв'язки між причинами та їх комбінований вплив на проблему, що може бути важливим для складних інформаційних систем або бізнес-процесів.

Приклад розробки діаграми Ісікава для аналізу збоїв в автентифікації користувачів через неправильні налаштування системи (за принципом 5M).

Короткий опис проблеми: користувачі не можуть увійти в систему через неправильно налаштовану автентифікацію. Це може вплинути на безпеку і доступність сервісу.

На початку виконується ідентифікація основних та другорядних причин у кожній з категорій принципу 5M (для зменшення обсягів текстової інформації на побудованій діаграмі Ісікава всі причини кодуються, наприклад, Номеркатегорії.M.Номерпричини.Номердругорядноїпричини).

Methods (Методи):

- неправильна конфігурація механізмів автентифікації – 1.M.1;

- незахищені протоколи – 1.M.1.1;

- недосконала автентифікація;

- відсутність двофакторної автентифікації (2FA) для підвищення безпеки – 1.M.2:

- виключення з політики безпеки: відсутність вимоги для введення додаткового коду (SMS, телефонний дзвінок або біометрія) – 1.M.2.1;

- встановлення слабких методів для MFA, таких як прості одноразові паролі – 1.M.2.2;

- проблеми з інтеграцією автентифікаційних систем – 1.M.3.

Materials (Матеріали):

- використання застарілих бібліотек чи фреймворків для автентифікації – 2.M.1;

- погано налаштовані сертифікати SSL/TLS для безпечної передачі даних – 2.M.2.

Machines (Машини):

- сервери, на яких розгорнуті автентифікаційні сервіси, мають недостатню продуктивність – 3.M.1;

- проблеми з мережевим обладнанням, що можуть призводити до затримок чи втрат підключень – 3.M.2.

Man (Людина):

- некваліфіковані фахівці, що займаються налаштуванням системи автентифікації – 4.M.1:

- недостатній досвід з безпекою – 4.M.1.1;

- відсутність досвіду в інтеграції безпечних методів автентифікації – 4.M.1.2;

- недостатнє навчання персоналу, що адмініструє автентифікаційні процеси – 4.M.2:

- неусвідомлення користувачами необхідності складних паролів – 4.M.2.1;

- ігнорування політики безпеки – 4.M.2.2;

- відсутність або недостатність тестування системи автентифікації до запуску – 4.M.3.

Measurement (Вимірювання):

- відсутність моніторингу та аналізу помилок автентифікації – 5M1:

- Не ведеться облік спроб входу – 5.M.1.1;

- Немає реагування на підозрілі дії – 5.M.1.2;

- невикористання інструментів для моніторингу безпеки автентифікації та трекінгу відмов – 5.M.2.

Для побудови діаграми Ісікава можна скористатись будь-яким програмним продуктом. На рис. 4.1 наведено побудовану діаграму для розглянутого прикладу засобами Microsoft Visio (шаблон схеми причинно-наслідкових зв'язків).

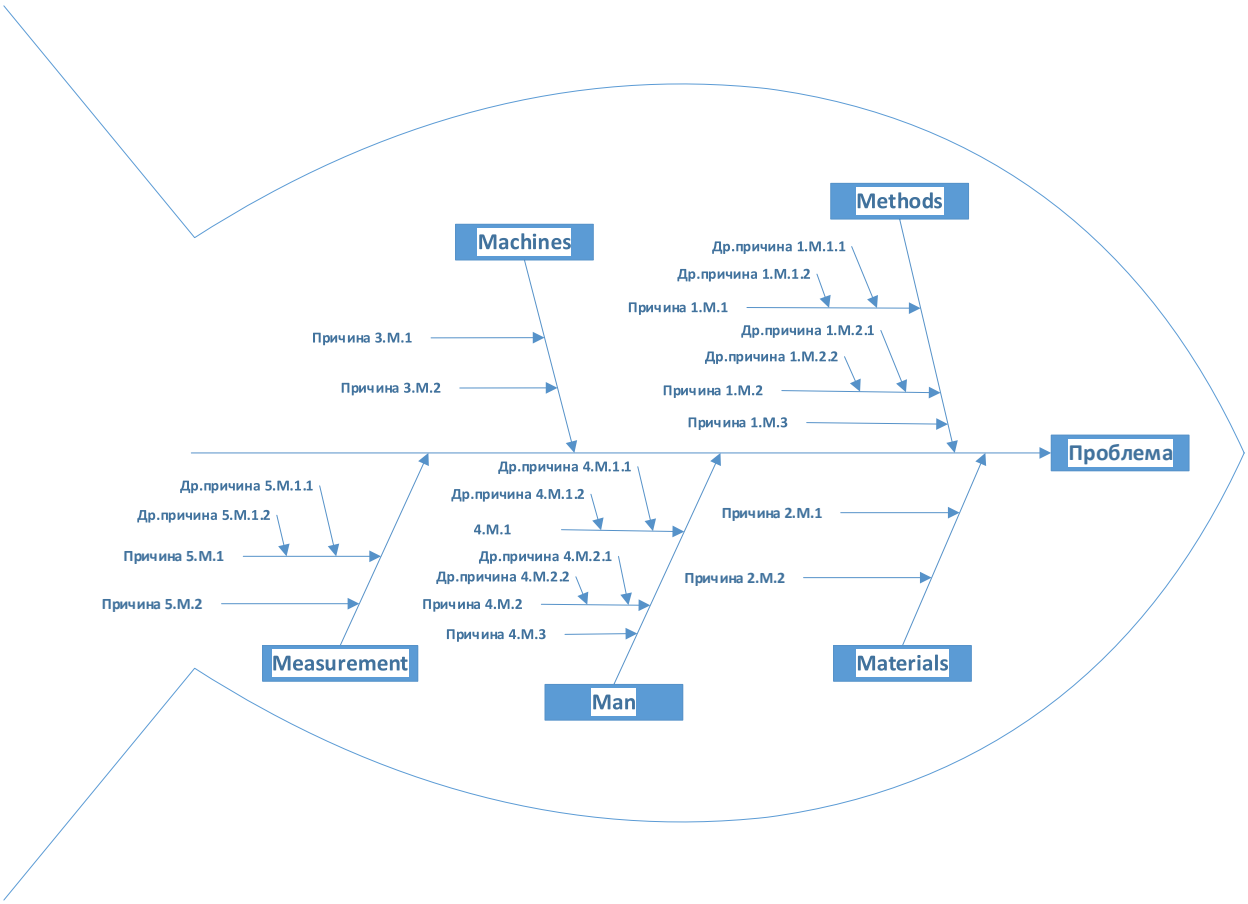

Рисунок 4.1 – Діаграма Ісікава

Наступним етапом виконується аналіз причин і можливі рішення:

Methods (Методи):

- перевірити та правильно налаштувати механізми автентифікації, використовуючи актуальні протоколи;

- впровадити двофакторну автентифікацію (2FA);

- проводити регулярні перевірки інтеграції автентифікаційних сервісів з іншими системами.

Materials (Матеріали):

- оновити бібліотеки для автентифікації на останні стабільні версії;

- перевірити налаштування сертифікатів SSL/TLS для захисту даних під час автентифікації.

Machines (Машини):

- оцінити і при необхідності оновити сервери або збільшити їх продуктивність;

- перевірити налаштування мережевих пристроїв, що забезпечують підключення до автентифікаційних сервісів.

Man (Людина):

- підвищити кваліфікацію спеціалістів, що відповідають за налаштування автентифікації;

- організувати регулярне навчання для співробітників, які працюють з автентифікаційними системами;

- тестувати систему автентифікації в різних сценаріях перед запуском.

Measurement (Вимірювання):

- впровадити моніторинг помилок автентифікації та налаштувати сповіщення про підозрілі активності;

- використовувати інструменти для аналізу безпеки та моніторингу автентифікації.

На останньому кроці виконується впровадження змін і оцінка результатів. Після впровадження змін необхідно провести тестування системи автентифікації та перевірити ефективність кожного з рішень та оцінити зниження кількості помилок.

4.3. Метод «Краватка-метелик»

Метод «Краватка-метелик» в аналізі ризиків може бути використаний для візуалізації взаємозв'язків між джерелами ризиків, подіями, що їх викликають, і наслідками цих подій для інформаційних систем. Структура діаграми цього методу допомагає організації систематизувати, як загрози можуть реалізуватися через конкретні події та які наслідки вони спричинлять.

Основні компоненти діаграми:

1. Ліва частина (Джерела ризиків). Це основні фактори, які можуть призвести до подій або атак. Джерела ризиків можуть бути як зовнішніми (наприклад, зловмисники), так і внутрішніми (наприклад, людські помилки, технічні уразливості).

2. Центр (Подія). У центрі діаграми розміщується сама подія або загроза, яка спричиняється джерелом ризику та реалізується через певну уразливість. Це може бути, наприклад, кібератака, збій у системі, витік даних тощо.

3. Права частина (Наслідки). Це наслідки події, які можуть виникнути після того, як загроза реалізувалася. Наслідки можуть бути фінансовими збитками, втратою даних, пошкодженням репутації, юридичними наслідками тощо.

Процес побудови діаграми полягає в таких кроках:

1. Визначення джерел ризиків. Для кожної ситуації або системи ідентифікуються можливі джерела ризиків. Це можуть бути зловмисники, технічні помилки, природні фактори тощо. Також, на шляху від джерел ризику до події визначаються бар'єри, які запобігають виникненню небажаних подій або загроз.

2. Ідентифікація подій або загроз. Далі аналізується, як джерела ризиків можуть викликати конкретні події. Це можуть бути кібератаки, людські помилки, несанкціонований доступ до системи, технічні збої.

3. Оцінка наслідків. Після визначення подій потрібно оцінити, які наслідки виникнуть у разі їх реалізації. Це можуть бути прямі фінансові збитки, витрати на відновлення даних, репутаційні втрати або юридичні наслідки. Також, на шляху від події до наслідків визначаються бар'єри, які запобігають небажаним наслідкам після виникнення події (дії по відновленню).

4. Створення діаграми. Всі елементи зображуються у вигляді діаграми «краватка-метелик», що дозволяє чітко побачити зв'язки між джерелами ризиків, подіями та наслідками.

Переваги методу «краватка-метелик»:

1. Чітка структура. Поділ на три основні частини (джерела, подія, наслідки) дозволяє чітко відокремити різні аспекти проблеми і забезпечує зрозумілу візуалізацію причинно-наслідкових зв'язків.

2. Універсальність. Метод можна застосовувати в різних сферах: виробництво, інформаційні системи, бізнес, інженерія тощо. Це робить його універсальним інструментом для аналізу ризиків.

3. Покроковий підхід. Підхід дає змогу покроково виявляти, які саме джерела ризику впливають на події і які наслідки можуть виникнути через це, що дозволяє ефективно планувати стратегії зменшення ризиків.

4. Покращення комунікації в команді. Використання діаграми сприяє спільному аналізу в команді. Всі учасники можуть наочно побачити, як причини впливають на події та наслідки, що полегшує прийняття рішень.

5. Ідентифікація ключових факторів. Дозволяє легко ідентифікувати основні причини проблеми, а також важливі наслідки, що можуть виникнути в результаті цих проблем.

6. Покращення управління ризиками. Завдяки виявленню джерел і наслідків можна розробити ефективні стратегії мінімізації ризиків та покращення процесів, що знижує загальний рівень ризику.

Недоліки методу «краватка-метелик»:

1. Складність у великих системах. У складних системах з численними джерелами ризиків та потенційними наслідками діаграма може стати занадто переповненою та складною для аналізу. Важко виділити головні ризики серед численних можливих причин і наслідків.

2. Не дає точних кількісних результатів. Метод зосереджується на якісному аналізі, тому він не дозволяє оцінити ймовірність або ступінь впливу ризиків в числовому вигляді. Для кількісної оцінки потрібно використовувати додаткові методи.

3. Вимагає глибоких знань предметної області. Для ефективного використання методу необхідно мати глибокі знання в обраній сфері. Це означає, що застосування методу може бути складним без відповідної експертизи.

4. Суб'єктивність аналізу. Оскільки метод базується на аналізі ймовірних причин і наслідків, можуть виникнути проблеми з визначенням найбільш важливих факторів, оскільки часто цей процес залежить від досвіду і думки конкретної особи чи групи.

5. Не завжди виявляє всі можливі причини. Оскільки діаграма побудована на основі того, що вже відомо, можуть бути пропущені деякі неочевидні або непрямі фактори, які також можуть впливати на подію чи ризик.

6. Часова складність. Побудова діаграми може зайняти багато часу, особливо якщо система складна або містить багато можливих причин і наслідків. Це може стати недоліком в умовах швидких змін.

Приклад розробки діаграми «краватка-метелик» для відсутності багаторазових перевірок паролів користувачів в інформаційній системі. При вирішенні необхідно відповісти на такі питання:

- Які можливі джерела ризику при відсутності багаторазових перевірок паролів користувачів?

- Яка подія може реалізувати цей ризик і які наслідки це може мати для організації?

Для зменшення обсягів текстової інформації на діаграмі також застосовано кодування джерел (Д), подій (П), наслідків (Н) та бар'єрів (Б).

Крок 1. Визначення джерел ризиків.

Джерела ризиків – це фактори, що можуть призвести до потенційних загроз або атак на систему. У цьому випадку відсутність багаторазових перевірок паролів є уразливістю, яка дозволяє зловмисникам здійснити атаки. Джерелами ризиків можна вказати такі:

1. Зловмисники (хакери) (Д1). Хакери можуть використовувати методи атаки, такі як брутфорс або перебір паролів, щоб отримати доступ до облікових записів користувачів.

Бар'єри (Д1Б):

- встановлення обмеження на кількість спроб введення пароля (Д1Б1);

- використання багатофакторної автентифікації (Д1Б2);

- використання засобів моніторингу для виявлення аномальних спроб входу (Д1Б3).

2. Ненавмисні помилки користувачів (Д2). Користувачі можуть використовувати слабкі або легкі для вгадування паролі. Відсутність багаторазових перевірок означає, що система не перевіряє складність пароля на етапі реєстрації або зміни паролю, що може призвести до використання ненадійних паролів.

Бар'єри (Д2Б):

- впровадження політики складності паролів при їх створенні або зміні (Д2Б1);

- налаштування на вимогу змінювати паролі після певного періоду часу (Д2Б2);

- проведення навчальних програм для співробітників щодо важливості надійних паролів (Д2Б3).

3. Недосконала політика безпеки в організації (Д3). Відсутність політики захисту паролів, що передбачає регулярну зміну паролів або перевірку їх складності, може бути джерелом ризику.

Бар’єри (Д3Б):

- створення та реалізація політики безпеки, яка зобов’язує користувачів обирати складні паролі (Д3Б1);

- впровадження регулярних аудитів безпеки для перевірки на відповідність політикам (Д3Б2);

- запровадження системи автоматичних нагадувань про зміну паролів (Д3Б3).

Крок 2. Визначення події.

Подія – це безпосередньо загроза або інцидент, що виникає через джерела ризиків. У даному випадку подія – це реалізація уразливості, яку можна використати зловмисниками або через помилку користувачів. Можна визначити два типи подій:

1. Атака брутфорс або підбір пароля (П1). Оскільки система не вимагає багаторазових перевірок пароля або не обмежує спроби введення неправильного пароля, зловмисник може використовувати методи брутфорс для підбору пароля. Це дозволить йому отримати доступ до облікових записів користувачів.

2. Використання слабких паролів (П2). Через відсутність перевірки на складність паролів користувач може вибрати слабкий пароль (наприклад, «123456» або «password»), який буде легко вгадати за допомогою автоматичних атак.

Крок 3. Оцінка наслідків.

Наслідки – це негативні наслідки, які можуть виникнути внаслідок реалізації цієї події. Вони можуть бути як фінансовими, так і репутаційними, або навіть юридичними. Можливі наслідки в даному випадку:

1. Втрата конфіденційності даних (Н1). Зловмисник може отримати доступ до чутливих або конфіденційних даних, таких як фінансова

інформація, особисті дані користувачів або інтелектуальна власність компанії.

Бар’єри (Н1Б):

- ідентифікація та блокування зловмисників (Н1Б1);

- інформування постраждалих осіб (Н1Б2);

- моніторинг витоку (Н1Б3).

2. Фінансові втрати (Н2). Витрати на відновлення після атаки, фінансові штрафи за порушення стандартів безпеки, таких як GDPR, якщо інформація про клієнтів була вкрадена або скомпрометована.

Бар’єри (Н2Б):

- перегляд фінансових стратегій (Н2Б1);

- страхування та відшкодування (Н2Б2).

3. Пошкодження репутації (Н3). Якщо атака буде успішною і дані будуть вкрадені або порушена безпека інформації, це може серйозно пошкодити репутацію компанії. Клієнти можуть втратити довіру до компанії, що призведе до втрати бізнесу.

Бар’єри (Н3Б):

- публічне визнання проблеми та план дій (Н3Б1);

- регулярне аудиторське оцінювання, публічні звіти про безпеку та комунікація із засобами масової інформації для покращення репутації (Н3Б2).

4. Юридичні наслідки (Н4). Якщо компанія порушить нормативні вимоги щодо захисту персональних даних, вона може зіткнутися з судовими позовами або штрафами з боку регуляторних органів (наприклад, за порушення правил GDPR або інших стандартів конфіденційності).

Бар’єри (Н4Б):

- виконання вимог регулюючих органів (Н4Б1);

- компенсації та позови (Н4Б2);

- покращення документації, щоб вона відповідала законодавчим вимогам (Н4Б3).

5. Доступ до корпоративних ресурсів (Н5). Зловмисники можуть отримати доступ не тільки до особистих даних, а й до внутрішніх ресурсів компанії, таких як електронні листи, корпоративні документи та внутрішні системи.

Бар'єри (Н5Б):

- відновлення доступу до систем: зміна паролів для всіх користувачів і встановлення багатофакторної автентифікації (Н5Б1);

- проведення детального аудиту безпеки (Н5Б2);

- розслідування інциденту, щоб зрозуміти, яким чином було здійснено атаку, і вжити заходів для запобігання подібним ситуаціям у майбутньому (Н5Б3).

Крок 4. Побудова діаграми «Краватка-метелик».

Від кожного джерела ризику проводиться лінія до центру діаграми – події. Якщо є бар'єри – вони зображуються як вертикальні лінії, що перетинають шляхи від джерел до події та від події до наслідків. Діаграма «краватка-метелик» наведена на рис. 4.2.

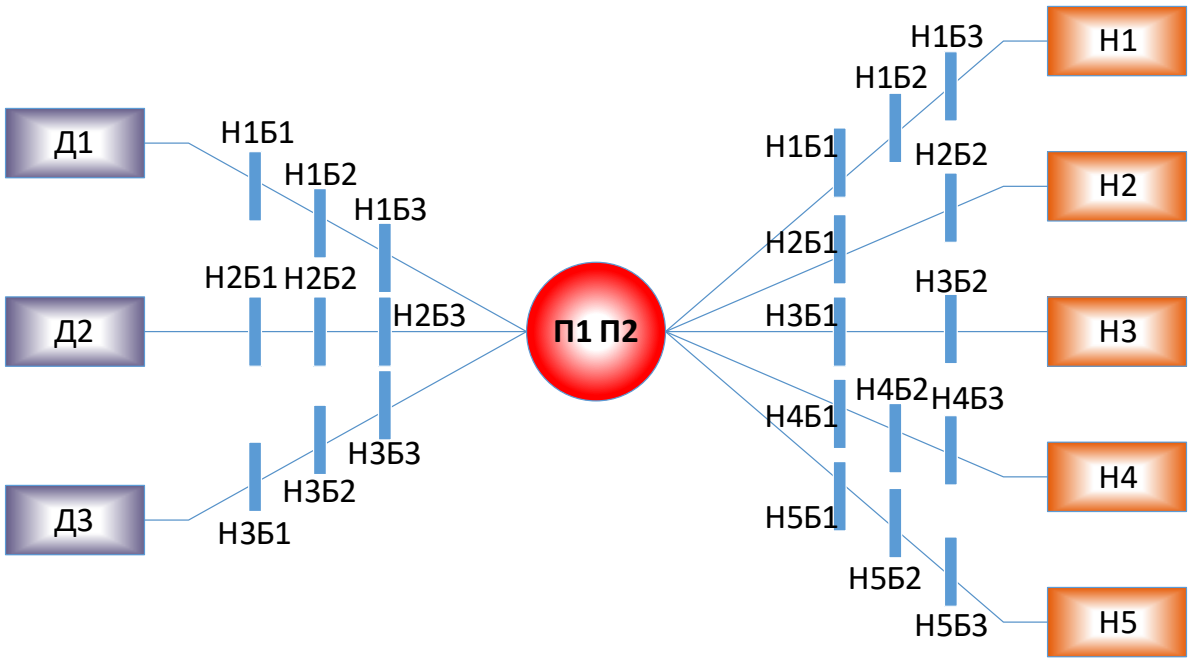

Рисунок 4.2 – Діаграма «краватка-метелик»

4.4. Індивідуальні завдання

Індивідуальні завдання складаються з вирішення 2 класів задач (методом діаграми Ісікава та методом «краватка-метелик»).

Варіанти задач для метода діаграми Ісікава (в дужках вказано, за яким принципом формувати основні та другорядні причини). Для кожної категорії необхідно сформулювати 2-3 основні причини, та для кожної основної причини сформулювати 1-3 другорядні причини:

1. Низька швидкість роботи вебсайту через неоптимізоване програмне забезпечення (Принцип 5M).
2. Збої в роботі бази даних під час високих навантажень (Принцип 6M).
3. Проблеми з безпекою інформаційної системи через вразливості в програмному забезпеченні (Принцип 5M).
4. Невідповідність програмного забезпечення вимогам бізнесу (Принцип 4P).
5. Невдача у виконанні регулярного резервного копіювання даних (Принцип 6M).
6. Невірне налаштування файрволів, що призводить до проблем з доступом до сервісів (Принцип 5M).
7. Збої в роботі мережі під час високого трафіку через неправильне налаштування мережевого обладнання (Принцип 7M).
8. Проблеми із забезпеченням конфіденційності даних через слабкі політики безпеки (Принцип 4S).
9. Порушення процесів обробки даних через некоректні алгоритми в програмному забезпеченні (Принцип 5M).
10. Збій у роботі CRM системи через відсутність підтримки нових версій браузерів (Принцип 5M).
11. Збої в роботі системи через відсутність оновлень програмного забезпечення (Принцип 7M).

12. Необґрунтовані витрати через надмірні вимоги до інфраструктури (Принцип 4Р).

13. Втрата даних через некоректно налаштовані системи зберігання інформації (Принцип 6М).

Варіанти задач для метода «краватка-метелик». Визначити від 3 до 5 джерел загроз, одну подію, від 3 до 5 наслідків. Також визначити сумарно по 6 бар'єрів в лівій та правій частині діаграми:

1. У компанії відсутній захист від фішингових атак, співробітники не мають достатнього досвіду для виявлення таких загроз.

2. Система управління даними має уразливість у версії програмного забезпечення, яке не оновлювалося довгий час.

3. Компанія обслуговує дані клієнтів, але виявлено, що їхня система безпеки не включає двофакторної автентифікації для доступу до важливих даних.

4. Через нестабільну роботу серверів виникли випадки втрати даних. Якщо сервери регулярно дають збої, це може призвести до втрати важливих даних або порушення роботи системи, що, у свою чергу, може викликати серйозні фінансові та операційні проблеми для компанії.

5. Під час процесу оновлення програмного забезпечення виникли помилки, які призвели до збоїв у роботі системи.

6. Оцінка можливих наслідків при відсутності плану відновлення після стихійних лих.

7. Випадок, коли персонал компанії неправильно налаштував систему безпеки, що дозволило зловмисникам отримати доступ до конфіденційних даних.

8. Виявлено, що під час проведення фінансових операцій через онлайн-платформу компанія не застосовує SSL-шифрування.

9. Організації загрожує атака через використання застарілого ПЗ. Використання застарілих версій програмного забезпечення є класичною

уразливістю, яка може сприяти атакам, таким як експлойти, що можуть призвести до знищення або викрадення важливих даних.

10. Неправильне управління доступом до даних (наприклад, коли доступ надається занадто широкому колу осіб).

11. Через несанкціонований доступ до корпоративних мереж зловмисники можуть викрасти важливі дані.

12. Компанія стикається з ризиком витоку даних через помилки в налаштуваннях бази даних.

13. Організація не проводить регулярні тести на вразливість системи

4.5. Контрольні запитання

1. Для чого використовується аналіз причин та наслідків інформаційних ризиків?

2. Що таке діаграма Ісікава?

3. За якими принципами будується діаграма Ісікава в контексті інформаційних систем?

4. Яким чином додаються другорядні категорії в діаграму Ісікава?

5. Які переваги та недоліки діаграми Ісікава?

6. Для чого використовується метод «краватка-метелик»?

7. Які складові діаграми «краватка-метелик»?

8. У чому полягає процес побудови діаграми «краватка-метелик»?

9. Для чого вводяться бар’єри в діаграмі «краватка-метелик»?

10. Які переваги та недоліки діаграми «краватка-метелик»?

5. СТАТИСТИЧНІ МЕТОДИ ОЦІНЮВАННЯ РИЗИКІВ

Мета заняття: ознайомитись з поняттям стохастичного ризику, а також навчитись виконувати оцінку стохастичних інформаційних ризиків за методом Монте-Карло та «дерева рішень».

5.1. Стохастичний ризик

Стохастичний ризик – це тип ризику, при якому невизначеність або варіативність майбутніх подій обумовлені випадковими факторами, що важко передбачити точно. У рамках стохастичних моделей ризику ймовірності подій оцінюються не як єдині числа, а через розподіли ймовірностей, що дозволяє більш точно враховувати можливі варіації в результатах. Відповідно, стохастичний ризик визначається як ризик, який виникає внаслідок випадкових змінних або випадкових процесів, які неможливо передбачити точно.

Стохастичні ризики в інформаційних системах виникають через невизначеність щодо поведінки окремих компонентів системи або зовнішніх загроз, що можуть вплинути на їхню роботу. Їх не можна передбачити точно, оскільки вони включають випадкові фактори або варіативність у результатах, які не завжди можуть бути чітко визначені через обмеження даних або складність виведення точних закономірностей.

Стохастичний ризик в інформаційних системах відображає ймовірність того, що системи зазнають порушення або збої через випадкові, непередбачувані події, такі як технічні помилки, зловмисні атаки або людські помилки. Оскільки ці події виникають не завжди з однаковою ймовірністю і можуть мати різні наслідки в залежності від контексту, стохастичний ризик дозволяє оцінити всі ці фактори на основі ймовірнісних моделей.

Основні аспекти стохастичних ризиків в інформаційних системах:

- загрози та вразливості. Загрози – це потенційні події, які можуть призвести до небажаних наслідків для інформаційних систем. Прикладом

стохастичних загроз є неочікувані збої в апаратному забезпеченні або атаки на систему, де ймовірність їх виникнення є випадковою і варіативною. Вразливості – це слабкі місця в системах, які можуть бути використані для атаки або пошкодження даних. Стохастичні моделі дозволяють оцінити не тільки наявність вразливостей, але і ймовірність їх експлуатації через різні зовнішні або внутрішні фактори;

- невизначеність. Стохастичний ризик в інформаційних системах виникає через невизначеність щодо ймовірності та серйозності майбутніх загроз. Замість того, щоб точно передбачати, коли і як виникне певна загроза, моделі стохастичного ризику враховують варіативність таких подій;

- оцінка наслідків та ймовірності. Врахування стохастичних факторів дозволяє більш точно оцінити ймовірність та наслідки конкретного інциденту, оскільки вони можуть змінюватися залежно від зовнішніх умов, поведінки користувачів або змін у конфігурації системи.

5.2. Оцінка стохастичних ризиків в інформаційних системах

Управління стохастичними ризиками має особливу важливість для інформаційних систем, оскільки ці системи часто працюють в умовах невизначеності. Наприклад, можна спостерігати варіативність в інтенсивності атак на систему, варіацію в поведінці користувачів або варіативність у системах для зберігання та обробки даних. Без застосування стохастичних моделей для оцінки цих ризиків організація не може повною мірою зрозуміти можливі наслідки різних інцидентів і їхній потенційний вплив на безпеку системи.

Детальна оцінка стохастичних ризиків дозволяє:

- зрозуміти ймовірність виникнення небезпечних ситуацій;

- визначити масштаби впливу цих ситуацій на бізнес-процеси;

- створити ефективні стратегії реагування на загрози;

- оптимізувати витрати на безпеку за допомогою точних оцінок ризиків.

Методи оцінки стохастичних ризиків:

1. Моделювання ймовірностей. Для оцінки стохастичних ризиків застосовуються різноманітні ймовірнісні моделі, які допомагають передбачити ймовірність виникнення конкретних подій. Це можуть бути різні розподіли ймовірностей (нормальний, експоненційний, біноміальний тощо), які дають можливість описати невизначеність у поведінці системи.

Наприклад, для оцінки ймовірності відмови обладнання можуть бути використані експоненційні розподіли для моделювання часу між відмовами в технічних компонентах системи. З іншого боку, для оцінки атак на систему, таких як DDoS-атаки, використовуються моделі ймовірності, які враховують змінні в кількості атакуючих точок і їх інтенсивності.

2. Метод Монте-Карло. Метод Монте-Карло є одним з найбільш популярних методів для оцінки стохастичних ризиків. Це статистична техніка, яка дозволяє проводити чисельну імітацію випадкових подій за допомогою комп'ютерного моделювання.

У контексті інформаційних систем цей метод може бути використаний для прогнозування ризиків збоїв у системі, атак на бази даних, а також для оцінки впливу різних інцидентів на конфіденційність, доступність та цілісність даних. Імітація дає можливість побудувати графіки ймовірностей, що дозволяють зрозуміти, які з інцидентів найбільш ймовірні та мають найбільший вплив на організацію.

3. Аналіз чутливості. Аналіз чутливості дозволяє оцінити, як зміни в певних параметрах або факторах можуть вплинути на загальний результат. У випадку стохастичних ризиків цей метод допомагає зрозуміти, які фактори (наприклад, зміни в налаштуваннях безпеки чи в поведінці користувачів) можуть найбільше вплинути на ймовірність або величину ризику.

Аналіз чутливості важливий для визначення тих елементів системи, які потребують додаткової уваги або посилення контролю.

4. «Дерева рішень» та сценарії. «Дерева рішень» є потужним інструментом для візуалізації та оцінки ризиків, особливо коли йдеться про

складні системи з численними варіантами розвитку подій. У цьому випадку «дерево рішень» допомагає визначити ймовірність кожного можливого сценарію та оцінити їх наслідки.

Сценарії розвитку допомагають у визначенні ймовірних напрямків розвитку інцидентів та виявленні найбільш критичних елементів системи.

Основні кроки для оцінки стохастичних ризиків в інформаційних системах:

1. Ідентифікація загроз та вразливостей. Першим кроком є виявлення можливих загроз та вразливостей в інформаційній системі. Це можуть бути технічні проблеми, людські помилки, вразливості програмного забезпечення або потенційні зловмисні атаки.

2. Моделювання ймовірностей подій. Використовуючи ймовірнісні моделі, визначаються ймовірності різних сценаріїв, зокрема, ймовірність відмови обладнання, успішності атак або виявлення вразливостей.

3. Оцінка наслідків. Оцінюється, якими будуть наслідки для організації у випадку реалізації кожного з ризиків. Це можуть бути фінансові втрати, втрата репутації, порушення конфіденційності чи доступності даних.

4. Прогнозування через імітаційне моделювання. Застосовуються методи, такі як Монте-Карло, для моделювання численних варіантів розвитку подій і оцінки ймовірних наслідків для кожного з них.

5. Прийняття рішень та управління ризиками. На основі проведеної оцінки ризиків приймаються рішення щодо впровадження відповідних заходів для зменшення ризиків, таких як оновлення програмного забезпечення, зміцнення політик безпеки або інші технічні та організаційні рішення.

5.3. Критерії оцінки стохастичного інформаційного ризику

Оцінка стохастичного інформаційного ризику – це процес виявлення, аналізу і визначення ймовірності виникнення та наслідків подій, що можуть негативно вплинути на безпеку та працездатність інформаційної системи.

Оскільки стохастичні ризики є випадковими, то їх оцінка здійснюється на основі ймовірнісних моделей, що дозволяє врахувати варіативність у результатах.

Основні критерії для оцінки стохастичного інформаційного ризику:

1. Ймовірність виникнення події (Probability of Occurrence). Ймовірність виникнення події – це базовий критерій для оцінки стохастичного ризику. Оскільки стохастичні події характеризуються невизначеністю, необхідно оцінити ймовірність того, що певна загроза або вразливість може реалізуватися в інформаційній системі. Для оцінки ймовірності використовуються:

- моделювання ймовірностей (статистичні розподіли: нормальний, експоненційний, біноміальний);

- аналіз попередніх подій або досвід з іншими системами;

- моделі на основі експертних оцінок або історичних даних.

2. Тяжкість наслідків (Severity of Consequences). Цей критерій оцінює, якою шкодою або збитками може бути пов’язана подія, що відбувається. Тяжкість наслідків вказує, на які саме наслідки варто зважати при плануванні заходів для мінімізації ризиків. Тяжкість наслідків може проявлятись у:

- фінансових збитках – скільки компанія може втратити в грошах у разі порушення безпеки (наприклад, штрафи, витрати на відновлення даних, витрати на репутаційні втрати);

- зниженні доступності – час, на який система або окремі сервіси будуть недоступні для користувачів;

- втраті даних – ймовірність і наслідки втрати або компрометації конфіденційної інформації;

- репутаційних втратах – вплив на довіру клієнтів, партнерів і акціонерів до організації.

3. Часова ймовірність (Time Probability). Часова ймовірність відображає ймовірність виникнення події в певний період часу. Наприклад, певні атаки

чи технічні збої можуть мати сезонні або тимчасові коливання в частоті виникнення. Методи оцінки:

- вивчення часових тенденцій для визначення періодів із підвищеним ризиком (наприклад, сезонні атаки на електронну комерцію в період святкових розпродажів);

- моделювання часових варіацій, щоб визначити, коли ризик найбільший.

4. Вплив на доступність, цілісність і конфіденційність (Impact on Availability, Integrity, and Confidentiality). Цей критерій оцінює, як конкретна подія або загроза впливає на три основні аспекти безпеки інформаційних систем: доступність, цілісність та конфіденційність даних. При оцінці впливу на доступність визначається як довго система буде недоступна після інциденту та як це вплине на операційні процеси компанії. При оцінці впливу на цілісність визначається чи можуть бути порушені дані в процесі інциденту, чи можна їх відновити без втрат. При оцінці впливу на конфіденційність визначається чи можуть бути розкриті або втрачені конфіденційні дані (наприклад, особисті дані клієнтів чи фінансова інформація).

5. Чутливість до змін (Sensitivity to Changes). Цей критерій оцінює, як зміни в налаштуваннях системи, поведінці користувачів або конфігураціях можуть вплинути на ризик. Важливо розуміти, які елементи інформаційної системи є найбільш чутливими до змін і як це може вплинути на загальний рівень ризику. Для оцінки використовуються методи аналізу чутливості для визначення, які зміни в системі мають найбільший вплив на безпеку. Це дозволяє вчасно виявити критичні точки системи та вжити відповідних заходів.

6. Технічна складність (Technical Complexity). Технічна складність ризику враховує, скільки ресурсів і часу необхідно для його реалізації або нейтралізації. Стохастичний ризик, який є технічно складним, зазвичай вимагає спеціалізованих знань, інструментів або ресурсів для його

подолання. При оцінці визначається, чи є вразливість у системі, яку складно експлуатувати або усунути. Оцінка технічної складності часто включає аналіз потенційних засобів захисту і їх ефективність.

7. Масштабність наслідків (Scalability of Consequences). Цей критерій оцінює, наскільки масштабними можуть бути наслідки події для всієї організації чи інфраструктури в цілому. Масштабність наслідків може залежати від кількості залучених користувачів, систем чи процесів, які постраждали від ризику. Оцінюється, наскільки серйозний буде вплив на всю інфраструктуру організації в разі реалізації конкретного ризику.

5.4. Метод Монте-Карло

Метод Монте-Карло (Monte Carlo Method) є потужним інструментом для аналізу стохастичних процесів і використовується для оцінки ризиків, де є значна невизначеність, зокрема в контексті інформаційних ризиків. Цей метод дає змогу здійснювати симуляції і моделювати варіанти розвитку подій, що дозволяє приймати більш обґрунтовані рішення в складних ситуаціях.

Метод Монте-Карло – статистичний метод для оцінки ймовірностей різних результатів у процесах, де впливають випадкові змінні. Суть методу полягає в тому, що для моделювання невизначеності використовуються випадкові величини, і на основі багатьох таких симуляцій будується оцінка ймовірних результатів.

Алгоритм методу Монте-Карло:

1. Визначення всіх стохастичних змінних у моделі (наприклад, ймовірність атаки, ймовірність втрати даних, витрати на відновлення тощо). Вони можуть бути представлені різними розподілами ймовірності (нормальним, експоненціальним, рівномірним тощо).

2. Проведення моделювання. Для кожної змінної генеруються випадкові значення на основі її ймовірнісного розподілу. Цей процес

повторюється багато разів (десятки, сотні, тисячі разів) для того, щоб забезпечити статистичну достовірність результатів.

3. Оцінка результатів. Після моделювання отримуються статистичні показники, такі як середнє значення, дисперсія, ймовірність того чи іншого результату.

4. Аналіз і прийняття рішень. Оцінка ймовірностей і наслідків різних подій дає змогу оцінити ризики і на основі цього зробити висновки щодо управління ризиками.

В інформаційних системах метод Монте-Карло часто використовується для моделювання ризиків, пов’язаних з кібератаками, витоками даних, відмовами обладнання, проблемами з безпекою програмного забезпечення тощо.

Приклад використання методу Монте-Карло для оцінки ризику кібератаки.

Умова задачі: організація хоче оцінити ризик кібератаки на свою мережу, де є декілька елементів з різним рівнем безпеки, і кожен елемент має свою ймовірність бути атакованим. Витрати на відновлення після атаки варіюються залежно від типу атаки та серйозності пошкоджень.

1. У мережі організації є три елементи, на які можлива кібератака:

- елемент 1 (ймовірність атаки: 0.2, витрати на відновлення від 80000 до 120000 $);

- елемент 2 (ймовірність атаки: 0.5, витрати на відновлення від 150000 до 250000 $);

-елемент 3 (ймовірність атаки: 0.7, витрати на відновлення від 200000 до 350000 $).

2. Проведення моделювання. Оцінка витрат на відновлення для кожного елемента мережі. Витрати на відновлення після атаки можуть бути випадковими і залежать від серйозності атак.

Текст програми для імітаційного моделювання:

```
#include <stdio.h>
#include <stdlib.h>
#include <time.h>

// Елемент мережі
typedef struct {
    double probability; // ймовірність атаки
    double min_recovery_cost; // мінімальні витрати на відновлення
    double max_recovery_cost; // максимальні витрати на відновлення
} NetworkElement;

// Генерація випадкового числа у діапазоні [0, 1]
double random_double() {
    return (double)rand() / RAND_MAX;
}

// Генерація витрат у заданому діапазоні (обрано рівномірний розподіл)
double random_recovery_cost(double min_cost, double max_cost) {
    return min_cost + (random_double() * (max_cost - min_cost));
}

// Моделювання Монте-Карло
void monte_carlo (NetworkElement elements[], int num, int count) {
    double total_risk = 0;
    for (int i = 0; i < count; i++) {
        double sim_cost = 0;
        // Перевірка ймовірності атаки по всіх елементах мережі
        for (int j = 0; j < num; j++) {
            if (random_double() < elements[j].probability) {
                // Якщо атака - додавання витрат на відновлення
                sim_cost +=
                  random_recovery_cost(elements[j].min_recovery_cost,
                                       elements[j].max_recovery_cost);
            }
        }
        // Накопичення загального ризику
        total_risk += sim_cost;
    }
    // Підрахунок середнього ризику
    double avr_risk = total_risk / count;
    printf("Середній ризик від кібератаки: $%.2f\n", avr_risk);
}

int main() {
    // Ініціалізація елементів мережі
    NetworkElement elements[] = {
        {0.2, 80000, 120000},  // Елемент 1
        {0.5, 150000, 250000}, // Елемент 2
        {0.7, 200000, 350000}  // Елемент 3
    };
    int num_elements = sizeof(elements) / sizeof(elements[0]);
    int num_simulations = 10000;
    srand(time(NULL));
    // Запуск моделювання Монте-Карло
    monte_carlo(elements, num_elements, num_simulations);
    return 0;
}
```

Приклад виведення в результаті роботи програми:

```
Середній ризик від кібератаки: $970000.00
```

Переваги використання методу Монте-Карло в аналізі інформаційних ризиків:

- дозволяє моделювати складні системи з багатьма стохастичними змінними та невизначеністю, що робить його ідеальним для аналізу інформаційних ризиків;

- дає можливість працювати з різними типами розподілів ймовірностей (нормальним, рівномірним, експоненціальним тощо), що дозволяє точно відобразити реальні умови;

- дозволяє отримати не тільки середнє значення очікуваного результату, а й оцінити ризик різних сценаріїв розвитку подій;

- можна побудувати графіки та гістограми, що допомагають краще зрозуміти варіативність результатів і ймовірності подій.

Але метод Монте-Карло має кілька важливих недоліків:

- для точних результатів потрібні численні симуляції, що може вимагати значних обчислювальних ресурсів і часу;

- якщо ймовірності та інші дані для моделювання неточні, це може спотворити результати;

- невірно вибраний розподіл для змінних може привести до неправильних оцінок ризику;

- через випадкові числа результат може коливатися, що потребує великої кількості симуляцій для надійності;

- оцінки для довгострокових періодів можуть бути менш точними через більшу невизначеність;

- важливі залежності між елементами можуть бути не відображені без додаткових налаштувань;

- дає лише кількісні оцінки, але не пропонує конкретних стратегій управління ризиками;

- використання методу для великих систем може бути дорого та часозатратно.

5.5. Метод «дерева рішень»

Метод «дерева рішень» (Decision Tree) – це інструмент для прийняття рішень в умовах невизначеності, який дає змогу оцінити можливі варіанти розвитку подій і вибрати найбільш вигідний чи безпечний шлях. У контексті аналізу інформаційних ризиків метод «дерева рішень» використовується для моделювання сценаріїв, пов’язаних із ризиками інформаційних систем, таких як кібератаки, витоки даних, збої в роботі обладнання, порушення безпеки тощо.

«Дерево рішень» – це графічна модель для вибору оптимального варіанту з множини можливих, при якому на кожному етапі розгалуження представляються варіанти дій, а також ймовірності їх виникнення та наслідки. «Дерево рішень» містить:

- вузли дерева. Вони представляють можливі варіанти рішень, події або ситуації;

- гілки дерева, які показують різні варіанти розвитку подій, кожна гілка має ймовірність її настання;

- листя дерева – кінцеві результати, які можуть бути як вигідними (позитивними), так і негативними (збитками).

Алгоритм побудови «дерева рішень»:

1. Визначення проблеми – спершу треба чітко визначити проблему або завдання, яке потрібно вирішити (наприклад, ризики, пов’язані з витоком конфіденційної інформації).

2. Створення варіантів рішень – для кожної ситуації (вузла) визначаються можливі варіанти рішень або сценарії (гілки дерева).

3. Призначення ймовірностей – для кожного варіанту розвитку подій на кожній гілці дерева визначають ймовірність того, що цей варіант справдиться.

4. Оцінка варіантів – для кожного кінцевого результату (листя дерева) визначають фінансові або інші наслідки. Це можуть бути витрати, втрати або вигоди.

5. Оцінка ймовірностей результатів – розраховуються ймовірності кінцевих результатів, а також їх вплив на загальний стан справ.

6. Вибір оптимального рішення – на основі результатів аналізу вибирається оптимальний варіант розвитку подій, що мінімізує ризики або максимізує вигоди.

Приклад використання методу «дерева рішень» для оцінки ризику кібератаки.

Умова задачі: організація стикається з ризиком кібератаки на свої сервери. Якщо атака відбудеться, можна зазнати фінансових втрат, а також є ймовірність, що дані будуть скомпрометовані. Необхідно оцінити ймовірність успіху атаки, витрат від неї і потенційні наслідки для даних.

Вихідні дані:

- ймовірність атаки = 0.3 (30 %);

- якщо атака сталася:

ймовірність втрати даних = 0.7 (70 %),

якщо дані втрачені, витрати на відновлення становлять 50,000 доларів,

якщо дані не втрачені, витрати на відновлення становлять 10,000 доларів;

- якщо атака не відбулася, витрат не буде.

Необхідно:

- побудувати «дерево рішень» для цієї ситуації;

- оцінити очікувані фінансові витрати (за допомогою ймовірностей і варіантів).

Побудова «дерева рішень» наведена на рис. 5.1.

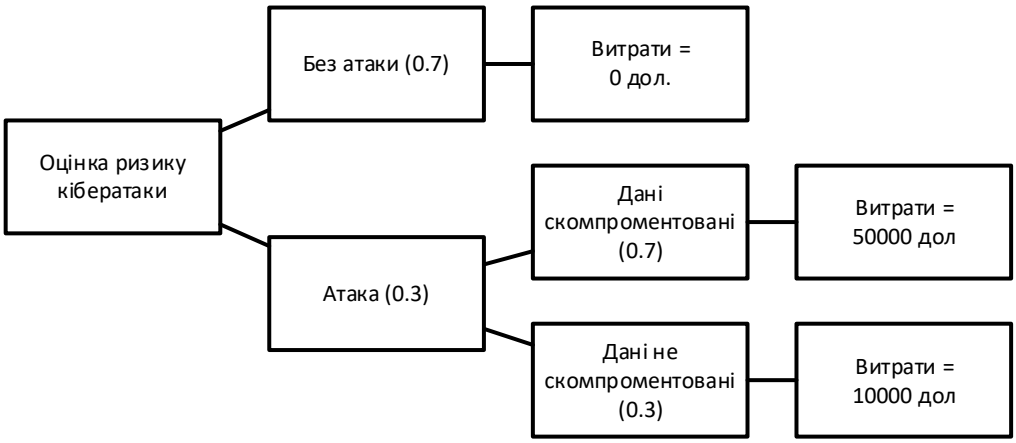

Рисунок 5.1 – «Дерево рішень»

Розрахунок очікуваних витрат.

Для кожної гілки «дерева рішень» обчислюються очікувані витрати, враховуючи ймовірність подій. Очікувані витрати для кожної гілки розраховуються за формулою:

$$\text{Очікувані витрати} = \sum(\text{Ймовірність події} \times \text{Витрати})$$

Для гілки «Атака»:

«Дані скомпрометовані» (ймовірність 0.7): 0.7×50000=35000 $

«Дані не скомпрометовані» (ймовірність 0.3): 0.3×10000=3000 $

Сумарні витрати для гілки «Атака»: 35000+3000=38000 $

Для гілки "Без атаки":

Витрати = 0 (немає атаки, немає витрат).

Очікувані витрати для всієї ситуації з урахуванням ймовірностей «Атака» та «Без атаки»: 0.3×38000+0.7×0=11400 $

Таким чином, очікувані витрати на рік для цієї організації складають 11400 доларів.

Переваги методу «дерева рішень» в аналізі інформаційних ризиків:

1. Простота розуміння та візуалізація. «Дерево рішень» є наочною і зрозумілою моделлю, що дозволяє легко побачити всі варіанти розвитку подій і їх наслідки.

2. Прийняття рішень на основі ймовірностей. Метод дає змогу приймати рішення на основі ймовірностей подій і їх фінансових наслідків, що дуже корисно при оцінці ризиків.

3. Гнучкість у моделюванні різних сценаріїв. «Дерево рішень» дозволяє моделювати як прості, так і складні сценарії ризиків, враховуючи різноманітні варіанти подій і їх ймовірності.

4. Аналіз різних результатів. Метод дає змогу оцінити не лише ймовірність того чи іншого результату, а й потенційні втрати, витрати або вигоди в кожному випадку.

5. Можливість оптимізації. Використовуючи «дерево рішень», можна знайти оптимальні варіанти для зменшення ризиків або максимізації вигоди.

Недоліки методу «дерева рішень» в аналізі інформаційних ризиків:

1. Складність для складних проблем. «Дерева рішень» можуть стати дуже великими та складними при розгляді великих кількостей варіантів або варіантів з багатьма етапами. Це може призвести до труднощів у побудові дерева та його інтерпретації: важко управляти та аналізувати «дерево рішень», що може призвести до втрати корисної інформації або неправильної інтерпретації результатів.

2. Оцінка ймовірностей та вартостей. Оцінка ймовірностей для кожної гілки дерева є важливим елементом дерева рішень. Невірні або приблизні оцінки можуть значно спотворити результати, що негативно вплине на стратегічні рішення щодо ризиків.

3. Неврахування взаємозв’язків між рішеннями. «Дерево рішень» передбачає, що всі гілки та рішення є незалежними, що не завжди відповідає реальній ситуації в інформаційних системах, де рішення можуть бути взаємозалежними. Якщо ж врахувати залежності між різними етапами або рішеннями, «дерево рішень» може стати занадто складним або навіть неможливим для побудови.

4. Перевантаження інформацією. При великій кількості альтернатив і варіантів «дерево рішень» може стати надто громіздким і складним для аналізу.

5. Лінійний характер оцінки рішень. «Дерево рішень» зазвичай аналізує ризики та варіанти лінійно, тобто по черзі, без гнучкості в процесі розгляду кількох варіантів одночасно, що може призвести до того, що складні або багатоступінчасті ситуації будуть розглядатися занадто спрощено.

6. Необхідність точного моделювання наслідків. Для точного оцінювання вартостей наслідків кожного варіанту в «дереві рішень» необхідне чітке моделювання ймовірних наслідків. Недостатня точність або недооцінка потенційних наслідків може призвести до неправильних рішень, що ставить під загрозу безпеку інформаційних систем.

7. Часові витрати на побудову та оновлення. Для створення «дерева рішень» потрібен значний час для аналізу ймовірностей, вартостей та можливих альтернатив. Якщо система постійно змінюється, дерево рішень також потребує регулярного оновлення.

8. Труднощі з багатокроковими ризиками. «Дерево рішень» важко застосувати для аналізу багатокрокових або довгострокових ризиків, де події можуть розвиватися з часом і між ними існують складні залежності.

9. Ризик оптимізації за допомогою узагальнень. Іноді «дерева рішень» потребують узагальнень для зменшення їх складності, що може призвести до втрати важливої деталізації, що може знизити точність результатів і упустити важливі аспекти ризику.

10. Висока потреба в експертних оцінках. Для побудови «дерева рішень» потрібні точні оцінки ймовірностей, вартостей та наслідків, що зазвичай вимагає експертних знань. Залежність від експертів може обмежити точність, оскільки оцінки можуть бути суб’єктивними або обмеженими наявними даними.

5.6. Індивідуальні завдання

Індивідуальні завдання складаються з вирішення 2 класів задач (методом Монте-Карло та методом «дерева рішень»). Для вирішення першої задачі обов’язково реалізувати програмне рішення.

Задачі 1 класу. Вирішити задачі з використанням методу Монте-Карло. Кількість кроків моделювання: 1000, 5000, 10000. Порівняти отримані результати. Варіанти задач:

1. Оцінка впливу на бізнес після кібератаки.

Умова: аналіз впливу кібератаки на фінансові показники компанії. Потрібно врахувати ймовірність атаки, час простою, витрати на відновлення, а також потенційні втрати від порушення контрактів і зниження довіри клієнтів.

Вихідні дані:

Ймовірність атаки: 0.1

Витрати на відновлення після атаки:

легка: 5000 USD

середня: 20000 USD

тяжка: 100000 USD

Втрати через простої:

1000 USD на годину

Час простою (години): 48 годин

2. Оцінка ризику несанкціонованого доступу через мобільні пристрої.

Умова: моделювання ймовірності несанкціонованого доступу до інформаційних систем через використання мобільних пристроїв співробітниками. Необхідно оцінити витрати на забезпечення безпеки мобільних пристроїв.

Вихідні дані:

Ймовірність доступу через мобільний пристрій: 0.05

Витрати на забезпечення безпеки мобільних пристроїв:

легке: 5000 USD

середнє: 15000 USD

тяжке: 30000 USD

3. Ризик втрати даних в хмарному середовищі.

Умова: моделювання ризику втрати даних через несправності в хмарному середовищі. Оцінити ймовірність втрати доступу до даних, витрати на відновлення, час на відновлення та ймовірність відновлення даних без втрат.

Вихідні дані:

Ймовірність втрати даних:

малий ризик: 0.02

середній ризик: 0.1

великий ризик: 0.2

Витрати на відновлення даних:

малий ризик: 2000 USD

середній ризик: 10000 USD

великий ризик: 50000 USD

Ймовірність успішного відновлення:

малий ризик: 0.95

середній ризик: 0.85

великий ризик: 0.5

4. Оцінка ризику компрометації користувацьких облікових записів.

Умова: визначення ризику компрометації облікових записів користувачів при використанні слабких паролів. Необхідно оцінити ймовірність компрометації для кожного типу пароля і витрати на відновлення доступу до системи.

Вихідні дані:

Ймовірність компрометації для різних типів паролів:

простий пароль (12345): 0.3

складний пароль: 0.05

Витрати на відновлення доступу:

простий пароль: 1000 USD

складний пароль: 500 USD

5. Аналіз впливу DDoS-атаки на веб-сайт.

Умова: моделювання наслідків DDoS-атаки на вебсайт. Врахувати ймовірність атаки, витрати на відновлення доступу, час відновлення після атаки, а також втрати від відсутності продаж через простій сайту.

Вихідні дані:

Ймовірність атаки DDoS: 0.1

Час простою сайту:

мала атака: 5 годин

середня атака: 12 годин

велика атака: 24 години

Втрати через простої: 500 USD на годину

6. Оцінка ризику витоку персональних даних через внутрішнього зловмисника.

Умова: моделювання ймовірності витоку персональних даних через зловмисника серед співробітників компанії. Оцінити витрати на відновлення, можливі штрафи і репутаційні втрати.

Вихідні дані:

Ймовірність витоку даних через співробітника: 0.05

Типи витоків і відповідні витрати:

легкий витік (ненавмисний): 5000 USD

середній витік (умисний): 25000 USD

значний витік (серйозне компрометування): 100000 USD

7. Визначення ризику аварійного відключення серверів.

Умова: оцінка ймовірності виходу з ладу критичних серверів компанії. Виконати моделювання витрат на відновлення, втрати часу через зупинку бізнес-процесів і можливі втрати даних.

Вихідні дані:

Ймовірність відключення серверу:

сервер 1: 0.02

сервер 2: 0.05

сервер 3: 0.1

Витрати на відновлення:

сервер 1: 10000 USD

сервер 2: 15000 USD

сервер 3: 30000 USD

Час на відновлення:

сервер 1: 3 години

сервер 2: 6 годин

сервер 3: 12 годин

8. Оцінка фінансових втрат від вразливостей програмного забезпечення.

Умова: моделювання ймовірності застосування вразливостей у програмному забезпеченні, яке використовує компанія. Оцінити витрати на виправлення.

Вихідні дані:

Ймовірність застосування вразливості:

висока: 0.1

середня: 0.2

низька: 0.05

Витрати на виправлення:

висока: 50000 USD

середня: 20000 USD

низька: 5000 USD

9. Ризик втрати клієнтських даних через слабку безпеку на стороні постачальника.

Умова: оцінка ризику втрати даних через компрометацію безпеки в стороннього постачальника послуг, з яким компанія має угоду. Промоделювати ймовірності компрометації і витрати на компенсації.

Вихідні дані:

Ймовірність компрометації постачальника: 0.05

Витрати на компенсації клієнтам:

легкий витік: 10000 USD

середній витік: 30000 USD

тяжкий витік: 50000 USD

10. Аналіз ризику, пов'язаного з непередбачуваними змінами в регуляціях.

Умова: оцінка ризику, пов'язаного з можливими змінами в регуляціях щодо обробки персональних даних. Виконати моделювання врахування ймовірності зміни регуляцій і витрат на адаптацію до нових вимог.

Вихідні дані:

Ймовірність зміни регуляцій: 0.1

Витрати на адаптацію до нових вимог:

легкі зміни: 5000 USD

середні зміни: 20000 USD

серйозні зміни: 100000 USD

11. Оцінка ризику компрометації через вразливості в API.

Умова: моделювання ймовірності компрометації даних через вразливості в API. Необхідно врахувати ймовірність використання вразливості для доступу до даних і витрати на виправлення ситуації.

Вихідні дані:

Ймовірність компрометації API: 0.15

Витрати на виправлення вразливостей:

легка вразливість: 3000 USD

середня вразливість: 15000 USD

тяжка вразливість: 50000 USD

12. Аналіз ризику хакерських атак через слабкі точки в програмному забезпеченні.

Умова: оцінка ймовірності атак через відомі вразливості в сторонньому програмному забезпеченні. Виконати моделювання витрат на виправлення, а також втрат через періоди простою.

Вихідні дані:

Ймовірність атак через вразливості:

Висока: 0.1

Середня: 0.3

Низька: 0.05

Витрати на захист від атак:

Висока ймовірність: 50000 USD

Середня ймовірність: 20000 USD

Низька ймовірність: 5000 USD

13. Оцінка ризику втрати довіри через публікацію негативних відгуків.

Умова: оцінка ймовірності втрати репутації компанії через негативні відгуки клієнтів про безпеку їхніх даних. Необхідно моделювати витрати на відновлення репутації та залучення нових клієнтів.

Вихідні дані:

Ймовірність публікації негативних відгуків: 0.1

Витрати на відновлення репутації:

легкі: 10000 USD

середні: 30000 USD

тяжкі: 50000 USD

14. Моделювання ризику несанкціонованого доступу до корпоративної мережі.

Умова: оцінка ймовірності несанкціонованого доступу до корпоративної мережі через фішинг-атаки. Виконати моделювання витрат на впровадження засобів безпеки та витрат на відновлення.

Вихідні дані:

Ймовірність несанкціонованого доступу через фішинг: 0.2

Витрати на відновлення після доступу:

легкий інцидент: 2000 USD

середній інцидент: 10000 USD

тяжкий інцидент: 50000 USD

Задачі 2 класу. Варіанти задач для використання методу «дерева рішень»:

Необхідно: побудувати «дерево рішень» для вказаної ситуації та оцінити очікувані фінансові витрати.

1. Ризик витоку даних через зловмисне ПЗ в результаті проникнення через стороннє програмне забезпечення.

Умова: організація використовує сторонні програмні продукти в обсязі 30 % від загальної кількості, що можуть мати вразливості, які зловмисники можуть використовувати для доступу до конфіденційних даних (у 40 % випадків). Ймовірність успішного і неуспішного проникнення однакова. У випадку успішного проникнення витік даних відбувається з ймовірністю 0.8 та витрати на відновлення становлять 600 тис. доларів, у випадку неуспішного проникнення витік даних відбувається з ймовірністю 0.2 та витрати на відновлення становлять 100 тис. доларів.

2. Ризик втрати доступу до даних через відмову серверів бази даних.

Умова: відмова (ймовірність якої складає 0.2) сервера бази даних може призвести до втрати (ймовірність 0.3) або тимчасової недоступності (ймовірність 0.7) важливих даних для компанії. У випадку втрати даних може знадобитися відновлення даних (ймовірність 0.6, витрати на відновлення 500 тис. доларів), в інших випадках витрат немає.

3. Ризик використання вразливості мережі через відсутність належного шифрування.

Умова: мережа компанії не використовує належне шифрування для передавання конфіденційної інформації, що збільшує ймовірність перехоплення даних. Обсяг конфіденційної інформації складає 30 % від загального обсягу інформації, що передається мережею. Належне шифрування при передачі конфіденційної інформації використовується лише в 40 випадках зі 100. При неналежному шифруванні ймовірність перехоплення даних складає 50 %, при цьому вартість на відновлення складає 400 тис. доларів, в інших випадках витрат немає.

4. Ризик витоку корпоративних даних через соціальну інженерію.

Умова: зловмисники можуть використовувати методи соціальної інженерії (у 25 % випадків) для отримання доступу до корпоративної інформації через співробітників. Ймовірність проведення атаки складає 0.4, при цьому можливий повний витік даних (у 70 % випадків) та, відповідно, витрати на відновлення 500 тис. доларів або частковий витік даних (у 30 % випадків) з витратами на штрафи в розмірі 200 тис. доларів.

5. Ризик безпеки при наданні доступу до важливих систем третім сторонам.

Умова: організація надає доступ (у половині випадків) до своїх систем для обслуговування. Доступ третім сторонам надається у 60 % всіх випадків надання доступу. При цьому не враховуються можливі ризики безпеки і атака через доступ може статися з ймовірністю 0.3. При цьому, витрати на

відновлення становлять 500 тис. доларів. В усіх інших випадках витрат немає.

6. Ризик порушення політик безпеки через недотримання стандартів управління доступом.

Умова: під час доступу до систем, який складає 20 % від загальної їх роботи, організація у 80 % випадків не дотримується принципів мінімальних прав доступу, що може призвести до порушення політики безпеки (60 % випадків з витратами на перевірку та оновлення в розмірі 100 тис. доларів). В інших випадках витрат немає.

7. Ризик відмови в роботі ключових компонентів інфраструктури через збої в апаратному забезпеченні.

Умова: інфраструктура організації може зазнати відмови через збої з ймовірністю 0.1. Серед них збої серверного обладнання становлять 20 % та призводять до зупинки роботи критичних систем. Ймовірність того, що потребується відновлення обладнання складає 0.5 та розмір витрат на таке відновлення – 600 тис. доларів. В інших випадках витрат немає.

8. Ризик втрати важливих даних через відсутність резервного копіювання.

Умова: організація не виконує належного резервного копіювання важливих даних, що підвищує ризик їх втрати через технічні проблеми чи інші загрози. Копіювання інформації займає 30 % від всіх операцій. Серед них резервне копіювання відбувається з ймовірністю 0.3. Якщо не використовується резервне копіювання можлива втрата даних (ймовірність 0.8) і витрати на їх відновлення складають 700 тис. доларів.

9. Ризик несанкціонованого доступу через неправильну конфігурацію прав доступу.

Умова: неправильна конфігурація прав доступу дозволяє співробітникам або стороннім особам отримати доступ до системи без необхідного дозволу. Кількість об’єктів, до яких були налаштовані права доступу – 40 % від загальної кількості. Правильно налаштовані права лише

для 40 % об’єктів. При несанкціонованому доступі до решти об’єктів, який складає 70 % випадків втрати на відновлення та штрафи складають 300 тис. доларів.

10. Ризик шахрайства через недостатній контроль за транзакціями.

Умова: фінансові транзакції складають 40 % від їх загальної кількості. 60 % фінансових транзакцій не мають належного контролю або перевірки, що може призвести до шахрайства чи зловживань, яке відбувається з ймовірністю 0.5. Витрати на розслідування та відшкодування в такому випадку складають 200 тис. доларів.

11. Ризик порушення політики використання паролів в організації.

Умова: співробітники використовують слабкі паролі для доступу до корпоративних систем, що збільшує ймовірність компрометації. Необхідність використання паролів складає 20 %, серед них слабкі паролі становлять 70 %. При компрометації паролів ймовірність несанкціонованого доступу складає 0.6 та витрати на відновлення 250 тис. доларів.

12. Ризик несанкціонованого доступу через соціальні мережі.

Умова: зловмисники використовують соціальні мережі для збору інформації про співробітників, щоб отримати доступ до корпоративних систем. Рівень користування соціальними мережами в організації складає 50 %. Зловмисниками для збору інформації рівень використання соціальних мереж для складає 40 %, при цьому успішне проникнення дорівнює 50 %, а витрати на відновлення після такого проникнення дорівнюють 400 тис. доларів.

13. Ризик втрати даних через збій в хмарних сервісах.

Умова: хмарні сервіси, на яких зберігається 30 % важливих корпоративних даних, можуть зазнати збоїв або відмов, що призведе до втрати доступу з ймовірністю 0.5. Ймовірність втрати даних при цьому складає 0.4, а витрати на відновлення – 300 тис. доларів.

14. Оцінка ризику внутрішнього витоку даних через помилки співробітників.

Умова: організація має внутрішні політики захисту даних, але співробітники можуть помилково надіслати конфіденційну інформацію стороннім особам або припустити інші помилки. Ймовірність помилок співробітників складає 0.1. Помилка може призвести до витоку даних або ні з однаковою ймовірністю. У 10 % випадків некритичних помилок необхідно додаткове навчання співробітників, яке оцінюється в 15 тис. доларів. Якщо помилка призвела до витоку даних, то може статись повний витік (ймовірність 0.3) або частковий витік (ймовірність 0.7). Витрати на відновлення або штрафи складають 250 тис. доларів та 50 тис. доларів відповідно.

5.7. Контрольні запитання

1. Що таке стохастичний ризик?
2. Через що виникають стохастичні ризики в інформаційних системах?
3. У чому полягає сутність методу Монте-Карло?
4. Що таке «дерево рішень»?
5. Які основні кроки для оцінки стохастичних ризиків в інформаційних системах?
6. Які є основні критерії для оцінки стохастичного інформаційного ризику?
7. Наведіть алгоритм методу Монте-Карло.
8. З чого складається «дерево рішень»?
9. Наведіть алгоритм побудови «дерева рішень».
10. Назвіть переваги та недоліки методу «дерева рішень» в аналізі інформаційних ризиків.

6. ЯКІСНІ МЕТОДИ ОЦІНЮВАННЯ РИЗИКІВ

Мета заняття: ознайомитись з методами якісного оцінювання ризиків, а також навчитись виконувати оцінку інформаційних ризиків за методом карт ризиків.

6.1. Методи якісного аналізу ризиків

Якісні методи оцінювання інформаційних ризиків орієнтовані на використання експертних оцінок, інтуїції та різних інтерпретацій для аналізу можливих загроз, вразливостей і впливу на інформаційні системи, не завжди потребуючи точних числових даних. Ці методи допомагають виявити потенційні проблеми на початкових етапах управління ризиками, коли немає достатньо статистичних або кількісних даних для більш точних моделей.

Деякі з методів якісної оцінки інформаційних ризиків:

1. Метод експертних оцінок. Як і в інших сферах, цей метод передбачає використання досвіду фахівців у галузі інформаційної безпеки для виявлення можливих інформаційних ризиків. Експерти аналізують поточну ситуацію, можливі загрози та вразливості, які можуть вплинути на інформаційні системи та дані. Під час використання методу залучаються фахівці з інформаційної безпеки, які на основі свого досвіду оцінюють потенційні загрози, наприклад, кібератаки, несанкціонований доступ або знищення даних. Перевагами методу експертних оцінок є швидкість збору інформації, врахування специфіки організації. Недоліками – суб’єктивність оцінок, залежність від досвіду та знань експертів.

2. SWOT-аналіз. Це метод стратегічного аналізу, що дозволяє оцінити сильні та слабкі сторони організації, а також зовнішні можливості і загрози, з якими вона може зіткнутися. Цей метод широко використовується для визначення стратегічних напрямів, планування, а також для оцінки інформаційних ризиків, зокрема в сфері інформаційної безпеки. Метод включає ідентифікацію:

- сильних сторін (Strengths) – переваг та ресурсів, які допомагають організації досягати своїх цілей і забезпечують конкурентні переваги. Сюди можна віднести: високий рівень захисту інформаційних систем (сучасні засоби криптографії, багатофакторну аутентифікацію, ефективні системи виявлення вторгнень тощо), професійні кадри (наявність кваліфікованих спеціалістів у сфері IT-безпеки), інноваційні технології (використання новітніх технологій для захисту інформації, таких як блокчейн, штучний інтелект для виявлення аномальних дій), наявність планів відновлення після інцидентів DRP/BCP (можливість відновлення діяльності після інформаційних інцидентів завдяки планам безперервності бізнесу та відновлення після катастроф);

- слабких сторін (Weaknesses) – факторів, що обмежують можливості організації або створюють проблеми в її діяльності. Прикладами є: неадекватний рівень безпеки даних (застарілі системи або відсутність належного захисту чутливих даних), вразливості в програмному забезпеченні (недостатньо оновлене програмне забезпечення або неефективна політика оновлення), недостатня обізнаність співробітників (низький рівень навчання персоналу щодо кібербезпеки), невизначена політика доступу до інформації: (відсутність чітких правил щодо доступу до важливих інформаційних систем та даних);

- можливостей (Opportunities) – зовнішніх умов, які можуть бути використані для розвитку, покращення ситуації або досягнення конкурентних переваг. Серед можливостей можна вказати: розвиток технологій кібербезпеки (впровадження нових технологій, таких як штучний інтелект для моніторингу і аналізу безпеки), зміни в законодавстві (вигоди від нових законів і стандартів, що стимулюють впровадження кращих практик в інформаційній безпеці), збільшення попиту на послуги безпеки (зростаючий попит може створити додаткові можливості для співпраці з іншими організаціями), автоматизація процесів безпеки (використання автоматичних

систем для моніторингу загроз та реагування на інциденти може зменшити ймовірність помилок людини та знизити ризики);

- загроз (Threats) – зовнішніх факторів, які можуть створювати ризики, перешкоди або загрози для успішної діяльності організації. Деякі загрози: кібератаки (зростання кількості та складності кібератак, таких як DDoS-атаки, ransomware, фішинг), загрози з боку співробітників (несанкціонований доступ до інформації або витік даних з боку співробітників чи підрядників), зовнішні загрози (регулювання, конкуренція, зміни в законодавчому середовищі або посилення вимог до захисту даних), природні катастрофи (втрата даних у разі стихійних лих або техногенних катастроф, таких як пожежі, повені).

Переваги SWOT-аналізу для інформаційних ризиків полягають у простоті та доступності (він не потребує складних технічних знань і може бути реалізований у будь-якій організації без значних витрат), всеохопленні (дозволяє одночасно оцінити як внутрішні аспекти, так і зовнішні фактори, що впливають на інформаційну безпеку) та гнучкості (можна використовувати для оцінки інформаційних ризиків як на рівні конкретних проєктів, так і для всієї організації). Серед основних недоліків SWOT-аналізу виділяють суб’єктивність та обмежену деталізацію.

3. Аналіз сценаріїв. Цей метод дозволяє створювати кілька можливих сценаріїв розвитку подій у разі виникнення інформаційних інцидентів. Сценарії ризиків допомагають ідентифікувати уразливості систем, посилюють розуміння потенційних загроз і забезпечують більш ефективне планування заходів для їх мінімізації. Під час реалізації створюються кілька сценаріїв розвитку ситуації:

- найгірший сценарій (катастрофічний). Він передбачає інцидент, який має катастрофічні довготривалі або навіть незворотні наслідки для організації. Такі наслідки можуть призвести до серйозних фінансових втрат, значних юридичних санкцій, тривалої зупинки роботи або повного знищення даних;

- сценарій з високим рівнем ризику. Він передбачає ситуацію, коли загроза має потенціал стати серйозною, якщо не буде вчасно усунена, але ще не є катастрофічною. Система безпеки може не забезпечити достатньо ефективного захисту, і необхідне активне реагування;

- сценарій середнього ризику. Цей сценарій передбачає помірний рівень наслідків, що впливає на організацію, але не призводить до катастрофічних результатів. Зазвичай такі інциденти потребують витрат на відновлення, але не ставлять під загрозу існування компанії. Наслідки можуть бути серйозними, але організація здатна їх швидко подолати;

- сценарій з незначним ризиком (незначні наслідки). Цей сценарій передбачає мінімальний вплив на організацію. Подібні інциденти, як правило, не призводять до значних змін у роботі компанії або її фінансових результатах, але все ж вимагають реагування.

- оптимальний сценарій. Оптимальний сценарій передбачає, що всі ризики або загрози виявлені і ефективно знижуються до мінімуму або навіть повністю усуваються. Такий сценарій може також включати ситуації, коли ризики, попри їх виникнення, мають незначні наслідки завдяки вжитим превентивним заходам.

Зазвичай обмежуються найгіршим сценарієм, сценарієм середнього ризику та оптимістичним сценарієм.

Переваги аналізу сценаріїв: гнучкість у моделюванні варіантів розвитку подій, усвідомлення ризиків на всіх рівнях, покращення обізнаності серед співробітників, порівняння альтернативних рішень, визначення пріоритетності заходів. До недоліків аналізу сценаріїв відносяться: суб’єктивність оцінки, невизначеність і складність прогностичних оцінок, труднощі в кількісній оцінці, залежність від доступних даних і ресурсів, можливість ігнорування малоймовірних, але катастрофічних сценаріїв.

4. Аналіз за допомогою карт ризиків (Risk Maps). Це метод візуалізації ризиків, який дозволяє організаціям оцінити та класифікувати ризики за допомогою графічного зображення, що наочно відображає ймовірність

настання певного ризику та його можливі наслідки. Мета методу – допомогти виявити та ідентифікувати найбільш значущі загрози, а також надати інформацію для прийняття рішень щодо управління цими ризиками. Карти ризиків зазвичай використовуються в рамках загальної стратегії управління ризиками, надаючи можливість для оперативного реагування та моніторингу змін. Кожен ризик має дві основні характеристики: ймовірність (Likelihood – шанс виникнення конкретного ризику) та вплив (Impact – наслідки цього ризику для інформаційної системи). Створюється карта з такими елементами: вісь ймовірності – відображає ймовірність виникнення конкретного ризику, яка вимірюється на шкалі від низької до високої, вісь наслідків – відображає серйозність наслідків у разі реалізації ризику, які можуть бути класифіковані за шкалою від низьких (незначні) до високих (катастрофічні) та ризикові квадранти – матриця поділяється на кілька секцій або квадрантів, кожен з яких позначає рівень ризику. Комбінація ймовірності та наслідків визначає, чи є цей ризик критичним або чи вимагає він негайного реагування.

Коли ризик оцінюється за допомогою карти, він потрапляє в певну категорію на основі своїх характеристик:

- низький ризик – має низьку ймовірність і незначні наслідки. Він потребує мінімальної уваги і може бути прийнятий або проігнорований;
- середній ризик – ризик з помірною ймовірністю або середніми наслідками. Він потребує деякої уваги і може вимагати заходів для його мінімізації;
- високий ризик – ризик з високою ймовірністю або значними наслідками. Він потребує негайного реагування і розробки плану дій для зниження його впливу;
- критичний ризик – ризик з дуже високою ймовірністю та катастрофічними наслідками. Такий ризик має найбільший потенційний вплив і потребує оперативних заходів.

Зазвичай використовується карта розміром 3x3 (рис. 6.1) або 5x5 (рис. 6.2).

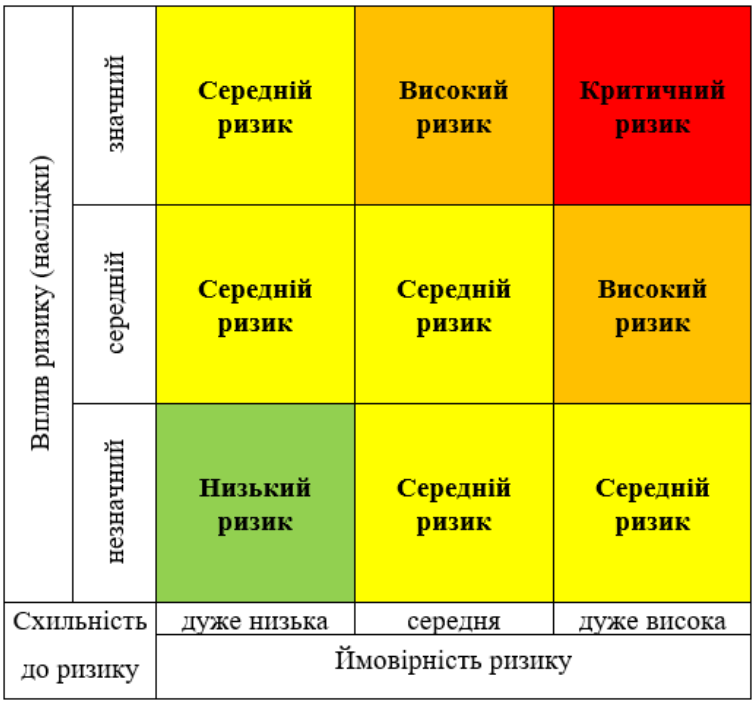

Рисунок 6.1 – Карта ризиків 3х3

Більшість організацій використовують наступні п’ять категорій для визначення ймовірності настання ризикової події:

1 – дуже низька. Ризики, що потрапляють у цю категорію, мають дуже низьку ймовірність настання;

2 – низька. Ризики мають відносно низьку ймовірність настання – від 11 % до 40 %. Однак вони все ж можуть вплинути на бізнес, тому варто тримати їх під контролем;

3 – середня. Ризики можуть виникнути в приблизно половині випадків – їх ймовірність становить 41-60 %, і вони потребують уваги;

4 – висока. Ризик, що потрапляє до цієї категорії, має ймовірність 61-90 % настання. Ці ризики потребують регулярної уваги, оскільки вони, ймовірно, будуть повторюватися, тому необхідно мати постійну стратегію зменшення їхнього впливу;

5 – дуже висока. Ризики майже гарантовано трапляються. Зазвичай ризики з ймовірністю 91 % і більше потрапляють до цієї категорії.

Якщо організація використовує карту ризиків 3×3, достатньо наступних трьох категорій ймовірності:

1 – дуже низька. Ризики в цій категорії мають відносно низьку ймовірність настання;

2 – середня. Ризики цієї категорії передбачаються як такі, що, ймовірно, трапляться, і потребують стратегії зменшення їхнього впливу;

3 – дуже висока. Ризики в цій категорії майже гарантовано трапляться і потребують негайних заходів для їхнього зменшення.

Вплив ризику (наслідки)						
	значний	**Середній ризик**	**Високий ризик**	**Критичний ризик**	**Критичний ризик**	**Критичний ризик**
	високий	**Середній ризик**	**Високий ризик**	**Високий ризик**	**Критичний ризик**	**Критичний ризик**
	середній	**Низький ризик**	**Середній ризик**	**Високий ризик**	**Високий ризик**	**Критичний ризик**
	незначний	**Низький ризик**	**Середній ризик**	**Середній ризик**	**Високий ризик**	**Високий ризик**
	мінімальний	**Низький ризик**	**Низький ризик**	**Низький ризик**	**Середній ризик**	**Середній ризик**
		дуже низька	низька	середня	висока	дуже висока
		Ймовірність ризику				

Рисунок 6.2 – Карта ризиків 5x5

Переваги використання карти ризиків: простота візуалізації, пріоритизація ризиків, покращення прийняття рішень, легке та швидке пояснення ситуації та стратегії управління ризиками. Недоліки карти ризиків: суб’єктивність оцінки, недостатня деталізація, обмеження в динаміці ризиків

(не відображає зміни ризиків протягом часу або в умовах швидко змінного середовища).

5. Метод Delphi. Включає кілька раундів анонімних опитувань експертів у сфері інформаційної безпеки для оцінки ймовірних загроз і вразливостей. Експерти оцінюють потенційні ризики для інформаційних систем і інфраструктури, надаючи свій погляд на ймовірність та серйозність кожного з них.

Основні етапи методу Delphi:

- визначення проблеми – це може бути ризикова ситуація, прогноз розвитку подій чи необхідність прийняття стратегічних рішень;

- вибір експертів – формується група, яка має необхідні знання в обраній галузі. Експерти можуть бути залучені як зсередини організації, так і ззовні (зазвичай 10-15 осіб);

- перший раунд опитування – експертам надсилаються анонімні анкети з питаннями або завданнями, що стосуються конкретної проблеми. Вони надають свої індивідуальні відповіді та оцінки;

- аналіз результатів – проводиться аналіз отриманих відповідей. Результати узагальнюються, визначаються найбільш поширені точки зору, а також можливі відмінності в оцінках;

- зворотний зв’язок – кожен експерт отримує зворотний зв’язок з узагальненими результатами попереднього раунду, а також можливими варіантами відповідей інших експертів. Експерти можуть переглянути свої оцінки та висловити нову думку з урахуванням колективних результатів;

- повторні раунди – процес повторюється кілька разів (зазвичай 2-3 раунди), поки не буде досягнута консенсусна оцінка або прогноз;

- підсумкове узагальнення – формується фінальний звіт, який містить загальний консенсус експертів і рекомендації, які базуються на їх оцінках.

Переваги методу Delphi: анонімність дозволяє зменшити вплив групового тиску, можливість збору експертних думок з різних сфер, ітераційний процес допомагає уточнювати і коригувати думки експертів на

основі зворотного зв’язку, незалежність оцінок, гнучкість. Недоліки методу Delphi: великі часові витрати, залежність від якості експертів, відсутність прямої дискусії, ризик упередженості.

6. Фокус-групи. Залучення групи осіб (наприклад, співробітників IT-відділу, фахівців з безпеки) для обговорення потенційних інформаційних загроз і вразливостей. Виконується обговорення наявних загроз, які можуть впливати на безпеку інформаційних систем (наприклад, зловживання доступом до чутливої інформації, ненавмисні помилки персоналу).

Основні етапи проведення фокус-групи:

- визначення мети – це може бути оцінка певного продукту, послуги, ідеї чи стратегічного рішення;

- вибір учасників – необхідно вибрати учасників, які мають спільні характеристики, що відповідають меті дослідження;

- підготовка питань – можуть бути як відкриті питання (наприклад, «Як ви оцінюєте цей продукт?»), так і питання, які передбачають більш конкретні відповіді;

- модерація обговорення – модератор керує дискусією, забезпечуючи рівномірний розподіл часу для всіх учасників та сприяючи відкритому обміну думками;

- запис та аналіз результатів – усі думки, ідеї та відповіді учасників фіксуються для подальшого аналізу.

Переваги методу фокус-груп: глибоке розуміння проблеми, динаміка обговорення, швидкість збору даних, гнучкість, доступність. Недоліки методу фокус-груп: обмежена кількість учасників (зазвичай 6-12 осіб), витрати часу та ресурсів, вплив модератора, груповий тиск, можливість домінування окремих учасників.

7. Метод «Мозковий штурм». Інтерактивна сесія з залученням фахівців для генерування ідей щодо потенційних інформаційних ризиків. Група фахівців без оцінки чи критики генерує різноманітні ідеї щодо можливих загроз для інформаційних систем організації (наприклад, загроза витоку

інформації через уразливі системи). На відміну від фокус-групи, де орієнтація зроблена на обговорення думок, почуттів, спостережень і досвіду учасників щодо конкретного ризику або ситуації, при «мозковому штурмі» генерується якомога більша кількість ідей або рішень для вирішення проблеми (у даному випадку – ідентифікації ризиків). Це менш структурований процес, де всі учасники активно висловлюють свої думки без обмежень. Мозковий штурм дозволяє генерувати ідеї щодо різноманітних типів ризиків, починаючи від очевидних до малоймовірних, і може бути корисним для створення першого списку ризиків для подальшого аналізу.

Переваги мозкового штурму для виявлення ризиків: швидке генерування ідей, різноманітність точок зору, спільне вирішення проблеми, креативність. Недоліки методу мозкового штурму: можливість домінування окремих учасників, може виникати хаос, не завжди реалістичні ідеї.

6.2. Приклад виконання аналізу за допомогою карт ризиків

Умова: у медичних організаціях особливо важливо забезпечити конфіденційність пацієнтів і зберігання медичних даних. Деякі ризики, які можуть виникнути:

R1: кібератака (включаючи вірусні атаки, шкідливе програмне забезпечення);

R2: витік конфіденційних медичних даних через слабкі паролі або ненадійні системи автентифікації;

R3: несанкціонований доступ до медичних записів через порушення політики доступу або внутрішні помилки;

R4: втрата або пошкодження медичних даних через технічні несправності або відсутність резервного копіювання;

R5: порушення законодавства щодо зберігання та обробки медичних даних (наприклад, порушення GDPR);

R6: недотримання процедур безпеки медичними працівниками (наприклад, передача паролів або відкритий доступ до пристроїв);

R7: збої в роботі медичних пристроїв, що підключені до мережі (наприклад, дефекти в медичних системах, що збирають або зберігають дані);

R8: витік даних через сторонні сервіси або підрядників (наприклад, хмарні сервіси, що зберігають медичні записи).

Необхідно виконати оцінку ймовірності та серйозність наслідків для кожного з наведених ризиків. Ймовірність оцінюється балами від 1 до 5, де 1 – дуже малоймовірно, а 5 – дуже ймовірно. Серйозність наслідків оцінюється балами від 1 до 5, де 1 – мінімальні наслідки, а 5 – катастрофічні наслідки.

Приклад проведення оцінки ризику R1 – кібератака (включаючи вірусні атаки, шкідливе програмне забезпечення).

Оцінка ймовірності (4 бали):

- зростання кіберзагроз – кібератаки стали більш поширеними в останні роки, зокрема в медичних організаціях, оскільки ці установи зберігають велику кількість чутливих даних, що приваблює кіберзлочинців;

- зловмисне програмне забезпечення та віруси – вірусні атаки, трояни, шпигунські програми та інші типи шкідливих програм можуть заражати медичні системи через слабкі місця в програмному забезпеченні, невстановлені оновлення або несанкціоновані підключення до мережі;

- фішинг та соціальна інженерія – крім технічних атак, існують також напади на людський фактор (фішинг) та інші методи соціальної інженерії, які можуть бути використані для отримання доступу до систем через медичних працівників або співробітників.

Оцінка наслідків (5 балів):

- витік або втрата даних – під час кібератаки можуть бути викрадені або знищені медичні дані пацієнтів, що спричинить серйозні проблеми в роботі організації та порушення конфіденційності;

- переривання роботи медичних систем – шкідливе програмне забезпечення може спричинити відмову в роботі важливих медичних систем,

таких як системи управління медичними записами або медичні прилади, що впливатиме на здатність організації надавати медичні послуги;

- юридичні наслідки – витік або знищення медичних даних може призвести до серйозних юридичних наслідків для медичної організації, включаючи штрафи за порушення законів про захист персональних даних;

- шкода репутації – кібератака, яка призводить до витоку чи знищення медичних даних, значно пошкодить репутацію медичної установи, що може призвести до втрати довіри пацієнтів і відтоку клієнтів;

- фінансові витрати – відновлення після кібератаки може вимагати значних фінансових витрат, пов'язаних з усуненням наслідків атаки, відновленням даних, виплатами штрафів та компенсаціями.

Інші ризики оцінюються подібним чином.

Результат оцінки наведено в табл. 6.1.

Таблиця 6.1 – Оцінка ймовірності ризиків та серйозності наслідків

Ризик	Ймовір-ність (1-5)	Наслідки (1-5)	Пояснення
1	2	3	4
R1	4	5	Ймовірність кібератак є високою (4), оскільки організації в медичній сфері часто є цілями для атак через цінність інформації. Наслідки від кібератаки є катастрофічними (5), оскільки в результаті може бути викрадено або знищено велику кількість медичних записів, що може завдати значної шкоди пацієнтам і організації в цілому.
R2	4	5	Ймовірність (4) – ризик виникнення витоку медичних даних через слабкі паролі або ненадійні системи автентифікації досить високий, оскільки це поширена проблема в багатьох медичних установах. Наслідки (5) – наслідки цього ризику є катастрофічними, оскільки порушення конфіденційності медичних даних може призвести до серйозних фінансових втрат, юридичних наслідків та шкоди репутації організації.
R3	3	5	Ймовірність (3) – ризик виникнення несанкціонованого доступу має середню ймовірність. Це може статися через помилки персоналу, неправильні налаштування доступу або недостатній моніторинг. Наслідки (5) – наслідки цього ризику є катастрофічними, оскільки порушення конфіденційності медичних даних може призвести до серйозних юридичних, фінансових та репутаційних втрат для організації.

Продовження табл. 6.1.

1	2	3	4
R4	2	4	Ймовірність (2) – ризик втрати або пошкодження медичних даних має відносно низьку ймовірність через наявність систем резервного копіювання та відновлення даних в більшості сучасних медичних установ. Наслідки (4) – наслідки цього ризику є серйозними, оскільки втрата медичних даних може серйозно вплинути на процес лікування пацієнтів, призвести до юридичних та фінансових санкцій.
R5	2	2	Ймовірність (2) – порушення законодавства щодо зберігання та обробки медичних даних має відносно низьку ймовірність завдяки наявності процедур, контролю та зовнішнім аудитам. Наслідки (2) – наслідки такого порушення помірно серйозні, включаючи штрафи та репутаційні збитки, але не настільки катастрофічні, щоб призвести до серйозних фінансових втрат або порушення роботи організації.
R6	4	4	Ймовірність (4) – ризик недотримання процедур безпеки медичними працівниками має високу ймовірність через людський фактор, недостатнє навчання або стрес на роботі. Наслідки (4) – наслідки цього ризику серйозні, оскільки порушення процедур безпеки може призвести до несанкціонованого доступу до медичних даних, фінансових штрафів та шкоди репутації.
R7	3	3	Ймовірність (3) – збої в роботі медичних пристроїв мають помірну ймовірність, оскільки технології, хоч і надійні, все ще можуть зазнавати непередбачуваних збоїв через складність їхніх систем. Наслідки (3) – наслідки від збоїв є помірними і можуть включати тимчасові порушення доступу до важливих даних або лікувального процесу, хоча ці наслідки зазвичай можна швидко мінімізувати завдяки наявності технічного обслуговування.
R8	3	5	Ймовірність (3) – витік даних через сторонні сервіси або підрядників має помірну ймовірність, оскільки медичні установи активно використовують зовнішні платформи для зберігання і обробки даних, що підвищує ризик. Наслідки (5) – наслідки цього ризику є катастрофічними, оскільки витік медичних даних призводить до серйозних юридичних, фінансових і репутаційних втрат для організації.

Побудова карти ризиків, яка дозволить візуалізувати, які ризики є найбільш критичними для медичної організації наведена на рис. 6.3.

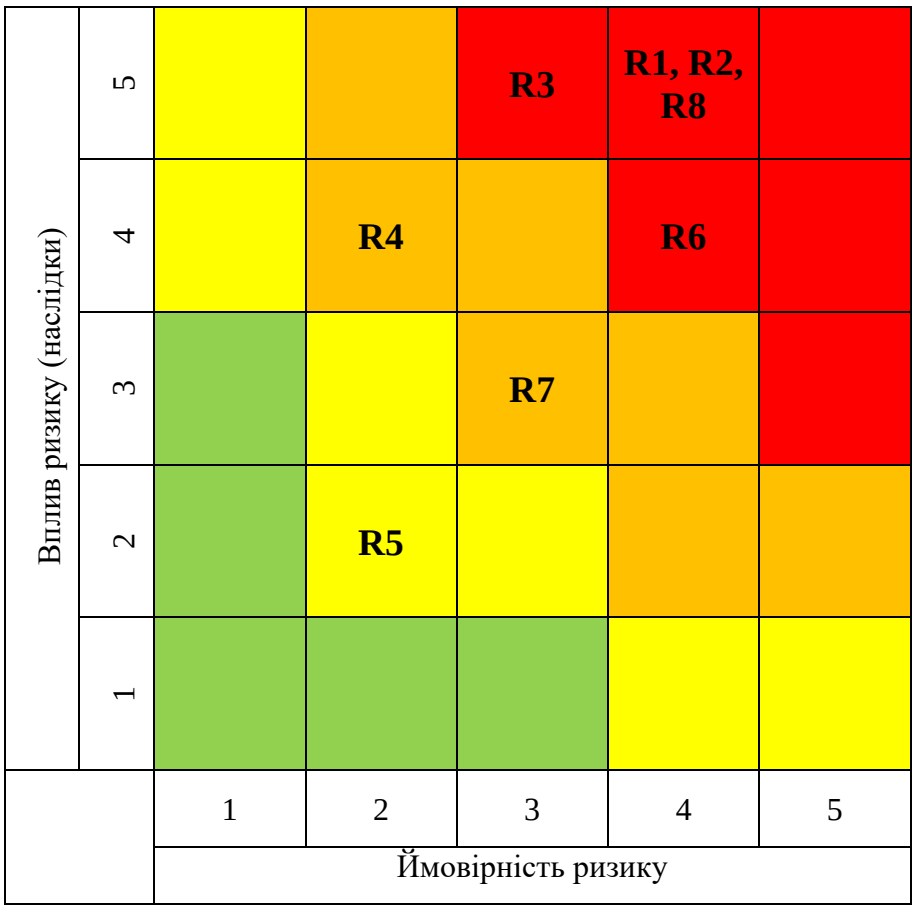

Рисунок 6.3 – Карта інформаційних ризиків медичної організації

До зони критичних ризиків потрапили ризики R1, R2, R3, R6, R8.

Оскільки йдеться про різні види загроз для конфіденційності та безпеки медичних даних, необхідно підходити до кожного ризику індивідуально, враховуючи ймовірність його виникнення, наслідки та рівень впливу на загальний процес. Можна прийняти одне з наступних рішень:

- прийняття ризику (якщо ймовірність низька або наслідки несерйозні);

- мінімізація ризику (якщо ймовірність висока або наслідки значні, але можна контролювати);

- уникнення ризику (якщо ризик є критичним і потребує повної ліквідації);

- передача ризику або страхування (якщо ризик можна передати іншим сторонам, наприклад, через аутсорсинг або страхування).

Для наведених ризиків пропонуються наступні рішення:

R1 – мінімізація ризику: впровадження заходів кібербезпеки, таких як антивірусне програмне забезпечення, файрволи, шифрування даних; регулярне оновлення програмного забезпечення та систем безпеки; проведення навчань для співробітників з питань безпеки та обережного використання мережі; впровадження політик щодо обмеження доступу до систем.

R2 – мінімізація ризику: встановлення надійних механізмів автентифікації (наприклад, двофакторної автентифікації); політика регулярної зміни паролів та створення складних паролів; шифрування медичних даних для додаткового рівня захисту.

R3 – мінімізація ризику: визначення чіткої політики доступу до даних; впровадження механізмів обмеження доступу (за принципом «мінімального необхідного доступу»); регулярні аудити доступу до чутливих даних; відстеження та моніторинг усіх спроб доступу.

R4 – мінімізація ризику: впровадження регулярних процедур резервного копіювання медичних даних; використання хмарних сервісів для зберігання даних з додатковими рівнями захисту; регулярне тестування процесу відновлення даних для забезпечення швидкого відновлення в разі втрати.

R5 – мінімізація ризику: підготовка до дотримання вимог GDPR та інших відповідних нормативних актів; проведення регулярних внутрішніх аудитів для перевірки відповідності; залучення зовнішніх консультантів або юристів для забезпечення належної юридичної відповідності.

R6 – мінімізація ризику: проведення регулярних тренінгів для медичних працівників щодо забезпечення конфіденційності і безпеки даних; створення політики щодо використання паролів та зберігання даних на робочих пристроях; забезпечення доступу лише уповноважених осіб до чутливих медичних даних.

R7 – мінімізація ризику: регулярне технічне обслуговування та перевірка медичних пристроїв; використання резервних пристроїв та систем

для забезпечення безперервної роботи; впровадження автоматизованих систем моніторингу стану медичних пристроїв для своєчасного виявлення збоїв.

R8 – уникнення ризику: вибір підрядників і сторонніх постачальників, які мають відповідні сертифікати безпеки та відповідають вимогам щодо захисту медичних даних; встановлення чітких угод з конфіденційності (NDA) з усіма постачальниками та підрядниками; регулярні перевірки та аудит зовнішніх постачальників, щоб забезпечити їх відповідність політикам безпеки медичних даних.

6.3. Індивідуальні завдання

Виконати аналіз вказаної ситуації за допомогою методу карт ризиків. Сформулювати не менше 6 ризиків, виконати та обґрунтувати оцінку їх ймовірності та можливі наслідки. Побудувати карту ризиків, визначити критичні ризики, прийняти рішення та описати обрані стратегії по управлінню кожним ризиком.

1. Кібератаки на інформаційні системи організації. Звернути увагу на частоту, з якою організація стикається з потенційними кіберзагрозами та наслідки, які можуть бути у випадку успішної атаки.

2. Витік конфіденційних даних через ненадійні системи автентифікації. Оцінити ймовірність витоку даних через недостатньо захищені паролі чи інші форми автентифікації.

3. Недотримання внутрішніх політик безпеки персоналом. Визначити ймовірність того, що співробітники не дотримуються внутрішніх політик безпеки (наприклад, передача паролів або доступ до несанкціонованих пристроїв).

4. Несанкціонований доступ до фінансових даних. Оцінити ризик несанкціонованого доступу до чутливих фінансових даних і його наслідки для компанії.

5. Технічні збої в критичних виробничих системах. Оцінити ризики, пов’язані з поломками або зупинками виробничого обладнання, що може призвести до значних виробничих витрат.

6. Витік даних через сторонні сервісні компанії. Оцінити, як може виникнути витік чутливих даних через посередників або сторонніх постачальників та які наслідки це може мати.

7. Збої в програмному забезпеченні, що управляє критично важливими системами. Визначити наслідки, якщо програмне забезпечення, що управляє важливими системами, зазнає збоїв.

8. Неякісне обслуговування та технічне обслуговування обладнання. Оцінити ймовірність того, що відсутність регулярного технічного обслуговування може призвести до збоїв у роботі важливих систем.

9. Порушення законодавства щодо зберігання та обробки даних. Визначити як часто організація може порушити вимоги законодавства (наприклад, норм захисту даних) і які наслідки це може мати.

10. Втрата або пошкодження критичних даних через технічні несправності. Визначити ймовірність втрати або пошкодження важливих даних через відсутність резервного копіювання або технічні збої.

11. Можливість саботажу або навмисних дій з боку внутрішніх співробітників. Визначити можливі наслідки дій недоброчесних співробітників, таких як саботаж або викрадення даних.

12. Невідповідність стандартам безпеки в інформаційних системах. Оцінити ймовірність того, що інформаційні системи не відповідають актуальним стандартам безпеки, що може привести до загроз.

13. Погіршення репутації компанії через несправність або недостатню безпеку продуктів. Оцінити негативний вплив несправностей у продуктах або послугах на репутацію організації.

14. Необхідність змін у законодавстві або нормативних вимогах. Оцінити вплив змін у законодавстві (наприклад, щодо захисту даних) на роботу організації та її стратегії безпеки.

15. Порушення стандартів безпеки при роботі з хмарними сервісами. Визначити ризики, які можуть виникнути при використанні хмарних сервісів, якщо вони не відповідають стандартам безпеки.

6.4. Контрольні запитання

1. На чому засновано метод експертних оцінок?
2. Які елементи ідентифікуються в методі SWOT-аналізу?
3. Що виконується під час аналізу сценаріїв?
4. Які розглядаються сценарії під час аналізу сценаріїв?
5. Що таке карти ризиків?
6. Які етапи виконання методу Delphi?
7. Чим відрізняються фокус-групи від «мозкового штурму»?
8. Як скласти карту ризику?
9. Які етапи при виконанні аналізу за допомогою карт ризиків?
10. Які виділяють категорії ризику?

7. МАТРИЧНІ МЕТОДИ ПРИЙНЯТТЯ РИЗИКОВИХ РІШЕНЬ В УМОВАХ НЕВИЗНАЧЕНОСТІ

Мета заняття: ознайомитись з матричним методом аналізу ризиків, а також отримати практичні навички при його застосуванні для аналізу інформаційних ризиків.

7.1. Матричний метод аналізу інформаційних ризиків

Матричний метод аналізу ризиків пов’язує активи, вразливості, загрози та засоби управління, визначаючи важливість різних засобів управління для конкретних активів організації. Під активами організації розуміються значущі об’єкти, які можуть бути як матеріальними, так і нематеріальними. Це можуть бути фізичні ресурси (наприклад, комп’ютери, сервери, програмне забезпечення) або нематеріальні ресурси (наприклад, дані, репутація компанії, інтелектуальна власність).

Методика, заснована на використанні матриць, основана на побудові трьох окремих матриць: матриці загроз, матриці вразливостей та матриці контролю. За допомогою цих матриць збираються дані для подальшого аналізу ризиків. Всі матриці взаємопов’язані між собою.

Матриця вразливостей показує зв’язки між активами і вразливостями, тобто, як конкретні активи можуть бути піддані різним вразливостям. Вразливості можуть бути технічними (наприклад, відсутність оновлень для програмного забезпечення), організаційними (наприклад, неефективні політики безпеки) або людськими (наприклад, помилки персоналу).

Матриця загроз демонструє взаємозв’язки між вразливостями та загрозами, що можуть виникнути. Загроза – це подія чи обставина, яка може скористатися вразливістю і призвести до негативних наслідків для активу. Наприклад, кіберзлочинці можуть скористатися вразливістю в системі, щоб здійснити кібератаку або витік даних.

Матриця контролю відображає зв’язок між загрозами і засобами управління, які можуть бути застосовані для запобігання, зменшення або пом’якшення наслідків цих загроз. Засоби управління включають технічні заходи (наприклад, антивірусне програмне забезпечення), організаційні (наприклад, навчання співробітників) або юридичні (наприклад, політики безпеки).

У кожній з матриць значення в клітинках показує важливість зв’язку між елементом рядка та елементом стовпця. Для цього зазвичай використовуються оцінки, такі як низька, середня та висока, що вказують на рівень ризику або необхідність застосування контролю. Наприклад, у матриці загроз зв’язок між певною вразливістю і загрозою може мати високу важливість, якщо ймовірність її реалізації велика.

Процес аналізу починається з формування списків активів, вразливостей, загроз і засобів управління. Потім ці дані вводяться в матриці, заповнюючи клітинки, що відображають зв’язки між елементами. Процес заповнення матриць здійснюється поетапно, шляхом внесення інформації про взаємозв’язки між елементами стовпців і рядків кожної матриці.

Першим етапом є заповнення матриці вразливостей, де визначають, які активи пов’язані з якими вразливостями. Активи розташовуються згідно зменшення значень їх відносної вартості C_j. Кожній вразливості присвоюється ранг пріоритету: 1 – не важливий, 2 – мінімально важливий, 3 – важливий, але не ключовий, 4 – важливий, але під впливом ключового, 5 – ключовий.

Значення в кожній клітинці має показувати рівень відношення між елементом рядка і стовпця матриці (активом і вразливістю), що визначається за наступною шкалою оцінки: 0 – немає впливу, 1 – слабкий вплив, 3 – помірний вплив, 9 – сильний вплив.

Загальний вигляд матриці вразливостей наведено на рис. 7.1.

Для визначення ваги та важливості кожної вразливості (її потенційного впливу) розрахунок ведеться за формулою:

$$V_i = \sum_{j=1}^{m} v_{ij} C_j,$$

де v_{ij} – відносний вплив вразливості v_i на актив a_j з його відносною вартістю C_j $(j = 1, \cdots, m)$.

Шкала взаємозв'язку: 0 – немає впливу 1 – слабкий вплив 3 – помірний вплив 9 – сильний вплив	Ранг пріоритету вразливості	Активи $a_j, j = 1 \ldots m$							Σ	Ранжирування
Вразливості $v_i, i = 1 \ldots n$		Актив a_1	Актив a_2	⋮	Актив a_j	⋮	Актив a_{m-1}	Актив a_m		
Відносна вартість C_j		m					2	1		
Вразливість v_1	$РП_1$								V_1	
Вразливість v_2	$РП_2$								V_2	
…	…								…	
Вразливість v_i	$РП_i$								V_i	
…	…								…	
Вразливість v_n	$РП_n$								V_n	

Рисунок 7.1 – Матриця вразливостей

Далі дані з цієї матриці переносяться до матриці загроз, де визначають, які загрози можуть використати ці вразливості. Вразливості розташовуються згідно їх ранжирування в матриці вразливостей.

Для оцінки потенційних ризиків інформаційної безпеки виконується розрахунок за формулою:

$$T_k = \sum_{i=1}^{n} t_{ki} V_i,$$

де t_{ki} – відносна можливість використання загрозою t_k вразливості v_i з її потенційним впливом V_i $(i = 1, \cdots, n)$.

Загальний вигляд матриці загроз наведено на рис. 7.2.

Шкала взаємозв'язку: 0 – немає впливу 1 – слабкий вплив 3 – помірний вплив 9 – сильний вплив	Ранг пріоритету загрози	Вразливості $v_i, i = 1 \dots n$							Σ	Ранжирування
Загрози $t_k, k = 1 \dots p$		Вразливість v_1	Вразливість v_2	…	Вразливість v_i	…	Вразливість v_{n-1}	Вразливість v_n		
Відносний вплив вразливості		n					2	1		
Загроза t_1	$РП_1$								T_1	
Загроза t_2	$РП_2$								T_2	
…	…								…	
Загроза t_k	$РП_k$								T_k	
…	…								…	
Загроза t_p	$РП_p$								T_p	

Рисунок 7.2 – Матриця загроз

На останньому етапі інформація з матриці загроз переноситься до матриці контролю, де визначаються відповідні засоби управління для кожної загрози. Ця матриця визначає необхідність застосування конкретних заходів або інструментів захисту для зменшення впливу загроз на один або кілька активів організації, тим самим знижуючи рівень ризиків.

Тоді потенційне пом'якшення загроз Z_l за допомогою конкретного засобу контролю l обчислюється за формулою:

$$Z_l = \sum_{k=1}^{p} e_{lk} T_k,$$

де e_{lk} – відносний вплив засобу контроля e_l на загрозу t_k з потенційним ризиком T_k $(k = 1, \cdots, p)$.

На рис. 7.3 наведено загальний вигляд матриці контролю.

І вже на основі даних результатів визначається доцільність використання тих чи інших механізмів забезпечення безпеки, надаються рекомендацій щодо побудови систем захисту інформації та плануються витрати на інформаційну безпеку організації.

Шкала взаємозв'язку: 0 – немає впливу 1 – слабкий вплив 3 – помірний вплив 9 – сильний вплив	Ранг пріоритету засобу	Загрози $t_k, k = 1 \dots p$							Σ	Ранжирування
Засоби контролю $e_l, l = 1 \dots r$		Загроза t_1	Загроза t_2	…	Загроза t_k	…	Загроза t_{p-1}	Загроза t_p		
Відносна можливість загрози		p					2	1		
Засіб контролю e_1	$РП_1$								Z_1	
Засіб контролю e_2	$РП_2$								Z_2	
…	…								…	
Засіб контролю e_l	$РП_l$								Z_l	
…	…								…	
Засіб контролю e_r	$РП_r$								Z_r	

Рисунок 7.3 – Матриця контролю

Таким чином, у результаті аналізу буде отримано список засобів контролю, ранжируваний по впливу на актуальні загрози інформаційній безпеці організації.

Цей метод дозволяє систематизувати всі елементи безпеки в організації і забезпечити комплексний підхід до управління ризиками. Крім того, він дає можливість визначити, де необхідно посилити заходи безпеки, а також оптимізувати витрати на управління ризиками, зосередивши увагу на найбільш важливих загрозах і вразливостях.

Однією з головних переваг цього методу є те, що його можна застосувати практично до будь-якої організації. Методологія містить досить зручні матричні шаблони, які можна вдосконалювати з появою нової інформації для аналізу. Цим методом можна скористатися самостійно, не звертаючись до фахівців.

Однак, перед прийняттям рішення щодо впровадження будь-якого методу управління ризиками необхідно впевнитися, що він у повній мірі враховує всі потреби організації, її параметри, а також відповідає досвіду

найкращих світових практик і відрізняється детальним описом процесів і дій, що здійснюються під час оцінки.

7.2. Приклад використання матричного методу аналізу інформаційних ризиків

Необхідно виконати аналіз ризиків інформаційної безпеки організації, яка займається розробкою програмного забезпечення та має філії за кордоном.

Для побудови матриці вразливостей було визначено відносну цінність активів, що дозволило здійснити їх ранжирування за рівнем важливості (від найвищого до найнижчого). Успіх організації, зокрема, значною мірою залежить від її здатності розвивати нові технології та забезпечувати їх захист. Тому саме ці активи були оцінені на найвищому рівні важливості. З огляду на це, акцент зроблено на інноваційних технологіях, оскільки їх розвиток є критично важливим для стабільності та зростання в умовах високої конкуренції.

Згідно з визначеними активами, було ідентифіковано основні вразливості, що можуть негативно вплинути на їх безпеку та стабільність. Кожній вразливості було присвоєно пріоритетний ранг, що відображає її потенційний вплив на активи. Наприклад, враховуючи, що зовнішні порушники повинні спершу обійти брандмауер для того, щоб отримати доступ до конфіденційної інформації, він був визначений як одна з найважливіших вразливостей у системі захисту. Це дає підстави розглядати брандмауер як перший бар’єр, який захищає ключові активи компанії від можливих атак.

Окрім того, враховуючи географічне розташування філій, що поширені на різні регіони, проблема передачі та синхронізації даних набуває особливої важливості. Потрібно враховувати, що будь-які збої в цих процесах можуть призвести до серйозних наслідків для безперебійної роботи, тому питання безпеки передачі даних також отримало високу оцінку при визначенні

вразливостей. Обмежений список вразливостей (відсортованих за рангами пріоритетів) та активів (відсортованих за відносною їх вартістю) наведено в матриці вразливостей на рис. 7.4. Взаємозв'язок між вразливостями та активами заповнено згідно міркувань щодо ступеню впливу кожної вразливості на кожний актив.

Шкала взаємозв'язку: 0 – немає впливу 1 – слабкий вплив 3 – помірний вплив 9 – сильний вплив	Ранг пріоритету вразливості	Активи $a_j, j = 1 \dots m$							Σ	Ранжирування
Вразливості $v_i, i = 1 \dots n$		Новітні розробки	Конф. інф. (програми)	Репутація	Доступність сервісів	Комунікації	Програмне забезпечення	Апаратні засоби		
Відносна вартість C_j		7	6	5	4	3	2	1		
Брандмауер	5	9	9	3	9	9	9	9	222	11
Передача даних та лінії зв'язку	4	9	9	3	9	9	3	9	210	10
Бази даних	4	9	9	3	3	1	9	1	166	7
Архітектура застосунків	4	9	3	9	3	1	9	9	168	8
Фізична безпека	4	9	9	3	1	1	3	9	154	6
Помилки конфігурації серверів	3	9	9	3	9	3	9	1	196	9
Стійкість паролів	3	9	9	1	1	3	9	1	154	5
Клієнтські ПК, ноутбуки	3	3	9	1	0	1	9	3	104	3
Апаратні засоби (вебсервер)	3	1	1	3	1	1	1	1	38	1
Безпровідний зв'язок	1	9	3	3	3	1	1	1	114	4
Перерви в електроживленні	1	1	1	1	9	3	1	1	66	2

Рисунок 7.4 – Матриця вразливостей організації

При розрахунку ваги V_i кожної вразливості було отримано два однакових значення (154), тому при ранжируванні було враховано ранги пріоритетів даних вразливостей: фізична безпека отримала вищий ранг, ніж стійкість паролів.

Наступним етапом є формування матриці загроз. Так само виконується заповнення можливими загрозами, відсортованими за встановленими пріоритетами. Вразливості беруться з матриці вразливостей та розташовуються згідно розрахованим рангам. Взаємозв'язок між загрозами

та вразливостями заповнено згідно міркувань щодо ступеню впливу кожної загрози на кожну вразливість. Після розрахунку оцінки потенційних ризиків T_k виконано ранжирування загроз. Отриману матрицю наведено на рис. 7.5.

Шкала взаємозв'язку: 0 – немає впливу 1 – слабкий вплив 3 – помірний вплив 9 – сильний вплив	Ранг пріоритету загрози	Вразливості $v_i, i = 1 \dots n$											Σ	Ранжирування
Загрози $t_k, k = 1 \dots p$		Брандмауер	Передача даних та лінії зв'язку	Помилки конфігурації серверів	Архітектура застосунків	Бази даних	Фізична безпека	Стійкість паролів	Безпровідний зв'язок	Клієнтські ПК, ноутбуки	Перерви в електроживленні	Апаратні засоби (вебсервер)		
Відносний вплив вразливості		11	10	9	8	7	6	5	4	3	2	1		
DoS/DDoS атака	5	9	9	9	0	0	1	1	3	1	1	3	301	4
Збої сервера	5	9	9	9	0	0	9	1	9	1	3	3	377	6
Несанкціонований доступ	5	9	3	9	3	9	9	9	3	9	1	9	446	7
Шкідливе ПЗ	4	1	1	9	9	3	1	1	1	9	1	1	240	2
Вторгнення (атака на пароль)	3	9	3	9	1	9	1	9	3	3	1	3	358	5
Фізичне пошкодження ІТС	3	1	9	3	1	3	9	0	3	3	3	9	247	3
Помилки працівника	2	1	1	3	3	3	3	3	1	9	1	1	160	1

Рисунок 7.5 – Матриця загроз організації

Останньою формується матриця контролю, до якої вносяться запропоновані засоби контролю з відповідним рангом пріоритету. Відносний вплив кожного засобу контролю на кожну загрозу встановлюється з використанням суб'єктивних суджень, після чого обчислюється потенційне пом'якшення загроз Z_l.

Сформована матриця контролю організації наведена на рис. 7.6.

Результати цього аналізу та зведені дані з матриць використовуються під час інтеграції виробничих процесів, бізнес-процесів, а також для вибору програмного забезпечення та апаратних засобів. Таким чином, за результатами аналізу отримано список засобів контролю, ранжируваний за підсумковим впливом на актуальні загрози інформаційної безпеки організації (на початку списку найбільш дійові засоби пом'якшення загроз):

1) міжмережеві екрани;

2) система виявлення вторгнень;

3) контроль території;

4) політика безпеки;

5) конфігурація архітектури мережі;

6) навчання персоналу.

Шкала взаємозв'язку: 0 – немає впливу 1 – слабкий вплив 3 – помірний вплив 9 – сильний вплив Засоби контролю $e_l, l = 1 \dots r$	Ранг пріоритету засобу	Загрози $t_k, k = 1 \dots p$							Σ	Ранжирування
		Несанкціонований доступ	Збої сервера	Вторгнення (атака на пароль)	DoS/DDoS атака	Фізичне пошкодження ІТС	Шкідливе ПЗ	Помилки працівника		
Відносна можливість загрози		7	6	5	4	3	2	1		
Система виявлення вторгнень	5	9	9	3	9	1	3	3	180	5
Міжмережеві екрани	5	9	9	9	9	1	3	1	208	6
Конфігурація архітектури мережі	5	3	9	1	9	0	0	1	117	2
Політика безпеки	4	9	1	9	3	1	9	3	150	3
Контроль території	4	9	3	9	1	9	3	1	164	4
Навчання персоналу	2	0	1	9	0	3	9	9	87	1

Рисунок 7.6 – Матриця контролю організації

7.3. Індивідуальні завдання

Виконати аналіз вказаної ситуації за допомогою матричного методу. Сформулювати та обґрунтувати вибір не менше 8 активів, 10 вразливостей, 8 загроз та 6 засобів контролю. Виконати аналіз та обґрунтувати вибір найбільш доцільних засобів реагування на ризикові ситуації.

1. Фінансова організація (Банк). Банк зберігає чутливу фінансову інформацію та проводить транзакції через інтернет-банкінг. Оцініть ризики, пов'язані з шахрайством, фішингом, та зломом онлайн-банкінгу. Створіть план заходів контролю для захисту платіжних систем.

2. Медична організація (Лікарня). Лікарня зберігає персональні дані пацієнтів та медичні записи. Оцініть ризики витоку особистої інформації, незаконного доступу до медичних даних та атаки на медичні пристрої. Розробіть план контролю доступу до медичних записів.

3. Фармацевтична компанія. Фармацевтична компанія зберігає дослідницькі дані та рецептури ліків. Оцініть ризики витоку конфіденційної інформації, зловживань даними лабораторних досліджень або кібернападів. Розробіть план заходів контролю для захисту наукових та комерційних даних.

4. Роздрібна торгова організація (Магазин). Організація продає товари онлайн та в офлайн-магазинах, зберігаючи дані про клієнтів. Оцініть ризики, пов’язані з крадіжкою платіжних карток, зломом онлайн-платформи та втратами через недбале зберігання даних. Розробіть стратегію захисту даних клієнтів.

5. Організація в сфері логістики. Логістична компанія здійснює доставку товарів по всьому світу. Оцініть ризики для інформаційних систем, пов’язаних з несанкціонованим доступом до маршрутів, перехопленням даних про вантажі, та зловживанням даними співробітниками. Розробіть заходи контролю для безпеки транспортних та логістичних даних.

6. Навчальний заклад (Університет). Університет зберігає студентські та наукові дані в електронному вигляді. Оцініть ризики витоку інформації, втрати наукових результатів або доступу сторонніх осіб до захищених баз даних. Розробіть стратегію захисту наукових та студентських даних.

7. Державна організація. Державний орган зберігає конфіденційну інформацію щодо політичних рішень і особистих даних громадян. Оцініть ризики несанкціонованого доступу до архівів, витоку персональних даних, а також атак на державні реєстри. Створіть матрицю контролю для захисту даних громадян.

8. Авіаційна компанія. Авіаційна компанія зберігає дані про пасажирів та маршрути рейсів. Оцініть ризики витоку особистої інформації пасажирів, атак на систему бронювання квитків або кібернападів на системи управління польотами. Розробіть заходи контролю для захисту пасажирських та рейсових даних.

9. Енергетична компанія. Енергетична компанія керує критичними інфраструктурними об’єктами, такими як енергетичні мережі і станції. Оцініть ризики фізичних і кібератак на ці системи, а також можливі внутрішні загрози з боку персоналу. Розробіть план з управління ризиками для критичних інфраструктур.

10. Туристична компанія. Туристична компанія зберігає інформацію про бронювання, маршрути та оплату клієнтів. Оцініть ризики зловживання правами доступу до персональних даних клієнтів, втрати бронювань, або шахрайства з платіжками. Розробіть план з управління ризиками для туристичної платформи.

11. Юридична компанія. Юридична компанія зберігає документи з конфіденційною інформацією для своїх клієнтів. Оцініть ризики витоку юридичних документів або несанкціонованого доступу до них. Створіть матрицю контролю для захисту конфіденційної інформації клієнтів.

12. Телевізійна та медіа організація. Медіа-компанія зберігає відео- та аудіофайли, що стосуються журналістських розслідувань. Оцініть ризики несанкціонованого доступу до матеріалів, витоку даних та кібератак. Розробіть стратегію для захисту медіа-контенту.

13. Рекламна та маркетингова організація. Маркетингова компанія збирає дані про поведінку користувачів на вебсайтах своїх клієнтів. Оцініть ризики витоку персональних даних, несанкціонованого доступу до баз даних, а також маніпуляцій з даними клієнтів. Розробіть план заходів контролю для захисту персональних даних.

14. Будівельна компанія. Будівельна компанія зберігає проєктні документи та дані про будівельні матеріали. Оцініть ризики, пов’язані з

витоком проєктної інформації, несанкціонованим доступом до матеріалів будівництва, а також зловживанням даними співробітниками. Розробіть заходи контролю для безпеки проєктних даних.

7.4. Контрольні запитання

1. Для чого використовується матричний метод прийняття ризикових рішень?
2. Які матриці будуються при виконанні матричного аналізу?
3. Що є вихідними даними для проведення матричного аналізу ризикових ситуацій?
4. Яким чином виконується оцінка потенційних ризиків?
5. Як заповнюється матриця загроз?
6. Як розраховується відносна цінність активів?
7. Яким чином формується перелік вразливостей?
8. Яким чином враховуються ранги пріоритетів вразливостей, загроз, засобів контролю?
9. Яким чином формується перелік засобів контролю?
10. Які переваги та недоліки матричного методу аналізу ризикових ситуацій?

8. КРИТЕРІЇ ПРИЙНЯТТЯ РИЗИКОВИХ РІШЕНЬ В УМОВАХ НЕВИЗНАЧЕНОСТІ

Мета заняття: ознайомитись з критеріями прийняття ризикових рішень, отримати практичні навички розрахунку різноманітних критеріїв при виконанні аналізу стратегій пом'якшення загроз для різних сценаріїв інформаційних ризиків.

8.1. Критерії прийняття рішень в умовах невизначеності в теорії ризиків

Прийняття рішень в умовах невизначеності є важливим аспектом управлінської практики організацій. Невизначеність може виникати через відсутність повної інформації, складність прогнозування розвитку подій, а також через швидкість змін у зовнішньому середовищі, таких як економічні кризи, технологічні інновації або політичні зміни. У цьому контексті важливо вибирати оптимальні стратегії і приймати обґрунтовані рішення, незважаючи на відсутність чіткої або точної інформації про розвиток подій.

Існує кілька підходів до прийняття рішень, які дозволяють знизити ризик і забезпечити максимальний виграш у разі можливих змін ситуації. Зазвичай, ці підходи базуються на аналізі ймовірностей настання різних подій, їх впливу на результат і пошуку найбільш збалансованих рішень у конкретних умовах. Багато рішень доводиться приймати в умовах значної невизначеності, коли ймовірності певних подій не можна точно визначити або ж ці ймовірності не є статичними. У таких випадках традиційні методи, які ґрунтуються на статистичних даних, часто не дають однозначних результатів або застосовуються з обмеженнями.

Тому для прийняття рішень в умовах невизначеності застосовуються спеціальні методи і критерії, які дозволяють аналізувати різні варіанти дій та оцінювати їх наслідки, враховуючи можливі зміни в зовнішньому середовищі.

Одним із таких інструментів є теорія прийняття рішень в умовах ризику та невизначеності, яка пропонує різноманітні підходи для оцінки та мінімізації можливих збитків, а також для максимізації очікуваного виграшу. Ці методи використовуються для вирішення таких завдань, як вибір оптимальних варіантів інвестицій, оцінка потенційних загроз для інформаційної безпеки, прогнозування розвитку бізнесу в умовах економічних коливань і багато інших.

Проблеми прийняття рішень в умовах невизначеності пов’язані з:

- недостатністю або неповнотою даних. У багатьох випадках організації не мають повної або точної інформації, необхідної для правильного вибору стратегії. Це може стосуватися як фінансових показників, так і зовнішніх факторів (економічних, політичних, технічних);

- складністю в оцінці ймовірностей. Багато ситуацій не піддаються чіткому визначенню ймовірностей, наприклад, у випадку технологічних інновацій або геополітичних змін. У таких випадках традиційні методи статистичного аналізу можуть бути непридатними, а прогнозування за допомогою моделей стає більш спекулятивним;

- неоднозначністю наслідків різних варіантів рішень. Для кожного з можливих варіантів можуть бути як позитивні, так і негативні наслідки, що ускладнює вибір стратегії;

- міжнародними факторами та глобальною невизначеністю. Міжнародні економічні кризи або зміни в політиці можуть впливати на стратегії, що застосовуються організаціями. Рішення, яке є оптимальним в одній країні, може бути ризикованим або навіть неефективним в іншій через різні умови.

З огляду на ці складнощі, для прийняття рішень застосовуються різноманітні критерії.

Найбільш відомі критерії прийняття рішень в умовах невизначеності:

1. Максимінний критерій Вальда (Maximin Criterion), критерій песимізму, критерій найбільшої обережності. Критерій максимінного вибору

передбачає, що рішення повинно бути прийнято таким чином, щоб у найгіршому можливому випадку (найменш вигідному результаті) воно давало найбільший можливий виграш. Цей підхід використовується, коли необхідно забезпечити максимально можливу стабільність у найгірших умовах:

$$R_{maximin} = \max_{i \in M_m} \left(\min_{j \in N_n} (R_{ij}) \right),$$

де R_{ij} – можливі результати для кожного варіанту j при i-й стратегії, m – число стратегій, n – число варіантів, $\min_{j \in N_n} (R_{ij})$ – мінімум для кожної стратегії i (найгірший можливий результат).

Критерієм песимізму керуються при виборі ризикових рішень в умовах невизначеності, як правило, суб'єкти, які не схильні до ризику або розглядають можливі ситуації як песиміст.

2. Мінімаксний критерій Севіджа (Savage Minimax Criterion), критерій оптимізму. Критерій Севіджа дозволяє приймати рішення на основі мінімізації шкоди у випадку невизначеності, де крім розгляду тільки найбільш несприятливого сценарію, оцінюються усі варіанти за різницею між оптимальним результатом і реальною можливістю. Значення критерію Севіджа – це найменше значення ризику, тобто гарантоване значення мінімальних втрат:

$$R_{Savage} = \min_{i \in N_m} \left(\max_{j \in N_n} (S_{ij}) \right), \; S_{ij} = \max_{i \in N_m} (R_{ij}) - R_{ij},$$

де R_{ij} – можливі результати для кожного варіанту j при i-й стратегії, m – число стратегій, n – число варіантів, S_{ij} – втрати при виборі i-ої стратегії в порівнянні з найбільшим виграшом при j-му варіанті.

Критерій Севіджа рекомендує вибирати в якості оптимальної стратегії ту, коли величина максимального ризику мінімізується в найгірших умовах.

3. Критерій недостатнього обґрунтування Лапласа (Laplace Criterion).

Критерій Лапласа використовується, коли ймовірності для різних варіантів не є відомими, а ми припускаємо, що всі варіанти мають рівну

ймовірність. Він дозволяє відокремити кращий варіант у тому випадку, якщо жодна з умов не має істотної переваги.

Оцінку середньої цінності кожної альтернативи можна обчислити за формулою середнього арифметичного всіх її можливих оцінок у різних варіантах. Оптимальною є та альтернатива, яка має найбільшу середню оцінку:

$$R_{Laplace} = \max_{i \in N_m} \left(\frac{1}{n} \sum_{j=1}^{n} R_{ij} \right),$$

де R_{ij} – можливі результати для кожного варіанту j при i-й стратегії, m – число стратегій, n – число варіантів.

Приклад використання критерію Лапласа – якщо не можна точно оцінити ймовірність різних сценаріїв (наприклад, різні варіанти захисту інформаційної системи), то він дозволяє вибрати той варіант, який у середньому дає найбільшу вигоду.

4. Критерій узагальненого песимізму-оптимізму Гурвіца (Hurwicz Criterion). Цей критерій є комбінацією оптимістичного (найкращого результату) і песимістичного (найгіршого результату) підходів. Значення критерію Гурвіца – найбільше середньозважене значення виграшу, причому частка песимізму задається за допомогою коефіцієнта оптимізму. Параметр, що використовується для важливості оптимістичного і песимістичного підходів, називається коефіцієнтом оптимізму α ($0 \leq \alpha \leq 1$):

$$R_{Hurwicz} = \max_{i \in N_m} \left(\alpha \max_{j \in N_n} \left(R_{ij} \right) + (1 - \alpha) \min_{j \in N_n} \left(R_{ij} \right) \right),$$

де R_{ij} – можливі результати для кожного варіанту j при i-й стратегії, m – число стратегій, n – число варіантів.

Наприклад, у випадку вибору між кількома варіантами технологій для захисту інформаційних систем, цей підхід дозволяє знайти оптимальний компроміс між максимальною вигодою та мінімізацією ризиків.

8.2. Приклад використання критеріїв прийняття рішень у ризикових ситуаціях

Умова задачі.

Організація, яка займається інформаційними технологіями, повинна вибрати стратегію для захисту своєї інфраструктури від кібератак. Вибір стратегії залежить від того, як змінюється рівень загроз на ринку в майбутньому, і компанія може вибрати одну з п’яти стратегій захисту:

1) інвестиція в антивірусне програмне забезпечення (AV);

2) інвестиція в систему виявлення вторгнень (IDS);

3) інвестиція в систему багатофакторної аутентифікації (MFA);

4) інвестиція в брандмауери (FW);

5) інвестиція в криптографічний захист даних (Crypto).

Існує п’ять можливих сценаріїв розвитку ситуації:

1) різке збільшення кількості кібератак;

2) помірне збільшення кількості атак;

3) стабільний рівень атак;

4) помірне зменшення кількості атак;

5) різке зменшення кількості атак;

Матриця виграшів/збитків для кожної стратегії та сценарію наведена в табл. 8.1.

Таблиця 8.1 – Матриця виграшів/збитків

Стратегії	Сценарії розвитку ситуації, вартість, грн.				
	1	2	3	4	5
AV	500 000	300 000	200 000	100 000	50 000
IDS	700 000	400 000	250 000	150 000	75 000
MFA	300 000	350 000	300 000	150 000	100 000
FW	450 000	300 000	250 000	200 000	100 000
Crypto	600 000	500 000	350 000	200 000	150 000

Примітка: у випадку наявності матриці витрат (збитків), її можна перетворити на матрицю виграшів: виграш у кожному випадку визначається як різниця між максимальними витратами за сценарієм та витратами на

конкретну стратегію захисту для цього сценарію. Виграш для стратегії визначається для кожного сценарію та показує, як ця стратегія допомагає економити витрати порівняно з найбільш витратними варіантами.

Рішення задачі виконується за допомогою різних критеріїв:

1. **Критерій Вальда**. За критерієм Вальда вибирається стратегія, яка максимізує мінімальний можливий виграш (найгірший можливий результат).

Пошук мінімальних виграшів для кожної стратегії:

$$\min_{j\in N_n}(R_{1j}) = \min_{j\in N_n}(500000, 300000, 200000, 100000, 50000) = 50000,$$

$$\min_{j\in N_n}(R_{2j}) = \min_{j\in N_n}(700000, 400000, 250000, 150000\ ,75000) = 75000,$$

$$\min_{j\in N_n}(R_{3j}) = \min_{j\in N_n}(300000, 350000, 300000,150000,100000) = 100000,$$

$$\min_{j\in N_n}(R_{4j}) = \min_{j\in N_n}(450000, 300000, 250000, 200000, 100000) = 100000,$$

$$\min_{j\in N_n}(R_{5j}) = \min_{j\in N_n}(600000, 500000, 350000, 200000, 150000) = 150000.$$

Вибір стратегії з найбільшим мінімальним результатом:

$$R_{maximin} = \max_{i\in M_m}(50000, 75000, 100000, 100000, 150000) = 150000.$$

Рішення за критерієм Вальда: вибір стратегії – інвестиція в криптографічний захист даних.

2. **Критерій Севіджа** полягає в тому, щоб мінімізувати максимальне «розчарування» – різницю між вибраною стратегією і найкращою стратегією для кожного сценарію.

Пошук максимального виграшу для кожного сценарію:

$$R_{Savage} = \min_{i\in N_m}\left(\max_{j\in N_n}(S_{ij})\right),\ S_{ij} = \max_{i\in N_m}(R_{ij}) - R_{ij},$$

$$\max_{i\in N_m}(R_{i1}) = \max_{i\in N_m}(500000, 700000, 300000, 450000, 600000) = 700000,$$

$$\max_{i\in N_m}(R_{i2}) = \max_{i\in N_m}(300000, 400000, 350000, 300000, 500000) = 500000,$$

$$\max_{i\in N_m}(R_{i3}) = \max_{i\in N_m}(200000, 250000, 300000, 250000, 350000) = 350000,$$

$$\max_{i\in N_m}(R_{i4}) = \max_{i\in N_m}(100000, 150000, 150000, 200000, 200000) = 200000,$$

$$\max_{i \in N_m}(R_{i5}) = \max_{i \in N_m}(50000, 75000, 100000, 100000, 150000) = 150000,$$

Обчислення «розчарування» для кожної стратегії в кожному сценарії.

Стратегія 1 (AV):

$$S_{11} = 700000 - 500000 = 200000,$$
$$S_{12} = 500000 - 300000 = 200000,$$
$$S_{13} = 350000 - 200000 = 150000,$$
$$S_{14} = 200000 - 100000 = 100000,$$
$$S_{15} = 150000 - 50000 = 100000.$$

Стратегія 2 (IDS):

$$S_{21} = 700000 - 700000 = 0,$$
$$S_{22} = 500000 - 400000 = 100000,$$
$$S_{23} = 350000 - 250000 = 100000,$$
$$S_{24} = 200000 - 150000 = 50000,$$
$$S_{25} = 150000 - 75000 = 75000.$$

Стратегія 3 (MFA):

$$S_{31} = 700000 - 300000 = 400000,$$
$$S_{32} = 500000 - 350000 = 150000,$$
$$S_{33} = 350000 - 300000 = 50000,$$
$$S_{34} = 200000 - 150000 = 50000,$$
$$S_{35} = 150000 - 100000 = 50000.$$

Стратегія 4 (FW):

$$S_{41} = 700000 - 450000 = 250000,$$
$$S_{42} = 500000 - 300000 = 200000,$$
$$S_{43} = 350000 - 250000 = 100000,$$
$$S_{44} = 200000 - 200000 = 0,$$
$$S_{45} = 150000 - 100000 = 50000.$$

Стратегія 5 (Crypto):

$$S_{51} = 700000 - 600000 = 100000,$$
$$S_{52} = 500000 - 500000 = 0,$$

$$S_{53} = 350000 - 350000 = 0,$$

$$S_{54} = 200000 - 200000 = 0,$$

$$S_{55} = 150000 - 150000 = 0.$$

Пошук максимального «розчарування» для кожної стратегії:

$$\max_{j \in N_n}(S_{1j}) = \max_{j \in N_n}(200000, 200000, 150000, 100000, 100000) = 200000,$$

$$\max_{j \in N_n}(S_{2j}) = \max_{j \in N_n}(0,100000, 100000, 50000, 750000) = 100000,$$

$$\max_{j \in N_n}(S_{3j}) = \max_{j \in N_n}(400000, 150000, 50000, 50000, 50000) = 400000,$$

$$\max_{j \in N_n}(S_{4j}) = \max_{j \in N_n}(250000, 200000, 100000, 0, 50000) = 250000,$$

$$\max_{j \in N_n}(S_{5j}) = \max_{j \in N_n}(100000, 0, 0, 0, 0) = 100000.$$

Вибір стратегії з найменшим максимальним розчаруванням:

$$R_{Savage} = \min_{i \in N_m}(200000, 100000, 400000, 250000, 100000) = 100000.$$

Таким чином, рішення за критерієм Севіджа: вибір стратегій – інвестиція в систему виявлення вторгнень або інвестиція в криптографічний захист даних.

3. **Критерій недостатнього обґрунтування Лапласа** передбачає, що ймовірності всіх сценаріїв однакові. Вибір стратегії ґрунтується на середньому результаті для кожної стратегії.

Обчислення для кожної стратегії середнього значення:

$$\frac{1}{n}\sum_{j=1}^{n} R_{1j} = \frac{1}{5}(500000 + 300000 + 200000 + 100000 + 50000) = 230000$$

$$\frac{1}{n}\sum_{j=1}^{n} R_{2j} = \frac{1}{5}(700000 + 400000 + 250000 + 150000 + 75000) = 315000$$

$$\frac{1}{n}\sum_{j=1}^{n} R_{3j} = \frac{1}{5}(300000 + 350000 + 300000 + 150000 + 100000) = 240000$$

$$\frac{1}{n}\sum_{j=1}^{n} R_{4j} = \frac{1}{5}(450000 + 300000 + 250000 + 200000 + 100000) = 260000$$

$$\frac{1}{n}\sum_{j=1}^{n} R_{5j} = \frac{1}{5}(600000 + 500000 + 350000 + 200000 + 150000) = 360000.$$

Вибір стратегії з найвищим середнім результатом:

$$R_{Laplace} = \max_{i \in N_m}(230000, 315000, 240000, 260000, 360000) = 360000.$$

Рішення за критерієм Лапласа: вибір стратегії – інвестиція в криптографічний захист даних.

4. **Критерій узагальненого песимізму-оптимізму**. Цей критерій комбінує песимістичний і оптимістичний підхід. Потрібно вибрати коефіцієнт оптимізму α, який визначає важливість оптимістичного або песимістичного результату:

$$\alpha = 0.6 \text{ (60 \% оптимізму)}.$$

Обчислення оптимістичного результату (найкращий результат для кожного сценарію):

$$\max_{j \in N_n}(R_{1j}) = \max_{j \in N_n}(500000, 300000, 200000, 100000, 50000) = 500000,$$

$$\max_{j \in N_n}(R_{2j}) = \max_{j \in N_n}(700000, 400000, 250000, 150000, 75000) = 700000,$$

$$\max_{j \in N_n}(R_{3j}) = \max_{j \in N_n}(300000, 350000, 300000, 150000, 100000) = 350000,$$

$$\max_{j \in N_n}(R_{4j}) = \max_{j \in N_n}(450000, 300000, 250000, 200000, 100000) = 450000,$$

$$\max_{j \in N_n}(R_{5j}) = \max_{j \in N_n}(600000, 500000, 350000, 200000, 150000) = 600000,$$

та песимістичного результату (найгірший результат для кожного сценарію):

$$\min_{j \in N_n}(R_{1j}) = \min_{j \in N_n}(500000, 300000, 200000, 100000, 50000) = 50000,$$

$$\min_{j \in N_n}(R_{2j}) = \min_{j \in N_n}(700000, 400000, 250000, 150000, 75000) = 75000,$$

$$\min_{j \in N_n}(R_{3j}) = \min_{j \in N_n}(300000, 350000, 300000, 150000, 100000) = 100000,$$

$$\min_{j \in N_n}(R_{4j}) = \min_{j \in N_n}(450000, 300000, 250000, 200000, 100000) = 100000,$$

$$\min_{j \in N_n}(R_{5j}) = \min_{j \in N_n}(600000, 500000, 350000, 200000, 150000) = 150000.$$

Та їх сума з урахуванням коефіцієнту оптимізму α:

$$0.6 \max_{j \in N_n}(R_{1j}) + 0.4 \min_{j \in N_n}(R_{1j}) = 0.6 \cdot 500000 + 0.4 \cdot 50000 = 320000,$$

$$0.6 \max_{j \in N_n}(R_{2j}) + 0.4 \min_{j \in N_n}(R_{2j}) = 0.6 \cdot 700000 + 0.4 \cdot 75000 = 450000,$$

$$0.6 \max_{j \in N_n}(R_{3j}) + 0.4 \min_{j \in N_n}(R_{3j}) = 0.6 \cdot 350000 + 0.4 \cdot 100000 = 250000,$$

$$0.6 \max_{j \in N_n}(R_{4j}) + 0.4 \min_{j \in N_n}(R_{4j}) = 0.6 \cdot 450000 + 0.4 \cdot 100000 = 310000,$$

$$0.6 \max_{j \in N_n}(R_{5j}) + 0.4 \min_{j \in N_n}(R_{5j}) = 0.6 \cdot 600000 + 0.4 \cdot 150000 = 420000.$$

Обчислення результату:

$$R_{Hurwicz} = \max_{i \in N_m}(320000, 450000, 250000, 310000, 420000) = 450000.$$

Вибір за критерієм песимізму-оптимізму: інвестиція в систему виявлення вторгнень (450 000 грн).

Результати:

- за критерієм Вальда найкраща стратегія – інвестиція в криптографічний захист даних.

- за критерієм Севіджа – інвестиція в систему виявлення вторгнень або інвестиція в криптографічний захист даних.

- за критерієм Лапласа – інвестиція в криптографічний захист даних.

- за критерієм узагальненого песимізму-оптимізму – інвестиція в систему виявлення вторгнень.

8.3. Індивідуальні завдання

Виконати вибір найкращої стратегії захисту для можливих сценаріїв атак. Розрахунок виконати за максимінним критерієм Вальда, мінімаксним критерієм Севіджа, критерієм недостатнього обґрунтування Лапласа та критерієм узагальненого песимізму-оптимізму Гурвіца (розрахунок виконати для коефіцієнту оптимізму α = 0.4, α = 0.6 та α = 0.8). У вихідних даних до задач наведено матриці витрат (необхідно перетворити на матриці виграшів).

1. Захист від DDoS-атак.

Сценарії (матриця збитків наведена в табл. 8.2):

1 Високий обсяг трафіку (DDoS-атака).

2. Помірний обсяг трафіку (неповна атака).

3. Відсутність атаки.

4. Часова затримка в мережі.

5. Доступність критичних ресурсів.

Таблиця 8.2 – Матриця збитків для 1 задачі

Стратегії	Сценарії розвитку ситуації, витрати, $				
	1	2	3	4	5
Встановлення брандмауера	5000	3000	500	1000	1500
Використання хмарного захисту	7000	4000	800	1500	2000
Апаратне прискорення	8000	5000	700	2500	2000
Фільтрація трафіку в реальному часі	6000	3500	600	1200	1800
Сегментація мережі	5500	4000	700	1100	1700

2. Захист конфіденційної інформації.

Сценарії (матриця збитків наведена в табл. 8.3):

1. Витік даних через електронну пошту.

2. Втрата даних через фізичні носії.

3. Високий рівень внутрішньої загрози.

4. Захист від шахрайства в онлайн-сервісах.

5. Атака на сервери баз даних.

Таблиця 8.3 – Матриця збитків для 2 задачі

Стратегії	Сценарії розвитку ситуації, витрати, $				
	1	2	3	4	5
Шифрування даних	7000	5000	6000	4000	8000
Використання двофакторної автентифікації	5000	3000	4000	2000	6000
Забезпечення фізичної безпеки носіїв	4000	8000	3500	1000	2000
Аудит та моніторинг доступу до даних	6000	4000	5000	3000	7000
Створення політик щодо використання паролів	3000	2000	2000	1000	3000

3. Захист від соціальної інженерії.

Сценарії (матриця збитків наведена в табл. 8.4):

1. Фішинг.
2. Співпраця з внутрішніми зловмисниками.
3. Використання слабких паролів.
4. Фіктивні запити на доступ до конфіденційних даних.
5. Атака через соціальні мережі.

Таблиця 8.4 – Матриця збитків для 3 задачі

Стратегії	Сценарії розвитку ситуації, витрати, $				
	1	2	3	4	5
Навчання співробітників з питань безпеки	6000	7000	5000	4000	3000
Регулярне оновлення паролів	2000	4000	3000	1000	1500
Використання антифішингових технологій	7000	5000	4000	2000	6000
Реалізація політики мінімальних привілеїв	5000	8000	3500	2500	5500
Застосування системи моніторингу	8000	6000	2000	3000	7000

4. Захист від шкідливого ПЗ.

Сценарії (матриця збитків наведена в табл. 8.5):

1. Виявлення нових вірусів.
2. Атака через веб-застосунки.
3. Шкідливе ПЗ через електронну пошту.
4. Втрата даних через експлойти.
5. Атака через флеш-накопичувачі.

Таблиця 8.5 – Матриця збитків для 4 задачі

Стратегії	Сценарії розвитку ситуації, витрати, $				
	1	2	3	4	5
Антивірусне програмне забезпечення	7000	5000	6000	4000	3000
Патч-менеджмент	6000	7000	4000	3000	5000
Контроль доступу до флеш-носіїв	4000	3000	2000	1000	7000
Моніторинг безпеки веб-застосунків	8000	9000	3000	5000	4000
Використання віртуальних машин для ізоляції програм	5000	6000	4000	3000	2000

5. Захист від внутрішніх загроз.

Сценарії (матриця збитків наведена в табл. 8.6):

1. Невірні або зловмисні співробітники.
2. Крадіжка інформації.
3. Необережність у роботі з даними.
4. Невідповідність політикам безпеки.
5. Порушення прав доступу.

Таблиця 8.6 – Матриця збитків для 5 задачі

Стратегії	Сценарії розвитку ситуації, витрати, $				
	1	2	3	4	5
Журнали аудиту доступу	5000	7000	3000	2000	6000
Контроль використання критичних даних	8000	9000	6000	4000	5000
Навчання співробітників	4000	3000	5000	2000	3000
Створення політик мінімальних привілеїв	6000	5000	4000	3000	7000
Системи моніторингу для виявлення аномалій	7000	6000	5000	4000	8000

6. Захист від фізичних атак.

Сценарії (матриця збитків наведена в табл. 8.7):

1. Фізичний доступ до серверів.
2. Пошкодження або крадіжка обладнання.
3. Напад на центр обробки даних.
4. Вандалізм.
5. Спостереження за серверною кімнатою.

Таблиця 8.7 – Матриця збитків для 6 задачі

Стратегії	Сценарії розвитку ситуації, витрати, $				
	1	2	3	4	5
Обмеження доступу до серверних кімнат	7000	4000	5000	2000	3000
Фізичне обладнання для захисту серверів	5000	8000	6000	3000	4000
Спостереження через камери відеоспостереження	3000	2000	3000	1500	2500
Охоронні системи	8000	7000	9000	5000	6000
Засоби блокування портів і кабелів	2000	3000	2500	1000	1500

7. Захист від атак на веб-сайт.

Сценарії (матриця збитків наведена в табл. 8.8):

1. SQL-ін’єкція.
2. XSS (Cross-site Scripting).
3. CSRF (Cross-Site Request Forgery).
4. Атаки через API.
5. Атака через хакерські скрипти.

Таблиця 8.8 – Матриця збитків для 7 задачі

Стратегії	Сценарії розвитку ситуації, витрати, $				
	1	2	3	4	5
Використання валідаторів для введених даних	7000	6000	4000	5000	4500
Шифрування веб-трафіку	5000	5500	3000	6000	4000
Аудит безпеки веб-застосунків	8000	7000	6000	8000	7000
Використання захисту від CSRF	3000	2500	2000	3500	3000
Підвищення безпеки API	6000	5500	4500	7500	5000

8. Захист від атак через мережу Wi-Fi.

Сценарії (матриця збитків наведена в табл. 8.9):

1. Спостереження за трафіком.
2. Несанкціонований доступ до мережі.
3. Відмова в обслуговуванні (DoS).
4. Атака на Wi-Fi маршрутизатор.
5. Атака через слабкий пароль.

Таблиця 8.9 – Матриця збитків для 8 задачі

Стратегії	Сценарії розвитку ситуації, витрати, $				
	1	2	3	4	5
Використання WPA3 шифрування	5000	4000	7000	8000	6000
Створення окремої мережі для гостей	3000	3500	4000	5000	4500
Регулярне оновлення ПЗ маршрутизаторів	4000	3000	5000	6000	5500
Підвищення безпеки маршрутизаторів	6000	5000	8000	7000	6500
Моніторинг безпеки мережі	7000	6000	7500	9000	8000

9. Захист від атак через VPN.

Сценарії (матриця збитків наведена в табл. 8.10):

1. Несанкціонований доступ через вразливість VPN.
2. Атака через компрометацію ключів.
3. Втрата шифрування.
4. Неправильне налаштування VPN.
5. Атака через розрив з'єднання.

Таблиця 8.10 – Матриця збитків для 9 задачі

Стратегії	Сценарії розвитку ситуації, витрати, $				
	1	2	3	4	5
Використання двофакторної автентифікації для VPN	5000	4000	7000	6000	4500
Вибір високоякісного шифрування	4000	5000	6000	7000	5500
Аудит налаштувань VPN	6000	5500	7500	8000	7000
Постійне оновлення програмного забезпечення VPN	4500	4000	6500	5000	4000
Використання лише перевірених VPN-постачальників	7000	6000	8500	7500	6500

10. Захист від атак через електронну пошту.

Сценарії (матриця збитків наведена в табл. 8.11):

1. Фішинг через електронну пошту.
2. Вірусні атаки через вкладення.
3. Спам.
4. Мануальне сканування електронної пошти.
5. Втрата важливих даних через пошту.

Таблиця 8.11 – Матриця збитків для 10 задачі

Стратегії	Сценарії розвитку ситуації, витрати, $				
	1	2	3	4	5
Використання антифішингових фільтрів	4000	5000	3000	6000	4500
Аудит вхідної пошти	6000	5500	3500	5000	4000
Використання шифрування електронної пошти	7000	6000	5000	8000	6500
Навчання співробітників	5000	4000	3000	7000	5500
Перевірка вкладень через антивірусне ПЗ	5500	4500	3500	6500	5000

11. Захист від атак на хмарні сервіси.

Сценарії (матриця збитків наведена в табл. 8.12):

1. Несанкціонований доступ до даних.

2. Атака через API.

3. Злом облікових записів.

4. Втрата даних через хмарне сховище.

5. Фізичний доступ до серверів в хмарі.

Таблиця 8.12 – Матриця збитків для 11 задачі

Стратегії	Сценарії розвитку ситуації, витрати, $				
	1	2	3	4	5
Використання шифрування даних	7000	8000	6000	7500	9000
Аудит доступу та журналювання	6000	5500	5000	6000	5000
Регулярне оновлення паролів	5000	4000	3500	4000	4500
Встановлення обмежень на API-запити	5500	6000	4500	5000	4000
Використання багатофакторної автентифікації	6500	7000	5500	6500	5000

12. Захист від атак через Bluetooth.

Сценарії (матриця збитків наведена в табл. 8.13):

1. Несанкціонований доступ до Bluetooth-пристроїв.

2. Атака через вразливості протоколів.

3. Глобальна крадіжка даних.

4. Фізичний доступ до пристроїв.

5. Інтерференція сигналу.

Таблиця 8.13 – Матриця збитків для 12 задачі

Стратегії	Сценарії розвитку ситуації, витрати, $				
	1	2	3	4	5
Використання паролів для підключень	3000	3500	4000	2500	2000
Вимкнення Bluetooth, коли не використовується	2500	2000	2500	1500	1000
Використання безпечних версій протоколів Bluetooth	4000	5000	6000	3500	3000
Постійний моніторинг підключених пристроїв	4500	4000	4500	3000	3500
Обмеження доступу до даних через Bluetooth	5000	5500	6000	4000	4500

13. Захист від атаки на сервери.

Сценарії (матриця збитків наведена в табл. 8.14):

1. Обхід брандмауера
2. Вразливості в операційній системі.
3. Втрата доступу через SSH.
4. Несанкціонований доступ через API.
5. Атака через слабкі паролі.

Таблиця 8.14 – Матриця збитків для 13 задачі

Стратегії	Сценарії розвитку ситуації, витрати, $				
	1	2	3	4	5
Встановлення і оновлення брандмауера	6000	5000	4000	5500	3000
Використання SSH ключів	5500	4000	6000	4500	2500
Регулярне оновлення операційної системи	4000	3500	2500	3000	2000
Використання складних паролів	3500	3000	2000	3500	5000
Використання двофакторної автентифікації	4500	4000	3000	4000	4500

14. Захист від втрачених даних через мобільні пристрої.

Сценарії (матриця збитків наведена в табл. 8.15):

1. Втрата мобільного телефону.
2. Несанкціоноване використання пристрою.
3. Втрата доступу до важливих корпоративних даних.
4. Порушення конфіденційності через застосунки.
5. Зловмисний доступ до пристроїв через Bluetooth.

Таблиця 8.15 – Матриця збитків для 14 задачі

Стратегії	Сценарії розвитку ситуації, витрати, $				
	1	2	3	4	5
Шифрування даних на пристроях	6000	5000	7000	4000	3500
Використання програм для відстеження пристроїв	3500	4000	3000	2500	2000
Встановлення політик безпеки для мобільних пристроїв	5000	4500	5500	3000	4000
Регулярні резервні копії даних	3000	2500	2000	3500	3000
Використання доступу через PIN-коди чи біометрію	4000	3500	5000	3000	4500

8.4. Контрольні запитання

1. Для чого застосовуються критерії прийняття рішень у теорії ризиків?
2. З чим пов’язані проблеми прийняття рішень в умовах невизначеності?
3. На чому базується максимінний критерій Вальда?
4. Яка ідея полягає в розрахунку мінімаксного критерію Севіджа?
5. Коли найбільш ефективне застосування критерію недостатнього обґрунтування Лапласа?
6. Як виконується розрахунок критерію узагальненого песимізму-оптимізму Гурвіца?
7. Яким чином можна перетворити матрицю витрат на матрицю виграшів?
8. Що може виступати в ролі сценаріїв розвитку?
9. Яким чином формуються стратегії захисту?
10. Чому бажано використовувати кілька критеріїв прийняття рішень для аналізу ризикової ситуації?

СПИСОК ЛІТЕРАТУРИ

1. Cichonski P., Millar T., Grance T., Scarfone K. Computer Security Incident Handling Guide. *Recommendations of the National Institute of Standards and Technology*, 2012. 79 p. URL : http://dx.doi.org/10.6028/NIST.SP.800-61r2 (дата звернення: 10.09.2024).

2. Goel S., Chen V. Information Security Risk Analysis – A Matrix-Based Approach. URL : https://www.albany.edu/~goel/publications/goelchen2005.pdf (дата звернення: 10.09.2024).

3. Kuzminykh I., Ghita B., Sokolov V., Bakhshi T. Information Security Risk Assessment. *Encyclopedia*. Basel Switzerland MDPI, 2021. Vol. 1. P. 602–617. https://doi.org/10.3390/encyclopedia1030050

4. Гуменюк В. Я., Міщук Г. Ю., Олійник О. О. Управління ризиками. Навчальний посібник. Рівне : НУВГП, 2009. 156 с.

5. Корченко О. Г., Казмірчук С. В., Ахметов Б. Б. Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія. Київ : ЦП «Компринт», 2017. 435 с.

6. Лісовська Ю. П. Кібербезпека : ризики та заходи : навч. посібник. Київ : Видавничий дім «Кондор», 2019. 272 с.

7. Машина Н. І. Економічний ризик і методи його вимірювання. Навчальний посібник. Київ : ЦНЛ, 2003. 188 с.

8. Мельник Г. В. Технологія управління інформаційними ризиками в маркетинговій підсистемі КІС. *Вісник Хмельницького національного університету*. Хмельницький, 2011. № 6, Т. 1. С. 226-232.

9. Олійник В. М., Фролов С. М., Кобушко І. М. Ризик – менеджмент у сфері фінансових послуг: конспект лекцій. Суми : Сумський державний університет, 2014. 132 с.

10. Терентьєв О. М., Зайченко С. В., Клещов А. Й., Шевчук Н. А. Технічні ризики. Теорія та практикум : навч. посібник. Київ, КПІ ім. Ігоря Сікорського, 2020. 168 с.

Навчальне видання

Методичні вказівки до виконання практичних робіт з навчальної дисципліни «Теорія ризиків» для студентів денної та заочної форми навчання за спеціальністю «Комп'ютерна інженерія»

Автори:

КОЛОМІЙЦЕВ Олексій Володимирович

ПАНЧЕНКО Володимир Іванович

Відповідальний за випуск проф. Олександр ЗАКОВОРОТНИЙ

Роботу до видання рекомендував проф. Микола ЗАПОЛОВСЬКИЙ

В авторській редакції

План 2024 р., поз. 915

Підп. до друку . Формат 60x84 1/16.
Папір офсет. Друк ризографічний. Ум. друк. арк. 5.

Видавничий центр НТУ «ХПІ»,
Свідоцтво про державну реєстрацію ДК № 5478 від 21.08.2017 р.
вул. Кирпичова, 2, м. Харків, 61002

Електронна версія