КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ІМЕНІ ТАРАСА ШЕВЧЕНКА

ФАКУЛЬТЕТ РАДІОФІЗИКИ ЕЛЕКТРОНІКИ ТА КОМП'ЮТЕРНИХ СИСТЕМ

Кафедра радіотехніки та радіоелектронних систем

До захисту допущено: «На правах рукопису»
Завідувач кафедри _____ Ігор АНІСІМОВ
19 грудня 2022 р.

КВАЛІФІКАЦІЙНА МАГІСТЕРСЬКА РОБОТА

на тему:

«Оцінка ризиків та розробка методів захисту інформації для програмно-технічного комплексу абонентського звя'зку»

Виконав:
студент 2-го курсу магістратури
денної форми навчання
спеціальності 172 Телекомунікації та радіотехніка
ОПП «Захист інформації в телекомунікаціях»
Рибка Андрій _____

Науковий керівник:
к.в.н., доц. Довбня Сергій Якович _____

Рецензент:
к.т.н., доц. Четверіков Іван Олександрович _____

Засвідчую, що у цій магістерській роботі
немає запозичень з праць інших авторів без
відповідних посилань
Студент _____

Робота допущена до захисту в ЕК рішенням кафедри радіотехніки та радіоелектронних систем від 19 грудня 2022 р., протокол № 9.

Завідувач кафедри радіотехніки та радіоелектронних систем,
доктор фіз.-мат. наук, професор
Анісімов Ігор Олексійович _____

Київ – 2022

Зміст

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

Аналіз ризику – систематичне використання інформації про ризик для ідентифікації його джерел і оцінки його величини. Інформація може включати історичні дані про ризик, дані про місця зберігання, думки співробітників про цінності активів і ін.

Доступність – властивість інформації, що полягає в наявності інформації для користувача, коли це необхідно.

Уникнення ризику – рішення не брати участь в ситуації, пов’язаної з ризиком, або відмова від виконання дії, яка може привести до реалізації ризику.

Ідентифікація ризику – процес, спрямований на знаходження і опис елементів ризику (вразливостей, загроз, ймовірності та збитку).

Загроза – умисна дія або випадкова подія, яка може статися з певною ймовірністю, і завдати шкоди організації.

Збиток – негативні наслідки для організації, пов’язані з реалізацією ризику. Можуть включати: фінансові втрати, зниження репутації і лояльності співробітників, несприятливі організаційні зміни і інші наслідки.

Інформаційна безпека (ІБ) – комплекс процесів, дій і документів щодо забезпечення конфіденційності, цілісності та доступності інформації.

Модель загроз ІБ – опис існуючих загроз ІБ, можливостей і наслідків для організації в разі їх реалізації.

Залишковий ризик – ризик, який залишається після обробки початкового оціненого ризику.

Оцінка ризику – процес порівняння оціночної величини ризику до встановлених критеріїв ризику для визначення рівня значущості ризику і подальших дій по його обробці.

Обробка ризику – процес вибору і реалізації заходів щодо модифікації ризику, що може включати дії щодо зниження, уникнення, передачі і прийняття ризику.

Передача ризику – передача частини відповідальності за управління ризиком третій стороні (страхової компанії або компанії, яка займається аутсорсингом процесів і послуг).

ПЗ – програмне забезпечення.

Ризик інформаційної безпеки (ІБ) – рівень збитку, який понесе компанія, в разі реалізації загрози з використанням уразливості місця зберігання і обробки інформації компанії.

Система управління інформаційною безпекою (СУІБ) – система управління, призначена для створення, впровадження, експлуатації, моніторингу, аналізу, супроводу і вдосконалення ІБ.

Управління ризиком – скоординовані дії організації з контролю за ризиками ІБ, що включає їх ідентифікацію, оцінку і обробку.

Уразливість – відсутність або неефективність контролю ІБ щодо захисту інформації в місці зберігання і обробки від порушення її конфіденційності, цілісності і доступності.

Цілісність – властивість інформації, що полягає в забезпеченні її точності і повноти.

ВП- внутрішній порушник.

ВСТУП

На сьогоднішній день інформаційна сфера є ведучою в діяльності держави і чинить вплив на всі елементи соціальних комунікацій. Динамічний розвиток інформаційної сфери спричиняє виникнення інформаційних ризиків і вразливостей захисту інформації. Всі суб′єкти інформаційних взаємин - держава, суспільство, юридичні та фізичні особи – є власниками інформаційних ресурсів, які потребують певного рівня захисту.

Одним і з першочергових етапів побудови комплексних систем захисту інформації є оцінка інформаційних ризиків. З цією метою в інформаційних системах використовуються спеціальні програмні засоби оцінки інформаційних ризиків.

З огляду на це мета наукового дослідження полягає в наступному: проведення аналізу програмних засобів управління інформаційними ризиками; розробка класифікації програмного забезпечення управління інформаційними ризиками, з умов вимог та можливостей суб’єкта інформаційних відносин.

Наукова новизна дослідження полягає в наступному: розроблено класифікацію програмного забезпечення управління інформаційними ризиками, з урахуванням базових можливостей актуальних програмних продуктів згідно сучасних стандартів інформаційної безпеки.

Проведено оцінку можливостей, якості та ефективності використання програмних засобів оцінки інформаційних ризиків. COBRA- засіб для на аналізу та управління інформаційними ризиками, згідно вимог ISO 17799 у вигляді тематичних запитів. RA Software Tool- засіб, який виконує оцінку інформаційних ризиків згідно вимог стандартів ISO 17799 та ISO 13335. CRAMM- програмний засіб, який доцільно використовувати для аналізу інформаційних систем з підвищенними вимогами до інформаційної безпеки, велика точність пошуку

ризиків, можливість заощадження матеріальних ресурсів. RiskWatch- потужний засіб для проведення аудиту інформаційної безпеки, в якості критеріїв для оцінки та управління ризиками використовують представлення річних затрат. OCTAVE використовується для оцінки ризиків за допомогою послідовності організованих внутрішніх семінарів, розташованих відповідним чином. Digilal Security Office засіб для розробки та управління політики безпеки інформаційної системи на основі стандартів ISO 17799, ISO 27001, ISO 27005. RA2 art of risk- для проектування та побудови системи управління інформаційної безпеки використовується процесний підхід, на базі ISO 17799.

РОЗДІЛ 1. ЕКСПЕРТНІ МЕТОДИ В ОЦІНЦІ РИЗИКІВ У СИСТЕМАХ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

1.1 Ризики в системі забезпечення інформаційної безпеки

В умовах дедалі більшої складності та інтеграції інформаційних систем питання інформаційної безпеки (ІБ) набуває все більшого значення. З одного боку, потрібна побудова єдиного інформаційного простору, швидкої інтеграції наявних і впроваджуваних інформаційних систем і комплексів в єдине рішення, що дозволяє здійснювати оперативне і стратегічне управління компанією і виробництвом. З іншого боку, крайня нерівномірність розвитку IT-служб й інфраструктури та різнорідність експлуатованих інформаційних систем перешкоджають забезпеченню необхідного рівня ІБ. Забезпечення ІБ стає одним із пріоритетних завдань з метою підтримки її нормальної діяльності. В умовах, що склалися необхідна побудова дійсно комплексної корпоративної системи інформаційної безпеки, що є однією з найбільш важливих складових в загальній системі компанії.

Для сучасної СУІБ характерний підхід, який передбачає розв’язання проблем не "в міру їх надходження", коли буває вже надто пізно ними займатися, а передбачає завчасний аналіз і попередження можливихпроблем, на основі оцінки можливих ризиків ІБ. Тому фундаментом для успішного впровадження і функціонування СУІБ є оцінка та аналіз ризиків ІБ [34].

У роботі визначимо ризик порушення ІБ як потенційну можливість використання вразливостей активів загрозами ІБ для заподіяння шкоди, яка вимірюється з урахуванням ймовірності реалізації загроз ІБ і величини збитку від реалізації загроз ІБ.

Таким чином, в представленому визначенні ризик ІБ є функція як мінімум двох змінних: величини потенційного (негативного) впливу – шкоди для організації і ймовірності реалізації загрози ІБ. Друга величина є комплексним показником.

Аналіз ризиків – це процедури виявлення факторів ризиків ІБ і оцінки їх вагомості. Аналіз ризиків ІБ включає оцінку ризиків і методи зниження ризиків або зменшення пов'язаних з ними несприятливих наслідків. При аналізі спочатку проводиться виявлення відповідних факторів і оцінка їх вагомості, повнота виявлених чинників збільшує якість і точність прогнозованих ризиків. До таких факторів належать безліч активів, вразливостей і загроз. Основна мета створення класифікації загроз ІБ – повна, детальна класифікація, що описує всі чинні загрози ІБ і яка найбільш застосовна для аналізу ризиків реальних інформаційних систем [23].

Аналіз і управління інформаційними ризиками - один з базових процесів, що визначають ефективність системи забезпечення інформаційної безпеки. При організації системи безпеки, що включає різнорідні заходи та способи забезпечення інформаційної безпеки, саме аналіз інформаційних ризиків визначає якість і ефективність функціонування цієї системи.

Користуючись поняттям ризику, можна кількісно і якісно визначити й такі поняття, як ефективність системи захисту інформації, рівень безпеки дій і оптимальність прийнятих рішень [8].

Незалежно від розмірів організації та специфіки її інформаційної системи, роботи по забезпеченню режиму ІБ зазвичай складаються з наступних етапів (рис. 1.1):

- Визначення політики безпеки.
- Визначення сфери (кордонів) системи управління інформаційною безпекою та конкретизація цілей її створення.
- Оцінка ризиків.
- Вибір контрзаходів, що забезпечують режим ІБ.
- Управління ризиками.
- Аудит системи управління ІБ.

Як правило, визначення політики безпеки зводиться до наступних практичних кроків:

1. Вибір національних і міжнародних керівних документів і стандартів в області ІБ, і визначення на їх основі основних вимог і положень політики ІБ компанії, включаючи:

- управління доступом до засобів обчислювальної техніки (ЗОТ), програмам і даним;
- антивірусний захист;
- питання резервного копіювання;
- проведення ремонтних і відновлювальних робіт;
- інформування про інциденти в області ІБ та ін.

2. Визначення підходів до управління інформаційними ризиками та прийняття рішення про вибір рівня захищеності ІС. Рівень захищеності відповідно до закордонних стандартів може бути мінімальним (базовим) або підвищеним. Цим рівням захищеності відповідають мінімальний (базовий) або повний варіант аналізу інформаційних ризиків [17].

3. Структуризація контрзаходів щодо захисту інформації за такими основними рівнями: нормативно-правовий, організаційно-управлінський, технологічний і апаратно-програмний.

4. Визначення порядку сертифікації та акредитації ІС на відповідність стандартам в області ІБ. Визначення періодичності проведення нарад за тематикою ІБ на рівні керівництва, включаючи періодичний перегляд положень політики ІБ, а також порядок навчання всіх категорій користувачів інформаційної системи з питань ІБ.

5. Визначення меж системи управління інформаційною безпекою і конкретизація цілей її створення.

На цьому етапі визначаються межі системи, для якої повинен бути забезпечений режим ІБ. Відповідно, система управління ІБ будуватися саме в цих межах [29].

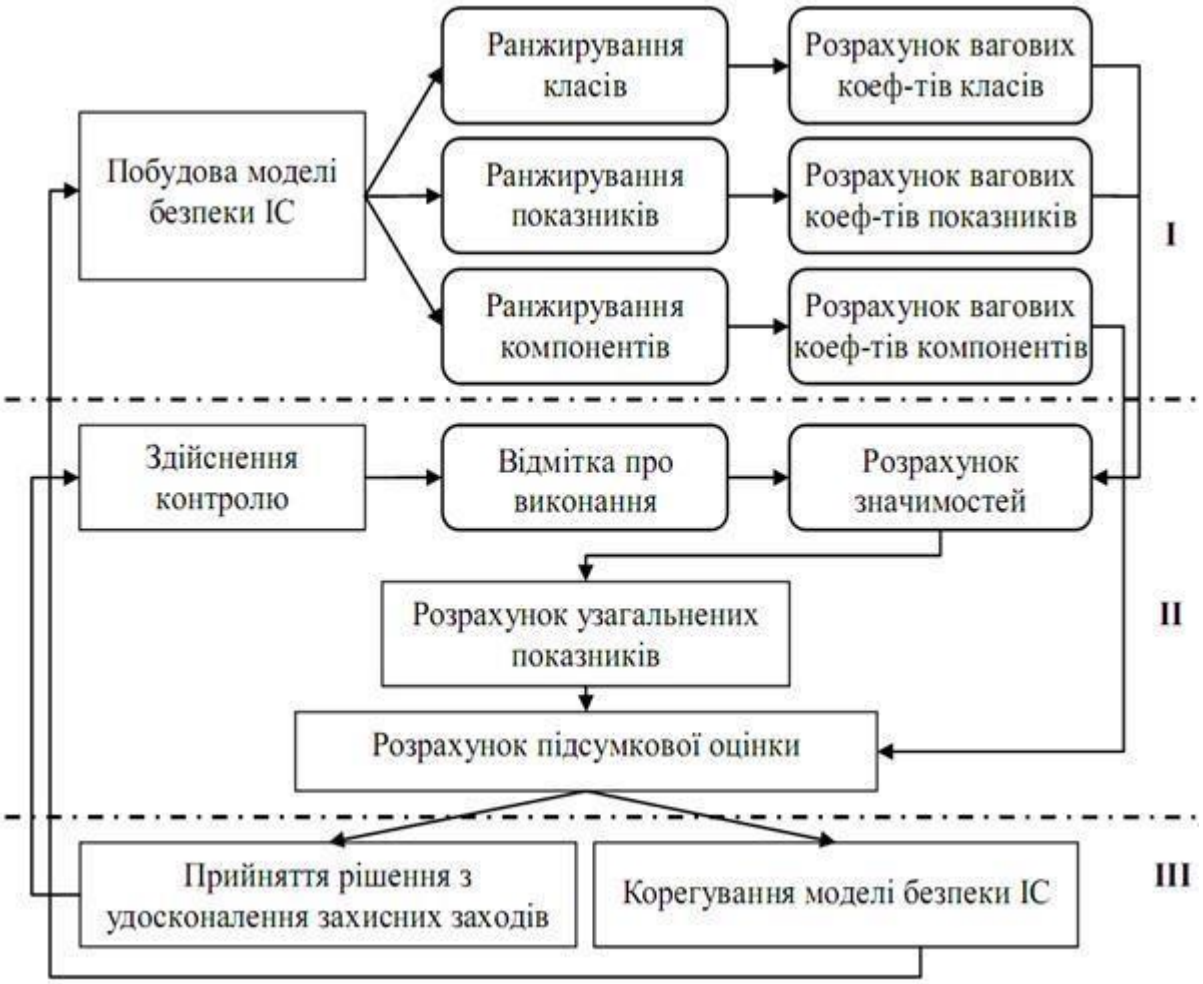


Рис. 1.1. Основні етапи забезпечення інформаційної безпеки

6. Формулювання завдання оцінки ризиків обґрунтовуються вимогами до методики оцінки інформаційних ризиків компанії. Вибір підходу залежить від рівня вимог, що пред'являються в організації до режиму інформаційної безпеки, характеру взятих до уваги загроз (спектра дії загроз) і ефективності потенційних контрзаходів щодо захисту інформації. Розрізняють мінімальні або базові, а також підвищені або повні вимоги до режиму ІБ.

Мінімальним вимогам до режиму ІБ відповідає базовий рівень ІБ. Такі вимоги застосовуються, як правило, до типових проєктних рішень. Існує ряд стандартів і специфікацій, в яких розглядається мінімальний (типової) набір найбільш ймовірних загроз, таких як: віруси, збої устаткування,

несанкціонований доступ тощо. Для нейтралізації цих загроз обов'язково повинні бути прийняті контрзаходи незалежно від ймовірності їх здійснення й уразливості ресурсів [21].

7. Управління ризиками. Розробляється деяка стратегія управління ризиками. Можливі такі підходи до управління інформаційними ризиками компанії:

Зменшення ризиків. Більшість ризиків можуть бути істотно зменшені шляхом використання досить простих і дешевих контрзаходів.

Ухилення від ризику. Від деяких класів ризиків можна ухилитися.

Зміна характеру ризику. Якщо не вдається ухилитися від ризику або ефективно його зменшити, можна прийняти деякі заходи страховки.

Прийняття ризику. Більшість ризиків не можуть бути зменшені до незначної величини. На практиці, після прийняття стандартного набору контрзаходів, ряд ризиків зменшується, але залишається все ще значним. Необхідно знати залишкову величину ризику.

В результаті виконання етапу для інформаційних ризиків компанії, що беруться до уваги, повинна бути запропонована стратегія управління ризиками.

8. Вибір контрзаходів, що забезпечують режим ІБ. На цьому етапі обґрунтовано вибирається комплекс різних контрзаходів щодо захисту інформації, структурованих по нормативно-правовому, організаційно управлінському, технологічному та апаратно-програмному рівнях забезпечення інформаційної безпеки. Надалі пропонований комплекс контрзаходів реалізується відповідно до обраної стратегії управління інформаційними ризиками. Якщо проводиться повний варіант аналізу ризиків, для кожного ризику додатково оцінюється ефективність комплексу контрзаходів щодо захисту інформації [18].

9. Аудит системи управління ІБ. Перевіряється відповідність обраних контрзаходів щодо захисту інформації цілям і задачам бізнесу, декларованим в політиці безпеки компанії, проводиться оцінка залишкових ризиків і, в разі необхідності, оптимізація ризиків.

Технологія аналізу ризиків

Мета процесу аналізу ризиків полягає у визначенні характеристик ризиків стосовно інформаційної системи (ІС) і її ресурсів (активів). На основі отриманих даних можуть бути обрані необхідні засоби захисту. При аналізі ризиків враховується багато факторів: цінність ресурсів, оцінки значущості загроз і вразливостей, ефективність чинних та планованих засобів захисту й багато іншого. Аналіз ризиків може бути базовим та повним [2,9,10].

Базовий аналіз ризиків – аналіз ризиків, що проводиться відповідно до вимог базового рівня захищеності. Базовий рівень безпеки – обов'язковий мінімальний рівень захищеності для ІС. Критерій досягнення базового рівня безпеки це виконання заданого набору вимог. Прикладні методи аналізу ризиків, орієнтовані на даний рівень, зазвичай не розглядають цінність ресурсів і не оцінюють ефективність контрзаходів. Методи даного класу застосовуються у випадках, коли до інформаційної системи не пред'являється підвищених вимог в області ІБ.

Повний аналіз ризиків – аналіз ризиків для інформаційних систем, що пред'являють підвищені вимоги в області ІБ. Містить визначення цінності інформаційних ресурсів, оцінку загроз і вразливостей, вибір адекватних контрзаходів, оцінку їх ефективності.

При аналізі ризиків порівнюється з витратами на заходи та засоби захисту, після чого приймається рішення щодо оцінюваного ризику, який може бути:

– знижений, наприклад, внаслідок впровадження засобів і механізмів захисту, що зменшують ймовірність реалізації загрози або коефіцієнт руйнування;
– усунутий шляхом відмови від використання схильного до загрози ресурсу;
– перенесений, наприклад, застрахований, в результаті чого в разі реалізації загрози безпеки, втрати буде нести страхова компанія, а не власник ресурсу;

Найбільш трудомістким є процес оцінки ризиків, який умовно можна розділити на наступні етапи: ідентифікація ризику; аналіз ризику; оцінювання ризику. На рис. 1.2. схематично зображено процес оцінки ризиків інформаційної безпеки.

Рис. 1.2. Процес оцінки ризиків інформаційної безпеки

Ідентифікація ризиків

Ідентифікація ризику полягає в складанні переліку та описі елементівризику: об'єктів захисту, загроз, вразливостей [13].

Прийнято виділяти такі типи об'єктів захисту:

− інформаційні активи;

− програмне забезпечення;

− фізичні активи;

− сервіси;

− люди, а також їх кваліфікації, навички та досвід;

− нематеріальні ресурси, такі як репутація та імідж організації.

Як правило, на практиці розглядають перші три групи. Решта об'єктів захисту не розглядаються через складність їх оцінки.

Складність задачі складання переліку і доказ його повноти залежить від того, які вимоги пред'являються до деталізації списку. На базовому рівні безпеки спеціальних вимог до деталізації класів, як правило, не пред'являється і досить використовувати будь-який відповідний в цьому випадку стандартний список класів ризиків.

Списки класів ризиків містяться в деяких посібниках, в спеціалізованомуПО аналізу ризиків. Прикладом є стандарт BSI, в якому є каталог загроз стосовно до різних елементів інформаційної технології. Як правило, для оцінки загроз та вразливостей використовуються різні методи, в основі якихможуть лежати:

− Експертні оцінки.

− Статистичні дані.

− Облік чинників, що впливають на рівні загроз і вразливостей.

Один з можливих підходів до розробки подібних методик – накопичення статистичних даних про події, що реально трапилися, аналіз і класифікація їх причин, виявлення чинників, від яких вони залежать. На основі цієї

інформації можна оцінити загрози та вразливості в інших інформаційних системах [27].

Практичні складності в реалізації цього підходу такі:

По-перше, повинен бути зібраний досить великий матеріал про події в цій галузі.

По-друге, застосування цього підходу виправдано далеко не завжди. Якщо інформаційна система досить велика (містить багато елементів, розташована на великій території), має давню історію, то подібний підхід, швидше за все, можна застосувати. Якщо система порівняно невелика, використовує новітні елементи технології (для яких поки немає достовірної статистики), оцінки загроз і вразливостей можуть виявитися недостовірними.

Найбільш поширеним в цей час є підхід, заснований на обліку різних факторів, що впливають на рівні загроз і вразливостей. Такий підхід дозволяє абстрагуватися від малоістотних технічних деталей, врахувати не тільки програмно-технічні, а й інші аспекти.

Оцінювання ризиків

Оцінка ризику полягає у визначенні його рівня (якісної або кількісної величини) і порівнянні цього рівня з максимально допустимим (прийнятним) рівнем, а також з рівнем інших ризиків.

Рівень ризику визначається шляхом комбінування двох величин: ймовірності події та розмірів його наслідків. Подія полягає в реалізації загрози, що використовує уразливість активу для впливу на цей актив і порушення його безпеки.

Всі відомі методики оцінки ризиків можна розділити на:

методики, що використовують оцінку ризику на якісному рівні (наприклад, за шкалою «високий», «середній», «низький»), до таких методик, зокрема, відноситься FRAP;

кількісні методики (ризик оцінюється через числове значення, наприклад, розмір очікуваних річних втрат).

До прийняття рішення про впровадження тієї чи іншої методики управління ризиками ІБ слід переконатися, що вона досить повно враховує бізне-спотреби компанії, її масштаби, а також відповідає кращим світовим практикам і має досить докладний опис процесів і необхідних дій [6].

Якісне визначення величини ризику

Точно визначити ймовірність загрози, величину уразливості або розмір збитку на практиці зазвичай не представляється можливим, тому мова може йти тільки про числові оцінки в деякому діапазоні величин. Кожному кількісному діапазону можна зіставити певний якісний рівень ризику. В результаті отримаємо якісну шкалу оцінки ризику, якій зіставляються деякі приблизні кількісні оцінки, без яких будь-яка якісна шкала позбавляється сенсу, тому що перестає бути пов'язаною з реальними втратами організації.

Матриця виникає в результаті розгляду ймовірності сценарію інциденту з урахуванням впливу на бізнес. У цій матриці по горизонталі відкладаються якісні значення ймовірності успішної реалізації загрози (сценарію інциденту), а по вертикалі - якісні рівні збитку (впливу на бізнес). Результативний ризик вимірюється за шкалою від 0 до 8, який може оцінюватися за критеріями прийняття ризиків, тобто порівнюватися з максимально допустимим рівнем ризику, в якості якого може бути вибрано, наприклад, значення 3. Мінімальний рівень ризику, що дорівнює 0, відповідає дуже низькій ймовірності інциденту і дуже низькому впливу цього інциденту на бізнес, а максимальний рівень ризику, що дорівнює 8, відповідає дуже високій ймовірності інциденту і дуже високому впливу на бізнес. Дана шкала ризиків також може бути зведена до простого загального рейтингу ризику, наприклад: низький ризик: 0-2, середній ризик: 3-5, високий ризик: 6-8. Всі ризики, значення яких перевищує 3, потребуватимуть обробки [32].

Вибір конкретного табличного методу і налаштування відповідних шкал є прерогативою конкретної організації.

Будь-якому якісному рівню, що виражається числовими значеннями або словами «низький», «середній», «високий» тощо, повинні відповідати певні діапазони оцінювальних кількісних величин. Без такого зіставлення використання якісних шкал для оцінки ризиків, звичайно, можливе, проте в цьому випадку оцінка ризиків втрачає економічний сенс.

Тому на практиці кількісний підхід завжди перетворюється в якісний і навпаки [2], у зв'язку з чим протиставлення якісних і кількісних методів оцінки ризиків є, взагалі кажучи, заняттям досить безглуздим.

Процес зіставлення якісних рівнів ризиків з відповідними кількісними діапазонами прогнозованого середньорічного збитку організації буде розглянуто далі у відповідному розділі.

Кількісне визначення величини ризику може здійснюватися різними методами. Вибір того чи іншого способу залежить, в першу чергу, відобсягу доступної, в тому числі статистичної, інформації про ризик інеобхідної точності оцінок. Також доводиться враховувати фактичнийрівень ризику. Чим менша ймовірність настання, тим важче виміряти ризик. Загальний принцип при виборі методів вимірювання зводиться до максимально можливого використання доступних статистичних даних.

Якщо їх немає, вони недостатні або непридатні, фактичний матеріал замінюється теоретичними гіпотезами або експертними оцінками [3]. Всього можна виділити чотири групи методів кількісної оцінки ризиків інформаційної безпеки:

1. статистичні методи;
2. ймовірнісно-статистичні;
3. теоретико-імовірнісні;
4. експертні.

В основі статистичних методів лежить оцінка ймовірності настання випадкової події виходячи з відносної частоти появи даної події в серії спостережень. Дані методи є найбільш переважними, оскільки, по-перше,вони досить прості, і, по-друге, їх оцінки базуються на фактичних даних [1]. Використання комбінації статистичних даних і теоретичних гіпотез для оцінки ризику становить основну ідею ймовірнісно-статистичних методів. Це розширює сферу застосування даної групи методів, але надійність отриманих результатів може виявитися нижче, ніж при використанні статистичних методів.

При управлінні ризиками інформаційної безпеки доводиться стикатися з необхідністю оцінки рідкісних подій, таких як розкриття інформації, прослуховування, заміна тощо, які допускають важкі наслідки. В цьому випадку статистика або взагалі відсутня, або належить до інших об'єктів, які суттєво відрізняються від досліджуваного. Це робить неможливим застосування статистичних і ймовірносно-статистичних методів.

Доводиться використовувати теоретико-імовірнісні методи, в основі яких лежить побудова математичної моделі досліджуваного ризику і теоретичної оцінки його параметрів. Дані методи дуже трудомісткі 1 мають відносно невисоку точність, але в ряді випадків є єдиним можливим науково обґрунтованим способом оцінки. Зокрема, вони застосовуються при розробці декларацій промислової безпеки підприємств [18].

При оцінюванні ризиків рекомендується розглядати такі аспекти:

- Шкали та критерії, за якими можна вимірювати ризики.
- Оцінка ймовірностей подій.
- Технології вимірювання ризиків.

Шкали й критерії, за якими вимірюються ризики

Для вимірювання якої-небудь властивості необхідно вибрати шкалу. Шкали можуть бути прямими (натуральними) або непрямими (похідними).

Прикладами прямих шкал є шкали для вимірювання фізичних величин, наприклад – літри для вимірювання об'єму, метри для вимірювання довжини. У ряді випадків прямих шкал не існує, доводиться використовувати або прямі шкали інших властивостей, пов'язаних з тими, що нас цікавлять, або визначати нові шкали. Прикладом є шкала для вимірювання суб'єктивної властивості «цінність інформаційного ресурсу». Вона може вимірюватися в похідних шкалах, таких як вартість відновлення ресурсу, час відновлення ресурсу та інших. Інший варіант – визначити шкалу для отримання експертної оцінки, що, наприклад, має три значення:

- Малоцінний інформаційний ресурс: від нього не залежать критично важливі завдання і він може бути відновлений з невеликими витратами часу і грошей.
- Ресурс середньої цінності: від нього залежить ряд важливих завдань, але в разі його втрати він може бути відновлений за час, що не перевищує критично допустимий, вартість відновлення – висока.
- Цінний ресурс: від нього залежать критично важливі завдання, в разі втрати час відновлення перевищує критично допустимий або вартість надзвичайно висока [17].

- Для вимірювання ризиків не існує природної шкали. Ризики можна оцінювати з об'єктивних або суб'єктивних критеріїв. Прикладом об'єктивного критерію є ймовірність виходу з ладу будь-якого обладнання, наприклад ПК, за певний проміжок часу. Прикладом суб'єктивного критерію є оцінка власником інформаційного ресурсу ризику виходу з ладу ПК. Для цього зазвичай розробляється якісна шкала з декількома градаціями, наприклад: низький, середній, високий рівень.

Для вимірювання ризиків не існує природної шкали. Ризики можна оцінювати з об'єктивних або суб'єктивних критеріїв. Прикладом об'єктивного критерію є ймовірність виходу з ладу будь-якого обладнання, наприклад ПК, за певний проміжок часу. Прикладом суб'єктивного критерію є оцінка власником інформаційного ресурсу ризику виходу з ладу ПК. Для цього зазвичай розробляється якісна шкала з декількома градаціями, наприклад: низький, середній, високий рівень.

Оцінка ймовірностей порушення ІБ

Процес отримання ймовірності подій порушень ІБ зазвичай поділяють три етапи: підготовчий етап, отримання оцінок, етап аналізу отриманих оцінок.

Перший етап. Під час цього етапу формується об'єкт дослідження – безліч подій, наводиться попередній аналіз властивостей цієї множини (встановлюється залежність або незалежність подій, дискретність або неперервність випадкової величини, що породжує дану множину подій). На основі такого аналізу вибирається один з відповідних методів отримання ймовірності. На цьому ж етапі проводиться підготовка експерта або групи експертів, ознайомлення їх з методом і перевірка розуміння поставленого завдання експертами [4].

Другий етап полягає в застосуванні методу, обраного на першому етапі. Результатом цього етапу є набір чисел, який відображає суб'єктивний погляд експерта або групи експертів на ймовірність тієї чи іншої події, проте далеко не завжди може вважатися остаточно отриманим розподілом, оскільки може бути суперечливим.

Третій етап полягає в дослідженні результатів опитування. Якщо ймовірності, отримані від експертів, не узгоджуються з аксіомами ймовірності, то на це звертається увага експертів і проводиться уточнення відповідей з метою приведення їх у відповідність до вибраної системи аксіом.

Для деяких методів отримання ймовірності третій етап не проводиться, оскільки

сам метод полягає у виборі ймовірного розподілу, що підкоряється аксіомі ймовірності, яке в тому чи іншому сенсі найближче до оцінок експертів. Особливу важливість третій етап набуває при агрегуванні оцінок, отриманих від групи експертів [12].

1.2 Аналіз методик управління ризиками інформаційної безпеки

Проаналізуємо три найвідоміші світові методики управління ризиками ІБ, які можна застосувати для аналізу ризиків ІБ у процесі забезпечення неперервності функціонування СЗІ в КМЗ, визначимо переваги та недоліки кожної з них. Аналізу підлягають: методика оцінки NIST 800-30 [4], методика CRAMM [5] та методика OCTAVE [6].

Однією з найпопулярніших та широковживаних методик управління ризиками є методика оцінки ризиків Національного інституту стандартів і технологій США (National Institute of Standards and Technology) NIST, зазначена в Керівництві з управління ризиками в інформаційних технологіях NIST 800-30 (NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems). Ця методика передбачає попереднє оцінювання двох параметрів: потенційного збитку та ймовірностіреалізації загрози [7].

Призначення системи управління ризиками безпосередньо пов’язане з можливістю компанії виконувати свої основні функції за умови постійного розширення сфери використання інформаційних технологій.

Методика оцінки ризиків, яка наведена в спеціальних рекомендаціях 800-30, охоплює широке коло завдань, що пов’язані зі стратегією управління ризиками і є основою для розроблення власної системи управління ризиками. Проте запропонований процес оцінювання ризику ІБ, який представлений у вигляді таблиці, що відображає залежність ризику від двох вхідних змінних:

потенційного збитку і ймовірності можливого інциденту. При цьому значення кожної змінної, зокрема ризику, оцінюється за трирівневою шкалою. Такий "жорсткий" механізм отримання оцінок ризику суттєво обмежує точність результатів, забезпечуючи їх оперативність та відтворюваність [7].

Алгоритм цієї методики зображено на рис. 1.3.

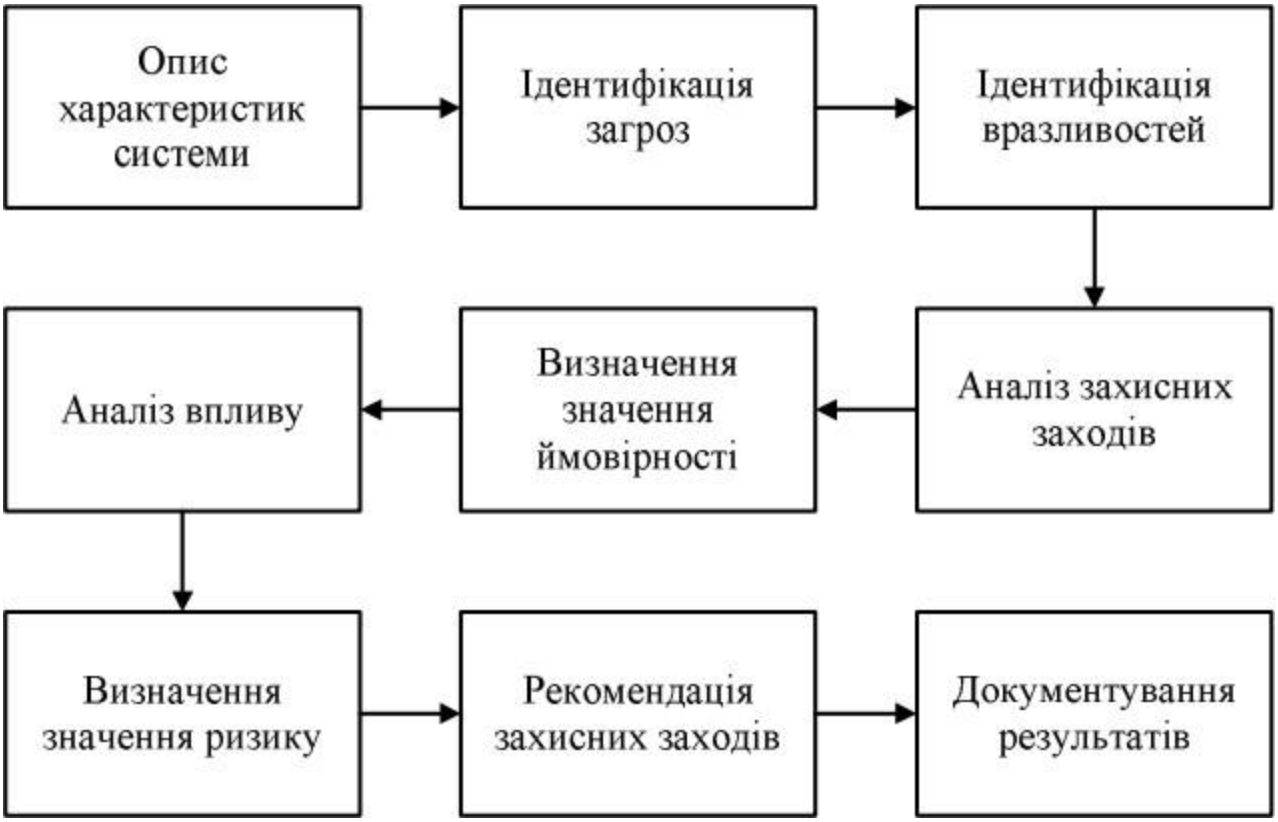


Рис.1.3. Алгоритм методики управління ризиками

Використання такої методики передбачає такі етапи:

- опис характеристик системи;
- ідентифікація загроз;
- ідентифікація вразливостей;
- аналіз наявних засобів/заходів захисту;
- визначення значення ймовірності;

- аналіз впливу;
- визначення значення ризику;
- вибір засобів/заходів захисту;
- документування отриманих результатів.

Наступною методикою, яку аналізують автори статті, є методика CRAMM (CCTA Risk Analysis and Managment Method), яку розробило Агентство з комп'ютерів і телекомунікацій Великобританії (Central Computer and Telecommunications Agency) за поданням Британського уряду і яка прийнята за державний стандарт. Цю методику використовують, починаючи з 1985 року, державні та комерційні організації Великобританії. За цей час CRAMM набула популярності у всьому світі. Фірма Insight Consulting Limited займається розробленням і супроводом однойменного програмного продукту, що реалізує метод CRAMM [8].

В основу методики CRAMM покладено комплексний підхід до оцінки ризиків, що поєднує кількісні та якісні методи аналізу. Методика є універсальною і придатна як для великих, так і для малих організацій, як державного, так і комерційного сектору. Версії програмного забезпечення CRAMM, орієнтовані на різні типи організацій, відрізняються своїми базами знань (profiles). Для комерційних організацій є комерційний профіль (Commercial Profile), для державних організацій – державний профіль (Government profile). Державний варіант профілю також дає змогу проводити аудит на відповідність вимогам американського стандарту ITSEC ("Помаранчева книга") [8].

Правильне використання методики CRAMM дає змогу економічно обґрунтувати витрати організації на забезпечення інформаційної безпеки та неперервності функціонування. Економічно обґрунтована стратегія

управління ризиками ІБ дає змогу, в кінцевому підсумку, заощаджувати кошти, уникаючи невиправданих витрат.

Методика CRAMM припускає поділ всієї процедури на три послідовні етапи. Завданням першого етапу є відповідь на запитання: “Чи достатньодля захисту системи застосування засобів базового рівня, що реалізують традиційні функції ІБ, чи необхідне проведення детальнішого аналізу?” На другому етапі здійснюється ідентифікація ризиків і оцінюється їх величина. На третьому етапі вирішується завдання про вибір адекватних контрзаходів.Методика CRAMM для кожного етапу визначає набір вихідних даних, послідовність заходів, анкети для проведення інтерв’ю, списки перевірки і набір звітних документів [8].

Алгоритм методики CRAMM подано на рис. 1.4.

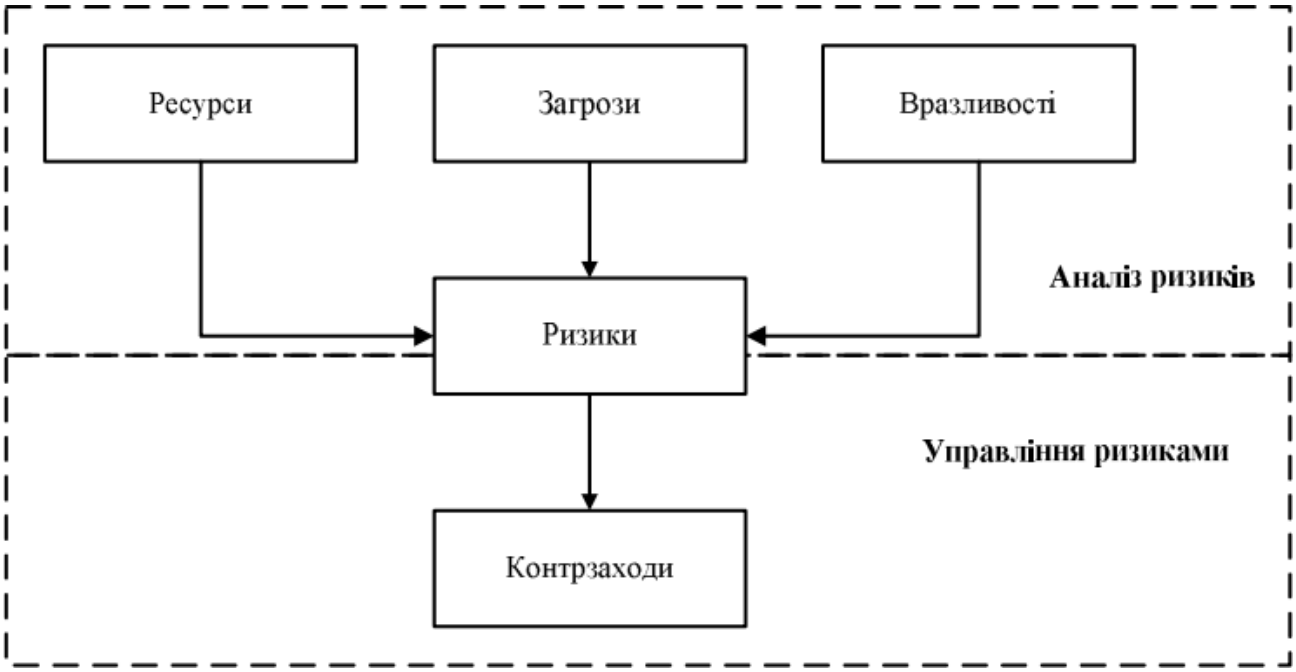


Рис.1.4. Алгоритм методики управління ризиками CRAMM

Методика OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) розроблена в Університеті Карнегі-Мелон (США) і передбачає оцінювання критичності загроз, активів і вразливостей.

Цю методику широко використовують у всьому світі, виконуючи роботи з оцінки ризиків ІБ та впровадження процесів управління ризиками в компанії загалом. Методика має ряд модифікацій, які розраховані на організації різного розміру та галузі діяльності [9].

Зміст методики OCTAVE полягає в тому, що для оцінки ризиків використовується послідовність відповідно організованих внутрішніх семінарів (workshops). Оцінка ризиків здійснюється в три етапи, яким передує набір підготовчих заходів: узгодження графіка семінарів, призначення ролей, планування, координація дій учасників проектної групи [9].

На першому етапі, в межах практичних семінарів, здійснюється розроблення профілів загроз, що містять в собі інвентаризацію та оцінку цінності активів, ідентифікацію застосовних вимог законодавства та нормативної бази, ідентифікацію загроз та оцінку їх ймовірності, а також визначення системи організаційних заходів з підтримки режиму інформаційної безпеки.

На другому етапі проводиться технічний аналіз вразливостей систем організації щодо загроз, чиї профілі розроблено на попередньому етапі, який містить ідентифікацію наявних вразливостей компанії та оцінюванняїх величини.

На третьому етапі виконується оцінка та оброблення ризиків інформаційної безпеки, що містить визначення величини та ймовірності завданої шкоди внаслідок реалізації загроз ІБ з використанням вразливостей, які ідентифіковано на попередніх етапах, визначення стратегії ІБ, а також вибір варіантів і прийняття рішень з оброблення ризиків.

Величина ризику визначається як середнє значення річних втрат компанії в результаті реалізації загроз ІБ.

Алгоритм цієї методики зображено на рис. 1.5.

Рис.1.5. Алгоритм методики управління ризиками OCTAVE

Отже, коротко охарактеризувавши три найпоширеніші методики з управління ризиками в сфері інформаційної безпеки [8, 10, 11] та здійснивши аналіз основних властивостей цих методик, автори визначили основні переваги та недоліки перелічених вище методик. Їх подано у вигляді табл. 2.1.

Таблиця 1.1.

Переваги та недоліки методик з управління ризиками ІБ

Методика	Переваги	Недоліки
NIST	– порівняно проста в реалізації; – придатна для підприємств різного розміру; – детально описує всі можливі ризики для інформаційних активів; – припускає використання як способів зниження ризиків всіх можливих варіантів (зниження, прийняття, перенесення, уникнення ризику); – існує автоматизоване програмне забезпечення, що реалізовує принципи методики; йому властива відносна легкість та зручністьвикористання.	– довготривалий процес аналізу; – розроблена для використання у федеральних організаціях США; – оцінювання ризиків проводиться за трирівневою шкалою, що істотно обмежує можливості методики загалом.

CRAMM	– є універсальною і підходить для організацій як державного, так та комерційного сектору; – використовує кількісні і якісні способи оцінки ризиків; – розроблені комерційні програмні продукти, що реалізовуютьположення CRAMM;	– використання методики потребує спеціальної підготовки і високої кваліфікації спеціаліста; – довготривалий процес аналізу; – програмний інструментарій генерує велику кількість паперової документації, яка не завжди виявляється корисною на практиці; – не дає змоги створювати власні шаблони звітів або модифікувати наявні; – припускає використання лише методів зниження рівня ризиків ІБ, такі способи управління ризиками, як “уникнення” або “прийняття”, не розглядаються.
OCTAVE	– швидко впроваджується; – можливе застосування для організацій різного розміру тагалузей зайнятості; – є комерційні програмні продукти,що реалізовують положенняметодики; – високий рівень гнучкості.	– не дає кількісної оцінки ризиків; – припускає використання як способів зниження ризиків лише його зниження і прийняття.

У випадку забезпечення неперервності функціонування СЗІ в МЗ, що є довготривалим та ресурсомістким процесом, аналіз ризиків ІБ, які можуть стати загрозою для неперервності функціонування СЗІ, є лише одним з багатьох етапів, що повинні бути успішно виконані. Саме тому дуже важлива можливість швидкого та порівняно простого управління ризикама ІБ, що входять в сферу впливу неперервності функціонування СЗІ в МЗ. Так, на основі проведеного аналізу, автори статті зробили висновок, що оптимальним варіантом для вибору методики управління ризиками ІБ в контексті забезпечення неперервності функціонування МЗ та СЗІ зокрема є адаптація та удосконалення відомих методик логічним поєднанням їх переваг та мінімізацією недоліків [11].

1.3Експертні методи оцінки ризику

В сучасних умовах стає все більш складно забезпечувати зростання ефективності інформаційної безпеки. Це пов'язано з постійним підвищення жорсткості вимог до систем управління. Саме тому в даний час питання про вдосконалення систем управління є досить актуальним.

Важливим фактором підвищення рівня інформаційної безпеки є використання при підготовці рішень математичних методів і моделей в цілях оцінки ризиків і можливого їх запобігання. Однак використання даних методів при вирішенні різноманітних задач часто є неможливим внаслідок їх складності. Тому більш широке поширення набув метод експертних оцінок [17].
Метод експертних оцінок зазвичай реалізується шляхом обробки думок досвідчених експертів (кваліфікованих фахівців). Тобто даний спосіб передбачає збір і вивчення оцінок, зроблених різними фахівцями на основі їх власної інтуїції, знань і досвіду, ймовірностей виникнення різних рівнів втрат. Ці оцінки базуються на обліку всіх факторів ризику, а також статистичних даних. Реалізація способу експертних оцінок значно ускладняється, якщо кількість

показників оцінки невелика.

Основними вимогами до залучення до аналізу експертам є:

- високий рівень креативності мислення;
- наявність спеціалізованих знань в залежності від сфери проведення експертизи;
- повна незалежність від системи;
- можливість проведення оцінки будь-якої кількості ідентифікованих ризиків;
- доступ до всієї необхідної інформації.

Ситуації, до яких застосовується даний метод, часто виникають в розробках сучасних систем управління інформаційної безпеки, а також при прогнозуванні та довгостроковому плануванні.

Для того щоб забезпечити умови для підвищення якості та ефективності експертних оцінок, необхідна активна і цілеспрямоване участь фахівців на кожному етапі (стадії) прийняття рішень.

Після стадійний підхід до оцінки ризиків заснований, перш за все, на те, що ризики визначаються для кожної стадії проекту окремо, а потім знаходиться підсумковий сумарний результат по всьому проекту [9].

Для отримання кінцевого результату (експертних оцінок) використовують різні методи, найбільшого поширення з яких отримали анкетні методи і методи групової експертизи. Тобто кожному експерту, що працює окремо, подається перелік первинних ризиків на основі опитувальних листів по всіх стадіях проекту і пропонується оцінити ймовірність настання ризиків у відповідності за наступною системою оцінок:

0 – ризик розглядається як несуттєвий;

25 – велика ймовірність, що ризик не реалізується;

50 – про настання події нічого певного сказати не можна;

75 – велика ймовірність, що ризик виявиться;

100 – ризик з повною упевненістю реалізується.

Оцінки експертів піддаються аналізу на несуперечливість, який виконується за певними правилами:

Максимально допустима різниця між оцінками двох експертів з будь-якого фактору не повинна перевищувати 50. Порівняння проводяться по модулю (знак плюс або мінус не враховується). Це дозволяє усунути неприпустимі відмінності в оцінках експертами ймовірності настання окремого ризику. Якщо кількість експертів три і більше, то оцінками піддаються попарно порівняльні думки.

Для оцінки узгодженості думок експертів по всьому набору ризиків, як правило, виявляється два експерта. Основним правилом при цьому є максимальне розбіжність думок цих експертів (мінімальна спільність). Для розрахунків розбіжності оцінки підсумовуються по модулю і результат ділиться на кількість простих ризиків. Частка від ділення не повинна перевищувати 25.

У разі виявлення між думками експертів протиріч (НЕ виконується хоча б одне з наведених правил), вони обговорюються на зборах з експертами. При відсутності протиріч всі оцінки експертів зводяться в середню (середньоарифметична), яка використовується в подальших розрахунках.

Існують і інші способи експертної оцінки ризику. Одним з них є метод ранжування, алгоритм реалізації якого наступний:

На першому етапі при обробці інформації необхідно впорядкувати всі оцінки по спадаючій.

Далі за формулою середнього арифметичного знаходиться середня величина всіх оцінок.

Отримані значення розбиваються на чотири рівних інтервали.

У разі потрапляння оцінок експертів в крайні інтервали, цих експертів просять обґрунтувати свою думку.

З їх обґрунтуванням знайомлять інших експертів (з умовою повної конфіденційності).

Врахування в наступних турах обговорення тих чинників, які були випадково втрачені фахівцями в першому турі опитування. В наслідок цього у другому турі менший розкид думок.

Також до числа найбільш поширених методів експертних оцінок ризику відносять метод Дельфі, попарне порівняння, метод бальних оцінок і інші.

Метод Дельфі передбачає виключення в процесі дослідження безпосереднього спілкування між експертами. Тобто суть даного методу полягає в індивідуальному опитуванні всіх членів групи за допомогою анкет з метою з'ясування їх думок на основі особистого досвіду і знань щодо майбутніх гіпотетичних подій [20].

Метод бальної оцінки ризику полягає в експертизі ризику на основі узагальнюючого показника, який визначається по ряду експертно оцінюваних приватних показників (факторів) ступеня ризику. При цьому передбачається проходження наступних етапів:

- вибір чинників, які безпосередньо впливають на ступінь ризику проекту;
- визначення узагальненого критерію і приватних показників, які характеризують кожен фактор;
- оцінка даного критерію щодо ступеня ризику;
- вироблення рекомендацій з управління ризиком.

Очевидно, що висока якість експертизи досягається в разі високої узгодженості думок експертів за кількома факторами. Однак при використанні будь-якого методу експертних оцінок виникає проблема, пов'язана з неточністю отриманих результатів внаслідок таких чинників як: неякісний підбір фахівців, домінування думки (як правило, «авторитетного лідера») і т.д. Саме тому необхідне проведення експертизи на достовірність

отриманих оцінок. Одним з таких показників оцінок є коефіцієнт конкордації Кендала, або коефіцієнт множинної рангової кореляції. Розраховується наступним чином:

$$W = \frac{12S}{m^2(n^3 - n)}$$

де:

m – кількість експертів в групі,

n – кількість досліджуваних факторів,

S – сума квадратів різниць рангів (відхилень від середнього).

Результати налізу знаходяться в наступних межах:

- W <0,2-0,4 – узгодженість експертів слабка;
- W> 0.6 - 0.8 – узгодженість експертів сильна;
- W = 1 – думки всіх експертів збігаються.

Розберемо розрахунок коефіцієнта на прикладі, в якому 5 експертів попросили проранжувати за важливістю 4 різних фактори. Вони розставили ранги від 1 до 4 і тепер необхідно це проаналізувати.

	Фактор 1	Фактор 2	Фактор 3	Фактор 4
Експерт 1	1	3	2	4
Експерт 2	3	2	1	4
Експерт 3	4	3	1	2
Експерт 4	2	3	4	1
Експерт 5	2	4	1	3

Рис.1.6. Результати опитування думок п'яти експертів по 4 факторам

На основі прикладу отримуємо: m = 5, n = 4.

Оскільки всі дані відомі, залишається тільки знайти суму квадратів різниць рангів (S), яка розраховується за однією з формул:

$$S = \sum_{i=1}^{n}(\sum_{j=1}^{m} R_{ij})^2 - \frac{(\sum_{i=1}^{n}\sum_{j=1}^{m} R_{ij})^2}{n}$$

$$S = \sum_{i=1}^{n}(\sum_{j=1}^{m} A_{ij} - \frac{1}{2}m(n+1))^2$$

Для обчислення потрібно додати два рядки: суму по стовпцю (сума оцінкиекспертів по кожному фактору) і квадрат цієї суми.

Сума	12	15	9	14	50
Квадрат суми	144	225	81	196	646

Рис.2.7. Приклад розрахунку коефіцієнта конкордації Кендалана основі думок п'яти експертів по 4 факторам

Таким чином, отримуємо:

$$S = 646 - 50^2/4 = 21$$

Далі отримуємо:

$$S = (12 - 12,5)^2 + (15 - 12,5)^2 + (9 - 12,5)^2 + (14 - 12,5)^2 = 21$$

Далі розраховується сам коефіцієнт Кендала:

$$W = (12 * 21) / (25 * (64 - 4)) = 0,168$$

Отримуємо дуже слабку узгодженість експертів (W <0,2).

Такий результат може бути зумовлений двома причинами:

1. в розглянутій групі фахівців практично відсутня спільність думок;
2. всередині даної групи існують коаліції з високою узгодженістюдумок, однак, узагальнені думки таких коаліцій протилежні [10].

Також, слід узагальнити основні переваги та недоліки даного методу.

Таблиця 1.2.

Переваги та недоліки метода експертних оцінок ризику

Переваги	**Недоліки**
Простота організації	Неповнота відповідей
Використання статистичної обробки	Можливість неправильного розуміння
Можливість охоплення великих груп	Суб'єктивний фактор опитуваних експертів

Таким чином, можна зробити висновок про те, що експертні оцінки ризику є досить ефективним і нескладним методом аналізу настання ймовірних несприятливих подій, особливо в таких сферах як системи управління інформаційною безпекою. Більш того, даний метод за рахунок своєї простої організації дозволяє охопити великий діапазон досліджуваних факторів [5].

Однак в силу виняткової суб'єктивності відповідей експертів, необхідно дотримуватися певних правил проведення експертизи, а також проводити аналіз ступеня узгодженості думок фахівців з метою виявлення якості цієї експертизи.

Висновки до розділу 1

Забезпечення інформаційної безпеки стає одним із пріоритетних завданьз метою підтримки її нормальної діяльності. В умовах, що склалися необхідна побудова дійсно комплексної системи інформаційної безпеки, що є однією з найбільш важливих складових в загальній системі управління безпекою.

У роботі визначимо ризик порушення як потенційну можливість використання вразливостей активів загрозами для заподіяння шкоди, яка вимірюється з урахуванням ймовірності реалізації загроз ІБ і величини збитку від реалізації загроз ІБ. Оцінка ризику полягає у визначенні його рівня і порівнянні цього рівня з максимально допустимим рівнем, а також з рівнем інших ризиків. Ризики можна оцінювати з об'єктивних або суб'єктивних критеріїв.

Розглянуто процес управління ризиком ІБ в контексті забезпечення неперервності функціонування СЗІ. Здійснено аналіз трьох поширення методик в сфері управління ризиками ІБ, що дало змогу визначити їх основні особливості, встановити переваги та недоліки.

Експертні оцінки ризику є досить ефективним і нескладним методом аналізу настання ймовірних несприятливих подій, особливо в таких сферах як системи управління інформаційною безпекою. Більш того, даний метод за рахунок своєї простої організації дозволяє охопити великий діапазон досліджуваних факторів.

РОЗДІЛ 2. МОДЕЛЬ ЗАГРОЗ ТА РЕЗУЛЬТАТ ОЦІНЮВАННЯ РИЗИКУ ПРИ ВИКОРИСТАННІ ПТКАЗ

2.1 Загальна класифікація загроз інформації

Згідно з нормативними документами системи ТЗІ (НД ТЗІ 1.1-002-99, НД ТЗІ 2.5-004-99) за результатом впливу на інформацію та систему її обробки загрози поділяються на такі класи:

- Порушення конфіденційності інформації (отримання інформації користувачами або процесами всупереч встановленим правилам доступу);
- Порушення цілісності інформації (повне або часткове знищення, викривлення, модифікація, нав'язування хибної інформації);
- Порушення доступності інформації (часткова або повна втрата працездатності системи, блокування доступу до інформації);
- Втрата спостереженості або керованості системи обробки (порушення процедур ідентифікації та автентифікації користувачів та процесів, надання їм повноважень, здійснення контролю за їх діяльністю, відмова від отримання або пересилання повідомлень).

За джерелом впливу загрози поділяються на:

- Загрози, обумовлені діями людини (викрадення, підміна, пошкодження інформації, паролів і атрибутів доступу, технічних та програмних засобів її обробки);
- Загрози, обумовлені технічними засобами (неякісні технічні та програмні засоби обробки інформації);
- Загрози, обумовлені стихійними факторами (пожежа, землетрус, повінь та інші).

За характером впливу на ПТКАЗ загрози поділяються на:

- Активні;
- Пасивні.

За способом впливу на об’єкт атаки загрози поділяються на:

- Загрози з безпосереднім впливом на об’єкт атаки;
- Загрози з впливом на систему прав доступа;
- Загрози з опосередкованим впливом.

За використовуваним для атаки компонентом ПТКАЗ загрози поділяються на:

- Загрози, які використовують технічні засоби ПТКАЗ;
- Загрози, які використовують технологічну інформацію ПТКАЗ;
- Загрози, які використовують програмні засоби ПТКАЗ.

За засобами атаки загрози поділяються на:

- Загрози з використанням стандартного програмного забезпечення або технічних засобів;
- Загрози з використанням спеціально розробленого програмного забезпечення або технічних засобів.

За станом об’єкту атаки загрози поділяються на:

- Загрози на об’єкт атаки, який знаходиться в стані зберігання;
- Загрози на об’єкт атаки, який знаходиться в стані обробки.

Загрози безпеки зв'язку в ПТКАЗ

Інтегральний підхід до забезпечення інформаційно-технічної безпеки в телекомунікаційних мережах системах передбачає насамперед виявлення можливих загроз і атак. Загальною метою розробки типових моделей загроз інформаційно-технічної безпеки телекомунікаційних мереж є визначення сукупності основних значних загроз, способів та засобів їх здійснення, рівня допустимих втрат, пов'язаних із можливими проявами загроз у типових умовах застосування.

Серед сучасних моделей загроз інформаційно-технічній безпеці телекомунікаційних мереж виділяються:

1) моделі загроз інформаційно-технічній безпеці мереж мобільного зв'язку 2-го покоління (2G);

2) моделі загроз інформаційно-технічній безпеці мереж мобільного зв'язку 3-го покоління (3G);

3) моделі загроз інформаційно-технічній безпеці мереж абонентського доступу;

4) моделі загроз інформаційно-технічній безпеці систем радіозв'язку;

5) моделі загроз інформаційно-технічній безпеці локальних обчислювальних мереж;

6) моделі загроз інформаційно-технічній безпеці мереж технологічного управління;

7) моделі загроз інформаційно-технічній безпеці транспортних мереж та систем передачі;

8) моделі загроз інформаційно-технічній безпеці автоматизованих систем документообігу.

2.2 Програмно-технічний комплекс абонентського зв'язку у складі:

Найменування	Характеристики, модель	Технології
Samsung Galaxy A10s	Програмне забезпечення : ОС Android (з оновленням до Android 11) Оболонка Android 9 (Pie)	Вразливості системи безпеки Adroid Бюлетень по безпеці за вересень 2022 року містить інф. про вразливості безпеки, впливаючих на пристрої з операційною системою Android включаючиAndroid 10, 11, 12, 13.

Рис.2.1. ПТКАЗ

На рис. 2.1 зображено наявний програмно технічний комплекс абонентського зв'язку для проведення подальших досліджень.

2.3 Модель загроз

Результати моделювання загроз для інформації в ПТАПЗ за об'єктом та суб'єктом впливу, метою впливу, способом впливу, результатом впливу на інформацію та систему її обробки наведено у таблицях 1-2.

Таблиця 2.1.

Результати моделювання загроз за об’єктом та суб’єктом впливу, результатом впливу на інформацію та систему її обробки

№	Об'єкт впливу	Вид Інформації	Порушення конфіденційності	Порушення цілісності	Порушення доступності	Втрата керованості	Примітки
1.	Операційна система	Технологічна	+	-	+	-	Найбільш вразлива до некоректних дій адміністратора
2.	Прикладне програмне забезпечення	ІзОД	+	+	-	-	Найбільш вразлива до некоректних дій користувача
		Відкрита	+	+	+	-	Найбільш вразлива до некоректних дій користувача
		Технологічна	-	-	+	-	Найбільш вразлива до некоректних дій адміністратора

Таблиця 2.2.

Результати моделювання загроз за способом реалізації загрози, суб’єктом впливу, метою впливу

Класифікація атак	№	Порушник	Спосіб реалізації загрози (атаки)	Мета впливу			
				Порушення конфіденційності	Порушення цілісності	Порушення доступності	Втрата керованості
Атака з використанням НСД	1.1	Внутрішній порушник	Несанкціонований доступ до даних з метою їх перегляду\модифікації\видалення	-	+	-	-
	1.2		Несанкціонований доступ до програмного забезпечення з метою його пошкодження	-	-	+	-
	1.3		Несанкціонований запуск програмних засобів	+	-	-	-
	1.4		Несанкціоноване отримання прав доступу	-	-	-	+
Незаконне використання повноважень	2.1	Внутрішній порушник	Незаконне використання адміністративних повноважень	+	-	+	+
	2.2		Незаконне використання повноважень користувача	+	+	+	+
Незаконний доступ до сумісно використовуваних ресурсів, звільнених іншим користувачем або процесом	3.1	Внутрішній порушник	Незаконний доступ до сумісно використовуваних ресурсів	-	+	-	-
Злом системи	4.1	Внутрішній порушник	Підбір або перехоплення пароля	+	-	-	+
Використання шкідливих програм	5.1	Внутрішній порушник	Захоплення надмірного обсягу ресурсів	-	+	-	+
	5.2		Впровадження програм «троянських коней»	+	+	-	+
	5.3		Впровадження вірусів	-	-	-	+

2.4 Модель порушника

Користувачі ПТКАЗ чи інші суб'єкти, які здійснюють спроби несанкціонованого доступу до об'єкта захисту (спроби ознайомлення, модифікації, знищення інформації, зміни режимів використання чи

функціонування ПТКАЗ, тощо) незалежно від успішності реалізації таких спроб – є порушниками.

Спроби несанкціонованого доступу до ресурсів ПТКАЗ, можуть бути здійснені порушниками навмисно (зловмисниками), чи ненавмисно (неправильні, непередбачені дії без злих намірів, внаслідок недбалості, тощо).

Потенційні порушники

Враховуючи умови функціонування ПТКАЗ потенційними порушниками може бути персонал, який має доступ до ПТКАЗ: особи, які не повинні мати доступу до ІзОД, але мають доступ до ПТКАЗ і потенційно можуть отримати доступ до ІзОД (внутрішній порушник (ВП)).

Ці особи мають можливість помилково, внаслідок необізнаності, цілеспрямовано, за злим наміром або без нього, використовуючи різні можливості, методи та засоби здійснити спробу виконати операції, які можуть призвести до порушення конфіденційності, цілісності або доступності ІзОД.

Загальна модель порушника

Модель порушника відображає його практичні та потенційні можливості, апріорні знання, час та місце дії, тощо.

Визначення категорій порушників, що прийняті у моделі, наведено в таблиці 1. У таблицях 2 - 6 наведено специфікації моделі порушника за мотивами здійснення порушень, за рівнем кваліфікації та обізнаності щодо ПТКАЗ, за показником можливостей використання засобів ПТКАЗ для реалізації загроз, за часом дії, за містом дії. У графі "Рівень загроз" зазначених таблиць наведено рейтингову оцінку загроз порушника

(можливих збитків). Рівень загрози характеризується наступними категоріями:

1- незначний (низький), 2- нижче середнього, 3- середній, 4- вище середнього, 5- значний (високий).

Виходячи із характеристики інформації, яка обробляється, категорії порушників, які мають потенційну можливість порушення конфіденційності та цілісності вважаються найбільш небезпечними, спостереженості - менш небезпечними, доступності - найменш небезпечними.

Таблиця 2.3.

Категорії порушників, що визначені в моделі

Позначення	Визначення категорії	Потенційний рівень загрози
П1	Авторизовані користувачі ПТКАЗ, яким надано право доступу до інформації з обмеженим доступом	3
П2	Авторизовані користувачі, яким надано повноваження контролювати дії користувачів та виконувати контроль за дотриманням правил доступу до ІзОД в ПТКАЗ	2
П3	Авторизовані користувачі, яким надано повноваження забезпечувати управління ПТКАЗ (системний адміністратор)	2
П4	Персонал, який забезпечує працездатність технічних засобів ПТКАЗ	3
П5	Особи, які не повинні мати доступу до ІзОД, але мають доступ ПТКАЗ, і потенційно можуть отримати доступ до ІзОД	2

Таблиця 2.4.

Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив порушення	Ефективний рівень загрози
М1	Безвідповідальність (недбалість)	5
М2	Корисна цілеспрямованість	2

Таблиця 2.5.

Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ПТКАЗ

Позначення	Основні кваліфікаційні ознаки порушника	Ефективний рівень загрози
К1	Не володіє знаннями та інформацією про порядок функціонування ПТКАЗ, не має навичок щодо користування штатними засобами системи.	5
К2	Має навички щодо користування ПТКАЗ на рівні користувача	4
К3	Володіє базовими знаннями щодо функціонування ПЗ та ОС, та практичними навичками роботи з засобами, що реалізовані в ПТКАЗ	3
К4	Володіє знаннями щодо функціону-вання засобів та механізмів захисту, що використовуються в ПТКАЗ та їх недоліків	2

Таблиця 2.6.

Специфікація моделі порушника за показником можливостей використання засобів ПТКАЗ для реалізації загроз

Позначення	Характеристика можливостей порушника	Еф. рівень загрози
З1	Має фізичний доступ до ПТКАЗ, але не є авторизованим користувачем ПТКАЗ	4
З2	Має можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;	3
З3	Має можливість керування функціонуванням ПТКАЗ, тобто конфігурує програмне забезпечення та КЗЗ ПТКАЗ	2

Таблиця 2.7.

Специфікація моделі порушника за часом дії

Позначення	Характеристика можливостей порушника	Еф. рівень загрози
Ч1	Під час бездіяльності компонентів системи (під час планових перерв у роботі, неробочий час)	4
Ч2	Під час функціонування ПТКАЗ	3
Ч3	Під час перерви у роботі для обслуговування та ремонту	2

Таблиця 2.8.

Специфікація моделі порушника за місцем дії

Позначення	Характеристика місця дії порушника	Еф. рівень загрози
Д1	Всередині приміщення, але без доступу до технічних засобів ПТКАЗ	5
Д2	З робочого місця користувача	2

Модель порушника, яку побудовано з урахуванням особливостей ПТКАЗ (що забезпечує певне виконання технологічних процесів створення об'єкту), технологій обробки інформації, категорій персоналу та користувачів, характеризується сукупністю значень характеристик, що наведені вище. Сукупність цих характеристик визначає профіль можливостей порушника.

Профілі можливостей порушників

На основі припущень щодо характеристик порушника, розроблені профілі можливостей порушника.

Профілі можливостей порушників всіх категорій наведені в таблиці 7. У графі "Ефективний рівень загроз" наведено рейтингову оцінку загроз порушника з відповідними характеристиками.

Таблиця 2.9.

Профілі можливостей порушників

Позначення	Визначення категорії	Характер дій порушника					Еф. рівень загроз
		Мотив порушення	Квалі-фікація	Можли-вості	Час дії	Місце дії	
П1	Авторизовані користувачі ПТКАЗ	М2	К2	З2	Ч1 Ч2	Д2	3
П2,П3	Системний адміністратор	М2	К3 К4	З2 З3	Ч3	Д2	2
П4	Персонал, який забезпечує працездатність технічних засобів ПТКАЗ	М2	К4	З2 З3	Ч1	Д1	3
П5	Особи, які не повинні мати доступу до ІзОД, але мають доступ до ПТКАЗ і потенційно можуть отримати доступ до ІзОД	М2	К4	З3	Ч1	Д2	2

При формуванні моделі загроз та оцінюванні ризиків враховувався міжнародний стандарт ISO/IEC 27005. Інформаційна технологія. Методи захисту. Менеджмент ризиків інформаційної безпеки.

2.5 Оцінювання ризиків

Ризик, пов’язаний з загрозою, може розглядатись як функція відносної імовірності, що загроза може бути реалізована, та очікуваних втрат, які будуть понесені в результаті реалізації загрози. В цьому випадку ризик розраховується наступним чином:

Ризик = Імовірність реалізації загрози * Втрата

Якщо значення втрат та імовірності реалізації загроз визначені як числа від 1 до 4, ризик може бути розрахований як число в інтервалі від 1 до 16 (значення від 1 до 3 вважаються низьким ризиком, від 4 до 8 - середнім ризиком, від 9 до 16 - високим).

В таблицях наведені результати оцінювання ризику відповідно до наведеної моделі загроз.

1. Модель загроз та результат оцінювання ризику

Результати моделювання загроз для інформації в ПТКАЗ за об’єктом та суб’єктом впливу, метою впливу, способом впливу, результатом впливу на інформацію та систему її обробки наведено у таблицях 1, 2.

Результати оцінювання ризиків відповідно до вказаних загроз – у таблицях 2.11, 2.13.

Таблиця 2.10.

Результати моделювання загроз за об’єктом та суб’єктом впливу, результатом впливу на інформацію та систему її обробки

Об'єкт впливу	Дескриптор загрози	Вид Інформації	Порушення конфіденційності	Порушення цілісності	Порушення доступності	Втрата керованості	Примітки
Операційна система	1	Технологічна	+	-	+	-	Найбільш вразлива до некоректних дій адміністратора
Прикладне програмне забезпечення	2	ІзОД	+	+	-	-	Найбільш вразлива до некоректних дій користувача
	3	Відкрита	+	+	+	-	Найбільш вразлива до некоректних дій користувача
	4	Технологічна	-	-	+	-	Найбільш вразлива до некоректних дій адміністратора

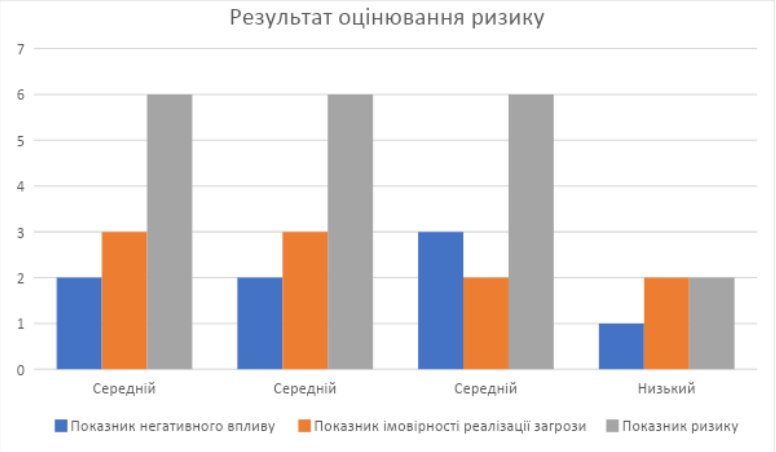
Таблиця 2.11.

Результат оцінювання ризику

Дескриптор загрози	Показник негативного впливу (втрат для ресурсу)	Показник імовірності реалізації загрози	Показник ризику	Ранг ризику, пов’язаного з загрозою
1	2	3	6	Середній
2	2	3	6	Середній
3	3	2	6	Середній
4	1	2	2	Низький

Вказані значення втрат, імовірностей реалізації загроз та ризиків, пов’язаних з даними загрозами, представлені у вигляді діаграми 1.

Діаграма 1. Результат оцінювання ризику



Таблиця 2.12.

Результати моделювання загроз за способом реалізації загрози, суб’єктом впливу, метою впливу

Класифікація атак	Дескриптор загрози	Порушник	Спосіб реалізації загрози (атаки)	Мета впливу			
				Порушення конфіденційності	Порушення цілісності	Порушення доступності	Втрата керованості
Атака з використанням НСД	1	Внутрішній порушник	Несанкціонований доступ до даних з метою їх перегляду\модифікації\видалення	-	+	-	-
	2		Несанкціонований доступ до програмного забезпечення з метою його пошкодження	-	-	+	-
	3		Несанкціонований запуск програмних засобів	+	-	-	-
	4		Несанкціоноване отримання прав доступу	-	-	-	+
Незаконне використання повноважень	5	Внутрішній порушник	Незаконне використання адміністративних повноважень	+	-	+	+
	6		Незаконне використання повноважень користувача	+	+	+	+
Незаконний доступ до сумісно використовуваних ресурсів, звільнених іншим користувачем або процесом	7	Внутрішній порушник	Незаконний доступ до сумісно використовуваних ресурсів	-	+	-	-
Злом системи	8	Внутрішній порушник	Підбір або перехоплення пароля	+	-	-	+
Використання шкідливих програм	9	Внутрішній порушник	Захоплення надмірного обсягу ресурсів	-	+	-	+
	10		Впровадження програм «троянських коней»	+	+	-	+
	11		Впровадження вірусів	-	-	-	+

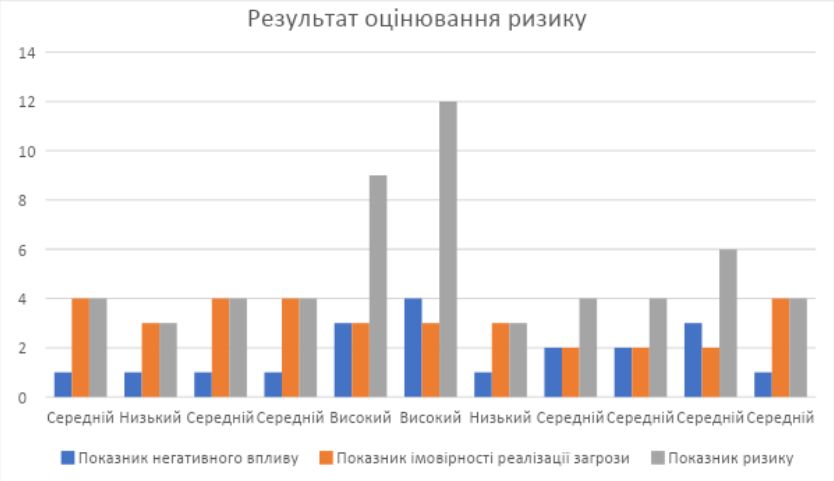
Таблиця 2.13.

Результат оцінювання ризику

Дескриптор загрози	Показник негативного впливу (втрат для ресурсу)	Показник імовірності реалізації загрози	Показник ризику	Ранг ризику, пов'язаного з загрозою
1	1	4	4	Середній
2	1	3	3	Низький
3	1	4	4	Середній
4	1	4	4	Середній
5	3	3	9	Високий
6	4	3	12	Високий
7	1	3	3	Низький
8	2	2	4	Середній
9	2	2	4	Середній
10	3	2	6	Середній
11	1	4	4	Середній

Вказані значення втрат, імовірностей реалізації загроз та ризиків, пов'язаних з даними загрозами, представлені у вигляді діаграми 2.

Діаграма 2. Результат оцінювання ризику



За результатами аналізу загроз та оцінювання ризиків визначено, що найвищий ризик для системи являють собою загрози, пов'язані з несанкціонованим доступом до даних з метою їх

перегляду\модифікації\видалення. У зв’язку з цим система захисту ПТКАЗ повинна забезпечувати:

- обов'язковість реєстрації усіх користувачів відповідно до встановленої політики безпеки;
- можливість здійснення однозначної ідентифікації та автентифікації кожного зареєстрованого користувача;
- створення захищеного середовища обробки інформації, в якому всі дії користувачів контролюються;
- запобігання несанкціонованому доступу до ПТКАЗ, фізичних та інформаційних ресурсів;
- блокування доступу до ресурсів ПТКАЗ користувача, які порушили встановлені правила розмежування доступу;
- контроль цілісності програмно-технічного середовища ПТКАЗ;
- комплексне застосування механізмів захисту інформації системного і функціонального ПЗ та спеціалізованих програмних засобів.

Висновок до розділу 2

В даному розділі розробленно моделей загроз, порушника та оцінка рисків для програмно-технічного комплексу абонентського зв’язку. Використовуючи модель смартфона Samsung Galaxy A10s, визначено характеристики та загрози порушника, а також розраховано оцінки ризику.

РОЗДІЛ 3. МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ПТКАЗ

Несанкціонований доступ (НСД) - канал спеціального впливу порушника, який, використовуючи штатні засоби доступу до інформаційних ресурсів, порушує встановлені правила розмежування доступу з метою реалізації будь-яких з основних видів загроз для інформації.

Для захисту інформації від несанкціонованого доступу до програмно-технічного комплексу абонентського зв'язку можуть використовуватись різні методи та технології. Нижче наведено деякі з них:

1. Аутентифікація та авторизація: ці процедури забороняють використовувати, чи є користувач дійсно тим, за кого він себе видає, та чи має він право на доступ до певної інформації. Для цього можна використовувати різні методи, такі як паролі, ключі, біометричні дані тощо.
2. Шифрування: це процес перетворення звичайного тексту на зашифрований, що забезпечує захист від перехоплення та зламу. Для шифрування можна використовувати різні алгоритми, такі як AES, RSA, Blowfish тощо.
3. Фізичний захист: це заходи захисту, що передбачають фізичний доступ до обладнання та інфраструктури. Це можуть бути захисні пристрої, контроль доступу, системи відеоспостереження тощо.
4. Захист від вірусів та інших шкідливих програм: для цього можна використовувати антивірусні програми, файли, системи виявлення та запобігання вторгненню (IDS/IPS) тощо.
5. Захист від соціального інженерінгу: це захист захисту, що передбачає попередження працівників від розголошення чутливої інформації через маніпулювання ними.

6. Резервне копіювання та відновлення даних: цей захист захисту дозволяє відновити дані після непередбачуваного результату, такого як аварія, вірус, злам тощо.

3.1 Обрання ключів шифрування

Довгостроковий ключовий елемент (далі - ДКЕ) - ключ, що визначає заповнення таблиць блока підстановки алгоритму криптографічного перетворення, визначеного ДСТУ ГОСТ 28147:2009;

Разовий (сеансовий) ключ (далі - РК) - ключ, який визначає порядок заповнення ключового запам'ятовувального пристрою засобу КЗІ, що реалізує алгоритм криптографічного перетворення, визначений ДСТУ ГОСТ 28147:2009.

Обрання ключів шифрування є критичним етапом процесу шифрування, що відбувається при виборі правильного ключа для шифрування та розшифрування даних. Ключі шифрування є секретними або публічними кодами, які використовуються для захисту даних від несанкціонованого доступу.

Обрання правильних ключів є дуже важливим для забезпечення безпеки та конфіденційності даних. Наприклад, якщо ключ шифрування занадто слабкий або простий, то зловмисники можуть легко зламати шифр і отримати доступ до конфіденційної інформації.

Для забезпечення високої безпеки шифрування використовуйте ключі великої довготи та складної структури. Крім того, ключі повинні бути збережені в безпечному місці та потім змінюватися для зменшення ризику несанкціонованого доступу до даних.

Для деяких шифрувальних алгоритмів, таких як RSA, ключі можуть бути створені тільки за допомогою складних математичних алгоритмів, що забезпечують високу стійкість до атак зловмисників. Для інших алгоритмів, таких як AES, ключі можуть бути створені за допомогою генерації випадкових чисел.

Загалом, правильний вибір та збереження ключів є важливою складовою процесу шифрування, яка забезпечує безпеку та конфіденційність даних.

Приклад ДКЕ, які рекомендуються до застосування у засобах КЗІ

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
К1	a	9	d	6	e	b	4	5	f	1	3	c	7	0	8	2
К2	8	0	c	4	9	6	7	b	2	3	1	f	5	e	a	d
К3	f	6	5	8	e	b	a	4	c	0	3	7	2	9	1	d
К4	3	8	d	9	6	b	f	0	2	5	c	a	4	e	1	7
К5	f	8	e	9	7	2	0	d	c	6	1	5	b	4	3	a
К6	2	8	9	7	5	f	0	b	c	1	d	e	a	3	6	4

Структура ключового файла, який містить ключові дані РК

РК довжиною 256 біт (32 байти) містить (умовно) 8 блоків (X0, X1,..., X7) по 32 біти (4 байти) у кожному. Блоки розміщуються один за одним в порядку зростання їх номерів.

Кожний блок (32-розрядне слово - 4 байти) визначає заповнення відповідного накопичувача ключового запам'ятовувального пристрою. При цьому молодший біт відповідає молодшому розряду накопичувача.

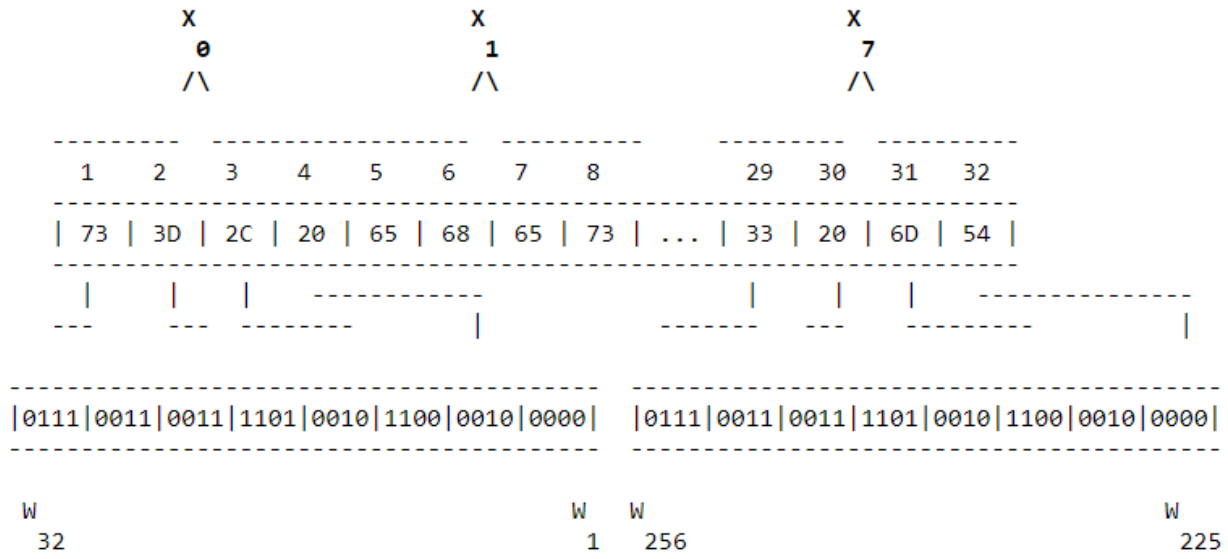


Рисунок 3.1. Структура РК

3.2 Практичне використання згенерованого РК

Використання архіву дає можливість зменшити займане файлами місце на комп'ютері за рахунок їх стиснення. Та й пересилати поштою або викладати в інтернеті набір файлів буває зручніше у вигляді архіву, ніж по одному. Але, крім стиснення файлів архіватори дають можливість обмежувати доступ до вмісту архіву за допомогою введення пароля. Таким чином, крім економії місця на диску, користувач отримує ще й захищені за допомогою шифрування файлів.

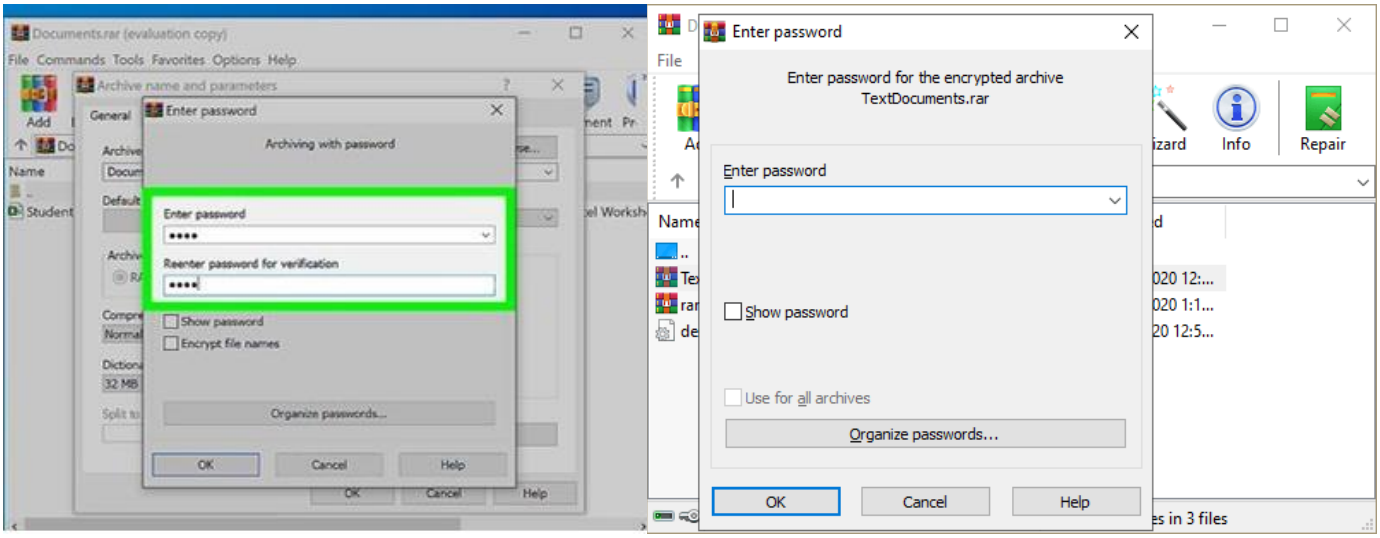


Рисунок 3.2. Шифрування файлів за допомогою архіватора

3.3 Застосування OpenVPN

OpenVPN є відкритим і безпечним протоколом для створення віртуальних приватних мереж (VPN). Протокол дозволяє забезпечити безпеку та конфіденційність цих даних, що передаються через мережу Інтернет, і використовувати для захисту приватної інформації, такої як логіни, паролі, фінансові дані тощо.

OpenVPN може бути використаний для різних цілей, включаючи:

- Забезпечення безпеки під час використання віддаленими серверами, такими як сервери віддаленого доступу до робочого столу або серверу веб-хостингу.
- Захист особистої інформації від зловмисників, які можуть перехоплювати дані, що передаються через мережу Інтернет.
- Доступ до обмеженого контенту або сайтів, які блокуються в деяких країнах або регіонах.

- Забезпечення безпеки віддалених підключень до комп'ютерів, що дозволяє працювати з даними на відстані, як у випадку дистанційної роботи.

OpenVPN дозволяє використовувати інші методи шифрування, такі як AES, Blowfish та DES, щоб забезпечити безпеку даних. Крім того, OpenVPN може бути налаштований для використання різних протоколів, таких як TCP і UDP, що дозволяє налаштувати його для різних потреб.

Для використання OpenVPN необхідно встановити програмне забезпечення на своєму комп’ютері чи мобільному пристрої та налаштувати підключення до віддаленого сервера OpenVPN. Віддалений сервер може бути налаштований власником VPN, або ви можете використовувати послуги провайдера VPN, що надає доступ до своїх серверів.

Для забезпечення безпеки керуючого каналу і потоку даних OpenVPN використовує бібліотеку OpenSSL. Це дає змогу задіяти весь набір алгоритмів шифрування, доступних у цій бібліотеці. Також може використовуватися пакетна аутентифікація HMAC, для забезпечення більшої безпеки, і апаратне прискорення для поліпшення продуктивності шифрування. Ця бібліотека використовує OpenSSL, а точніше протоколи SSLv3/TLSv1.2. OpenVPN використовується в операційних системах Solaris, OpenBSD, FreeBSD, NetBSD, GNU/Linux, Apple Mac OS X, QNX, Microsoft Windows, Android, iOS.

OpenVPN пропонує користувачеві кілька видів аутентифікації.

- Попередньо встановлений ключ - найпростіший метод.
- Сертифікатна аутентифікація - найбільш гнучкий у налаштуваннях метод.
- За допомогою логіна та пароля - може використовуватися без створення клієнтського сертифіката (серверний сертифікат все одно потрібен).

Висновок до розділу 3

В даному розділі розроблено відповідній методи захисту інформації щодо обрання програмного забезпечення, та блокування спроб НСД до інформації ПТКАЗ, порядку оновлення ОС, використання СПЗ для виявлення та блокування спроб НСД до інформації ПТКАЗ.

ВИСНОВКИ:

Проведено оцінку можливостей, якості та ефективності використання програмних засобів оцінки інформаційних ризиків. COBRA- засіб для на аналізу та управління інформаційними ризиками, згідно вимог ISO 17799 у вигляді тематичних запитів. RA Software Tool- засіб, який виконує оцінку інформаційних ризиків згідно вимог стандартів ISO 17799 та ISO 13335. CRAMM- програмний засіб, який доцільно використовувати для аналізу інформаційних систем з підвищенними вимогами до інформаційної безпеки, велика точність пошуку ризиків, можливість заощадження матеріальних ресурсів. RiskWatch- потужний засіб для проведення аудиту інформаційної безпеки, в якості критеріїв для оцінки та управління ризиками використовують представлення річних затрат. OCTAVE використовується для оцінки ризиків за допомогою послідовності організованих внутрішніх семінарів, розташованих відповідним чином. Digilal Security Officesасіб для розробки та управління політики безпеки інформаційної системи на основі стандартів ISO 17799, ISO 27001, ISO 27005. RA2 art of risk- для проектування та побудови системи управління інформаційної безпеки використовується процесний підхід, на базі ISO 17799.

Проведений аналіз методів оцінки ризиків дав змогу розробити модель загроз, оцінити ризики та на підставі цього визначити основні методи захисту інформації від несанкціонованого доступу ПТКАЗ.

Запропоновані методи захисту (програмне забезпечення, порядок оновлення ОС, використання СПЗ для виявлення та блокування спроб НСД до обробляємої інформації) дозволяють забезпечити безпечну обробку конфідеційної інформації за допомогою ПТКАЗ.

Основною перевагою запропонованих методів є простота да доступність їх використання достатня для захисту конфіденційної інформації.

В ході виконання роботи розроблено відповідній методи захисту інформації щодо обрання програмного забезпечення, та блокування спроб НСД до інформації ПТКАЗ, порядку оновлення ОС, використання СПЗ для виявлення та блокування спроб НСД до інформації ПТКАЗ.

Запропонований метод створення ключа шифрування для програм архіваторів файлів, дає змогу провести циклічне блокове шифрування, а також дешифрування попередньо підготовлених файлів, але даний метод не доведено до програмної реалізації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Alberts C. J. Operationally Critical Threat, Asset and Vulnerability Evaluation / C.J. Alberts, S. G. Behrens, R. D. Pethia, W. R. Wilson. – 2018. – P. 84.
2. Endorf C. F. Measuring ROI on security / Carl F. Endorf // Information security management handbook / Edited by Harold F. Tipton and Micki Krauze. – 6th edition. – Boca Raton: Auerbach Publications, 2017. – Part 1, Section 1.1, Ch. 12. –P. 133-137.
3. Henry K. Risk management and analysis / Kevin Henry // Information Security Management Handbook / Edited by Harold F. Tipton, Micki Krauze. – 6th edition. – Boca Raton: Auerbach Publications, 2017. – Part 1, Section 1.4, Ch. 28. – P. 321- 329.
4. ISO/IEC 27035. Information technology. Security techniques. Information security incedent management. – 2011. – 78 p.
5. Landoll D. The security risk assessment handbook: a complete guide for performing security risk assessments / Douglas J. Landoll. – Boca Raton: Auerbach Publications, 2016. – 504 p.
6. Rittinghouse J. W. Business continuity and disaster recovery for infosec managers / John W. Rittinghouse, James F. Ransome. – Oxford: Elsevier, 2015. – 408 p.
7. Spedding L. Business risk management handbook: a sustainable approach / Linda Spedding, Adam Rose. – Oxford: Elsevier, 2018. – 768 p.
8. Андріанов В. В. Забезпечення інформаційної безпеки бізнесу / В. В. Андріанов, С. Л. Зефіров, В. Б. Голованов. - М.: ЦІПСіР, 2016. - 373 с.
9. Балашов П. А. Оцінка ризиків інформаційної безпеки на основі нечіткої логіки / П. А. Балашов, В. П. Безгузіков, Р. І. Кислов // 96 [Електронний ресурс]. - Режим доступу: http://www.nwaktiv.ru/textstat2/index.html
10. Баранова Є. К. Методики та програмне забезпечення для оцінки ризиків у сфері інформаційної безпеки // Управління ризиком. 2013. No 1 (49). -С. 15-26.
11. Branch, Jordan (24 September 2020). "What's in a Name? Metaphors and Cybersecurity". International Organization. Cambridge University Press (CUP). 75 (1): 39–70.
12. Гарасим Ю. Р. Аналіз систем захисту, які мають властивість живучості / Ю. Р. Гарасим // Військово-технічний збірник. - 2016. No 1 (4). - С. 87-95.
13. Гарасим Ю. Р. Забезпечення живучості та неперервності функціонування систем захисту інформації / Ю. Р. Гарасим, В. О. Ромака, М. М. Рибій // Вісник Нац. ун-ту “Львівська політехніка” “Автоматика, вимірювання та керування”. - 2014. - No 741. - С. 105-112.
14. Дубінін Є. А. Оцінка відносної шкоди безпеки інформаційної системи: монографія / Є. А. Дубінін, Ф. Б. Тебуєва, В. В. Копитов. - М.: ІЦ РІОР: НІЦ ІНФРА-М, 2014. - 192 с.
15. Замула О. О. Аналіз міжнародних стандартів у галузі оцінювання ризиків інформаційної безпеки / О. О. Замула, В. І. Черниш // Системи обробки інформації: збірних наукових праць. - Х.: ХУ ПС, 2014. - Віп. 2(92). - С. 53-56.
16. Замула А. А., Северінов А. В., Корнієнко М. А.Аналіз моделей оцінки ризиків інформаційної безпеки для побудови системи захисту інформації. - Наука і техніка Повітряних Сил Збройних Сил України, 2017, – No 2(15). - С. 47-52. 97
17. Кисельова І. А., Іскаджян С. О. Інформаційні ризики: методи оцінки та аналізу // ІТпортал, 2017. No2 (14). - С.142-146.
18. Козлова Є. А. Оцінка ризиків інформаційної безпеки за допомогою методу нечіткої кластеризації та обчислення взаємної інформації. Молодий вчений. Щомісячний науковий журнал No5(52)/2015. - С. 45-51.
19. Корченко А. Г. Побудова систем захисту на нечітких множинах. Теорія та практичні рішення - К.: МК-Прес, 2016. - 324 с.
20. Легчекова Є. В., Тітов О. В. Метод розрахунку ризику інформаційної безпеки. [Електронний ресурс]. – Режим доступу: http://lib.ibteu.by/bitstream/handle/22092014/3600/Легчекова%20Е.В.%2С %20Тітов %20О.В.%20 Метод%20расчета.pdf
21. Малюк А. А. Теорія захисту інформації. - М.: Гір. лінія-телеком, 2015. - 184 с.

22. Методологія OCTAVE з метою оцінки інформаційних ризиків [Електронний ресурс]. - Режим доступу: http://www.risk24.ru/octave.htm
23. Методології управління IT-ризиками [Електронний ресурс]. – Режим доступу: http://www.iso27000.ru/chitalnyi-zai/upravlenie-riskamiinformacionnoe bezopasnosti/metodologii-upravleniya-it-riskami
24. Милославська Н. Г., Сенаторів М. Ю., Толстой А. І. Управління ризиками інформаційної безпеки. Навчальний посібник для вишів. - М.: Гаряча лінія- Телеком, 2016. - 245 с.
25. Петренко С. А., Петренко А. А. Аудит безпеки Intranet. - М.: ДМК Прес, 2016. - 416 с.
26. Fuller, Christopher J (11 June 2018). "The Roots of the United States' Cyber (In)Security" (DOC). Diplomatic History. Oxford University Press (OUP). 43 (1): 157–185.
27. Плетньов П. В., Бєлов В. М. Методика оцінки ризиків інформаційної безпеки на підприємствах малого та середнього бізнесу // Доповіді ТУСУРу No 1 (25), частина 2, червень 2016. - С. 35-38.
28. Montagnani, Maria Lillà; Cavallo, Mirta Antonella (2018). "Cybersecurity and Liability in a Big Data World". Market and Competition Law Review. Elsevier BV. 2 (2): 71–98.
29. Сааті Т. Прийняття рішень. Метод аналізу ієрархій/Томас Сааті: Пер. з англ. Р. Вачнадзе. – Радіо та зв'язок, 2013. – 320 с.
30. Сердюк В. А. Аналіз сучасних тенденцій побудови моделей інформаційних атак / В. А. Сердюк // Інформаційні технології. - 2014. - No 5. - С. 94-101.
31. Сердюк В. А. Організація та технології захисту інформації. Виявлення та запобігання інформаційним атакам в автоматизованих системах підприємств. - Вища Школа Економіки, 2015. - 576 с.
32. Ткаченко В. Сучасні підходи до оцінки ризиків інформаційних технологій / В. Ткаченко, В. Сисоєв // [Електронний ресурс]. – Режим доступу: http://www.cbz.com.ua/resources/files/12224515494d0f29e1cacc9.pdf
33. Харитонов Є. В. Узгодження вихідної суб'єктивної інформації в методах аналізу ієрархій // Математична морфологія. -2017. - Т. 3. - Вип. 2. - С. 41-51
34. Черниш В. І. Методи оцінювання інформаційних ризиків компанії / В. І. Черниш // Матеріали XV Міжнародного ювілейного молодіжного форуму «Радіоелектроніка та молодь у XXI столітті»: Зб. тез, 18–20 квітня 2015 р., Т.5. - Х.: ХНУРЕ, 2015. - С. 195.
35. Шаньгін В. Ф. Інформаційна безпека та захист інформації. - К.: ДМК Прес, 2016. - 702 с.