Міністерство освіти і науки України
Державний вищий навчальний заклад
«Національний гірничий університет»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
дипломної роботи

магістра
(ступінь підготовки)

галузь знань ***12 Інформаційні технології***
(шифр і назва галузі знань)

напрям підготовки (спеціальність) ***125 Кібербезпека***
(код і назва напряму підготовки)

спеціалізація (освітня програма) ***Кібербезпека***
(код і назва спеціальності)

ступінь підготовки ***магістр***
(назва освітнього рівня)

кваліфікація ***професіонал із організації інформаційної безпеки***
(код і назва кваліфікації)

на тему: ***«Оцінка ризиків інформаційної безпеки з використанням алгоритму нечіткої кластеризації k-середніх»***

Виконавець: студент *6* **курсу, групи** *125м-16-1*

Ковальов Ігор Дмитрович
(підпис) (прізвище ім'я по-батькові)

Керівники	Прізвище, ініціали	Оцінка	Підпис
роботи	к.ф.-м.н., доц. Герасіна О.В.		
розділів:			
спеціальний	к.ф.-м.н., доц. Герасіна О.В.		
економічний	к.е.н., доц. Волотковська Ю.О.		
Рецензент			
Нормоконтроль	к.ф.-м.н., доц. Гусєв О.Ю.		

Дніпро
2018

Міністерство освіти і науки України
Державний вищий навчальний заклад
«Національний гірничий університет»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
д.т.н., професор _____ Корнієнко В. І.

«_____»_____20___року

ЗАВДАННЯ
на виконання кваліфікаційної роботи магістра
спеціальності *125 Кібербезпека*
(код і назва спеціальності)

студенту **125м-16-1** **Ковальову Ігору Дмитровичу**
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи ***Оцінка ризиків інформаційної безпеки з використанням алгоритму нечіткої кластеризації k-середніх»***

1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Наказ ректора Державного ВНЗ «НГУ» від ___26 грудня 2017_____№_2127-л__

2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень *Методи кількісного аналізу ризиків інформаційної безпеки*

Предмет досліджень *Методика аналізу ризиків інформаційної безпеки, яка заснована на кластеризації значень ймовірності реалізації загроз інформаційної безпеки на активи підприємства*

Мета НДР *Підвищення інформаційної безпеки підприємства*

Вихідні дані для проведення роботи *Законодавство України та міжнародні стандарти у сфері інформаційної безпеки, наукові публікації вітчизняних та іноземних авторів.*

3 ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна *для виділення однорідних груп ризиків інформаційної безпеки з різними показниками методом кластеризації «к-середніх» дозволяє отримати узагальнену характеристику оцінки ризиків на підприємстві*

Практична цінність *полягає в розробці методики оцінки ризиків, що дозволяє ефективно вирішувати завдання управління ризиками підприємств*

4 ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Результати повинні відповідати вимогам Закону України «Про телекомунікації», Закону України «Про інформацію», Закону України «Про внесення змін до Закону України «Про телекомунікації»

5 ЕТАПИ ВИКОНАННЯ РОБІТ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Огляд джерел за темою та напрям досліджень	15.09.17-10.10.17
Методи досліджень	11.10.17-27.11.17
Результати досліджень	28.11.17-20.12.17
Виконання економічного розділу	21.12.17-31.12.17

6 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект *від реалізації результатів роботи очікується позитивним завдяки правильній оцінці ризиків інформаційної безпеки підприємств*

Соціальний ефект *правильна оцінка ризиків інформаційної системи скорочує економічні втрати та втрати робочого часу персоналу підприємств*

7 ДОДАТКОВІ ВИМОГИ

Завдання видав _____ Герасіна О.В.
(підпис) (прізвище, ініціали)

Завдання прийняв до виконання _____ Ковальов І.Д.
(підпис) (прізвище, ініціали)

Дата видачі завдання: 01.09.17р

Термін подання дипломної роботи до ДЕК 17.01.18р.

РЕФЕРАТ

Пояснювальна записка: XXX с., XX рис., XX табл., XX додатків, XX джерел.

Об’єкт дослідження: методи кількісного аналізу ризиків інформаційної безпеки.

Мета роботи: підвищення інформаційної безпеки підприємств.

Методи дослідження: методи теорії кластерного аналізу, теорії ймовірностей, поняття і методи теорії захисту інформації.

У спеціальній частині дана характеристика існуючих технологій аналізу ризиків ІБ в системі забезпечення інформаційної безпеки організації.

У роботі досліджені методи кількісного аналізу ризиків ІБ. Запропонована методика застосування в кластерного аналізу при виділенні однорідних груп ризиків з різними показниками.

В економічному розділі визначена економічно доцільна політика безпеки, розраховані збитки від реалізації можливих загроз і зіставлені з витратами на розробку і впровадження політики безпеки.

Практичне значення роботи полягає в розробці методики оцінки ризиків, що дозволяє ефективно вирішувати завдання управління ризиками підприємств.

Результати здійснених у дипломній роботі (проекті) досліджень можуть бути використані на підприємствах малої та середньої форм власності.

Наукова новизна дослідження полягає у виділенні однорідних груп ризиків ІБ з різними показниками, що дозволяє отримати узагальнену характеристику оцінки ризиків.

АНАЛІЗ РИЗИКІВ ІБ, КЛАСТЕРИЗАЦІЯ, МЕТОД К – СЕРЕДНІХ.

РЕФЕРАТ

Пояснительная записка: XXX с., XX рис., XX табл., XX приложений, XX источников.

Объект исследования: методы количественного анализа рисков информационной безопасности.

Цель работы: повышение информационной безопасности предприятий.

Методы исследования: методы теории кластерного анализа, теории вероятностей, понятия и методы теории защиты информации.

В специальной части дана характеристика существующих технологий анализа рисков ИБ в системе обеспечения информационной безопасности организации.

В работе исследованы методы количественного анализа рисков ИБ.

Предложена методика применения в кластерного анализа при выделении однородных групп рисков с различными показателями.

В экономическом разделе определена экономически целесообразная политика безопасности, рассчитаны убытки от реализации возможных угроз и сопоставлены с затратами на разработку и внедрение политики безопасности.

Практическое значение работы состоит в разработке методики оценки рисков, позволяющей эффективно решать задачи управления рисками предприятий.

Результаты проведенных в дипломной работе (проекте) исследований могут быть использованы на предприятиях малой и средней форм собственности.

Научная новизна исследования заключается в выделении однородных групп рисков ИБ с различными показателями, позволяющими получить обобщенную характеристику оценки рисков.

АНАЛИЗ РИСКОВ ИБ, КЛАСТЕРИЗАЦИЯ, МЕТОД К – СРЕДНИХ.

ABSTRACT

Explanatory note: XX page, XX figure, XX table, XX applications XX sources.

The object of research: methods of quantitative analysis of information security risks.

Objective: to improve information security of enterprises.

Methods of research: methods of the theory of cluster analysis, probability theory, concepts and methods of information protection theory.

In a special section, the characteristics of existing technologies for analyzing the risks of information security in the organization's information security system are given.

The methods of quantitative analysis of IS risks are investigated.

The technique of application in the cluster analysis is offered at allocation of homogeneous groups of risks with various indicators.

In the economic section, an economically viable security policy has been defined, losses from the implementation of possible threats have been calculated and compared with the costs of developing and implementing a security policy.

The practical significance of the work is to develop a methodology for risk assessment that allows to effectively solve the tasks of enterprise risk management.

The results of studies carried out in the thesis (project) can be used at small and medium-sized enterprises.

The scientific novelty of the study is to isolate homogeneous risk groups of information security with different indicators, which makes it possible to obtain a generalized characteristic of risk assessment.

ANALYSIS OF RISKS OF INFORMATION SECURITY, CLUSTERING, METHOD K - MEANS.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АЗ - апаратне забезпечення

БД - база даних

БЗ - база знань

ЕР - елементи ризику

ЗОТ - засоби обчислювальної техніки

І - імітаційного моделювання

ІБ - інформаційна безпека

ІС - інформаційна система

ІТ - інформаційна технологія

КБ - кібербезпека

ЛТ - лінгвістичні терми

ОІБ - організація інформаційної безпеки

ОС - операційна система

ПЗ - програмне забезпечення

ПК - персональний комп'ютер

ПР - правила для ризиків

СВ - структури впливу

СМІБ - система менеджменту інформаційної безпеки

СУІБ - система управління інформаційною безпекою

ФВ - фактори впливу на загрози

ЗМІСТ

ВСТУП

У сучасних умовах однією з актуальних практичних задач є оцінка ефективності заходів щодо захисту інформації в інформаційних комп'ютерних системах. Дослідження цієї задачі дасть можливість розробникам і власникам інформаційних комп'ютерних систем отримувати обґрунтовану оцінку техніко-економічної доцільності різних заходів та способів захисту інформації і формувати раціональний комплекс заходів для забезпечення інформаційної безпеки, економно витрачаючи виділені на ці цілі ресурси. Сьогодні не викликає сумнівів необхідність вкладень в забезпечення інформаційної безпеки сучасного бізнесу. Основне питання сучасного бізнесу - як оцінити необхідний рівень вкладень в інформаційну безпеку (ІБ) для забезпечення максимальної ефективності інвестицій в дану сферу. Для вирішення цього питання існує тільки один спосіб - застосовувати системи / комплекси аналізу ризиків, що дозволяють оцінити існуючі в системі ризики і вибрати оптимальний з точки зору ефективності варіант захисту (по співвідношенню існуючих в системі ризиків / витрат на ІБ).

Основні терміни та визначення.

Загроза безпеки - це потенційно можлива подія, яка може вплинути на інформацію в системі.

Вразливість - це характеристика системи, яка робить можливим виникнення загрози.

Атака - це дія з використання вразливості; атака - це реалізація загрози.

Загроза конфіденційності - загроза розкриття інформації.

Загроза цілісності - загроза зміни інформації.

Загроза доступності - загроза порушення працездатності системи при доступі до інформації.

Збитки - це вартість втрат, яких зазнає компанія в разі реалізації загроз конфіденційності, цілісності, доступності по кожному виду цінної інформа-

ції. Збитки залежать тільки від вартості інформації, яка обробляється в автоматизованій системі. Збитки є характеристикою інформаційної системи і не залежать від її захищеності.

Ризик - це ймовірні збитки, які залежать від захищеності системи. За визначенням ризик завжди вимірюється в грошах.

Аналіз ризиків ІБ - систематичне використання інформації (історичних даних, результатів теоретичного аналізу, поінформованої думки) для визначення джерел і кількісної оцінки ризиків ІБ. Це процес розуміння походження ризику і визначення рівня ризику. Аналіз ризиків ІБ забезпечує базу для оцінювання ризиків ІБ, заходів щодо зниження ризиків ІБ і прийняття ризиків. Він є складовою частиною управління інформаційними ризиками, в процесі якого оцінюються вразливості інформаційної системи до загроз безпеці, їх критичність і ймовірність шкоди для компанії, виробляються контрзаходи по зменшенню ризиків до прийнятного рівня і забезпечується контроль захисту інформаційної системи компанії. Підготовлено більше десятка різних стандартів і специфікацій, що детально регламентують процедури управління інформаційними ризиками, серед яких найпопулярнішими стали міжнародні специфікації і стандарти ISO 17799−2002 (BS 7799), GAO і FISCAM, SCIP, NIST, SAS 78/94 і COBIT. В даний час управління інформаційними ризиками є одним з найбільш актуальних напрямків, що динамічно розвиваються у галузі захисту інформації, і тому актуальність теми дипломної роботи не викликає сумнівів.

У цій дипломній роботі запропонована методика застосування кластерного аналізу при виділенні однорідних груп ризиків з різними показниками.

Метою дипломної роботи є підвищення інформаційної безпеки підприємств.

Об'єктом досліджень в дипломній роботі є методи кількісного аналізу ризиків ІБ.

Предметом дослідження є методика аналізу ризиків ІБ заснована на кластеризації значень ймовірності реалізації загроз ІБ на активи підприємства.

Методи дослідження. Для вирішення поставленого завдання в даній роботі використовувалися методи теорії кластерного аналізу, теорії ймовірностей поняття і методи теорії захисту інформації.

Достовірність і обґрунтованість результатів магістерської роботи забезпечується застосуванням коректних вихідних даних, апробованих методів, перевіркою несуперечності висновків і результатами аналізу тестових програм.

Наукова новизна роботи визначається тим, що для виділення однорідних груп ризиків ІБ з різними показниками, використовується метод кластеризації "к-середніх", що дозволяє отримати узагальнену характеристику оцінки ризиків на підприємстві.

Практичне значення магістерської роботи полягає в тому, що розроблена методика оцінки ризиків дозволяє ефективно вирішувати певні завдання з управління ризиками підприємств. Розроблена методика може застосовуватися фахівцями, що не володіють специфічними знаннями та навичками в галузі захисту інформації.

Особливий внесок здобувача. Автор самостійно сформулював мету, завдання дослідження, наукові положення і результати, виконав теоретичну і практичну частини роботи.

Структура і обсяг роботи. Робота складається з вступу, трьох розділів і висновків. Містить 99 сторінок друкованого тексту, в тому числі 79 сторінок тексту основної частини з 28 рисунками, списку використаних джерел з 16 найменуваннями на 2 сторінках, 3 додатків на 20 сторінках с 2 рисунками.

РОЗДІЛ 1
ХАРАКТЕРИСТИКА ОБ'ЄКТА ДОСЛІДЖЕННЯ

В умовах дедалі більшої складності і інтеграції інформаційних систем питання інформаційної безпеки (ІБ) набуває все більшого значення. З одного боку, потрібна побудова єдиного інформаційного простору підприємства, 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 та інфраструктури і різнорідність експлуатованих інформаційних систем перешкоджають забезпеченню необхідного рівня ІБ. Забезпечення ІБ стає одним із пріоритетних завдань підприємств і організацій з метою підтримки її нормальної діяльності, стійкості на ринку і успішного розвитку. В умовах, що склалися необхідна побудова дійсно комплексної корпоративної системи менеджменту інформаційної безпеки (СМІБ), що є однією з найбільш важливих складових в загальній системі менеджменту компанії.

Для сучасного менеджменту ІБ характерний підхід, який передбачає вирішення проблем не "по мірі їх надходження", коли буває вже надто пізно ними займатися, а передбачає завчасний аналіз і попередження можливих проблем, на основі оцінки можливих ризиків ІБ, керуючись при цьому міркуваннями економічної доцільності [1-3]. Тому фундаментом для успішного впровадження і функціонування СМІБ є оцінка та аналіз ризиків ІБ.

У дипломній роботі визначимо [13,16] ризик порушення ІБ як потенційну можливість використання вразливостей активів організації загрозами ІБ для заподіяння шкоди організації, 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

бізнесу 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 [4, 16]. До таких факторів належать безліч активів, вразливостей і загроз. Основна мета створення класифікації загроз ІБ - повна, детальна класифікація, що описує всі існуючі загрози ІБ і яка найбільш застосовна для аналізу ризиків реальних інформаційних систем [7,8]

1.1 Ризики в системі забезпечення інформаційної безпеки організації

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

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

Незалежно від розмірів організації і специфіки її інформаційної системи, роботи по забезпеченню режиму ІБ зазвичай складаються з наступних етапів (див. 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 зарубіжними стандартами може бути мінімальним (базовим) або підвищеним. Цим рівням захищеності відповідають мінімальний (базовий) або повний варіант аналізу інформаційних ризиків.

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.

Рис. 1.1 - Основні етапи забезпечення інформаційної безпеки

Сам опис меж системи рекомендується виконувати за таким планом:

– Структура організації. Опис існуючої структури і змін, які передбачається внести в зв'язку з розробкою (модернізацією) автоматизованої системи.

- Ресурси інформаційної системи, що підлягають захисту. Рекомендується розглянути ресурси автоматизованої системи наступних класів: СВТ, дані, системне і прикладне ПЗ. Всі ресурси представляють цінність з точки зору організації. Для їх оцінки повинна бути обрана система критеріїв і методика отримання оцінок за цими критеріями.
- Технологія обробки інформації та розв’язувані задачі. Для вирішуваних завдань повинні бути побудовані моделі обробки інформації в термінах ресурсів.
- Розміщення засобів СВТ і підтримуючої інфраструктури.

6. Постановка 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 проектних 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 і уразливості ресурсів.

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. Наприклад, грамотне управління паролями знижує ризик несанкціонованого доступу.
- 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 і 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.

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.

1.2 Технологія аналізу ризиків

Мета процесу аналізу ризиків полягає у визначенні характеристик ризиків по відношенню до 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 зна-

чущості загроз і вразливостей, ефективність існуючих і планованих засобів захисту і 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. Включає в себе визначення цінності інформаційних ресурсів, оцінку загроз і вразливостей, вибір адекватних контрзаходів, оцінку їх ефективності.

При аналізі ризиків, очікуваний збиток в разі реалізації загроз, порівнюється з витратами на заходи і засоби захисту, після чого приймається рішення щодо оцінюваного ризику, який може бути:

- знижений, наприклад, за рахунок впровадження засобів і механізмів захисту, що зменшують ймовірність реалізації загрози або коефіцієнт руйнування;
- усунутий за рахунок 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;
- прийнятий.

Найбільш трудомістким є процес оцінки ризиків, який умовно можна розділити на наступні етапи: ідентифікація ризику; аналіз ризику; оцінювання ризику.

На рисунку1.2 схематично зображено процес оцінки ризиків інформаційної безпеки.

Рисунок 1.2 - Процес оцінки ризиків інформаційної безпеки

1.1.1 Ідентифікація ризиків

Ідентифікація ризику полягає в складанні переліку та описі елементів ризику: об'єктів захисту, загроз, вразливостей.

Прийнято виділяти такі типи об'єктів захисту:

- інформаційні активи;
- програмне забезпечення;
- фізичні активи;
- сервіси;
- люди, а також їх кваліфікації, навички і досвід;
- нематеріальні ресурси, такі як репутація та імідж організації.

Як правило, на практиці розглядають перші три групи. Решта об'єктів захисту не розглядаються в силу складності 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 даному випадку стандартний список класів ризиків.

Списки класів ризиків містяться в деяких посібниках, в спеціалізованому ПО аналізу ризиків. Прикладом є стандарт BSI [16-17], в якому є каталог загроз стосовно до різних елементів інформаційної технології.

Як правило, для оцінки загроз та вразливостей використовуються різні методи, в основі яких можуть 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.

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 даний 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.

1.2.2 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 бізнес-потреби компанії, її масштаби, а також відповідає кращим світовим практикам і має досить докладний опис процесів і необхідних дій.

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.

У таблиці 1.2 наведено приклад матриці для визначення величини ризику. Така матриця виникає в результаті розгляду ймовірності сценарію інциденту з урахуванням впливу на бізнес. У цій матриці по горизонталі відк-

ладаються якісні значення ймовірності успішної реалізації загрози (сценарію інциденту), а по вертикалі - якісні рівні збитку (впливу на бізнес). Результуючий 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.

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 оціночних 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], в 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 [4, 9, 15-17]. Вибір того чи іншого способу залежить, в першу чергу, від обсягу доступної, в тому числі статистичної, інформації про ризик і необхідної точності оцінок. Також доводиться враховувати фактичний рівень 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.

Всього можна виділити чотири групи методів кількісної оцінки ризиків інформаційної безпеки:

1) статистичні методи;

2) ймовірносно-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.

Використання комбінації статистичних даних і теоретичних гіпотез для оцінки ризику становить основну ідею ймовірносно-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 відноситься 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 і мають відносно невисоку точність, але в ряді випадків є єдиним можливим науково об-

ґрунтованим способом оцінки. Зокрема, вони застосовуються при розробці декларацій промислової безпеки підприємств.

При оцінюванні ризиків рекомендується [2,3] розглядати такі аспекти:

– Шкали і критерії, за якими можна вимірювати ризики.
– Оцінка ймовірностей подій.
– Технології вимірювання ризиків.

1.2.2.1 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.

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. У методиках аналізу ризиків, як правило, використовуються суб'єктивні критерії, вимірювані в якісних шкалах, оскільки:

– Оцінка повинна відображати суб'єктивну точку зору власника інформаційних ресурсів.
– Чи повинні бути враховані різні аспекти, не тільки технічні, але і організаційні, психологічні тощо.

Для отримання суб'єктивної оцінки з оцінкою ризику виходу з ладу ПК, можна використовувати або пряму експертну оцінку, або визначити функцію, яка буде відображати об'єктивну ймовірність в суб'єктивну шкалу ризиків.

Суб'єктивні шкали можуть бути кількісними та якісними, але на практиці, як правило, використовуються якісні шкали з 3-7 градаціями. З одного боку, це просто і зручно, з іншого - вимагає грамотного підходу до обробки даних.

1.2.2.2 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 ймовірнос-

ті. На цьому ж етапі проводиться підготовка експерта або групи експертів, ознайомлення їх з методом і перевірка розуміння поставленого завдання експертами.

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 аксіом ймовірності, яке в тому чи іншому сенсі найближче до оцінок експертів. Особливу важливість третій етап набуває при агрегуванні оцінок, отриманих від групи експертів.

1.2.2.3 Вимірювання ризиків

Сьогодні існує ряд підходів до вимірювання ризиків. Найбільш поширені два підходи до оцінки ризиків: за двома і за трьома чинниками. Оцінка ризиків за двома чинниками. У найпростішому випадку використовується оцінка двох чинників: ймовірність події і тяжкість можливих наслідків. Зазвичай вважається, що ризик тим більше, чим більша ймовірність події і тяжкість наслідків. Загальна ідея може бути виражена формулою 1.1:

$$РИСК = Р_{происшедствие} * ЦЕНА\ ПОТЕРИ \qquad (1.1)$$

Якщо змінні є кількісними величинами - ризик це оцінка математичного очікування втрат.

Якщо змінні є якісними величинами, то метрична операція множення не визначена. Таким чином, в явному вигляді ця формула використовуватися не повинна.

Розглянемо варіант використання якісних величин (ситуація, що найбільш часто зустрічається) [1, 16].

Спочатку повинні бути визначені шкали.

Визначається суб'єктивна шкала ймовірностей подій, приклад такої шкали:

A - Подія практично ніколи не відбувається

B - Подія трапляється рідко

З - Імовірність події за розглянутий проміжок часу ≈0.5

D - Швидше за все, подія відбудеться

E - Подія майже обов'язково станеться

Крім того, визначається суб'єктивна шкала серйозності подій, наприклад:

N - Впливом можна знехтувати

M_i - Незначна подія: наслідки легко переборні, витрати на ліквідацію наслідків не великі, вплив на інформаційну технологію незначний.

M_o - Подія з помірними результатами: ліквідація наслідків не пов'язана з великими витратами, вплив на інформаційну технологію не великий і не зачіпає критично важливі завдання.

S - Подія з серйозними наслідками: ліквідація наслідків пов'язана зі значними витратами, вплив на інформаційні технології відчутний, впливає на виконання критично важливих завдань.

C - Подія призводить до неможливості вирішення критично важливих завдань.

Для оцінки ризиків визначається шкала з трьох значень:

– Низький ризик

– Середній ризик

– Високий ризик

Тоді ризик, пов'язаний з певною подією, залежить від двох чинників і може бути визначений таким чином (див. табл. 1.1).

Таблиця 1.1 - Ризики подій

	N	Mi	Mo	S	C
A	Низкий риск	Низкий риск	Низкий риск	Средний риск	Средний риск
B	Низкий риск	Низкий риск	Средний риск	Средний риск	Высокий риск
C	Низкий риск	Средний риск	Средний риск	Средний риск	Высокий риск
D	Средний риск	Средний риск	Средний риск	Средний риск	Высокий риск
E	Средний риск	Высокий риск	Высокий риск	Высокий риск	Высокий риск

Оцінка ризиків за трьома чинниками. У зарубіжних методиках, розрахованих на більш високі вимоги, ніж базовий рівень, використовується модель оцінки ризику з трьома чинниками: загроза, вразливість, ціна втрати. Загрозу і вразливість визначимо наступним чином:

Загроза - сукупність умов і факторів, які можуть стати причиною порушення цілісності, доступності, конфіденційності інформації.

Уразливість - слабкість в системі захисту, яка робить можливим реалізацію загрози.

Імовірність події, яка в даному підході може бути об'єктивною або суб'єктивної величиною, залежить від рівнів (ймовірностей) загроз і вразливостей:

$$P_{происшествия} = P_{угрозы} * P_{уязвимости} \quad (1.2)$$

Тоді, ризик визначається наступним чином:

$$РИСК = Р_{угрозы} * Р_{уязвимости} * ЦЕНА\ ПОТЕРИ \quad (1.3)$$

Цей вираз можна розглядати як математичну формулу, якщо використовуються кількісні шкали, або як формулювання загальної ідеї, якщо хоча б одна з шкал - якісна. В останньому випадку використовуються різного роду табличні методи для визначення ризику в залежності від трьох чинників.

Наприклад, показник ризику може вимірюватися за шкалою від 0 до 8 і тоді матриця ризиків бути визначена як в таблиці 1.2.

Таблиця 1.2 - Визначення ризику в залежності від трьох чинників

Степень серьезности происшествия (цена потери)	Уровень угрозы								
	Низкий			Средний			Высокий		
	Уровень уязвимостей			Уровень уязвимостей			Уровень уязвимостей		
	Н	С	В	Н	С	В	Н	С	В
N	0	1	2	1	2	3	2	3	4
Mi	1	2	3	2	3	4	3	4	5
Mo	2	3	4	3	4	5	4	5	6
S	3	4	5	4	5	6	5	6	7
C	4	5	6	5	6	7	6	7	8

В даній таблиці рівні уразливості Н, С, В означають відповідно: низький, середній і високий рівні.

Подібні таблиці використовуються як в «паперових» варіантах методик оцінки ризиків, так і в різного роду інструментальних засобах - ПО аналізу ризиків.

1.2.3 Інструментальні засоби аналізу ризиків

Інструментальні засоби аналізу ризиків дозволяють автоматизувати роботу спеціалістів в області захисту інформації, які здійснюють оцінку або переоцінку інформаційних ризиків підприємства.

Спеціалізоване ПЗ, що реалізує методики аналізу ризиків, може відноситись до категорії програмних продуктів (продається на ринку) або бути власністю відомства або організації і не продаватися. Якщо ПЗ розробляється як програмний продукт, воно повинно бути в достатній мірі універсальним. Відомчі варіанти ПЗ адаптовані під особливості постановок задач аналізу та управління ризиками, і дозволяють врахувати специфіку інформаційних технологій організації.

Пропоноване на ринку ПЗ орієнтоване в основному на рівень інформаційної безпеки, який трохи перевищує базовий рівень захищеності. У 2005 році був прийнятий міжнародний стандарт ISO / IEC 27001: 2005, за основу якого було взято Британський стандарт BS 7799. В результаті більшість інструментальних засобів (ПЗ аналізу ризику) було останнім часом модифіковано таким чином, щоб забезпечити відповідність вимогам саме цього стандарту. Давайте розглянемо спеціалізоване ПЗ, яке умовно розділимо на дві групи: ПЗ базового рівня і ПЗ повного аналізу ризиків.

Для розв'язання задачі оцінки ризиків інформаційної безпеки в даний час найбільш часто використовуються наступні програмні комплекси: CRAMM, FRAP, RiskWatch, Microsoft Security Assessment Tool (MSAT), ГРИФ, CORAS і ряд інших. Всі відомі методики 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 цього класу належить методика RiskWatch;
- методики, що використовують змішані оцінки (такий підхід використовується в CRAMM, методикою MSAT).

CRAMM

Дана методика не враховує супровідної документації, такої як опис бізнес-процесів або звітів по проведеним оцінками ризиків. Відносно стратегії

роботи з ризиками CRAMM передбачає використання тільки методів їх зниження. Такі методи управління ризиками, як обхід або прийняття, не розглядаються. У методиці відсутні: процес інтеграції способів управління і опис призначення того чи іншого способу; моніторинг ефективності використовуваних способів управління і способів управління залишковими ризиками; перерахунок максимально допустимих величин ризиків; процес реагування на інциденти.

Практичне застосування CRAMM пов'язане з необхідністю залучення фахівців високої кваліфікації; трудомісткістю і тривалістю процесу оцінки ризиків. Крім того, слід зазначити високу вартість ліцензії.

ГРИФ

Методика ГРИФ використовує кількісні і якісні методи оцінки ризиків, а також визначає умови, при яких останні можуть бути прийняті компанією, включає в себе розрахунок повернення інвестицій на впровадження заходів безпеки. На відміну від інших методик аналізу ризиків, ГРИФ пропонує всі способи зниження ризиків (обхід, зниження і прийняття). Дана методика враховує супровідну документацію, таку як опис бізнес-процесів або звітів по проведеним оцінками ризиків ІБ.

Risk Watch

Ця методика використовує кількісні і якісні методи оцінки ризиків. Трудомісткість робіт з аналізу ризиків з використанням цього методу порівняно невелика. Такий метод підходить, якщо потрібно провести аналіз ризиків на програмно-технічному рівні захисту без урахування організаційних і адміністративних чинників. Істотною перевагою RiskWatch є інтуїтивно зрозумілий інтерфейс і велика гнучкість методу, що забезпечується можливістю введення нових категорій, описів, питань тощо.

CORAS

CORAS не передбачає такої ефективної заходи з управління ризиками, як «Програма підвищення інформованості співробітників в області інформаційної безпеки». Така програма дозволяє знизити ризики ІБ, пов'язані з по-

рушеннями режиму інформаційної безпеки співробітниками компанії через їх необізнаність щодо корпоративних вимог в цій області і правил безпечного використання інформаційних систем. Також в CORAS не передбачена періодичність проведення оцінки ризиків та оновлення їх величин, що свідчить про те, що методика придатна для виконання разових оцінок і не годиться для регулярного використання.

Позитивною стороною CORAS є те, що програмний продукт, який реалізує цю методику, поширюється безкоштовно і не вимагає значних ресурсів для установки і застосування.

MSAT

Ключовими показниками для даного програмного продукту є: профіль ризику для бізнесу (величина зміни ризику в залежності від бізнес-середовища, дійсно, важливий параметр, який не завжди враховується при оцінці рівня захищеності системи в організаціях різних сфер діяльності) та індекс ешелонованого захисту (зведена величина рівня захищеності). MSAT не дає кількісної оцінки рівня ризиків, проте, якісні оцінки можуть бути прив'язані до рангової шкали. MSAT дозволяє оцінити ефективність інвестицій, вкладених у впровадження заходів безпеки, але не дає можливості знайти оптимальний баланс між заходами, спрямованими на запобігання, виявлення, виправлення або відновлення інформаційних активів.

1.3 Основи кластеризації

Цілі кластеризації можуть бути різними в залежності від особливостей конкретної прикладної задачі:

- Зрозуміти структуру множини об'єктів, розбивши його на групи схожих об'єктів. Спростити подальшу обробку даних і прийняття рішень, працюючи з кожним кластером окремо (стратегія «розділяй і володарюй»).

– Скоротити обсяг збережених даних, в разі надвеликої вибірки об'єктів залишивши по одному найбільш типовому представникові від кожного кластера.
– Виділити нетипові об'єкти, які не підходять до жодного з кластерів. Цю задачу називають однокласовою класифікацією, виявленням нетиповісті або новизни.

Кластерний аналіз широко використовується в прогнозуванні поведінки того чи іншого **об'єкта** по набору ознак, що визначають поведінку цього об'єкту.

Основа кластерного аналізу полягає в розподілі множини точок групи таким чином, щоб кожна точка належала тільки одній виділеній підмножині. При цьому в кожній підмножині ділення точки розташовані досить щільно один до одного і є подібними за певними ознаками, в той час як точки, що належать різним підмножини, різнорідні. Ці точки можуть бути змінними, об'єктами, індивідуумами і іншими величинами, які містяться в матриці вихідних даних. Таким чином, за допомогою кластерного аналізу здійснюється угруповання первинних даних, що становить основу подальшої роботи з отриманою інформацією [4].

Методи кластерного аналізу класифікуються за такими ознаками [4, 5, 11]:

– способу обробки даних (ієрархічні, неієрархічні);
– способу аналізу даних (чіткі і нечіткі);
– кількості застосувань алгоритмів кластеризації (з одноетапною, багатоетапною кластеризацією);
– обсягом даних (масштабовані, що не масштабовані);
– часу виконання кластеризації (потокові, що не потокові).

Застосування кластерного аналізу в загальному вигляді зводиться до наступних етапів:

1) Відбір вибірки об'єктів для кластеризації.

2) Визначення множини змінних, за якими будуть оцінюватися об'єкти у вибірці. За необхідності - нормалізація значень змінних.

3) Обчислення значень міри схожості між об'єктами.

4) Застосування методу кластерного аналізу для створення груп схожих об'єктів (кластерів).

5) Представлення результатів аналізу.

В даний час розроблені різні алгоритми кластеризації, які можна розбити на наступні класи [4, 5]:

– Евристичні графові алгоритми
– Статистичні алгоритми (метод к-середніх)
– Кластеризация з частковим навчанням
– Ієрархічна кластеризація

Розглянемо приклад ієрархічного кластерного аналізу.

Першим кроком при практичній реалізації кластерного аналізу є формування матриці спостережень.

Припустимо, у нас є множина об'єктів $\{X_1, X_2, \ldots X_n\}$. Кожен з n об'єктів описується деякою множиною спостережуваних і вимірюваних показників або характеристик.

Вищевказану матрицю спостережень, позначивши її через X, можна представити таким чином:

$$X = \begin{bmatrix} x_{11} & x_{12} & \ldots & x_{1m} \\ x_{21} & x_{22} & \ldots & x_{2m} \\ \ldots & \ldots & \ldots & \ldots \\ x_{n1} & x_{n2} & \ldots & x_{nm} \end{bmatrix} \qquad (1.4)$$

де n - число об'єктів, m - число показників.

Задача кластерного аналізу полягає в тому, щоб на підставі даних, що містяться в матриці X, розбити множину об'єктів $\{X_1, X_2, \ldots X_n\}$ на підмножини так, щоб кожен об'єкт належав одній і тільки одній підмножині розбиття і щоб об'єкти, що належать одній і тій самій підмножині, були подібними, в

той час як об'єкти, що належать різним підмножинам, були різнорідними. Варто відзначити, що ознаки, включені в матрицю спостережень, можуть абсолютно різними, оскільки описують різні властивості об'єктів. Крім того, розрізняються їх одиниці виміру, що ще більш ускладнює їх зіставлення.

Найважливішим поняттям для кількісного відображення подібності пари об'єктів є показник (метрика) близькості між ними. З урахуванням особливості інформаційних систем і простоти обчислення евклідова відстань (квадрат евклідової відстані) є найбільш зручною метрикою. Квадрат евклідової відстані між об'єктами може бути розрахований за формулою (1.5) [4]:

$$d^2(X_iX_j) = \sum_{l=1}^{k}(x_{il} - x_{jl})^2 \qquad (1.5)$$

де x_{il}, x_{jl} - величина компоненти з показником l і-го та j-го об'єкта (l=1,2..k, ij=1,2,3..,n); $d(X_i,X_j)$ - відстань між будь-якою парою досліджуваних об'єктів ($X_1X_2,...X_n$).

Результаты расчетов мер близости могут быть представлены в виде симметричной матрицы расстояний D^2 в формуле 1.5:

$$D^2 = \begin{bmatrix} 0 & d_{12}^2 & d_{13}^2 & \dots & d_{1n}^2 \\ d_{21}^2 & 0 & d_{23}^2 & \dots & d_{2n}^2 \\ d_{31}^2 & d_{32}^2 & 0 & \dots & d_{3n}^2 \\ \dots & \dots & \dots & 0 & \dots \\ d_{n1}^2 & d_{n2}^2 & d_{n3}^2 & \dots & 0 \end{bmatrix} \qquad (1.6)$$

При цьому спочатку елементи множини, що розбивається, розглядаються як окремі кластери, тобто вся множина $\{X_1X_2,...X_j,..X_n\}$ розглядається як множина кластерів$\{\{X_l\}_t\{X_2\},...\{X_j\}, ...\{X_n\}\}$.

Далі об'єднуються два найближчих кластера. Близькість між елементами визначається як мінімум квадрата евклідової відстані між об'єктами:

$$min\{d_{ik}^2\}, j \neq k \qquad (1.7)$$

Нехай це будуть кластери $\{X_j\}$ і $\{X_k\}$. За якимось заздалегідь відомим правилом ці два кластери об'єднуються в новий кластер. Таким чином, нова множина кластерів, що складається вже з $(n-1)$ елементів, буде $\{X_i\}_f\{X_2\}_t...{}_i\{X_j+X_k\},.,.,\{X_l,\}$.

Повторюючи процес, отримаємо послідовні безлічі кластерів, що складаються з $(n-2)$, $(n-3)$ и т.д. кластерів. По завершенню цієї процедури вийде кластер, що складається з n об'єктів і збігається з початковою множиною $\{X_x\}$, $\{X_2\},...,\{X_j\},...,\{X_n\}$.

Вибір числа кластерів, на якому припиняється робота алгоритму, може бути здійснений особою, яка приймає рішення. Основним міркуванням при виділенні будь-якої групи в якості кластера є її стійкість протягом декількох кроків алгоритму. Доцільно брати до уваги відстань між групами, що об'єднуються. Якщо для декількох кроків відстань між групами, що об'єднуються, залишається приблизно однаковою, а потім різко збільшується, то це може бути ознакою того, що об'єднуються два самостійних кластера [5].

Наведемо приклад вищеописаного алгоритму.

Для простоти візьмемо інформаційну систему, кожен елемент якої описуються двома параметрами. Цими параметрами можуть бути, наприклад, ймовірності реалізації двох загроз інформаційній безпеці, виражені в процентах. Припустимо, що матриця спостережень для 10 об'єктів має вигляд, показаний на рисунку 1.3а.

Пронумеруємо об'єкти інформаційної системи від 1 до 10 згідно з початковою матрицею.

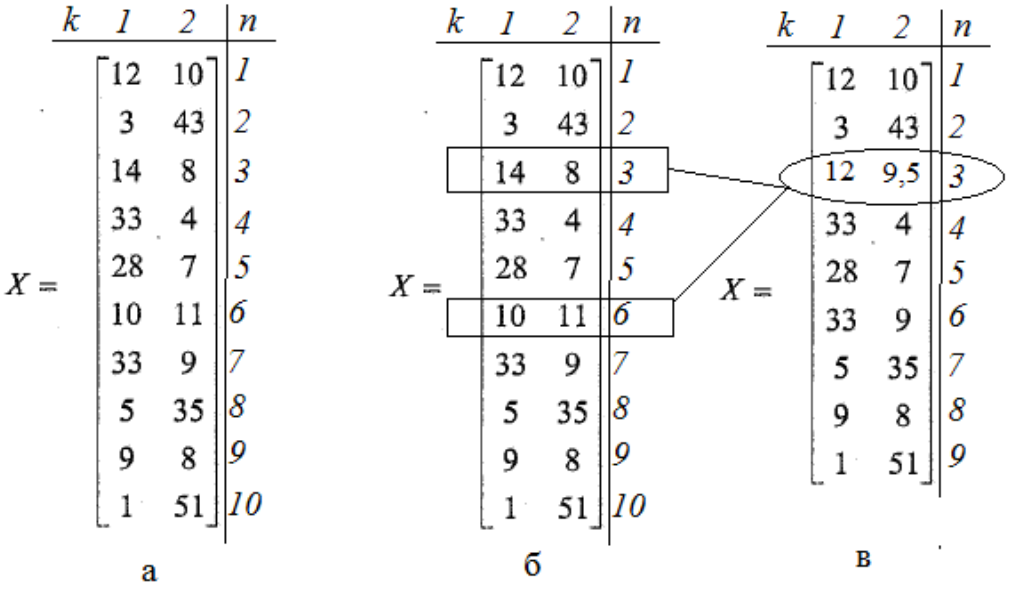

Рисунок 1.3 - Матриці спостережень

Обчислимо d^2_{12}:

$$d^2_{12} = (12-3)^2+(10-43)^2=1170 \quad (1.8)$$

Проводячи аналогічні обчислення для всіх пар, отримаємо матрицю квадратів евклідових відстаней D^2 (див. рис. 1.4), які відповідають першій ітерації розрахунків (виходячи з її симетричності).

	1	2	3	4	5	6	7	8	9	10
1	0	1170	8	477	265	5	442	674	13	1802
2		0	1346	2421	1921	1073	2056	68	1261	68
3			0	377	197	25	362	810	25	2018
4				0	34	578	3233	1745	592	3233
5					0	340	29	1313	362	2665
6						0	533	601	10	1681
7							0	1460	577	2788
8								0	745	272
9									0	1913
10										0

Рисунок 1.4 - Матриця квадратів евклідових відстаней

Результати розрахунку цієї матриці показують, що мінімальні значення евклідових відстаней будуть в 6-му і 3-му об'єктах (див. рис. 1.3б). Об'єднуємо ці об'єкти в один кластер, центр якого буде мати значення 9,5 і 12, що визначає рівновіддалену точку від цих об'єктів (див. рис. 1.5).

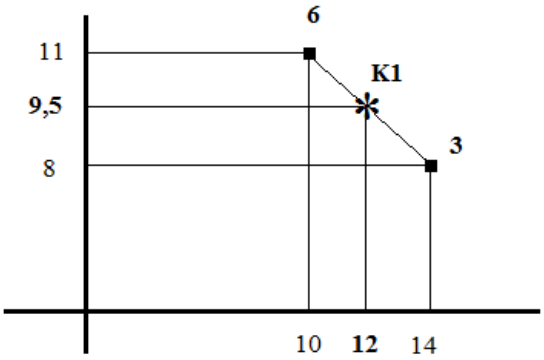

Рис 1.5 - Об'єднання об'єктів в один кластер

Замінюємо в матриці спостережень об'єкти 3 і 6 на отриманий кластер і отримуємо зменшену матрицю спостережень (див. рис. 1.3в)

Повторюючи процес, отримаємо послідовні множини кластерів, що складаються з *(n - 2), (n - 3)* і т. д. кластерів.

Якщо продовжити обчислення до трьох кластерів, то результатом роботи цього алгоритму кластеризації буде розбиття на 3 кластера, що містять такі об'єкти: {1,3,6,9}, {2,8,10}, {4,5,7}.

Вибір числа кластерів, на якому припиняється робота алгоритму, може бути здійснений особою, яка приймає рішення. Основним міркуванням при виділенні будь-якої групи в якості кластера є її стійкість протягом декількох кроків алгоритму. Доцільно брати до уваги відстань між групами, об'єднуються. Якщо для декількох кроків відстань між групами, що об'єднуються залишається приблизно однаковою, а потім різко збільшується, то це може бути ознакою того, що об'єднуються два самостійних кластера.

Кластерний аналіз дозволяє [4] розбити досліджуване простір на підпростори (кластери), де параметри обраної моделі статистично однорідні. Дана властивість корисна при сегментації ризиків в кластер. Це дозволяє виділити однорідні групи ризиків з різними показниками, а також виділити суттєві ризики, що буде корисно для аналізу розвитку динаміки ризиків на підп-

риємстві. Виділення класів за рівнем ризику сприятиме адекватному вибору стратегії управління ризиками для різних класів. На малюнку 1.6 показана схема однієї з можливих інформаційних технологій аналізу ризиків [4], в якій застосовується кластеризація.

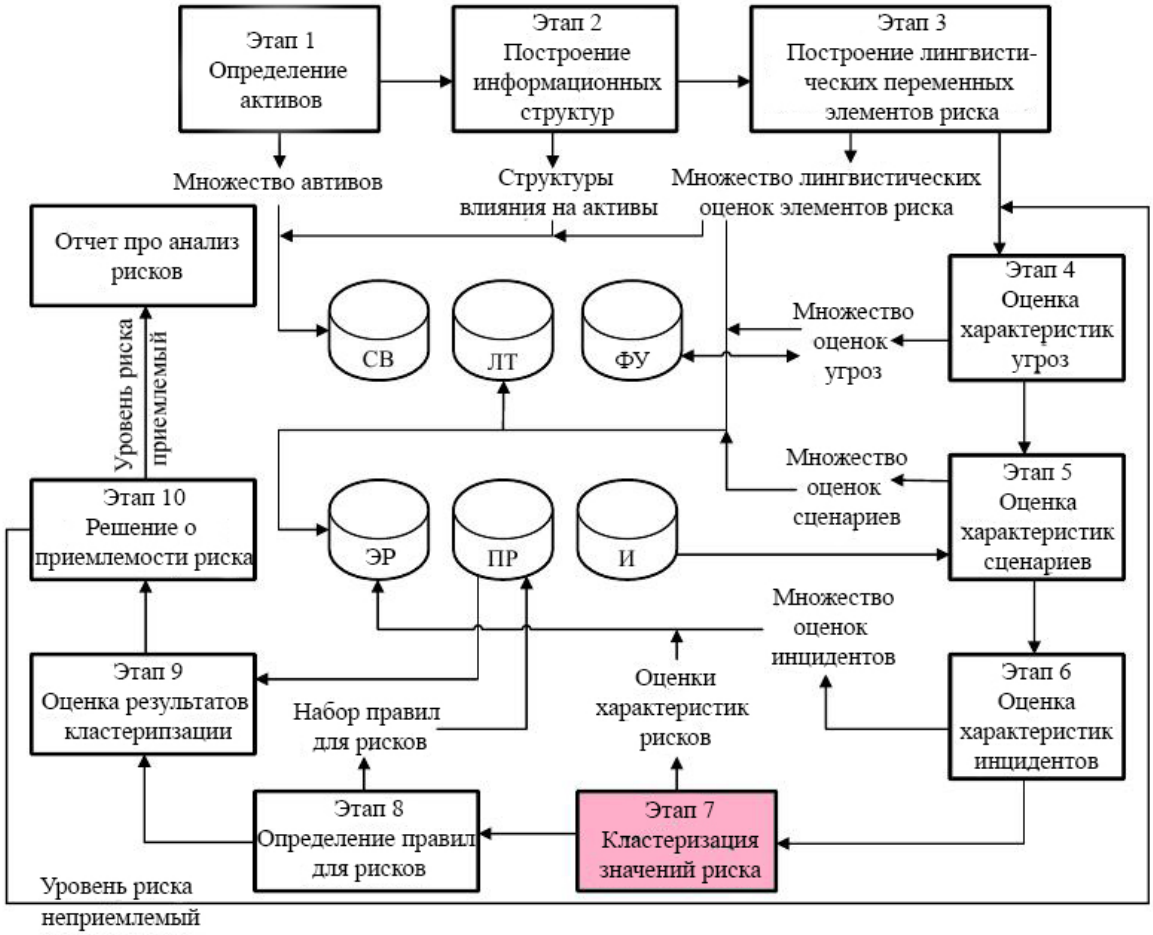

Рисунок 1.6 — Інформаційна технологія аналізу ризиків

де СВ — БД структури впливу на активи;

ЛТ — БД лінгвістичні терми;

ФВ - БД фактори впливу на загрози;

ЭР — БЗ елементи ризику;

ПР — БЗ правила для ризиків;

И - БЗ імітаційне моделювання.

Перевага кластерного аналізу стосовно СМІБ в тому, що він дозволяє виконувати розбивку об'єктів не по одному параметру, а по цілому набору ознак. Дана властивість корисна, так як інформаційні ризики залежать від величезної кількості чинників (джерела загроз, уразливість, ймовірність загрози, цінність активу тощо). При оцінці ризиків інформаційних систем в ряді випадків виникає задача розподілу елементів систем на класи в залежності від значень, вибраних в якості характеристик, по яким проводиться класифікація. Такими характеристиками, наприклад, може стати час експлуатації елемента і розмір матеріальної шкоди в разі його відмови тощо. Крім того, кластерний аналіз дозволяє розглядати досить великий обсяг інформації і різко скорочувати, стискати великі масиви інформації, робити їх компактними і наочними [11]. Тому, його доцільно застосовувати в досить великих організаціях і компаніях, де процес аналізу та управліннями ризиками досить трудомісткий.

Кластерний аналіз на відміну від більшості математико-статистичних методів не накладає ніяких обмежень на вид розглянутих об'єктів, і дозволяє розглядати множину вихідних даних практично довільної природи. Ця властивість корисна при застосуванні комбінованих методів оцінки ризиків, де використовується якісні і кількісні показники. Наприклад, в методиці OCTAVE застосовуються опитувальні листи для складання проблемно-орієнтованих таблиць, де використовуються різні типи даних. Аналіз буде особливо корисний для розбиття думок експертів при відсутності їх узгодженості. Угруповання таких даних кластерним методом, дозволить підвищити об'єктивність отриманих результатів.

Даний вид аналізу також дозволяє проводити вивчення імовірнісних характеристики процесу переходів з кластера в кластер. Ця властивість особливо цінна при виборі стратегій забезпечення КБ на підприємстві, а також при аналізі ефективності впроваджених контрзаходів. Наприклад, ефективність можна оцінити, розглядаючи ймовірності переходу ризиків з кластера "високі ризики" в кластер "низькі ризики" тощо.

При застосуванні кластерного методу в оцінці ризиків СМІБ слід враховувати наступні особливості:

1) Склад і кількість кластерів залежить від обраних критеріїв розбиття. Слід врахувати, що склад і кількість кластерів для різних типів підприємств буде різнитися. Тому доцільно передбачити так звані "профілі" для різних типів підприємств з характерними ознаками.

2) Основним критерієм якості та обґрунтованості отриманого розбиття є змістовний аналіз результатів, заснований на осмисленні дослідником можливих причинних механізмів відокремлення отриманих груп об'єктів. Для оцінки ризиків інформаційної безпеки може використовуватися підхід, в якому кожна ітерація кластеризації повинна бути оцінена експертом.

3) Ознаки, включені в матрицю спостережень, неоднорідні, оскільки описують різні властивості об'єктів. Необхідно виконувати попереднє перетворення, яке полягає в стандартизації ознак. Стандартизація, таким чином, являє собою перехід до деякого однакового опису для всіх ознак, до введення нової умовної одиниці, що допускає формальне зіставлення об'єктів.

4) При зведенні вихідного масиву даних до більш компактного виду можуть виникати певні спотворення, а також можуть губитися індивідуальні риси окремих об'єктів за рахунок заміни їх характеристиками узагальнених значень параметрів кластера. Наприклад, при оцінці різних активів в грошовому вираженні об'єкти можуть бути згруповані за фінансовими збитками, при цьому не будуть враховані відмінності впливу на безпеку інших об'єктів тощо. На думку авторів, цей недолік є неминучою "жертвою" при використанні даного методу. Завдання розробника системи мінімізувати ці втрати.

5) Завдання кластеризації відноситься до статистичної обробки. При цьому основним недоліком є залежність від обсягу накопиченої статистики у вигляді експертних або кількісних оцінок.

Наведений аналіз вказує на той факт, що при "поверхневому" розгляді конкретної системи (підприємства) велика ймовірність неточної кластеризації для оцінки ризиків ІБ. Тому універсальні програмні продукти, що викори-

стовуються для оцінки ризиків ІБ з використанням кластеризації, імовірно можуть мати багато неточностей, які будуть негативно відбиватися на кінцевому результаті. Доцільно використовувати кластерний аналіз в великих організаціях, де існують схожі за типами ризики в різних інформаційних системах. Для отримання максимального ефекту від використання кластерного аналізу необхідно передбачити так звані "профілі" для різних типів підприємств з характерними ознаками показників, за якими буде відбуватися групування.

Висновки до розділу 1

У цьому розділі:

1. Описано ризики в системі забезпечення інформаційної безпеки організації.
2. Показані існуючі технології аналізу ризиків ІБ.
3. Наведено теоретичні основи кластеризації.

РОЗДІЛ 2
ОЦІНКИ РИЗИКІВ З ВИКОРИСТАННЯМ МЕТОДУ К-СЕРЕДНІХ

2.1 Опис методу к-середніх

Припустимо, є гіпотези щодо числа *m* кластерів (по змінним або спостереженням).

Тоді можна задати програмі створити рівно *m* кластерів так, щоб вони були настільки різні, наскільки це можливо. Саме для вирішення завдань цього типу призначений метод *k-means* (к-середніх). Гіпотеза може ґрунтуватися на теоретичних міркуваннях, результати попередніх досліджень або здогаду. Виконуючи послідовне розбиття на різне число кластерів, можна порівнювати якість одержуваних рішень.

Принцип кластеризації методом к-середніх описується наступним алгоритмом

1. Випадковим чином в просторі призначається m центрів майбутніх кластерів.
2. Створюється m порожніх множин R_i (i = 1 ... m).
3. Для всіх k об'єктів розраховується евклідова відстань до кожного центру кластера (центроїда):

$$d^2(X_i, X_j) = \sum_{l=1}^{k} (x_{il} - x_{jl})^2 \quad (2.1)$$

4. З усіх m відстаней від j-об'єкта до i-центроїда визначається найменша відстань і цей об'єкт входить до відповідного безліч R_i. Тобто кожен об'єкт «приписується» до свого центру.

5. Після того як всі об'єкти «приписані» до відповідним множинам, розраховується середнє значення координат кожного безлічі. Ці середні координати є координатами нових центроїдів, і процес повторюється з п. 2.
6. Цей процес повторюється до тих пір, поки центри тяжіння не перестануть «мігрувати» в просторі.

Існує варіант МакКін алгоритму к-середніх, який відрізняється тим, що кожного разу, коли деякий об'єкт X_i переходить з одного кластера в інший, центри обох кластерів перераховуються.

Алгоритм к-середніх (k-means) вкрай чутливий до вибору початкових наближень центрів. Випадкова ініціалізація центрів на кроці 1 може призвести до поганих кластеризацій.

Для формування початкового наближення можна виділити m найбільш віддалених точок вибірки: перші дві точки виділяються по максимуму всіх попарних відстаней; кожна наступна точка вибирається так, щоб відстань від неї до найближчої вже виділеної було максимальною.

Інша рекомендація - виконати кластеризацію кілька разів, з різних випадкових початкових наближень і вибрати кластеризацію з найкращим значенням заданого функціонала якості.

Кластеризація може виявитися неадекватною і в тому випадку, якщо число кластерів буде спочатку невірно угадано. Стандартна рекомендація провести кластеризацію при різних значеннях m і вибрати те, при якому досягається різке поліпшення якості кластеризації по заданому функціоналу.

На рисунку 2.1 показана картинка, яка приблизно демонструє роботу цього алгоритму:

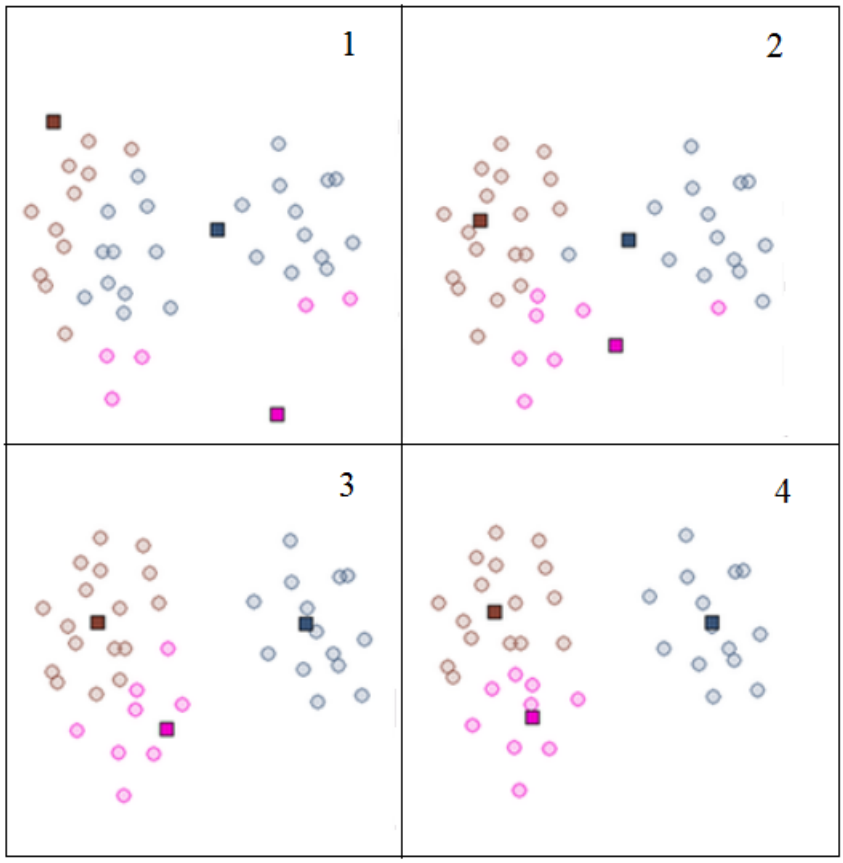

Рисунок 2.1 - Демонстрація методу к-середніх

2.2 Методика аналізу ризиків з використанням методу к-середніх

Оцінка ризиків ІБ розглядається в ISO / IEC 27001: 2005 як процес [16]. Вхідними даними цього процесу є область дії, кордони і встановлена організація (структура) процесу управління ризиками ІБ [16,17].

Суть процесу оцінки ризиків ІБ полягає в їх ідентифікації, кількісному або якісному описі і пріоритетності відповідно до критеріїв і завдань оцінювання ризиків ІБ, які можуть застосовуватися до організації. Оскільки ризики ІБ є комбінацією наслідків, що виявляються в результаті реалізації небажаних подій і ймовірності їх виникнення, кількісна або якісна оцінка ризиків ІБ описує ці ризики і дозволяє керівництву встановити пріоритети ризиків ІБ відповідно до їх очікуваної значущості (серйозності) або іншим встановленим критеріям.

Згідно [16] діяльність з оцінки ризиків ІБ включає наступні складові:

1) аналіз ризиків ІБ;

2) оцінювання ризиків ІБ.

Справжня методика призначена для проведення **аналізу ризиків** інформаційної безпеки (ІБ) в рамках побудови або вдосконалення системи інформаційної безпеки на підприємствах малого та середнього бізнесу.

Основним завданням розв'язуваної за допомогою цієї методики полягає у визначенні чисельного показника ризику з метою прийняття ефективних заходів щодо захисту інформації.

У цій методиці процедура кількісної оцінки ризиків реалізації хоча б однієї загрози з усього переліку актуальних загроз визначається **щодо кожного типу активу**, на який впливає сукупність загроз ІБ, що дозволяє дискретно визначити ризик настання несприятливих подій на кожен тип активу.

Передбачається, що в результаті такого аналізу можна буде отримати якісну динаміку ризиків, що сприятиме адекватному вибору стратегії управління ризиками.

Запропонована методика дозволяє виконати повноцінний аналіз та оцінку ризиків тільки з залученням експертів.

2.2.1 Опис методики аналізу ризиків

У розділі 1 описано, що кількісна оцінка ризиків інформаційної безпеки в більшості випадків оцінюється за трьома факторами представляється у вигляді формули:

$$R = P(v) * P(t) * S \qquad (2.2)$$

де S - цінність активу (ступінь тяжкості наслідків),

$P(v)$ - ймовірність реалізації загрози інформаційної безпеки,

$P(t)$ - ймовірність використання уразливості.

Деякі загрози ІБ можуть ставитися відразу до кількох активів і навпаки - для одного активу можуть існувати кілька загроз різних класів.

В роботі [6] показані відмінності між ризиками для конфіденційності, цілісності і доступності і при цьому використовуються відповідні значення вартості активу в якості величини збитку і, внаслідок цього, для кожного активу розглядаються три різних ризику ІБ.

Там же пропонується розділити процедуру розрахунку ризику на наступні етапи:

– обчислення значення технічного ризику;
– обчислення потенційного збитку.

Під технічним ризиком мається на увазі значення ризику інформаційної безпеки, що складається з ймовірностей реалізації загроз і використання вразливостей кожного компонента інформаційної інфраструктури з урахуванням рівня їх конфіденційності, цілісності та доступності.

Для першого етапу можна навести такі формули:

$$R_c = K_c \cdot P(T) \cdot P(V); \quad (2.3)$$

$$R_i = K_i \cdot P(T) \cdot P(V); \quad (2.4)$$

$$R_a = K_a \cdot P(T) \cdot P(V), \quad (2.5)$$

де R_c - значення ризику конфіденційності;

K_c - коефіцієнт конфіденційності інформаційного активу;

$P(T)$ - ймовірність реалізації загрози;

$P(V)$ - ймовірність використання вразливості;

R_i - значення ризику цілісності;

K_i - коефіцієнт цілісності інформаційного активу;

R_a - значення ризику доступності;

K_a - коефіцієнт доступності інформаційного активу.

Далі обчислюється значення збитку. Для цього використовується усереднене значення ризику кожного інформаційного активу і розмір потенційних втрат. Значення шкоди (L) розраховується за такою формулою:

$$L = R_{cp} \cdot S \qquad (2.6)$$

де R_{cp} - середнє значення ризику,

S - ступінь тяжкості наслідків, ум. од.

Стверджується що, застосування даного методу розрахунку дозволить зробити більш детальну оцінку ризику і отримати в результаті значення ймовірності виникнення ризику компрометації кожного інформаційного активу окремо.

Скористаємося цією методикою для подання ризиків у вигляді тривимірної матриці (див. рис. 2.2) елементами *Kxyz* якої будуть значення коефіцієнтів K_c, K_a, K_i, а її індексами будуть наступні показники:

– загрози ІБ (можливі події);

– види загроз по цілі впливу;

– вид інформаційних активів.

Візьмемо для прикладу такі сценарії інцидентів ІБ:

i=1– несанкціонована зміна повноважень на доступ в обхід механізмів захисту;

i=2 – ненавмисне зараження комп'ютера вірусами;

i=3 – пошкодження даних на носії;

i=4 – переривання обслуговування.

і такі активи:

j=1 – база даних програми 1С бухгалтерія

j=2 – документи щодо укладення контрактів

j=3 – жорсткий диск сервера

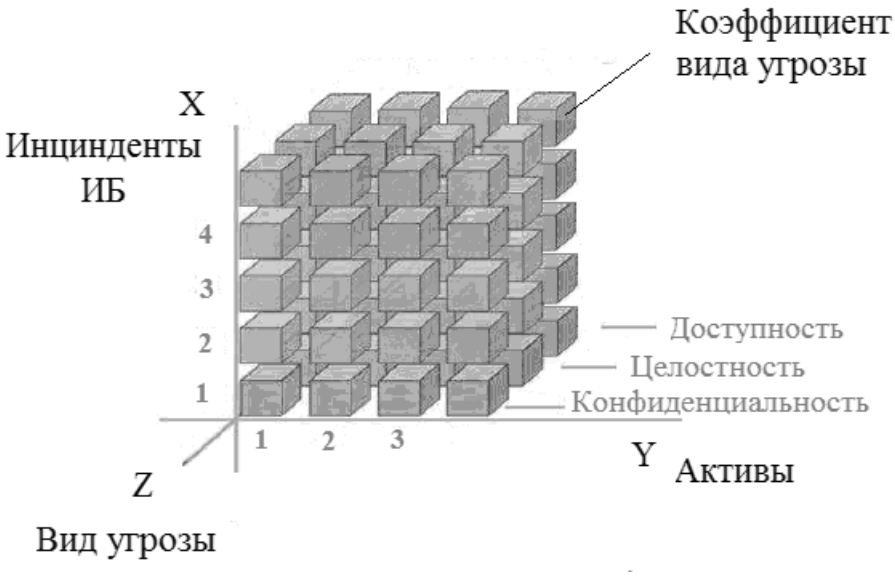

Рисунок 2.2 - Матриця коефіцієнтів

Тоді K_{121} буде позначати значення коефіцієнта K_a при реалізації атаки на документи щодо укладення контрактів при якій буде порушена їх доступність (див. рис. 2.2).

З метою виділення однорідних груп ризиків з різними показниками застосуємо кластерний аналіз і розіб'ємо весь досліджуваний простір ризиків на 3 кластера - високого, середнього та низького рівня ризиків. Тоді кількість елементів у відповідному кластері буде визначати пріоритет ризиків ІБ відповідно до їх очікуваної значущості.

2.2.3 Порядок виконання процедур аналізу ризиків

2.2.3.1 Етапи аналізу ризиків

Для визначення величини ризиків ІБ необхідно виконати кілька етапів з аналізу ризиків.

Етап 1 - ідентифікація активів.

Етап 2 - ідентифікація загроз ІБ.

Етап 3 - ідентифікація існуючих засобів управління ризиками ІБ.

Етап 4 - ідентифікація вразливостей.

Етап 5 - ідентифікація наслідків.

Етап 6 - оцінка ймовірностей.

Етап 7 - визначення рівня (величини) ризиків ІБ.

І тільки після виконання цих етапів можна переходити до кількісної оцінки ризиків ІБ.

Коротко розглянемо зміст цих етапів.

Етап 1 - Ідентифікація активів

Суть процесу ідентифікації активів визначена в [7, 8] і зводиться до виявлення (інвентаризації) всіх активів у встановленій області дії оцінки ризиків ІБ. Опису активів допомагають забезпечити наявність результативної захисту активів.

Основними активами будь-якої організації є: бізнес-процеси (підпроцеси) і бізнес-діяльність; інформація.

До допоміжних активів відносяться апаратні засоби, носії даних, ПО, бізнес-додатки, мережі, персонал.

До активів організації можна віднести:

- фізичні об'єкти: обладнання та апаратура зв'язку, носії інформації, інше технічне обладнання і приміщення, використовувані для підтримки обробки інформації;
- програмні ресурси: прикладне ПО, системне ПО, додатки операційної системи (ОС), самі ОС, процеси, породжувані ОС, засоби розробки, сервіс DNS-імен, поштові клієнти, веб-браузери, віддалені термінали і т. д .;
- різні види інформаційних ресурсів - службова інформація, фінансово-аналітична, керуюча тощо;
- процеси, включаючи технологічні і бізнес-процеси (бізнес-плани, фінансові кошториси, прогнози, аналітична інформація, системна документація, експлуатаційні або підтримують процедури, заходи з нейтралізації ризиків ІБ тощо);

– продукти і послуги, що надаються клієнтам організації: обчислювальні і комунікаційні сервіси (наприклад, Інтернет).

Для кожного активу або групи активів обов'язково визначається їх власник, що забезпечує відповідальність за активи і їх облік. Ідентифікація активів виконується з відповідним ступенем деталізації, необхідної для отримання інформації для правильної оцінки ризиків ІБ і може здійснюватися за допомогою, наприклад, інтерв'ювання або анкетування їх власників. Тоді для кожного з активів складаються анкети, які включають відомості, що характеризують даний актив.

Також обов'язково виявляються види залежностей одних активів від інших, оскільки їх наявність може вплинути на оцінку активів.

Результатом процесу ідентифікації активів є два обґрунтованих списку - активів, схильних до ризиків ІБ, котрі відносяться до даної області дії СУІБ, за їх місцезнаходженням та власниками і бізнес-процесів, пов'язаних з цими активами.

Етап 2 - Ідентифікація загроз ІБ

Згідно з ISO / IEC 27005: 2011 вихідними даними для процесу є інформація про загрози ІБ, отримана зі звітів про інциденти ІБ, від власників активів, користувачів і з інших джерел, включаючи зовнішні каталоги загроз ІБ.

Основним видом дій на даному етапі є ідентифікація загроз ІБ і їх джерел.

Джерело загрози ІБ - це суб'єкт (фізична особа, матеріальний об'єкт або фізичне явище), що активізує загрозу ІБ і переводить її з розряду потенційної небезпеки порушення властивостей ІБ (конфіденційності, доступності, цілісності тощо) активів організації в реальне порушення цих властивостей.

Джерела загроз ІБ можна розділити на три класи: антропогенні, техногенні та стихійні.

Згідно з вже класичним підходом для інформації взагалі виділяються різні загрози ІБ, пов'язані з її основними властивостями:

- конфіденційності - розкрадання (копіювання) інформації і засобів її обробки тощо;
- цілісності - модифікація (спотворення) інформації, заперечення її справжності, нав'язування неправдивої інформації тощо;
- доступності - блокування інформації;
- знищення інформації і засобів її обробки тощо;
- неспростовності - відмова користувача від факту виконання ним транзакції тощо;
- автентичності - відмова від авторства щодо електронного документа тощо;
- обліковості - відсутність місця на жорсткому диску для запису всіх подій тощо;
- функціональності - коли немає відповідності між навмисною поведінкою користувача і результатами роботи додатків.

Існують і інші види класифікацій. Так, загрози ІБ бувають випадковими і навмисними, зовнішніми і внутрішніми, такими, що викликають несанкціоновані дії, фізичний збиток або відмови устаткування. Вони можуть завдати шкоди інформації, процесам, системам і організації в цілому. Деякі загрози ІБ можуть відноситися відразу до кількох активів і навпаки - для одного активу можуть існувати кілька загроз різних класів.

При проведенні оцінки ризиків ІБ всі типи загроз ІБ для активів організації та їх джерела ідентифікуються і відносяться до певних класів.

Для визначення ймовірності реалізації загрози ІБ вихідні дані можна отримати від власників активів і користувачів, співробітників, керівників об'єктів, фахівців з ІБ, експертів з фізичного захисту та інших організацій.

Важливо застосовувати в нових умовах і власний досвід інцидентів ІБ, що відбувалися раніше, і минулих оцінок загроз ІБ, але пам'ятаючи, що в середовищі ведення бізнесу і в ІС і в ІТ відбуваються постійні зміни. Також ва-

рто звернутися до статистик загроз ІБ (можливо, специфічних для організації або її бізнесу), що допоможе створити найбільш повний список загроз ІБ, які можна застосувати до організації.

Приклади загроз ІБ відповідно до ISO / IEC 27002: 2005 наведені в додатку.

Етап 3 - Ідентифікація існуючих засобів управління ризиками ІБ

Під засобами управління ризиками ІБ маються на увазі існуючі процеси, політики, пристрої, практики та інші дії, включаючи захисні заходи, які мінімізують негативні ризики або підвищують позитивні можливості для забезпечення достатньої впевненості щодо досягнення поставлених цілей в області ОІБ, а також будь-яка міра або дія, яка модифікує ризик ІБ.

На основі наявних даних необхідно ідентифікувати існуючі і плановані до використання засоби управління, що реалізують ОІБ для кожного з активів. Якщо засоби управління не працюють, як це очікувалося, то можуть виникнути вразливості.

Слід окремо розглянути ситуації, коли обраний засіб управління (або стратегія) не виконує свої функції і, отже, потрібні додаткові кошти для ефективного усунення виявлених ризиків ІБ. Способом оцінити дієвість засобу є з'ясування того, як це засіб знижує ймовірність реалізації загрози ІБ, ускладнює використання вразливостей або пом'якшує наслідки інциденту ІБ.

Аналіз з боку керівництва і аудиторські звіти дають інформацію про ефективність існуючих засобів управління. Плановані до використання відповідно до планів обробки ризиків ІБ засоби управління розглядаються аналогічно як і вже існуючі засоби. Існуючі та заплановані кошти управління можуть бути ідентифіковані як неефективні, недостатні або невиправдані. У двох останніх випадках ці кошти необхідно перевірити для визначення того, чи варто їх видалити, замінити іншими більш придатними, або залишити, наприклад, з міркувань вартості.

Для ідентифікації існуючих і запланованих коштів управління можуть бути корисні наступні дії [3, 4]:

- перегляд документів, що містять інформацію про засоби управління (наприклад, плани обробки ризиків ІБ);
- перевірка, яка проводиться спільно з відповідальними за ОІБ і користувачами інформаційних процесів в ІС, для яких реально реалізовані засоби управління, що розглядаються;
- аналіз на місці фізичних засобів управління, порівняння реально реалізованого і того, що повинно бути, і перевірка коректності та ефективності реалізації;
- розгляд результатів внутрішніх аудитів ІБ.

Вихідними даними процесу є список існуючих і запланованих коштів управління ризиками ІБ і інформація про стан їх впровадження і використання.

Етап 4 - Ідентифікація вразливостей

На цьому етапі ідентифікуються вразливості, які можуть бути використані загрозами ІБ (точніше джерелами загроз ІБ) для заподіяння шкоди активів або всієї організації в цілому.

Існує кілька різних класифікацій вразливостей [9-10, 12]: за причинами виникнення, за місцем знаходження, за ступенем критичності наслідків від її використання погрозами ІБ, а також за ймовірністю реалізації.

За причинами виникнення вразливості поділяються на три класи:

- проектування, що використовують аналіз алгоритму ПЗ і АЗ;
- реалізації, що використовують аналіз вихідного тексту (його синтаксису, семантики, конструкцій тощо) або виконуваного файлу (його атрибутів, процесу виконання - операції з пам'яттю, робота з покажчиками, виклик функцій), зовнішніми впливами- коли на вхід подаються різні граничні і малоймовірні значення змінних, а також значення змінних отриманих при дизасемблювання і аналізу коду;
- експлуатації, включаючи слабкості системної політики, помилки налаштування ПЗ і АЗ та ін.

За місцем знаходження вразливості можуть бути ідентифіковані в наступних областях:

- організація в цілому;
- її процеси і процедури (організація робіт);
- усталена практика управління і адміністрування;
- персонал;
- фізичне середовище;
- конфігурації ІС;
- апаратне, програмне і телекомунікаційне обладнання;
- залежність від зовнішніх сторін.

Вразливість може бути присутня в активі, а може перебувати і в засобі забезпечення його ІБ. Також виділяють вразливості на рівні мережі, окремого хоста (пристрої з унікальною адресою) або додатка.

За ступенем критичності (рівнем ризику) вразливості діляться наступним чином:

- високий рівень ризику - вразливості, що дозволяють атакуючому отримати доступ до хосту з правами суперкористувача, а також вразливості, які роблять можливим обхід засобів захисту для потраплянння в інтернет організації;
- середній рівень ризику - вразливості, що дозволяють атакуючому отримати інформацію, яка з високим ступенем ймовірності дозволить отримати доступ до окремого хосту і вразливості, що призводять до підвищеної витрати ресурсів системи (за рахунок атак «відмова в обслуговуванні»);
- низький рівень ризику - вразливості, що дозволяють здійснювати збір критичної інформації про систему (наприклад, невикористовувані служби, поточний час на комп'ютері для подальших атак на криптоалгоритми тощо).

Вразливості можна оцінити по ймовірності реалізації на її основі загрози ІБ, наприклад:

- з високою ймовірністю або ймовірна - дану уразливість легко використовувати, захист відсутній або дуже слабкий;
- можлива - вразливість може бути використана, але є захист;
- малоймовірна або неможлива - дану уразливість використовувати важко, є хороший захист.

Сама по собі вразливість (просто її наявність) не завдає шкоди - для цього потрібні: загроза ІБ і її джерело, які нею скористаються. Вразливість лише створює потенційні умови для реалізації загрози ІБ.

Вразливість, для якої не виявлено відповідної загрози ІБ, може і не вимагати реалізації засобів управління, але вона все одно повинна бути усвідомлена і повинен здійснюватися моніторинг її змін. І навпаки, загроза ІБ, для реалізації якої в системі немає вразливості, не актуальна для цієї системи і не тягне за собою ризику ІБ. Вразливості можуть бути пов'язані з властивостями активу. Спосіб і цілі використання активу можуть відрізнятися від планованих при його придбанні або створенні. Необхідно враховувати вразливості різного походження, наприклад, внутрішні чи зовнішні по відношенню до даного активу.

Вихідними даними цього етапу є ймовірності P (V) використання вразливостей активів.

Етап 5 Ідентифікація наслідків.

Згідно з ISO / IEC 27005: 2011 вхідними даними процесу є списки активів, бізнес-процесів, загроз ІБ і вразливостей (при можливості із зазначенням активів) і їхня соціальна вагомість. Повинні бути визначені прямі і непрямі наслідки можливої втрати активами конфіденційності, цілісності і доступності, викликаної інцидентами ІБ. Такими наслідками можуть бути зниження ефективності, несприятливі операційні умови, втрата бізнесу, збиток для репутації тощо. Можливі сценарії інцидентів ІБ описуються як реалізації загроз ІБ на основі використання однієї або декількох існуючих вразливостей.

Вплив інциденту ІБ визначається з урахуванням критеріїв оцінки наслідків, виділених в процесі встановлення контексту управління ризиками ІБ. Наслідки можуть торкнутися одного або кількох активів або частини активу, можуть носити тимчасовий і постійний характер (як у випадку руйнування активу). Активи при їх пошкодженні або компрометації, можуть бути співставлені як зі значення фінансових втрат, так і з наслідками для всього бізнесу організації.

Негативні наслідки від впливу ризиків ІБ можуть бути двох типів:

– миттєві наслідки, наприклад, відмова обладнання;
– накопичувані наслідки, наприклад, відмова обладнання в результаті вичерпання його ресурсу.

Вихідні дані етапу подаються у вигляді списку сценаріїв інцидентів ІБ з їх наслідками для конкретних активів і бізнес-процесів.

Етап 6 - Оцінка ймовірностей

Згідно з ISO / IEC 27005: 2011 вхідні дані процесу - список можливих ідентифікованих сценаріїв ІБ, включаючи ідентифіковані загрози ІБ, активи, використані вразливості і наслідки для активів і бізнес-процесів, а також списки всіх існуючих і запланованих елементів управління ризиками ІБ, їх ефективність, статус впровадження і використання.

Повинні бути оцінені ймовірності реалізації конкретних сценаріїв інцидентів ІБ. При цьому найчастіше застосовуються три підходи:

– історичні дані,
– передбачення ймовірностей;
– експертні оцінки.

Після ідентифікації сценаріїв інцидентів ІБ необхідно оцінити ймовірність реалізації кожного сценарію і прояви наслідків інциденту ІБ, використовуючи якісні та кількісні підходи.

При цьому враховується наступне:

- наскільки часто реалізуються загрози ІБ, і наскільки просто використовувати вразливості, розглядаючи досвід і відповідні статистичні дані по можливостям реалізації загроз ІБ;
- вразливості, що розглядаються окремо і спільно, що може багаторазово збільшити втрати організації;
- загрози ІБ, що розглядаються окремо і спільно, що може багаторазово збільшити втрати організації;
- ймовірність реалізації деякої комбінації загроз ІБ і вразливостей;
- для умисних джерел загроз ІБ - мотивація і можливості, які змінюються з часом, а також ресурси, доступні потенційним зловмисникам;
- для випадкових джерел загроз ІБ - наскільки часто вони можуть виникати, відповідно до досвіду, статистикою тощо;

Залежно від необхідної точності, активи можуть бути згруповані або навпаки - один актив може бути розділений на елементи, що, в кінці кінців, повинно бути зв'язане зі сценаріями інцидентів ІБ. Інформація, яка використовується для оцінки загроз ІБ і вразливостей, може бути отримана від тих, хто має відношення до даної СУІБ і відповідних бізнес-процесів.

Вихідними даними цього етапу є ймовірності P (T) реалізації сценаріїв інцидентів ІБ.

Етап 7 - Визначення рівня (величини) ризиків ІБ

Отримавши значення ймовірностей P (T) сценаріїв інцидентів ІБ (етап 6) і ймовірностей P (V) використання вразливостей активів (етап 4) експертним шляхом для кожного активу визначаються відповідні коефіцієнти: коефіцієнт конфіденційності інформаційного активу, коефіцієнт цілісності інформаційного активу і коефіцієнт доступності інформаційного активу (див. 2.2.1).

Таким чином, всі необхідні дані для виконання кількісного аналізу ризиків отримані.

2.3 Реалізація методу к-середніх при аналізі ризиків

Наведемо методику для активів і загроз наведених у розділі на умовному спрощеному прикладі. Припустимо після виконання всіх етапів по аналізу ризиків, зазначених в п. 2.2.2 за методикою показаною в п. 2.2.1, отримані кількісні оцінки ризиків R для 3-х активів А при 4-х можливих реалізаціях сценаріїв інцидентів для трьох типів загроз.

Тобто є 3 таблиці виду 2.1.

Таблиця 2.1 – Оцінка ризиків

Активы	Инциденты нарушения ИБ			
	$У_1$	$У_2$	$У_3$	$У_4$
A_1	R_{1k}	R_{2k}	R_{3k}	R_{4k}
A_2	R_{5k}	R_{6k}	R_{7k}	R_{8k}
A_3	R_{9k}	R_{10k}	R_{11k}	R_{12k}

де k- тип класу загроз:

k=1 – порушення цілісності,

k=2 – порушення доступності,

k=3 – порушення конфіденційності.

Ці таблиці фактично представляють собою матриці спостережень, що використовуються в кластерному аналізі (див.п.1.4).

Припустимо, що для всіх них проведено кластерний аналіз методом к-середніх і отримані результати, показані на рис 2.3.

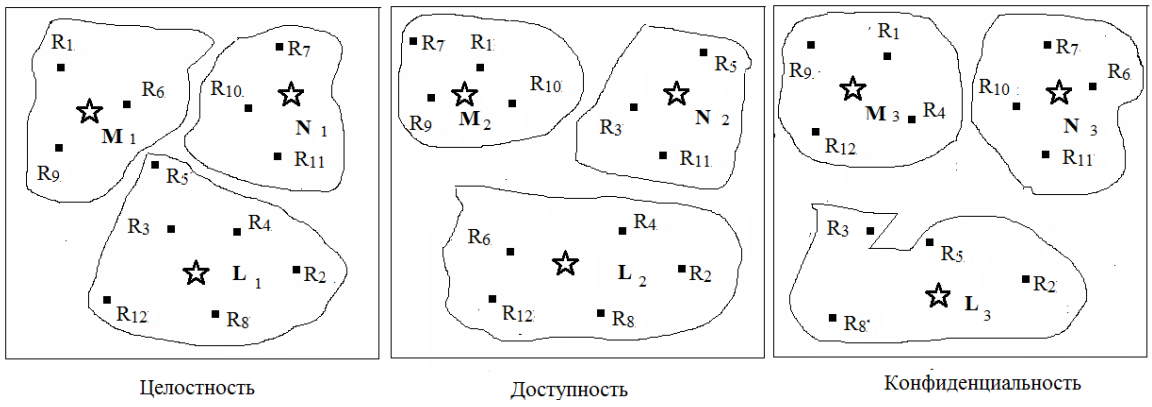

Рис 2.3 - Результати кластерного аналізу

На рис. 2.3: M-високий ризик; N - середній ризик; L - низький ризик.

Для кожного об'єкта визначимо тип кластера, в якому він знаходиться по кожному типу загроз (див. табл. 2.2).

Таблиця 2.2 - Належність об'єктів

Оценка	Целостность	Доступность	Конфиденц.
R1	M	M	M
R2	L	L	L
R3	L	N	L
R4	L	L	M
R5	L	N	L
R6	M	L	N
R7	N	M	N
R8	L	L	L
R9	M	M	M
R10	N	M	N
R11	N	N	N
R12	L	L	M

Далі з таблиці визначимо, які об'єкти знаходяться в одних і тих же кластерах, створимо їх множини і випишемо їх в окрему таблицю 2.3.

Таблиця 2.3 - Множини об'єктів з однаковими узагальненими параметрами

№ множества	Имя множества	Оценки
1	MMM	R1,R9
2	LLL	R2, R8
3	LNL	R3, R5
4	LLM	R4, R12
5	MLN	R6
6	NMN	R7, R10
7	NNN	R11

Оцінки ризику, що належать одній і тій же множині, володіють деякими однаковими узагальненими характеристиками, і тому така таблиця може служити показником оцінки всіх ризиків для розглянутих активів при розглянутих сценаріях інцидентів ІБ.

Крім цього результату можна отримати і її інтегральну оцінку - частоту рівнів ризику за видами вразливостей.

Для нашого прикладу частота появи M-6, N-7, L-8.

Висновки до розділу 2

У цьому розділі дипломної роботи:

1. Описано метод к-середніх;

2. Описана запропонована методика аналізу ризиків;

3. Описано основні етапи вихідних даних для виконання аналізу ризиків;

4. Із застосуванням умовного спрощеного прикладу описаний метод якісної оцінки ризиків з використанням методу кластеризації «к-середніх».

РОЗДІЛ 3
ЕКОНОМІЧНИЙ РОЗДІЛ

Даний дипломний проект передбачає розробку політики безпеки, що є концептуальною та методологічною основою щодо забезпечення інформаційної безпеки.

Вихідною посилкою при організації інформаційної безпеки є припущення, що з одного боку, при порушенні системи захисту інформації завдається шкода, з іншого боку - забезпечення інформаційної безпеки пов'язане з витрачанням коштів. Економічно доцільним буде вважатися, якщо витрати на забезпечення інформаційної безпеки не будуть перевищувати збиток при реалізації можливої загрози. Тому для обґрунтування економічної доцільності розробки і впровадження політики інформаційної безпеки необхідно розрахувати збитки від реалізації можливих загроз і порівняти їх з витратами на розробку і впровадження політики безпеки.

Розрахунок збитку від реалізації можливої атаки здійснюється наступним чином:

Вхідні дані:

- час простою внаслідок атаки, $t_П$ (в годинах)

- час відновлення після атаки, $t_В$ (в годинах)

- час повторного введення втраченої інформації, $t_{ВИ}$ (в годинах)

- зарплата обслуговуючого персоналу (адміністраторів та ін.), $Z_О$ (грн. в місяць)

- зарплата співробітників атакованого вузла або сегмента, $Z_С$ (грн. в місяць)

- число обслуговуючого персоналу (адміністраторів та ін.), $N_О$

- число співробітників атакованого вузла або сегмента, $N_С$

- обсяг продажу атакованого вузла або сегмента, О (грн. на рік)

- вартість заміни обладнання або запасних частин, $П_{зч}$ (грн.)

- число атакованих вузлів або сегментів, I

- число атак на рік, n

Вартість втрат від зниження продуктивності співробітників атакованого вузла або сегмента буде дорівнює

$$П_П = \frac{\sum_{N_С} Z_С}{176} \cdot t_П,$$

де місячний фонд робочого часу при 40-а годинному робочому тижні 160 годин.

Вартість відновлення працездатності атакованого вузла або сегмента складається з декількох складових:

$$П_В = П_{ВИ} + П_{ПВ} + П_{Зч},$$

де $П_{ВИ}$ - вартість повторного введення інформації;

$П_{ПВ}$ - вартість відновлення вузла (переустановлення системи, конфігурація тощо);

$$П_{ВИ} = \frac{\sum_{N_С} Z_С}{168} \cdot t_{ВИ}$$

$$П_{ПВ} = \frac{\sum_{N_О} Z_О}{168} \cdot t_В$$

Упущена вигода від простою атакованого вузла або сегмента становить:

$$U = П_П + П_В + V,$$

де $V = \frac{o}{52 \cdot 10 \cdot 8} \cdot (t_П + t_В + t_{ВИ})$

Таким чином, загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складе:

$$ОУ = \sum_{год} \sum_{i} U$$

3.1 Розрахунок збитків від реалізації можливої атаки на ІС Банку

- час простою внаслідок атаки, $t_П$ = 4 години
- час відновлення після атаки, $t_В$ = 4 години
- час повторного введення втраченої інформації, $t_{ВИ}$ = 15 годин
- зарплата обслуговуючого персоналу, $Z_О$ = 7000 грн.
- зарплата співробітників атакованого вузла або сегмента, $Z_{С=}$ 9000 (грн. в місяць)
- число обслуговуючого персоналу (адміністраторів та ін.), $N_О$ = 3
- число співробітників атакованого вузла або сегмента, $N_С$ = 1
- обсяг угод атакованого вузла або сегмента, О = 7 600 000 000 грн./рік
- вартість заміни обладнання або запасних частин, $П_{Зч}$ = 0 грн.
- число атакованих вузлів або сегментів, i = 1
- число атак на рік, n = 12

Вартість втрат від зниження продуктивності співробітників атакованого вузла або сегмента буде дорівнює:

$$П_П = 9000/160*4=225 \text{ грн.}$$

Де місячний фонд робочого часу при 40-ка годинному робочому тижні - 160 годин.

Вартість повторного введення інформації:

$$П_{ВИ} = 9000/160*4=225 \text{ грн.}$$

Вартість відновлення вузла:

$$П_{ПВ} = 7000/160*4=175 \text{ грн.}$$

Вартість заміни обладнання або запасних частин:

$$П_{зч} = 0 \text{ грн.}$$

$$V = (7\ 600\ 000\ 000 / 52 \cdot 10 \cdot 8) \cdot (4+4+15) = 42\ 019\ 230{,}77 \text{ грн.}$$

Упущена вигода від простою атакованого вузла або сегмента становить:

$$U = П_П + П_В + V,$$

$$П_В = N_О + Z_О(\text{в час}) * t_В = 175 \text{ грн.}$$

$$U = 225 + 175 + 42\ 019\ 230{,}77 = 42\ 019\ 630{,}77 \text{ грн.}$$

Таким чином, загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складе:

$$ОУ = \sum_{год} \sum_{i} U = 42\ 019\ 630{,}77 * 8 = 336\ 157\ 046{,}16 \text{ грн.}$$

3.2 Розрахунок оплати праці фахівця з розробки політики безпеки

Згідно з середньостатистичними даними, середня зарплата фахівця з розробки політики безпеки в Україні становить не менше 500 грн / год.

Виходячи з того, що для аналізу існуючої безпеки на підприємство і розробки політики безпеки фахівця знадобиться не менше 30 робочих (8 годинних) днів, зробимо розрахунок:

$$ОТС = 30*8*500 = 120000 \text{ грн.}$$

3.3 Розрахунок витрат на реалізацію політики безпеки

Корпоративні тренінги: 30000 грн. на рік;

Підписка на журнали в області інформаційної безпеки: 5000 грн. на рік;

Навчально-роз'яснювальні семінари: 20000 грн. на рік;

ЗРПБ = 55000 грн.

Висновки до розділу 3

В економічному розділі розрахований загальний збиток від реалізації атаки (можливу загрозу інформаційній безпеці) який склав 336 157 046,16 грн. і витрати, необхідні на розробку і впровадження політики безпеки, які склали З = ОТС + ЗРПБ = 175000 грн. Порівнюючи ці показники, можна зробити висновок про те, що виконується необхідна вимога: витрати на забезпечення інформаційної безпеки не повинні перевищувати збиток при реалізації можливої загрози. Отже, запропонований проект є економічно доцільним.

ВИСНОВКИ

У дипломній роботі розв’язано актуальне наукове завдання щодо розробки нових методів якісної оцінки ризиків інформаційної безпеки підприємств. В ході розв’язання поставлених задач були отримані наступні наукові та практичні результати

1. Проведено аналіз існуючих технологій аналізу ризиків ІБ в системі забезпечення інформаційної безпеки організації і детально описані основні етапи для отримання вихідних даних для проведення цього аналізу;

2. Наведено теоретичні основи кластерного аналізу і детально описаний метод кластеризації «к-середніх»;

3. Запропоновано метод оцінки ризиків ІБ заснований на застосуванні кластеризації при спільному аналізі інцидентів порушення ІБ для всіх активів підприємства при різних типах загроз. На умовному спрощеному прикладі показано порядок виконання всіх етапів цього методу.

4. Проведено аналіз політики безпеки, для якого розрахований загальний збиток від реалізації атаки (можливу загрозу інформаційній безпеці) на підприємство.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Петренко С.А. Анализ рисков в области защиты информации. Методическое пособие. - ООО «Издательский Дом «Афина» г. Санкт-Петербург, 2009.

2. Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление рисками информационной безопасности. Учебное пособие для вузов. - М.: Горячая линия-Телеком, 2013.

3. Ковальская И.А., Тимофеев Д.С. Методы измерения рисков информационной безопасности.

URL: http://ir.nmu.org.ua/bitstream/handle/123456789/1644/3.pdf

4. Козлова Е.А. Оценка рисков информационной безопасности с помощью метода нечеткой кластеризации и вычисления взаимной информации. Молодой учёный. Ежемесячный научный журнал №5 (52)/2013.

5. Лось А.Б., Кабанов А.С., Трунцев В.К. Особенности использования кластерного анализа в системе менеджмента информационной безопасности. Промышленные контроллеры. Ежемесячный научный журнал «Научтехлитиздат» 8\2013.

6. Легчекова Е.В., Титов О.В. Метод расчета риска информационной безопасности.

URL: http://lib.i-bteu.by/bitstream/handle/22092014/3600/Легчекова%20Е.В.%2С%20Титов%20О.В.%20 Метод%20расчета.pdf

7. Киселева И. А., Искаджян С.О. Информационные риски: методы оценки и анализа // ИТпортал, 2027. №2 (14).

8. П.В. Плетнев, В.М. Белов. Методика оценки рисков информационной безопасности на предприятиях малого и среднего бизнеса // Доклады ТУСУРа № 1 (25), часть 2, июнь 2012.

9. Баранова Е.К. Методики и программное обеспечение для оценки рисков в сфере информационной безопасности // Управление риском. 2009. № 1(49). -С. 15-26.

10. Левченко В.Н. Этапы анализа рисков.

URL: http://www.cfin.ru/finanalysis/risk/ stages.shtml

11. Воронцов К. В. Лекции по алгоритмам кластеризации и многомерного шкалирования.

URL:

12. Булдакова Т. И., Миков Д.А. Реализация методики оценки рисков информационной безопасности в среде MATLAB.

URL: http://cyberrus.com/wp-content/uploads/2015/10/vkb_12_7.pdf

13. Владимирцев А.В., Марцынковский О.А. Использование метода экспертных оценок при анализе и оценке рисков системы менеджмента. - Ассоциация по сертификации «Русский Регистр» - Санкт-Петербург: 2007.

14. Замула А.А., Северинов А.В., Корниенко М.А. Анализ моделей оценки рисков информационной безопасности для построения системы защиты информации. - Наука і техніка Повітряних Сил Збройних Сил України, 2014, № 2(15).

15. Sanjay Goel, Vicki Chen. Анализ рисков информационной безопасности - матричный подход. Перевод: С.С. Химка Источник: http://www.docstoc.com/.

16. Международный стандарт ISO/IEC 27001:2005 «Information technology. Security techniques. Information security management systems. Requirements».

17. Международный стандарт ISO/IEC 27005:2011 «Information technology. Security techniques. Information security risk management».

ВОЗМОЖНАЯ КЛАССИФИКАЦИЯ УГРОЗ ИБ

1 Происшествия, связанные с техническими причинами:

– отказ (сбой) в работе технических средств;
– повреждение кабелей или линий связи;
– колебания напряжения (перенапряжение, импульсные выбросы);
– перебои в системе электропитания;
– воздействие статического электричества, индустриальных помех и технических наводок;
– сбой (ошибки) в работе ПО, отказ ПО;
– отказ (сбой, ошибки) в работе СЗИ, средств мониторинга, контроля и администрирования;
– отказ в обслуживании вследствие перегрузки (сети, сервера и т. п.);
– воздействие вредоносных программ (вирусы, «черви», «троянские кони», закладные устройства);
– ошибки при передаче данных;
– неправильная маршрутизация сообщений;
– потеря (повреждение) данных на носителе информации (выход из строя дискового накопителя с повреждением диска, повреждение магнитных носителей);
– другие угрозы со стороны технических и программных средств (отказы электронных схем компьютеров и периферийного оборудования).

2. Происшествия, связанные со стихийными бедствиями:

– пожар;
– затопление при аварии водопровода, отопления, канализации;
– разрушение ветхих элементов конструкции здания;
– прямое попадание молнии или наводка импульсных токов во время грозы.

3. Происшествия, связанные с ненамеренными действиями людей:

– невыход персонала на работу;

- ошибки пользователя;
- ошибки администрирования;
- отсутствие надлежащего технического обслуживания, ошибки при его проведении;
- некомпетентное использование, настройка или неправомерное отключение средств защиты информации (СЗИ) персоналом подразделения безопасности;
- неумышленная порча оборудования;
- неумышленное повреждение силовых и телекоммуникационных линий/кабелей связи;
- неумышленная порча носителей информации;
- неумышленное удаление (искажение) защищаемой информации;
- неумышленное разглашение конфиденциальной информации;
- неуспешное внесение изменений в ИС;
- внедрение ПО, содержащего ошибки;
- нарушение ИБ в процессе разработки, внедрения и вывода из эксплуатации ИС и их компонентов;
- предоставление некачественных услуг третьей стороной;
- халатность, игнорирование установленных правил при работе в ИС (в том числе, правил обеспечения ИБ);
- неумышленное нарушение технологии обработки информации;
- неумышленное удаление (нарушение работы) программ;
- несанкционированная установка и запуск программ;
- непреднамеренное заражение компьютера вирусами;
- разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования или электронной цифровой подписи (ЭЦП), идентификационных карточек, пропусков и т. п.);
- создание потенциальной опасности нарушения ИБ при использовании мобильных компьютеров и носителей информации вне организации;

– создание потенциальной опасности нарушения ИБ при дистанционной работе;
– злоупотребление ресурсами;
– другие непреднамеренные действия.

4. Злоумышленные действия людей:

– забастовка, преднамеренный невыход персонала на работу;
– диверсия;
– наблюдения и фотографирование (визуальный перехват информации, выводимой на экран дисплеев или вводимой с клавиатуры для выявления паролей, идентификаторов и процедур доступа);
– раскрытие, перехват, хищение атрибутов разграничения доступа (паролей, ключей шифрования или ЭЦП, идентификационных карточек, пропусков и т. п.);
– проникновение в систему через внешний (телефонный) канал связи с присвоением полномочий легального пользователя (ЛП) с целью подделки, копирования, уничтожения данных о платежах (реализуется угадыванием или подбором паролей, выявлением паролей и протоколов через агентуру в организации, перехватом паролей при подключении к каналу во время сеанса связи, дистанционным перехватом паролей в результате приема электромагнитного излучения);
– проникновение в систему через телефонную сеть при перекоммутации канала на модем злоумышленника после вхождения ЛП в связь и предъявления им своих полномочий с целью присвоения его прав на доступ к данным;
– копирование финансовой информации и паролей при негласном пассивном подключении к кабелю или при приеме электромагнитного излучения сетевого адаптера;
– выявление паролей ЛП при негласном подключении к коммуникационной сети при имитации запроса сетевой ОС;

- анализ трафика при пассивном подключении к каналу связи или при перехвате электромагнитного излучения аппаратуры для выявления протоколов обмена;
- подключение к каналу связи в качестве активного ретранслятора для фальсификации платежных документов, изменения их содержания, порядка следования, повторной передачи, доставки с задержкой или
- упреждением;
- блокировка канала связи собственными сообщениями, вызывающая отказ в обслуживании для пользователей;
- отказ абонента от факта приема (передачи) платежных документов или формирование ложных сведений о времени приема (передачи) сообщений для снятия с себя ответственности за выполнение этих операций;
- отказ от авторства сообщений;
- формирование ложных утверждений о полученных (переданных) платежных документах;
- манипуляции с передаваемыми по сети данными (имитация, подмена, замена, вставка, удаление, изменение, повторное использование);
- перенаправление потоков данных (в частности, на системы, контролируемые злоумышленником);
- блокирование потоков данных;
- ввод некорректных (ложных) данных и значений параметров (время и т.п.);
- скрытая НС передача конфиденциальной информации в составе легального сообщения для выявления паролей, ключей и протоколов доступа;
- незаконное объявление пользователем себя другим пользователем (маскировка) для нарушения адресации сообщений или отказа в законном обслуживании;

- маскарад в сети (попытка злоумышленника выдать свою систему за легальный объект);
- считывание информации с жестких и гибких дисков (в том числе и остатков «стертых» файлов), магнитных лент при копировании данных с оборудования на рабочих местах в нерабочее время, при копировании данных с использованием терминалов, оставленных без присмотра в рабочее время;
- копирование данных с магнитных носителей, оставленных на столах или в компьютерах; копирование данных с оборудования и магнитных носителей, убранных в специальные хранилища, при их вскрытии или взломе;
- сбор и анализ использованных распечаток, документации и других материалов для копирования информации или выявления паролей, идентификаторов, процедур доступа и ключей;
- негласная переработка оборудования или ПО на фирме-изготовителе, фирме-поставщике, в месте складирования или в пути следования к заказчику с целью внедрения средств НСД к информации извне (программ-перехватчиков и «троянских коней», аппаратуры вывода информации и т. п.), а также уничтожение информации или оборудования (например, с помощью вирусов, ликвидаторов с дистанционным управлением или замедленного действия);
- намеренная порча технических средств, носителей информации; повреждение силовых и телекоммуникационных линий/кабелей связи;
- разрушение информации или создание сбоев в ИС с помощью вирусов для дезорганизации деятельности организации (реализуется загрузкой вирусов в нерабочее время, подменой игровых программ или вручением сотруднику «подарка» в виде новой игры или другой занимательной программы);
- повреждение (удаление) регистрационной, конфигурационной или иной информации, влияющей на безопасность ИС;

- похищение оборудования, в том числе отдельных плат, дисководов, дорогостоящих микросхем, кабелей, дисков, лент, с целью продажи, что влечет за собой потерю работоспособности системы, а иногда и уничтожение данных;
- похищение магнитных носителей с целью получения доступа к данным и программам;
- разрушение оборудования, магнитных носителей или дистанционное стирание информации (например, с помощью магнитов);
- установка ликвидаторов замедленного действия или с дистанционным управлением (программных, аппаратных или аппаратно-программных с исполнительным механизмом взрывного, химического, электрического или вирусного действия) с целью уничтожения информации или оборудования;
- злоупотребление полномочиями;
- внесение изменений в данные и программы для подделки и фальсификации финансовых документов при включении системы во время негласного посещения в нерабочее время; использование оставленного без присмотра оборудования в рабочее время; внесение изменений в данные, записанные на оставленных без присмотра магнитных носителях;
- несанкционированное изменение своих полномочий на доступ или полномочий других пользователей в обход механизмов защиты;
- установка скрытых передатчиков для вывода паролей с целью копирования данных или доступа к ним по легальным каналам связи с ИС в результате негласного посещения в нерабочее время, посещения с целью ремонта, настройки, профилактики оборудования или отладки ПО, скрытой подмены элементов оборудования при оставлении их без присмотра в рабочее время;

– внесение изменений в базу данных или в отдельные файлы в пределах выделенных полномочий для подделки или уничтожения финансовой информации.