Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційно роботи магістра

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

спеціальність *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*

освітньо-наукова програма *Кібербезпека*
(назва освітньої програми)

на тему: Оцінка ризиків інформаційної безпеки в розподілених інформаційних системах

Виконавець: студент ІІ курсу, групи КБм-21

_____ **Максим ГАЛЬМІЗ**
(підпис) (Ім'я, ПРІЗВИЩЕ)

	Ім'я, ПРІЗВИЩЕ	**Підпис**
Науковий керівник	Тетяна БАБЕНКО	
Нормоконтроль	Сергій ДАКОВ	

Київ 2023

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Сергій ТОЛЮПА
«24» жовтня 2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*

Здобувача(ки) КБм-21 (група) Гальміза Максима Вікторовича (прізвище ім'я по-батькові)

Тема кваліфікаційної роботи Оцінка ризиків інформаційної безпеки в розподілених інформаційних системах

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 3 від 20.10.2022

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень процес оцінки ризиків інформаційної безпеки в розподілених інформаційних системах.

Предмет досліджень методи та підходи оцінки ризиків інформаційної безпеки в розподілених інформаційних системах.

Мета синтез моделі оцінки ризиків інформаційної безпеки в розподілених інформаційних системах

Вихідні дані для проведення роботи Методи оцінки ризиків, вибірка експертних оцінок.

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна створення моделі оцінки ризиків інформаційної безпеки в розподіленій інформаційній системі

Практична цінність Створення моделі оцінки ризиків в розподіленій інформаційній системі та її інтерпретація.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота виконана у повному обсязі відповідно до теми.

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Розробка плану для досягнення мети роботи	24.10.2022 – 23.01.2022
Аналіз літературних джерел	24.01.2022 – 14.02.2022
Синтез моделі оцінки ризиків в розподіленій інформаційній системі та її інтерпретація	15.02.2022 – 24.04.2022
Оформлення і друк пояснювальної записки	25.04.2022 – 19.05.2023

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект Отримання доходу, за рахунок скорочення витрат на усунення наслідків реалізації ризиків

Соціальний ефект Покращення технологій оцінки ризиків інформаційної безпеки на підприємствах.

7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ Тетяна БАБЕНКО
(підпис) (Ім'я, ПРІЗВИЩЕ)

Завдання прийняв до виконання _____ Максим ГАЛЬМІЗ
(підпис) (Ім'я, ПРІЗВИЩЕ)

Дата видачі завдання: 24.10.2022 р.
Термін подання кваліфікаційної роботи до ЕК 19.05.2023 р.

УДК. 004.432.16

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної магістерської роботи «Оцінка ризиків інформаційної безпеки в розподілених інформаційних системах»: 70 сторінка, 16 рисунків та 40 літературних джерел.

Об’єкт дослідження – процес оцінки ризиків інформаційної безпеки в розподілених інформаційних системах.

Мета роботи – синтез моделі оцінки ризиків інформаційної безпеки в розподілених інформаційних системах.

Методи дослідження – спостереження, порівняння, розрахунок, аналіз і синтез.

У роботі досліджено сучасні вразливості та загрози в розподілених системах. Проведено аналіз основних підходів до оцінки ризиків. Запропоновано модель оцінки ризиків інформаційної безпеки в розподілених інформаційних системах.

Наукова новизна: створення моделі оцінки ризиків інформаційної безпеки в розподіленій інформаційній системі.

Актуальність теми: Актуальність теми досягається за рахунок створення можливості допомогти організаціям в Україні захистити конфіденційну інформацію, забезпечити безперервність основних послуг, протидіяти дезінформації та сприяти міжнародній співпраці в складний період війни. Під час конфлікту часто відбувається ескалація кіберзагроз і атак. Ворожі учасники можуть націлитися на розподілені інформаційні системи, щоб порушити критичну інфраструктуру, скомпрометувати конфіденційні дані або поширити дезінформацію. Оцінка ризиків інформаційної безпеки допомагає організаціям в Україні визначити потенційні вразливості та зміцнити свої системи проти цих загроз..

Ключові слова: оцінка ризиків, ризик інформаційній безпеці, розподілена інформаційна система, інформаційна безпека.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

AI	–	Artificial Intelligence
DNS	–	Domain Name System
IDL	–	Interface description language
ISO	–	International Organization for Standardization;
NIST	–	National Institute of Standards and Technology;
Octave	–	Operationally Critical Threats, Assets and Vulnerability Evaluation
CVE	–	Common Vulnerabilities and Exposures
CERT	–	Community Emergency Response Team
ICAT	–	International Centre for Automotive Technology
CA	–	Competitive advantage
F/J	–	Fines and judgments
FAIR	–	Factor Analysis of Information Risk
ERM	–	Enterprise Risk Management
МГК	–	Метод головних компонентів
ФА	–	Факторний аналіз

ЗМІСТ

ВСТУП

Актуальність. Тема оцінки ризиків інформаційної безпеки в розподілених інформаційних системах дуже актуальна в сучасному цифровому ландшафті. Організації все більше використовують розподілені інформаційні системи для виконання своїх операцій, зберігання даних і комунікаційних потреб. Ці системи зазвичай складаються з взаємопов'язаних мереж, серверів, баз даних і різних кінцевих точок. З розвитком хмарних обчислень і віддаленої роботи складність і масштаб розподілених систем значно зросли. Оцінка ризиків безпеці, пов'язаних із такими системами, має вирішальне значення для забезпечення конфіденційності, цілісності та доступності важливої інформації.

Основною задачею цієї кваліфікаційної роботи є розробити модель оцінки ризиків інформаційної безпеки в розподілених інформаційних системах та перевірити її на адекватність.

Науковою новизною цієї кваліфікаційної роботи є створення моделі оцінки ризиків інформаційної безпеки в розподіленій інформаційній системі.

Об'єктом дослідження процес оцінки ризиків інформаційної безпеки в розподілених інформаційних системах.

Предметом дослідження є методи та підходи оцінки ризиків інформаційної безпеки в розподілених інформаційних системах.

Метою даної роботи є синтез моделі оцінки ризиків інформаційної безпеки в розподілених інформаційних системах.

Для досягнення заданої мети в роботі були поставлені наступні завдання:

- на основі аналізу літературних даних визначити, які існують підходи до оцінки ризиків у розподілених системах;
- визначити вимоги до моделі оцінки ризиків у розподіленій системі;
- розробити модель оцінки ризиків;
- перевірити розроблену модель.

У зв’язку зі швидким розвитком таких технологій, як периферійні обчислення, блокчейн і контейнеризація, виникає потреба вивчити їхній вплив на ризики інформаційної безпеки в розподілених системах. Новизна теми полягає в дослідженні наслідків цих нових технологій та їх інтеграції в методології оцінки ризиків, тим самим покращуючи розуміння їх наслідків для безпеки та сприяючи базі знань щодо оцінки ризиків у розподілених інформаційних системах.

Практична цінність отриманих результатів полягає в використанні запропонованої в роботі моделі в системах інформаційної безпеки підприємства.

РОЗДІЛ 1
ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1.1 Огляд ризиків інформаційної безпеки

Інформаційна безпека стає все більш важливою частиною бізнесу. Згідно з дослідженням Ponemon Institute[1], середня вартість витоку даних минулого року зросла до 4,24 мільйона доларів США (приблизно 3,1 мільйона фунтів стерлінгів), що свідчить про серйозність проблеми.

Щоб зменшити ці витрати, організації повинні провести оцінку ризиків, щоб визначити, як вони можуть стати вразливими.

Як правило, визначення ризику інформаційної безпеки охоплює все, що може загрожувати конфіденційності, цілісності або доступності інформації.

Це може включати ризики, пов’язані з фізичними записами, цифровими активами, системами та серверами, а також інциденти, під час яких інформація втрачається, викрадається або стає тимчасово недоступною.

Більш точне визначення ризику інформаційної безпеки полягає в тому, що він охоплює негативні наслідки після того, як конфіденційність, цілісність або доступність інформації опинилися під загрозою.

Вразливість — це відомий недолік, який можна використати для пошкодження або компрометації конфіденційної інформації[2].

Вона часто пов’язана з недоліками програмного забезпечення та способами, якими злочинні хакери можуть використовувати їх для виконання завдань, для яких вони не призначені. Це також може включати фізичні вразливості, такі як властиві людські слабкості, такі як наша сприйнятливість до фішингу або ймовірність того, що втратиться конфіденційний файл.

Загалом, вразливі місця - це засоби, за допомогою яких інформація може бути скомпрометована.

Загроза виникає, коли працівник користується вразливістю або стає її жертвою. Отже, якщо використовувати наведені вище приклади, загрози включають злочинний хакер, який використовує недолік програмного забезпечення або обманює співробітника, надсилаючи фальшиву електронну пошту.

Іншими словами, загрози - це дії, які призводять до зламу інформації.

У випадку злочинного хакера, який фішингує працівника, існує ризик того, що він отримає доступ до робочого облікового запису працівника та викраде конфіденційну інформацію. Це може призвести до фінансових втрат, втрати конфіденційності, шкоди репутації та регуляторних заходів.

Ризики інформаційної безпеки можна розбити на такі категорії[2]:

1) Людська помилка. Щось таке просте, як включення неправильної особи в поле «Копія» електронного листа або вкладення неправильного документа до електронного листа, може призвести до витоку даних.

Кожен схильний робити помилки – це людська природа, – але співробітники повинні розуміти найважливіші елементи інформаційної безпеки. Тим часом увесь персонал, технічний чи нетехнічний, повинен ознайомитися з політикою та процедурами безпеки організації.

2) Зловмисні інсайдери. Ключовою частиною заходів безпеки в організації є контроль доступу. Це обмежує інформацію, доступну для працівників, гарантуючи, що вони можуть отримати доступ лише до записів, які стосуються їх роботи. Водночас необхідно встановити суворий контроль над конфіденційною інформацією, щоб забезпечити доступ до інформації лише надійним співробітникам найвищого рівня.

Це зменшує ризик того, що працівник навмисно порушить інформацію, незалежно від того, чи робить він це з особистих чи фінансових причин.

3) Фізична крадіжка. Більшість дискусій про безпеку зосереджуються на цифрових даних, але багатьом організаціям необхідно так само піклуватися про захист фізичних записів. Це можуть бути файли, що зберігаються на території організації, записи, які роздруковують співробітники, або пристрої, на яких зберігається інформація.

Оскільки гібридна робота стає нормою, організації повинні усунути ризики, пов’язані з тим, що співробітники тримають корпоративні ноутбуки вдома. Подібним чином може статися витік даних, якщо знімні пристрої або корпоративні телефони втрачені або викрадені.

4) Фішинг. Електронні листи є звичайною частиною нашого повсякденного життя, що робить їх популярним вектором атак для кіберзлочинців. Шахраї можуть використовувати, здавалося б, законні облікові дані таких організацій, як страховики, банки тощо, щоб отримати доступ до вашої особистої інформації, заохочуючи вас натиснути небезпечне посилання або завантажити зловмисне вкладення.

Фішинг також є одним із найпоширеніших способів нападу кіберзлочинців на організації, щоб розмістити зловмисне програмне забезпечення, а програмне забезпечення-вимагач швидко стає їхнім улюбленим методом.

Атаки здійснюються шляхом зараження організації зловмисним програмним забезпеченням, яке проникає через системи організації, шифрує дані та змушує жертву зупиняти операції, які потребують цих систем.

Потім злочинці вимагають організації викуп, вимагаючи оплати в обмін на ключ дешифрування.

Експерти з кібербезпеки закликають жертв не платити, оскільки немає гарантії, що зловмисники дотримають свого слова, але багато хто все одно ризикує – тому атаки програм-вимагачів залишаються такими плідними.

1.2 Розподілені інформаційні системи та їх характеристика

Розподілена система — це програмна система, в якій компоненти, розташовані на мережевих комп’ютерах, обмінюються даними та координують свої дії, передаючи повідомлення. Компоненти взаємодіють один з одним для досягнення спільної мети[3].

Це визначення має кілька важливих аспектів. Перший полягає в тому, що розподілена система складається з автономних компонентів (тобто комп’ютерів).

Другий аспект полягає в тому, що користувачі (люди чи програми) думають, що мають справу з однією системою. Це означає, що так чи інакше автономні компоненти повинні співпрацювати. Те, як налагодити цю співпрацю, лежить в основі розробки розподілених систем. Зауважимо, що жодних припущень щодо типу комп'ютерів не зроблено. В принципі, навіть в одній системі вони можуть варіюватися від високопродуктивних мейнфреймів до невеликих вузлів у сенсорних мережах. Так само не робиться жодних припущень щодо того, як комп'ютери взаємопов'язані.

Розподілена система – це сукупність незалежних комп'ютерів, яка виглядає для своїх користувачів як єдина злагоджена система – комп'ютер (Tanenbaum & Van Steen).

Іншим визначенням для розподіленої системи буде це система, призначена для підтримки розробки додатків і служб, які можуть використовувати фізичну архітектуру, що складається з кількох автономних елементів обробки, які не спільно використовують основну пам'ять, а співпрацюють, надсилаючи асинхронні повідомлення через мережу зв'язку (Blair & Stefani).

Розподілена система – це система, яка заважає вам виконувати будь-яку роботу, коли машина, про яку ви навіть не чули, виходить з ладу (Leslie).

Однією з важливих характеристик є те, що відмінності між різними комп'ютерами та способи їхнього обміну даними здебільшого приховані від користувачів. Те саме стосується внутрішньої організації розподіленої системи. Ще одна важлива характеристика полягає в тому, що користувачі та програми можуть взаємодіяти з розподіленою системою узгодженим і рівномірним способом, незалежно від того, де і коли відбувається взаємодія.

В принципі, розподілені системи також повинні бути відносно легкими для розширення або масштабування. Ця характеристика є прямим наслідком наявності незалежних комп'ютерів, але водночас приховує те, як ці комп'ютери насправді беруть участь у системі в цілому. Розподілена система зазвичай буде постійно доступною, хоча, можливо, деякі частини можуть тимчасово вийти з ладу.

Користувачі та програми не повинні помічати, що частини замінюються або виправляються, або що нові частини додаються для обслуговування більшої кількості користувачів або програм.

Щоб підтримувати різнорідні комп'ютери та мережі, пропонуючи єдину систему, розподілені системи часто організовуються за допомогою рівня програмного забезпечення, тобто логічно розташовані між рівнем вищого рівня, що складається з користувачів і програм, і шаром під ним, що складається з операційних систем і основних комунікаційних засобів, як показано на (рис.1.1) Відповідно, таку розподілену систему іноді називають проміжним програмним забезпеченням.

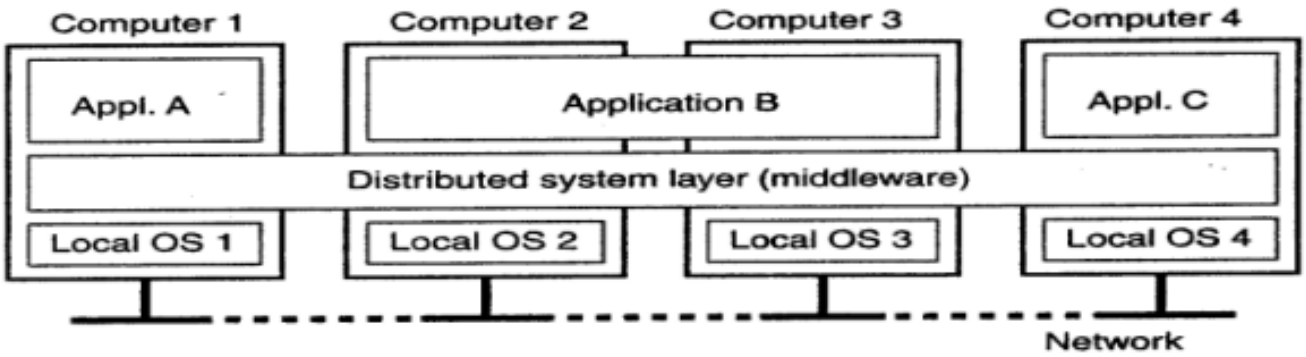

Рисунок 1.1 – Організація розподіленої системи як проміжної ланки

Рівень проміжного програмного забезпечення поширюється на кілька машин і пропонує кожній програмі однаковий інтерфейс. На (рис.1.1) показано чотири мережеві комп'ютери та три програми, з яких програма B розподілена між комп'ютерами 2 і 3. Кожна програма має однаковий інтерфейс. Розподілена система забезпечує засоби для спілкування компонентів однієї розподіленої програми один з одним, а також дозволяє обмінюватися даними між різними програмами. У той же час він приховує, наскільки це можливо, відмінності в апаратному забезпеченні та операційних системах від кожної програми.

Основна мета розподіленої системи — полегшити користувачам доступ до віддалених ресурсів, а також надавати до них контрольований і ефективний спосіб.

Ресурсами може бути будь-що, але типові приклади включають такі речі, як принтери, комп’ютери, сховища, дані, файли,

Веб-сторінки та мережі – це лише деякі з них. Є багато причин для бажання поділитися ресурсами.

Однією з очевидних причин є економіка. Наприклад, дешевше дозволити принтер використовувати кільком користувачам у невеликому офісі, ніж купувати та підтримувати окремий принтер для кожного користувача. Подібним чином, має економічний сенс спільне використання дорогих ресурсів, таких як суперкомп’ютери, високопродуктивні системи зберігання даних, засоби встановлення зображень та інші дорогі периферійні пристрої.

Підключення до «Інтернету» зараз призводить до появи численних віртуальних організацій, у яких географічно розсіяні групи людей працюють разом за допомогою групового програмного забезпечення, тобто програмного забезпечення для спільного редагування, телеконференцій тощо. Подібним чином підключення до «Інтернету» уможливило електронну комерцію, що дозволяє купувати та продавати всілякі товари, фактично не відвідуючи магазин чи навіть виходячи з дому.

Однак у міру збільшення можливостей підключення та спільного доступу безпека стає все більш важливою. У поточній практиці системи забезпечують слабкий захист від прослуховування або вторгнення в комунікацію.

Важлива мета розподіленої системи — приховати той факт, що її процеси та ресурси фізично розподілені між кількома комп’ютерами. Розподілена система, яка здатна представити себе користувачам і програмам так, ніби це лише одна комп’ютерна система, називається прозорою.

Прозорість доступу має справу з приховуванням відмінностей у представленні даних і способу доступу користувачів до ресурсів. На базовому рівні приховуються відмінності в архітектурі машин, але більш важливим є досягнення згоди щодо того, як дані мають бути представлені різними машинами та операційними системами. Наприклад, розподілена система може мати комп’ютерні системи, які працюють під керуванням різних операційних систем, кожна з яких має власні правила іменування

файлів. Відмінності в угодах про іменування, а також способи роботи з файлами мають бути приховані від користувачів і програм.

Хоча прозорість розповсюдження, як правило, вважається кращою для будь-якої розподіленої системи, є ситуації, коли спроба повністю приховати всі аспекти розповсюдження від користувачів не є хорошою ідеєю.

Існує також компроміс між високим ступенем прозорості та продуктивністю системи. Наприклад, багато додатків неодноразово намагаються зв'язатися з сервером, перш ніж остаточно відмовитися. Отже, спроба замаскувати тимчасовий збій сервера перед спробою іншого може уповільнити систему в цілому. У такому випадку, можливо, було б краще відмовитися раніше або, принаймні, дозволити користувачеві скасувати спроби встановити зв'язок. Іншим прикладом є те, що потрібно гарантувати, що кілька копій, розташованих на різних континентах, повинні бути узгодженими за часом. Іншими словами, якщо змінено одну копію, цю зміну слід поширити на всі копії, перш ніж дозволити будь-яку іншу операцію. Зрозуміло, що виконання однієї операції оновлення тепер може тривати навіть секунди, що неможливо приховати від користувачів.

Нарешті, є ситуації, коли зовсім не очевидно, що приховування розповсюдження є хорошою ідеєю. Оскільки розподілені системи розширюються до пристроїв, які люди носять із собою, і де саме поняття розташування та усвідомлення контексту стає все більш важливим, можливо, краще фактично розкривати поширення, а не намагатися його приховати.

Висновок полягає в тому, що прагнення до прозорості розподілу може бути гарною метою при проектуванні та впровадженні розподілених систем, але його слід розглядати разом з іншими питаннями, такими як продуктивність і зрозумілість. Ціна неможливості досягти повної прозорості може бути напрочуд високою.

Іншою важливою метою розподілених систем є відкритість. Відкрита розподілена система — це система, яка пропонує послуги відповідно до стандартних правил, що описують синтаксис і семантику цих служб. Наприклад, у комп'ютерних мережах стандартні правила регулюють формат, зміст і значення повідомлень, що надсилаються та отримуються. Такі правила оформляються протоколами.

Послуги зазвичай визначаються через інтерфейси, які часто описуються мовою визначення інтерфейсу (IDL). Визначення інтерфейсу, написані в IDL, майже завжди охоплюють лише синтаксис служб. Іншими словами, вони точно вказують назви доступних функцій разом із типами параметрів, значеннями, що повертаються, можливими винятками, які можна викликати, тощо. Складна частина полягає в тому, щоб точно визначити, що ці служби роблять, тобто семантику інтерфейсів. На практиці такі специфікації завжди надаються неформально за допомогою природної мови.

Якщо правильно вказано, визначення інтерфейсу дозволяє довільному процесу, якому потрібен певний інтерфейс, спілкуватися з іншим процесом, який надає цей інтерфейс. Це також дозволяє двом незалежним сторонам створювати абсолютно різні реалізації цих інтерфейсів, що призводить до двох окремих розподілених систем, які працюють однаково.

Всесвітнє підключення через Інтернет швидко стає таким же поширеним, як можливість надіслати листівку будь-кому в будь-якій точці світу. Маючи це на увазі, масштабованість є однією з найважливіших цілей проектування для розробників розподілених систем. Масштабованість системи можна виміряти принаймні за трьома різними вимірами [40].

По-перше, система може бути масштабованою щодо свого розміру, тобто можливо легко додати більше користувачів і ресурсів до системи. По-друге, географічно масштабована система — це система, у якій користувачі та ресурси можуть лежати далеко один від одного. По-третє, система може бути адміністративно масштабованою, так що нею можна легко керувати, навіть якщо вона охоплює багато незалежних адміністративних організацій. На жаль, система, яка масштабується в одному або кількох із цих вимірів, часто демонструє деяку втрату продуктивності під час масштабування системи.

Коли система потребує масштабування, необхідно вирішити дуже різні типи проблем. Якщо потрібно підтримувати більше користувачів або ресурсів, часто виникають обмеження централізованих служб, даних і алгоритмів. Наприклад, багато

служб централізовані в тому сенсі, що вони реалізуються за допомогою лише одного сервера, що працює на певній машині в розподіленій системі.

Проблема цієї схеми очевидна: сервер може стати вузьким місцем із зростанням кількості користувачів і програм. Навіть якщо є практично необмежена ємність для обробки та зберігання, зв'язок із цим сервером зрештою заборонить подальше зростання. На жаль, використання лише одного сервера іноді неминуче.

Є служби для керування дуже конфіденційною інформацією, такою як медичні записи, банківські рахунки тощо. У таких випадках найкраще реалізувати таку послугу за допомогою єдиного сервера в окремій кімнаті з високим рівнем безпеки та захисту від інших частин розподіленої системи за допомогою спеціальних мережевих компонентів. Копіювання сервера в кілька місць для підвищення продуктивності може бути неможливим, оскільки це зробить службу менш безпечною.

Система доменних імен (DNS) зберігає інформацію про мільйони комп'ютерів у всьому світі та є важливою службою для пошуку веб-серверів. Якби кожен запит на вирішення URL-адреси мав бути перенаправлений на цей єдиний DNS-сервер, це було б так дорого, що ніхто не користувався б «Інтернетом».

Централізовані алгоритми також є поганою ідеєю. У великій розподіленій системі величезна кількість повідомлень має бути маршрутизовано через багато ліній. З теоретичної точки зору оптимальний спосіб зробити це — зібрати повну інформацію про навантаження на всі машини та лінії, а потім запустити алгоритм для обчислення всіх оптимальних маршрутів. Цю інформацію потім можна поширювати по системі для покращення маршрутизації.

Характеристики розподіленої системи:

- Спільне використання ресурсів: це можливість використовувати будь-яке обладнання, програмне забезпечення або дані будь-де в системі.
- Відкритість: пов'язано з розширеннями та вдосконаленнями в системі (тобто наскільки відкрито програмне забезпечення розробляється та надається іншим).
- Одночасність: вона природно присутня в розподілених системах, які мають справу з тією самою діяльністю або функціями, які можуть виконувати окремі

користувачі, які знаходяться у віддалених місцях. Кожна локальна система має свої незалежні операційні системи та ресурси.

- Масштабованість: це збільшує масштаб системи, оскільки кілька процесорів спілкуються з більшою кількістю користувачів шляхом пристосування для покращення чуйності системи.
- Відмовостійкість: дбає про надійність системи, якщо в апаратному чи програмному забезпеченні стався збій, система продовжує працювати належним чином без погіршення продуктивності системи.
- Прозорість: вона приховує складність розподілених систем від користувачів і прикладних програм, оскільки в кожній системі повинна бути конфіденційність.
- Неоднорідність: мережі, комп'ютерне обладнання, операційні системи, мови програмування та реалізації розробників можуть відрізнятися між компонентами розосередженої системи.

Переваги розподіленої системи:

- Програми в розподілених системах є за своєю суттю розподіленими програмами.
- Інформація в розподілених системах розподіляється між територіально розподіленими користувачами.
- Спільне використання ресурсів (автономні системи можуть спільно використовувати ресурси з віддалених місць).
- Система має краще співвідношення якості та гнучкості.
- Система має менший час відгуку та вищу пропускну здатність.
- Система має більш високу надійність і готовність до відмови компонентів.
- Система має розширюваність, щоб системи можна було розширити у віддалених місцях, а також поступове зростання.

Недоліки розподіленої системи:

- Безпека є проблемою через легкий доступ до даних, оскільки ресурси спільно використовуються кількома системами.

- Навантаження мережі може спричинити перешкоду в передачі даних, тобто якщо є затримка в мережі, користувач зіткнеться з проблемою доступу до даних.
- Порівняно з однокористувальницькою системою, база даних, пов’язана з розподіленими системами, комплексна та складніша в управлінні.
- Якщо кожен вузол у розподіленій системі намагається надіслати дані одночасно, мережа може стати перевантаженою.

Область застосування розподіленої системи:

Фінанси та комерція: Amazon, eBay, онлайн-банкінг, веб-сайти електронної комерції.

Інформаційне суспільство: пошукові системи, Вікіпедія, соціальні мережі, хмарні обчислення.

- Хмарні технології: AWS, Salesforce, Microsoft Azure, SAP.
- Розваги: онлайн-ігри, музика, youtube.
- Охорона здоров'я: Інтернет-документи пацієнтів, медична інформатика.
- Освіта: E-learning.
- Транспорт і логістика: GPS, Google Maps.
- Екологічний менеджмент: Сенсорні технології.

Проблеми розподілених систем:

- Хоча розподілені системи пропонують багато переваг, вони також створюють деякі проблеми, які необхідно вирішити. Ці виклики включають:
- Затримка мережі: мережа зв’язку в розподіленій системі може викликати затримку, що може вплинути на продуктивність системи.
- Розподілена координація. Розподілені системи потребують координації між вузлами, що може бути складним через розподілену природу системи.
- Безпека: через розподілену природу системи розподілені системи більш вразливі до загроз безпеці, ніж централізовані системи.
- Узгодженість даних: підтримання узгодженості даних на кількох вузлах у розподіленій системі може бути складним завданням.

1.3 Вразливості та загрози в розподілених системах

Вразливості системи безпеки, які спостерігаються в розподіленій системі, можуть бути навмисно використані або випадково активовані. Загрози використання або ініціювання є лише потенційними та матеріалізуються як атака чи нещасний випадок. Ефективне усунення та маскування вразливостей і загроз вимагає аналізу ризиків на основі витрат.

Вразливості існують в мережах, операційних системах, системах баз даних і програмах. Кожен день відкриваються нові. Інформацію про виявлені вразливості та загрози можна отримати з відомих баз даних інцидентів безпеки або метабаз, таких як ICAT, CERT або CVE, із систем сповіщень, таких як Cassandra [4], або з інших джерел інформації про інциденти безпеки.

Застосування принципів надійності та відмовостійкості до досліджень безпеки Багато ідей або алгоритмів із досліджень надійності та відмовостійкості надають корисні аналогії дослідженням безпеки. Приклади включають вимикання кворумів для заборони доступу, використання контрольних точок для виявлення вторгнень і адаптацію до часу, серйозності, тривалості та масштабу атак.

Вразливість можна визначити як недолік або слабкість у процедурах безпеки системи, дизайні, реалізації або внутрішньому контролі[5].

Вразливість може бути випадково запущена або навмисно використана, спричиняючи порушення безпеки.

Моделювання вразливостей включає аналіз їхніх особливостей, їх класифікацію та створення таксономій, а також надання формалізованих моделей. У літературі доступно багато різноманітних моделей вразливостей у різних середовищах і за різних припущень. Детальний аналіз чотирьох поширених комп’ютерних вразливостей визначає їхні характеристики, очікувані політики, які порушуються внаслідок їх використання, і кроки, необхідні для усунення таких вразливостей у майбутніх випусках програмного забезпечення. Модель життєвого циклу вразливості було застосовано до трьох прикладів, які показують, як системи залишаються вразливими ще довго після виправлень безпеки[6]. Протягом свого

життя вразливість може перебувати в будь-якому з наступних шести станів: народження, відкриття, розкриття, виправлення, оприлюднення та смерть.

Техніка аналізу на основі моделі для виявлення вразливостей конфігурації в розподілених системах передбачає формальну специфікацію бажаних властивостей безпеки, абстрактну модель системи, яка фіксує її поведінку, пов'язану з безпекою, і методи перевірки, щоб перевірити, чи задовольняє абстрактна модель властивості безпеки.

Можна виділити два типи вразливостей: операційну та інформаційну. Перші включають несподіваний пошкоджений зв'язок у розподіленій базі даних, а другі включають неавторизований доступ (секретність/конфіденційність), несанкціоновану модифікацію (цілісність) та аналіз трафіку (проблема висновку).

Постійно відчувати загрозу через вразливість небажано. Вразливості існують не лише через помилки чи упущення, але можуть бути побічним ефектом законної системної функції, як це було у випадку з командою setuid UNIX [7, 37]. Деякі вразливості існують у системах і не завдають шкоди протягом їх життєвого циклу. Деякі відомі з них доводиться терпіти через економічні чи технологічні обмеження. Видалення інших може зменшити зручність використання. Вимагання паролів не лише для входу в систему, але й для будь-якого значного запиту ресурсу може зробити це безпечним, але знизить зручність використання.

Конструкція системи не повинна повідомляти зловмиснику про вразливості, невідомі власнику системи.

Шахрайство можна визначити як обман, який свідомо практикується з метою отримання несправедливої або незаконної вигоди[8]. Розголошення конфіденційної інформації неавторизованим особам або неавторизований продаж списків клієнтів продавцям телемаркетингу є шахрайством. Це свідчить про збіг шахрайства з порушенням конфіденційності.

Шахрайство може зробити системи більш уразливими до наступного шахрайства. Для цього потрібні захисні механізми, щоб уникнути пошкоджень у майбутньому. Шахраї отримують законні телекомунікаційні рахунки та користуються послугами без наміру оплачувати рахунки.

Шахрайство передбачає зловживання довірою[9, 10]. Шахрай прагне представити себе надійною людиною та другом. Зрозуміло, що чим більше хтось довіряє іншим, тим більш вразливим він стає.

Вразливості, як і несправності, сприяють збоям і атакам. Їх можна охарактеризувати як недоліки в дизайні, реалізації або розгортанні. Серйозність дефекту та його вплив на програму потребують аналізу. Якісний вплив може бути виражений як низький/середній/високий ступінь погіршення продуктивності та доступності. Кількісний вплив визначається економічними втратами, вимірними каскадними ефектами та часом, необхідним для відновлення. Це може включати кількісну оцінку повторних збоїв або атак.

Для ефективного вилучення характеристик і властивостей відомих вразливостей необхідні процедури та методи. Це аналогічно розумінню того, як виникають несправності. Інструменти, які шукають відомі вразливості в метабазах, мають обмеження. Механізми безпеки, які додають або змінюють записи в метабазах, можуть лише стежити за кроками зловмисника, а не передбачати їх. Характеристики можна дізнатися з поведінки зловмисника або за допомогою таких ідей, як приманки.

Необхідно побудувати комплексну класифікацію вразливостей для різних областей застосування. Медичні системи можуть мати критичні вразливості конфіденційності, тоді як уразливості в системах захисту можуть знищити або спотворити ресурси та можливості. Хороша таксономія полегшить як запобігання, так і усунення вразливостей.

Метабаза вразливостей розкриває характеристики недоліків для запобігання не тільки ідентичним, але й подібним вразливостям. Це також сприяє ідентифікації пов’язаних вразливостей, у тому числі небезпечних синергічних. Характеристика та модель набору синергетичних вразливостей може призвести до виявлення загроз бандитських атак або інцидентів. Слід зазначити, що характеристики для набору, загалом, є більш ніж простою «сумою» окремих характеристик.

Необхідні формалізми для представлення вразливостей та їхнього контексту. Завдання полягає в тому, щоб дослідити, як вразливість в одному контексті

поширюється на інший. У різних контекстах можна наголошувати на різних типах вразливостей.

Кількісні моделі життєвого циклу вразливостей слід будувати після ретельного аналізу вразливостей для певного типу програми чи системи з використанням їхніх унікальних характеристик. На кожній фазі життєвого циклу слід визначити сукупну вразливість системи та розпізнати найнебезпечніші або найпоширеніші типи вразливостей. Знання ступеня вразливості системи, тривалості фаз життєвого циклу та відомих типів уразливостей для даної фази буде корисним для захисту системи від цих типів уразливостей. Найкращі захисні процедури можна адаптивно вибрати з попередньо визначеного набору.

Моделі життєвого циклу повинні допомогти вирішити кілька проблем. По-перше, вони повинні допомогти уникнути вразливостей у розгорнутій системі найбільш ефективно, виявляючи та усуваючи їх на етапах проектування та впровадження. По-друге, вони повинні сприяти оцінці та вимірюванню вразливостей у системних компонентах і підсистемах і системі в цілому на кожному етапі життєвого циклу. По-третє, моделі допоможуть у найефективнішому виявленні вразливостей у розгорнутій системі до того, як їх використає зловмисник або станеться збій. Вони допоможуть у найбільш ефективному усуненні або маскуванні цих вразливостей, напр. заснований на принципах, аналогічних відмовостійкості. Крім того, зловмисник може залишатися в невідомості або бути невпевненим щодо важливих параметрів системи, наприклад, через недетерміновану або оманливу поведінку системи, збільшення різноманітності компонентів або кілька ліній захисту.

Дослідження повинні забезпечити методи оцінки впливу вразливостей на безпеку програм і систем. Вони повинні створювати формальні описи впливу вразливостей і розробляти методи кількісної оцінки впливу вразливостей.

Отриманий рейтинг допоможе в аналізі ризиків. Дослідники можуть визначити фундаментальні принципи проектування та вказівки щодо роботи з уразливими місцями системи на будь-якому етапі життєвого циклу системи. На основі цих принципів і вказівок слід розробити найкращі практики для зменшення вразливості на різних етапах життєвого циклу. Нарешті, слід розробити інтерактивні або повністю

автоматичні інструменти та інфраструктури, які заохочують або примусово використовують ці найкращі практики, на кожному етапі життєвого циклу. Необхідно також дослідити вразливості в самих механізмах безпеки та вразливості через нешкідливе, але створююче загрози використання інформації[11].

Загрози для систем визначаються як об’єкти, які можуть навмисно використовувати або ненавмисно викликати певні вразливості системи, щоб спричинити порушення безпеки[5, 12]. Атака — це навмисне використання вразливостей, а нещасний випадок — це ненавмисне спрацьовування вразливостей. Обидва матеріалізують загрози, перетворюючи їх із потенційних на реальні.

Загрози можна класифікувати за діями та наслідками [13, 38]. Дії можуть бути наступних типів: спостереження, знищення, модифікація та імітація загроз. Наслідки включають розкриття, виконання, спотворення та скасування загроз, загроз цілісності. Загрозу можна прийняти або усунути залежно від ступеня ризику, прийнятного для програми. Загроза життю людини може вимагати повного усунення. Загрозу надлишковому програмному або апаратному забезпеченню можна терпіти короткочасно. Загрозам можна протистояти шляхом їх уникнення (попередження) або терпимості.

Аналогію між уникненням несправностей у сфері надійності та уникненням загроз слід враховувати при проектуванні системи. Після розгортання системи розробники не можуть змінювати основні структури та механізми системи. Закостенілі в системі методи уникнення загроз ефективні лише проти менш складних атак. Виконавці найвитонченіших атак мають мотивацію, ресурси та весь час життя системи, щоб виявити її вразливі місця. До таких атак потрібно підходити з точки зору стійкості до загроз, і можна використовувати знання щодо уникнення помилок у сфері надійності.

Розуміння різних джерел загроз необхідно для ефективного уникнення загроз. Атаки можна класифікувати як атаки за цільовою можливістю, проміжні атаки або складні атаки [14]. Кілька дослідницьких зусиль зосереджено на наданні вказівок для кращого дизайну, який запобігає загрозам.

Відмовостійкі схеми не займаються кожним окремим збоєм і не витрачають усі ресурси на їх вирішення. Тимчасові та некатастрофічні помилки та збої ігноруються, якщо це може принести користь системі. Таким же чином нам потрібно провести дослідження щодо використання форми стійкості до вторгнень для боротьби з меншими порушеннями безпеки, які є поширеними у повсякденній діяльності. Застосовуючи підхід відмовостійкості до атак на безпеку систем баз даних [15, 39, 40], можливо перерахувати наступні фази: уникнення атак, виявлення атак, обмеження пошкоджень, оцінка пошкоджень, реконфігурація, ремонт і лікування несправностей для запобігання повторенню подібних атак.

Загрози шахрайства можна розглядати як особливу категорію загальних загроз безпеці та як перший крок у деяких стійких до загроз рішень. Системи виявлення шахрайства широко використовуються в телекомунікаціях, онлайн-транзакціях, комп'ютерній та мережевій безпеці та страхуванні. Ефективне виявлення шахрайства використовує як правила шахрайства, так і аналіз шаблонів. Через нерівний розподіл випадків шахрайства однією з проблем у виявленні шахрайства є дуже високий рівень помилкових тривог.

1.4 Основні підходи до оцінки ризиків

Існує багато різних методів аналізу інформаційних ризиків для розподілених систем. Головна їхня відмінність полягає в підходах і шкалах оцінки рівня ризику: кількісних чи якісних.

Умовно серед методів оцінки ризику можна виділити три групи [16]:

1. Статистичні методи.
2. Методи експертних оцінок.
3. Методи моделювання.

1.4.1 Статистичні методи оцінки ризиків.

При оцінці ризиків інформаційної безпеки можна використовувати різні підходи, включаючи якісний, кількісний або комбінацію обох.

Кількісні методи передбачають оцінку ризиків за допомогою числових значень. Ці методи зазвичай використовують накопичену статистичну інформацію про інциденти та порушення, а також метаінформацію про поточний стан і конфігурацію компонентів вузла розподіленої системи як вхідні дані для оцінки. Однак часта відсутність достатньої статистики може обмежити адекватність результатів оцінювання. Ці методи також є складними, трудомісткими та тривалими, особливо при аналізі розподілених систем. Незважаючи на ці обмеження, кількісний підхід пропонує такі переваги, як точна оцінка ризику, чіткі результати та можливість порівняти значення ризику у фінансовому вираженні з інвестиціями, необхідними для пом’якшення цих ризиків.

З іншого боку, частіше використовуються якісні методи, але вони часто спираються на спрощену шкалу з трьома рівнями оцінки ризику (високий, середній, низький). Ці методи базуються на експертних опитуваннях, а перспективних інтелектуальних методів недостатньо. Недоліки якісних підходів включають обмежену видимість і складність використання результатів аналізу ризиків для економічного обґрунтування та оцінки доцільності інвестування в заходи реагування на ризики. Проте якісні методи пропонують простоту та мінімізують витрати часу та праці на проведення оцінки ризику.

Комбінований підхід поєднує як якісні, так і кількісні методи, використовуючи переваги кожного з них. Поєднуючи ці підходи, організації можуть отримати повне розуміння ризиків інформаційної безпеки.

За даними «The Marsh Microsoft 2019 Global Cyber Risk Perception Survey» [17], популярність кількісних підходів в оцінці ризиків інформаційної безпеки значно зросла порівняно з 2017 роком, хоча залишається відносно низькою.

Загалом, у сучасній ситуації більшість компаній переважно використовують якісні шкали для оцінки ризиків інформаційної безпеки.

1.4.2 Методи експертних оцінок ризиків

У ситуаціях, коли статистичні методи неможливо застосувати для аналізу ризиків у розподіленій системі через такі фактори, як недостатня кількість даних, обмежена інформація про фактори ризику або складність інфраструктури, методи експертної оцінки стають важливими. Експертні оцінки передбачають проведення комплексного аналізу проблеми шляхом поєднання якісних і кількісних оцінок гіпотез з наступною обробкою результатів. Незважаючи на те, що цей метод простий і практичний, він вимагає експертів із значним рівнем компетентності та великим практичним досвідом.

При застосуванні експертних методів оцінка рівнів ризику базується на аналізі ймовірності настання несприятливих подій з урахуванням факторів, що на них впливають. Практичне застосування цього методу передбачає встановлення переліку факторів, які сприяють певному виду ризику, та визначення зв’язку між природою цих факторів і результуючим рівнем ризику.

Для забезпечення об’єктивності та неупередженості результатів ідентифікацію та оцінку ризиків інформаційної безпеки мають проводити спеціалізовані експерти або експертні групи, які мають необхідний досвід та підготовку у цій специфічній галузі [18].

Покладаючись на експертні оцінки, організації можуть отримати цінну інформацію про ризики, пов’язані з їхніми розподіленими системами, навіть у випадках, коли статистичні методи неможливі.

1.4.3 Методи моделювання

Методи моделювання, зокрема нейронні мережі, довели свою високу ефективність при аналізі ризиків інформаційної безпеки в розподілених системах [19]. Нейронні мережі використовують інструменти аналізу даних для виявлення та точної оцінки ризиків інформаційної безпеки. Отримання цінних, практичних і раніше невідомих знань із необроблених метаданих про роботу системи додає нетривіальний вимір цій проблемі.

Штучний інтелект (AI) не є новою концепцією, але в останні роки компанії почали визнавати та досліджувати його повний потенціал. Інтелектуальні системи стають все більш вирішальними в управлінні мережами, а методи штучного інтелекту значною мірою покладаються на дослідження систем виявлення вторгнень і оцінки ризиків. Ці методи використовуються для розробки, впровадження та вдосконалення систем моніторингу безпеки.

Традиційним методам кібербезпеки часто важко виявити останні оновлення зловмисного програмного забезпечення та прогрес у кібератаках. Нейронні мережі пропонують значну перевагу у своїй здатності «навчатися» на вхідних даних, розпізнаючи елементи, які відрізняються від раніше спостережуваних шаблонів у системі. Нові алгоритми штучного інтелекту використовують машинне навчання для швидкої адаптації, аналізу нових даних, покращення результатів і виявлення нових векторів ризику. Багато сучасних методів виявлення атак і оцінки ризиків покладаються на аналіз на основі правил або статистичні підходи, використовуючи попередньо визначені правила, встановлені адміністраторами або системами безпеки.

На відміну від експертних систем, які дають остаточні відповіді на основі заздалегідь визначених правил бази знань, нейронні мережі аналізують інформацію та пропонують можливість оцінювати та співвідносити дані з визнаними характеристиками, на яких їх навчили [20].

Отже, прогнозування та моделювання рівнів ризику, координація та інтелектуальна обробка різноманітних даних щодо факторів ризику та встановлення комплексного підходу до оцінки ризику в розподілених інформаційних системах залишаються критичними напрямами дослідження.

1.4.4 Факторний аналіз

Факторний аналіз інформаційного ризику (FAIR) – це систематика факторів, які сприяють ризику, і того, як вони впливають один на одного. Це в першу чергу стосується встановлення точних ймовірностей для частоти та величини подій втрати

даних. Це не методологія для проведення оцінки ризику підприємства (або окремої особи).[32]

FAIR також є системою управління ризиками, розробленою Джеком А. Джонсом, і вона може допомогти організаціям зрозуміти, проаналізувати та виміряти інформаційний ризик згідно з Whitman & Mattord (2013)[33].

Низка методологій пов'язана з управлінням ризиками в IT-середовищі або IT-ризиками, пов'язаними із системами управління інформаційною безпекою та такими стандартами, як серія ISO/IEC 27000.

FAIR доповнює інші методології, надаючи спосіб вироблення послідовних, обґрунтованих тверджень щодо ризику.[32]

Основним документом FAIR є «Вступ до факторного аналізу інформаційного ризику (FAIR)», Risk Management Insight LLC, листопад 2006 р. [34].

Вміст цього технічного документу та саму структуру FAIR опубліковано за ліцензією 2.5 Creative Commons Attribution-Noncommercial-Share Alike. Документ спочатку визначає, що таке ризик. У розділі «Ризик і аналіз ризиків» обговорюються концепції ризиків і деякі реалії, пов'язані з аналізом і ймовірностями ризиків. Це забезпечує загальну основу для розуміння та застосування FAIR. Розділ «Компоненти ландшафту ризиків» коротко описує чотири основні компоненти, які складають будь-який сценарій ризику. Ці компоненти мають характеристики (фактори), які в поєднанні один з одним спричиняють ризик. Факторинг ризиків починає розкладати інформаційний ризик на основні частини. Отримана таксономія описує, як фактори поєднуються, щоб спричинити ризик, і закладає основу для решти структури FAIR.

Розділ «Елементи керування» коротко представляє три виміри ландшафту елементів керування. Вимірювання ризику коротко обговорює концепції вимірювання та виклики, а потім забезпечує обговорення високого рівня вимірювання факторів ризику.

FAIR підкреслює, що ризик є невизначеною подією, і слід зосереджуватися не на тому, що можливо, а на тому, наскільки ймовірною є дана подія. Цей ймовірнісний підхід застосовується до кожного фактора, який аналізується. Ризик — це ймовірність втрати, пов'язаної з активом. У FAIR ризик визначається як «ймовірна частота та

ймовірна величина майбутніх втрат» [35]. FAIR далі розкладає ризик шляхом розбиття різних факторів, які складають ймовірну частоту та ймовірні втрати, які можна виміряти кількісно. Ці фактори включають: частоту загрозливих подій, частоту контактів, ймовірність дії, вразливість, загрозливу здатність, складність, частоту втрат, первинну величину втрат, частоту вторинних втрат, величину вторинних втрат і вторинний ризик.

Потенціал втрати активу залежить від вартості, яку він представляє, та/або відповідальності, яку він створює для організації [34]. Наприклад, інформація про клієнта забезпечує цінність через її роль у створенні прибутку для комерційної організації. Ця сама інформація також може спричинити відповідальність для організації, якщо існує юридичний обов'язок її захищати або якщо клієнти очікують, що інформація про них буде належним чином захищена.

FAIR визначає шість видів втрат [34]:

- продуктивність – обмеження організації для ефективного виробництва товарів або послуг з метою створення вартості;
- відповідь – ресурси, витрачені під час дій після несприятливої події;
- заміна – витрати на заміну/ремонт пошкодженого активу;
- штрафи та судові рішення (F/J) – вартість повної судової процедури, пов'язаної з несприятливою подією;
- конкурентна перевага (CA) - втрачені можливості через інцидент безпеки;
- репутація – втрачені можливості або продажі через погіршення корпоративного іміджу після події.

FAIR визначає цінність/відповідальність як [34, 36]:

- критичний – вплив на продуктивність організації;
- вартість – чиста вартість активу, вартість заміни скомпрометованого активу;
- дефіцитність – витрати, пов'язані з розкриттям інформації, далі поділяються на:

  - збентеження – у розкритті йдеться про неадекватну поведінку керівництва компанії;

- конкурентна перевага – втрата конкурентної переваги, пов’язаної з розкриттям інформації;
- юридичні/нормативні – витрати, пов’язані з можливими порушеннями законодавства;
- загальні – інші втрати, пов’язані з конфіденційністю даних.

1.5 Огляд міжнародних стандартів керування ризиками в інформаційній безпеці

Стандарти управління ризиками є результатом спільних зусиль провідних країн і організацій, які займаються вирішенням питань управління ризиками. Концепція управління ризиками охоплює аналіз та оцінку сильних і слабких сторін організації по відношенню до зовнішніх факторів, а також планування запобіжних заходів як у короткостроковій, так і в довгостроковій перспективі. Управління ризиками є життєво важливим компонентом стратегічного управління організацією.

Розробка та прийняття стандартів мають вирішальне значення для досягнення консенсусу щодо кількох ключових аспектів, зокрема:

- мета управління ризиками;
- використана термінологія;
- основні етапи та процеси практичного використання.

На сьогодні кожна розвинена країна виробляє значну кількість стандартів у сфері аналізу та оцінки ризиків інформаційної безпеки. Ці стандарти передусім включають міжнародні та національні рамки управління ризиками, такі як ISO/IEC 31000, COSO II, FERMA, KING II, а також стандарти оцінки та управління інформаційною безпекою, такі як ISO/IEC 27001, ISO/IEC 27005:2018, ISO/ IEC 17799, BS7799, NIST 800-30, BSI-стандарт 200-3, ISO/IEC 15408. Крім того, існують стандарти аудиту, які стосуються питань безпеки інформації, зокрема COBIT, SAS 55/78, SAC та інші.

Стандарт ISO 31000 — це міжнародний стандарт, який надає підприємствам рекомендації та принципи управління ризиками [23]. Ініціативи щодо відповідності

нормативним вимогам зазвичай стосуються конкретної країни та застосовуються до підприємств певного розміру або підприємств у певних галузях. Однак ISO 31000 призначений для використання в організаціях будь-якого розміру. Його концепції однаково добре працюють у державному та приватному секторах, у великих чи малих підприємствах та некомерційних організаціях.

Структура управління ризиками складається з шести окремих областей [23]:

- Лідерство. Керівники всередині організації мають проявити ініціативу, щоб переконатися, що ISO 31000 прийнято та застосовано таким чином, який узгоджується з культурою та бізнес-цілями організації.
- Інтеграція. Хоча важливо інтегрувати пом’якшення ризиків у якомога більше організаційних процесів, важливо не створювати вузьких місць у роботі та не перешкоджати виконанню основних бізнес-процесів.
- Дизайн. Організаціям потрібно буде розробити стратегію управління ризиками, яка працюватиме для організації на основі її потреб.
- Реалізація. Процес впровадження інтегрує проект управління ризиками організації в бізнес-процеси. Впровадження, як правило, є офіційним процесом із заявленими цілями, кінцевими термінами та вимогами до звітності.
- Оцінка. Оцінка оцінює дизайн, щоб визначити, що працює, а що, можливо, потребує доопрацювання.
- Поліпшення. Організації повинні постійно шукати способи вдосконалення впровадження ISO 31000.

ISO 31000 має на меті допомогти організаціям застосувати методичний підхід до управління ризиками, роблячи три ключові речі:

- визначити ризики;
- оцінити ймовірність виникнення події, пов'язаної з ідентифікованим ризиком;
- визначити серйозність проблем, викликаних подій, що сталася.

Таким чином, ISO 31000 не спрямований на усунення ризиків, оскільки повне усунення всіх ризиків неможливо. Замість цього він призначений для того, щоб допомогти організаціям визначити їхні ризики та розробити стратегію пом’якшення

Структура корпоративного управління ризиками (ERM) COSO найчастіше використовується в організаціях, які більшою мірою зосереджені на регулюванні чи відповідності [24].

Структура COSO представляє підхід до управління ризиками, зосереджений навколо п’яти взаємопов’язаних компонентів:

- управління і культура;
- стратегія та постановка цілей;
- продуктивність;
- огляд і перегляд;
- інформація, комунікація та звітність;

Ці п’ять компонентів містять серію з 20 загальних принципів, які містять конкретні вказівки для всього, від управління до моніторингу. Вони описують конкретні дії та практики, які можна масштабовано застосовувати до організацій усіх типів, але підкреслюють загальний зв’язок між ефективністю цих заходів, пов’язаних із ризиком, і успішним досягненням стратегії та бізнес-цілей організації.

ISO 27001:2013 — це міжнародний стандарт безпеки, який визначає найкращі практики щодо того, як організації мають керувати своїми даними [25]. Він описує, як компанії повинні керувати ризиками інформаційної безпеки шляхом створення системи управління інформаційною безпекою (СУІБ). Цей підхід вимагає керівництва виконавчої влади, одночасно впроваджуючи безпеку даних на всіх рівнях організації. Стандарт є добровільним, але організації, які дотримуються його вказівок, можуть отримати сертифікат ISO 27001.

ISO/IEC 27005 забезпечує структуру управління ризиками інформаційної безпеки для організацій [26]. Зокрема, він містить вказівки щодо виявлення, аналізу, оцінки, лікування та моніторингу ризиків інформаційної безпеки. Стандарт підтримує вказівки ISO 31000 і є особливо корисним для організацій, які прагнуть захистити свої інформаційні активи та досягти цілей інформаційної безпеки. Процес управління ризиками, заснований на ISO/IEC 27005, передбачає встановлення ітеративного підходу до оцінки ризиків, впровадження варіантів обробки ризиків, постійне спілкування та консультації із зацікавленими сторонами, моніторинг і перегляд

процесу управління ризиками, а також документування процесів управління ризиками та результати.

ISO/IEC 27005 може бути справді корисним для організацій, які прагнуть відповідати вимогам ISO/IEC 27001 щодо управління ризиками [26]. Встановлюючи процес управління ризиками на основі ISO/IEC 27005, організації підвищують ефективність своїх СУІБ, усувають ризики інформаційної безпеки та встановлюють відповідні практики управління ризиками інформаційної безпеки.

ISO/IEC 17799:2005 встановлює вказівки та загальні принципи для ініціювання, впровадження, підтримки та вдосконалення управління інформаційною безпекою в організації[27]. Окреслені цілі надають загальні вказівки щодо загальновизнаних цілей управління інформаційною безпекою. ISO/IEC 17799:2005 містить передову практику цілей контролю та засобів контролю в таких сферах управління інформаційною безпекою:

- політика безпеки;
- організація інформаційної безпеки;
- управління активами;
- забезпечення людськими ресурсами;
- фізична та екологічна безпека;
- комунікації та управління операціями;
- управління доступом;
- придбання, розробка та супровід інформаційних систем;
- управління інцидентами інформаційної безпеки;
- управління безперервністю бізнесу;
- відповідність.

Цілі контролю та засоби контролю в ISO/IEC 17799:2005 призначені для реалізації для виконання вимог, визначених оцінкою ризику. ISO/IEC 17799:2005 призначений як загальна основа та практичне керівництво для розробки організаційних стандартів безпеки та ефективних практик управління безпекою, а також для сприяння зміцненню довіри в міжорганізаційній діяльності.

NIST SP 800-30 — це стандарт, розроблений Національним інститутом стандартів і технологій [28]. Опублікований як спеціальний документ, розроблений для оцінки ризиків інформаційної безпеки, він стосується особливо IT-систем.

Документ NIST SP 800-30 є рекомендаційним керівництвом щодо захисту IT-інфраструктури з суто технічної точки зору. NIST SP 800-30 був одним із перших стандартів оцінки ризиків, і більшість інших стандартів підпали під його вплив. Він широко використовується для оцінки ризиків інформаційної безпеки в усьому світі та актуальний для будь-якого бізнесу з IT-компонентом.

NIST SP 800-30 розглядає безпеку інфраструктури, на якій зберігаються дані. Тут організаційні ризики чи бізнес-вимоги не є мірилом для вимірювання ризику, як у випадку з ISO 27005 або OCTAVE. Оцінка ризику відповідно до NIST SP 800-30 включає дев’ять кроків у три окремі етапи [28]:

1. Рішучість.

a. Характеристика системи.

b. Ідентифікація загрози.

c. Ідентифікація вразливості.

d. Контрольний аналіз.

2. Аналіз.

a. Визначення ймовірності.

b. Аналіз впливу.

c. Визначення ризику.

3. Пом'якшення.

a. Рекомендації щодо контролю та документування ризиків.

BSI-Standard 200-3 разом зі стандартами BSI 200-1 і 200-2 утворюють основні елементи методології IT-Grundschutz Федерального відомства з інформаційної безпеки (BSI) [29]. Стандарт призначений для таких установ, як компанії або органи державної влади.

Серед іншого, він містить процедури для створення та виконання аналізу ризиків на основі базового дослідження захисту IT. Стандарт BSI об’єднує всі кроки, пов’язані з ризиком, для реалізації базового захисту IT.

200-3 можна використовувати, якщо такі установи, як державні органи чи компанії, вже працюють з методологією IT-Grundschutz і хотіли б виконати аналіз ризиків на додаток до аналізу IT-Grundschutz. Базуючись на концепції безпеки BSI та компендіумі IT-Grundschutz, 200-3 представляє аналіз ризиків, який можна виконати в окремі кроки.

COBIT — це методологія, яка використовується в передовій практиці управління та управління IT [30]. Організації застосовують COBIT для розробки, впровадження, моніторингу та вдосконалення IT-структур.

Структура COBIT включає різні ключові компоненти, такі як структури, описи процесів, цілі контролю, моделі зрілості та керівні принципи. За своєю суттю структура COBIT служить багатофункціональним інструментом підтримки, який допомагає IT-менеджерам вирівнювати бізнес-ризики, технічні проблеми та передумови контролю в організації.

COBIT може отримати вигоду для різних посад у IT-секторі, зокрема для аналітиків з управління IT, керівників інформаційної безпеки (CISO), інженерів з IT-безпеки, адміністраторів систем безпеки та аналітиків ризиків у сфері інфосекцій. Користувачі можуть отримати офіційну відповідність COBIT на своєму підприємстві за допомогою трьох методів сертифікації: COBIT Bridge, COBIT 2019 Foundation або COBIT 2019 Design and Implementation.

1.6 Постановка задач дослідження

Метою цього дослідження є створення моделі оцінки ризиків інформаційної безпеки. Аналіз, проведений у попередньому розділі, показує, що розроблена модель має бути придатною для оперативного оцінювання ризиків інформаційної безпеки, бути зручною для користувача та доступною для малих підприємств. Крім того, отримана оцінка повинна запропонувати як кількісне, так і якісне розуміння ризиків інформаційної безпеки.

Для досягнення цієї мети в ході магістерської роботи необхідно розробити модель, яка використовує математичні інструменти для оцінки ризиків інформаційної безпеки підприємства.

Висновки за розділом 1

Розподілені системи стають все більш популярними завдяки своїй високій доступності, масштабованості та відмовостійкості. Однак вони також створюють певні проблеми, які необхідно вирішити. Розуміючи характеристики та проблеми розподілених систем, розробники можуть проектувати та впроваджувати ефективні розподілені системи, які відповідають потребам їхніх користувачів.

Численні вітчизняні та міжнародні нормативні документи та стандарти містять вимоги до управління інформаційними ризиками. Однак багато з цих стандартів передусім використовують концептуальний підхід, пропонуючи рекомендації, не пропонуючи чітких вказівок щодо впровадження заходів безпеки. У результаті компанії часто змушені розробляти власні методології та підходи до оцінки ризиків інформаційної безпеки через відсутність чітких інструкцій стандартів.

Таким чином в даній роботі, згідно досліджуваної мети, необхідно розглянути наступні задачі:

- визначити вимоги до моделі оцінки ризиків;
- розробити модель оцінки ризиків;
- перевірити розроблену модель.

РОЗДІЛ 2
РОЗРОБКА МАТЕМАТИЧНОЇ МОДЕЛІ ОЦІНЮВАННЯ

2.1 Вимоги до моделі оцінки ризиків

Процес оцінки ризику спирається на метод факторного аналізу [32-35], який виявляється дуже придатним при роботі з невизначеними, суперечливими та неоднозначними оцінками окремих факторів. Цей метод дозволяє об'єднати як якісні, так і кількісні аспекти аналізу.

Щоб забезпечити надійність і зручність використання розробленої моделі в майбутньому, вона повинна відповідати декільком вимогам. Запропонована модель оцінки ризиків інформаційної безпеки має відповідати наступним критеріям:

- Модель повинна точно відображати досліджуваний процес і давати результати, які дуже схожі на реальні результати.
- Модель повинна відображати поточний стан інформаційної безпеки на підприємствах.
- Модель повинна забезпечувати комплексну оцінку ризиків інформаційної безпеки, охоплюючи як кількісні, так і якісні аспекти.
- Модель має дозволити ідентифікувати найбільш критичні фактори ризику та пов'язану з ними ймовірність.
- Модель має сприяти використанню оцінок ризиків інформаційної безпеки для підтримки процесів прийняття управлінських рішень.

Для отримання достовірних вхідних даних для моделі експертні оцінки потребують відповідної підготовки експертів. Це включає чітке визначення цілей і завдань опитування, залучення компетентних і незалежних експертів з досвідом у відповідній галузі та використання відповідних методів обробки оцінок експертів.

Для покращення аналізу загроз інформаційній безпеці на підприємствах і оптимізації їх обробки вкрай важливо встановити існуючі зв'язки між факторами вразливості, які впливають на загальний рівень ризиків інформаційної безпеки.

Після розробки моделі оцінки ризиків інформаційної безпеки співробітники відділу інформаційної безпеки та керівники структурних підрозділів отримають простий спосіб моніторингу та оцінки ризиків інформаційної безпеки. Це стосується як окремих підрозділів, так і підприємства в цілому.

Успішне впровадження цієї моделі оптимізує завдання всіх вищезазначених працівників, дозволяючи їм більш ефективно виконувати свої обов'язки. Це дозволить їм зосередитися на ризиках, які створюють більшу ймовірність спричинити небезпечні ситуації. Крім того, це сприятиме оперативному виявленню, запобіганню та реагування на такі ризики. Ця підвищена ефективність дозволить їм виконувати свої обов'язки з більшою точністю, забезпечуючи більш ефективний підхід до управління ризиками в майбутньому.

2.2 Формування ознакового простору моделі

На основі досліджень [21, 22], можна виділити ризики інформаційної безпеки: порушення конфіденційності (X_1), втрата цілісності (X_2), порушення доступності (X_3), порушення роботи системи (X_4), крадіжка інформації (X_5), фальсифікація інформації (X_6), знищення інформації (X_7), віруси (X_8) та апаратні та програмні збої (X_9). Допустимими значеннями для кожної змінної є від 1 до 3.

Для визначальних факторів оцінки ризиків інформаційної безпеки надано функціональну модель методу головних компонент, що представлено на (рис. 2.1).

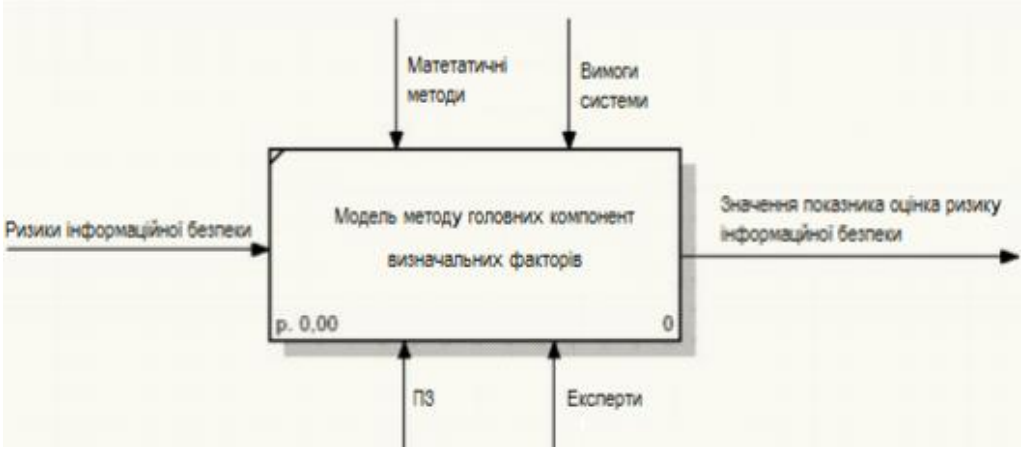

Рисунок 2.1 – Модель методу головних компонент визначальних факторів

2.3 Розробка математичної моделі оцінки ризиків

У певних ситуаціях використання статистичних або розрахунково-аналітичних методів може бути неможливим через різні причини, часто пов’язані з відсутністю надійної інформації. У таких випадках в дію вступають евристичні або експертні методи оцінки, які значною мірою спираються на досвід та інтуїцію.

Однією з помітних характеристик цих методів є відсутність жорстких математичних доказів на підтримку оптимальності рішень. Натомість ці підходи використовують людський досвід як засіб генерації кількісних оцінок процесів і суджень, які неможливо безпосередньо виміряти через неповну або недостовірну інформацію.

Загальний процес проведення експертних опитувань включає такі основні етапи:

1.1 Відбір експертів та формування експертних груп.

1.2 Формулювання питань і складання анкет.

1.3 Співпраця з експертами для збору їхніх ідей.

1.4 Встановлення правил агрегування оцінок окремих експертів у загальні оцінки.

1.5 Аналіз та обробка експертних оцінок.

Як індивідуальні, так і групові (колективні) експертні оцінки знаходять практичне застосування в різних сферах. Вони сприяють процесам прийняття рішень, використовуючи знання та погляди досвідчених людей або команд експертів.

Цілі індивідуальних експертних оцінок включають:

- Прогнозування майбутнього розвитку подій і явищ, а також оцінка їх поточного стану.
- Аналіз та узагальнення результатів, наданих іншими експертами.
- Формулювання сценаріїв дій.
- Надання висновків іншим фахівцям і організаціям шляхом оглядів, оцінок, експертиз тощо.

Індивідуальні оцінки мають певні переваги, такі як оперативність отримання інформації для прийняття рішень і відносно низькі витрати.

Однак важливо визнати потенційні недоліки індивідуальних оцінок, які включають високий рівень суб’єктивності та, як наслідок, недостатню впевненість у вірогідності отриманих оцінок. Ці недоліки усуваються шляхом включення групових експертних оцінок, спрямованих на пом’якшення або зменшення впливу індивідуальних упереджень.

Було використано дані (рис.2.2), що складають 20 ймовірних вибірок оцінок експертів. Кожний ризик оцінюється як низька, середня, висока небезпека або у числовому вигляді від 1 до 3 відповідно.

	1 X1	2 X2	3 X3	4 X4	5 X5	6 X6	7 X7	8 X8	9 X9
1	3	2	2	1	3	1	2	2	3
2	2	1	1	1	2	1	2	3	2
3	3	1	2	2	1	2	2	1	3
4	2	2	1	3	2	3	13	3	2
5	1	3	2	3	1	1	2	3	1
6	2	1	1	1	3	3	1	1	1
7	3	1	2	1	3	1	2	2	1
8	2	3	1	1	1	1	2	2	1
9	3	1	1	3	1	3	3	1	2
10	1	2	3	2	1	2	1	1	3
11	3	1	1	3	1	2	1	3	2
12	1	1	2	3	3	1	3	1	2
13	1	1	1	1	1	1	2	3	3
14	2	1	3	1	3	1	1	1	2
15	1	2	3	1	2	1	1	3	1
16	2	3	2	3	1	2	1	1	3
17	3	1	2	1	2	3	1	1	3
18	2	2	2	1	3	3	3	1	3
19	1	1	3	1	3	2	3	1	2
20	3	1	1	1	2	1	3	2	2

Рисунок 2.2 – Вибірка даних

При роботі зі складними системами пряме вимірювання факторів, що визначають їхні властивості, часто неможливо. Крім того, кількість і природа цих факторів можуть бути невідомі. Однак можна виміряти інші значення, на які впливають ці фактори.

У випадках, коли невідомий фактор впливає на кілька вимірюваних характеристик, між цими характеристиками існує певний зв'язок, наприклад кореляція. Отже, загальна кількість факторів може бути значно меншою за кількість виміряних ознак. Факторний аналіз використовується для виявлення та виділення таких основних факторів. Зменшення кількості факторів також може бути необхідним для забезпечення конвергенції алгоритмів для подальшого аналізу даних, мінімізації вимог до пам'яті комп'ютера, скорочення часу обробки та полегшення візуалізації результатів, серед інших причин.

Процес оцінки ризику базується на методі факторного аналізу, який виявляється дуже придатним при роботі з невизначеністю, суперечливою інформацією та неоднозначною оцінкою окремих факторів. Цей метод дозволяє об'єднати в аналіз як якісні, так і кількісні компоненти.

Запропонований факторний підхід є універсальним і застосовним для оцінки ризиків на різних етапах розвитку підприємства, а також при виборі та обґрунтуванні стратегій мінімізації ризиків інформаційної безпеки.

Для ефективного проведення факторного аналізу необхідно виконати певні умови:

- Усі досліджувані характеристики повинні піддаватися кількісному виміру.
- Кількість спостережуваних змінних має бути принаймні вдвічі більшою за кількість ознак.
- Зразок, що аналізується, повинен бути однорідним.

Дотримуючись цих обов'язкових умов, факторний аналіз може дати цінну інформацію про чинники, що лежать в основі складних систем, і зробити внесок у комплексний процес оцінки ризиків.

Розглянемо сценарій, коли N експертів призначено для оцінки інформаційної безпеки на підприємстві. Кожен експерт оцінює K вимірних ризиків інформаційної безпеки, в результаті чого генеруються випадкові багатовимірні значення.

Ці значення можна представити так:

$$X_t = (X_{1t}, X_{2t}, \dots, X_{kt}), \tag{2.1}$$

де t = 1,2,...,N.

Тут на значення випадкових багатовимірних величин, позначених як t, впливають певні об'єктивні фактори. Ці фактори, які називаються F_1 і F_2, вважаються прихованими і не можуть бути безпосередньо виміряні. Важливо зазначити, що кількість факторів завжди менша за кількість вимірних ризиків інформаційної безпеки (K). Хоча ці фактори є гіпотетичними, тому факторний аналіз не надає методи виявлення їх присутності.

У контексті інформаційної безпеки визначимо чотири ризики, на які впливають два фактори, а саме F_1 і F_2. Фактор F_1 фіксує загальний вплив усіх ризиків на безпеку інформації, тоді як F_2 конкретно описує вплив на ризики X_2 і X_3.

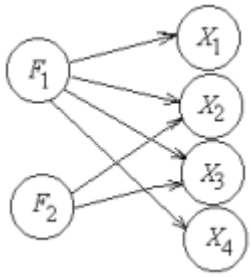

Рисунок 2.3 – зв'язок між факторами та ризиками

Таким чином, на значення ризиків X_1і X_4 впливає виключно фактор F_1 , тоді як на ризики X_2 і X_3 впливає сукупний вплив факторів F_1 і F_2. Однак на даний момент не достатньо інформації про цей зв’язок. Завдання полягає в тому, щоб оцінити силу впливу факторів F_1 і F_2на кожен із ризиків X_i, а також визначити та виділити частини X_i, які виникають внаслідок індивідуальних ефектів F_1 і F_2.

Щоб вирішити цю проблему, припускається, що кожен ризик X_i лінійно залежить від факторів Fm, де m може приймати значення 1 або 2.

$$X_i = a_{i1} \cdot F_1 + a_{i2} \cdot F_2 \,, \tag{2.2}$$

де i =1,2,3,4;

a_{i1}, a_{i2} – факторне навантаження.

На основі цієї гіпотези можливо вивести дві моделі факторного аналізу:

Метод головних компонентів (МГК): у цій моделі значення оцінки кожного ризику можна представити як лінійні комбінації факторних навантажень (a_{ij}) і факторів (Z_j), де j коливається від 1 до m (кількість факторів) . Формула для моделі PCM така:

$$R_F = \sum_{j=1}^{m} a_{ij} Z_j \tag{2.3}$$

Модель фактичного факторного аналізу (ФА): у цій моделі на спостережувані ризики впливають не лише фактори, але й вплив локальних випадкових змінних. Формула для моделі ФА:

$$R_F = \sum_{j=1}^{m} a_{ij} Z_j + e_i \tag{2.4}$$

У факторному аналізі початкові значення характеристик вибіркової сукупності центруються та нормалізуються за допомогою перетворення, яке можна виразити як:

$$Z_i = \frac{X_i - \bar{X}_i}{\sigma_i}, \tag{2.5}$$

де $\bar{X}_i$ – середнє значення i-ї змінної; σ_i – середньоквадратичне відхилення i-ї змінної.

Це перетворення гарантує належну підготовку даних для подальшого аналізу в рамках факторного аналізу.

Використовуючи розраховані головні компоненти, можливо створити простішу, але високоінформативну систему для опису ризиків. Ця система дозволяє оцінити силу причинно-наслідкового зв'язку між факторами та вибраними головними компонентами.

Крім того, результати групування на основі певних компонентів можуть бути використані для проведення порівняльного аналізу факторів, які сприяли найбільш значним покращенням безпеки. Такий аналіз дозволяє виявити прогресивні тенденції підвищення ефективності використання виробничих ресурсів.

Метод головних компонентів визначає k-компоненти, які враховують усі дисперсії та кореляції, присутні у вихідних k випадкових величинах. Ці компоненти побудовані в порядку зменшення їх частки в поясненні загальної дисперсії вихідних значень. Часто достатньо розглянути кілька перших компонентів, оскільки вони охоплюють більшу частину поясненої дисперсії.

Перший головний компонент, F_1, визначає напрямок у просторі ознак, уздовж якого набір об'єктів (точок) демонструє найбільшу дисперсію.

Другий головний компонент, F_2, побудований ортогонально до напрямку F_1 і спрямований на пояснення якомога більшої залишкової дисперсії. Ця модель продовжується для k-го головного компонента, Fk, забезпечуючи повне охоплення дисперсії, що залишилася в даних.

Оскільки головні компоненти відбираються в порядку спадання за дисперсією, яку вони пояснюють, найбільший вплив на диференціацію досліджуваних об'єктів справляють ознаки з великими коефіцієнтами, що входять до складу першого основного компонента. Це перетворення дозволяє скоротити інформацію шляхом відкидання координат, що відповідають напрямкам з мінімальною дисперсією.

Факторний аналіз також використовує інші міри інформативності, допомагаючи визначити кількість значущих факторів. Одним із таких показників є критерій Кайзера, запропонований психологом Генрі Феліксом Кайзером. Цей критерій передбачає, що в модель повинні бути включені лише фактори з власними значеннями, більшими або рівними одиниці. По суті, це означає, що такі фактори мають дисперсію, еквівалентну або більшу, ніж дисперсія однієї змінної. І навпаки, фактори з власними значеннями нижче одиниці не вважаються значущими та виключаються з моделі. Однак цей критерій іноді може призводити до надмірної кількості змінних, що зберігаються в моделі.

Інший критерій, відомий як критерій відсіву, передбачає побудову графіка. На графіку відображаються порядкові номери власних значень на осі абсцис та їхні відповідні значення на осі у. Це графічне представлення допомагає визначити відповідну кількість факторів для збереження на основі точки, у якій графік показує значне падіння або вирівнювання власних значень.

Відповідно до підходу Р. Кеттела, важливо визначити точку найбільшого уповільнення спаду власних значень. Тільки фактори, що відповідають власним значенням, розташованим ліворуч від цієї точки, слід вважати значущими. Цей критерій не має статистичних підстав і може призвести до виключення деяких значущих факторів із моделі. Однак у випадках, коли серед великої кількості змінних є кілька значущих факторів, обидва критерії можуть бути застосовані практично.

На практиці розрахунки часто включають кілька критеріїв, і вибирається модель, яка включає найбільшу кількість факторів із значущими інтерпретаціями. Якщо врахувати всі загальні фактори, що дорівнюють числу параметрів, вони разом пояснюють 100% дисперсії. Якщо сума відсотків, що пояснюється факторами, перевищує 100%, це свідчить про наявність негативних власних значень і комплексних власних векторів, що може бути наслідком неправильного скорочення вихідної кореляційної матриці. У таких випадках рекомендується двоетапна процедура аналізу. На першому етапі максимальна кількість факторів заздалегідь не визначена. Після проведення цього первинного аналізу досліджуються дисперсії, оцінюється приблизна кількість факторів і виконується наступний аналіз.

Оцінка ризику забезпечує спрощене відображення реальності. Це є індикатором того, що, незважаючи на впровадження превентивних заходів, підприємства все ще стикаються зі значним рівнем небезпеки. Однак розрахунки дозволяють побудувати уніфіковану шкалу, за якою можна ранжувати всі ризики.

Висновки за розділом 2

В даному розділі було викладено основні вимоги до моделі оцінювання, сформовано ознаковий простір моделі, та розроблено математичну модель оцінювання.

На основі цієї гіпотези можливо вивести дві моделі факторного аналізу: метод головних компонентів та модель фактичного факторного аналізу.

Використовуючи розраховані головні компоненти, можливо створити простішу, але високоінформативну систему для опису ризиків. Ця система дозволяє оцінити силу причинно-наслідкового зв'язку між факторами та вибраними головними компонентами.

Крім того, результати групування на основі певних компонентів можуть бути використані для проведення порівняльного аналізу факторів, які сприяли найбільш значним покращенням безпеки. Такий аналіз дозволяє виявити прогресивні тенденції підвищення ефективності використання виробничих ресурсів.

РОЗДІЛ 3
ПЕРЕВІРКА АДЕКВАТНОСТІ МОДЕЛІ

3.1 Програмна реалізація побудованої моделі

Факторний аналіз пропонує рішення шляхом поділу характеристик на незалежні джерела варіації (фактори). Тоді кожен фактор представляє шкалу, засновану на емпіричних зв’язках між характеристиками.

Для реалізації використано пакет аналізу даних STATISTICA.

Statistica — це вдосконалений аналітичний пакет програмного забезпечення, спочатку розроблений StatSoft і наразі підтримується TIBCO Software Inc.[31]. Statistica забезпечує аналіз даних, керування даними, статистику, аналіз даних, машинне навчання, текстову аналітику та процедури візуалізації даних.

Маючи на вході вибірку даних, створюється кореляційна матриця.

Отримаємо таку таблицю коефіцієнтів кореляції для досліджуваних ознак (рис.3.1). Таким чином отримуємо існування зв’язку між ризиками, не лише в прямій направленості залежності, а й в оберненій.

Переменная	**Порушення конфіденційності**	Втрата цілісності	Порушення доступності	Порушення роботи системи	Крадіжка	Фальсифікація	Знищення	Віруси	Збої
Порушення конфіденційності	1,00	0,18	-0,04	0,45	0,28	0,19	0,50	0,10	0,16
Втрата цілісності	0,18	1,00	0,19	-0,16	0,44	0,08	-0,16	-0,32	-0,08
Порушення доступності	-0,04	0,19	1,00	0,27	0,02	-0,02	0,34	0,15	-0,07
Порушення роботи системи	0,45	-0,16	0,27	1,00	-0,05	-0,04	0,46	0,36	0,18
Крадіжка	0,28	0,44	0,02	-0,05	1,00	-0,31	0,01	-0,47	0,13
Фальсифікація	0,19	0,08	-0,02	-0,04	-0,31	1,00	-0,01	0,28	-0,34
Знищення	0,50	-0,16	0,34	0,46	0,01	-0,01	1,00	0,32	0,01
Віруси	0,10	-0,32	0,15	0,36	-0,47	0,28	0,32	1,00	0,25
Збої	0,16	-0,08	-0,07	0,18	0,13	-0,34	0,01	0,25	1,00

Рисунок 3.1 – Матриця кореляції

Додаток дає можливість встановити рівень для мінімального значення для власних змінних. Якщо значення менше за цей рівень, то розрахунок не розпочнеться. Також у МГК максимально можлива кількість змінних буде дорівнювати кількості

вибірок. Кожній змінні буде відповідати рівень дисперсії, тобіж мінливість. Її прийнято називати власним значенням, що відповідає змінним. Вхідні параметри для моделі зображено на (рис. 3.2).

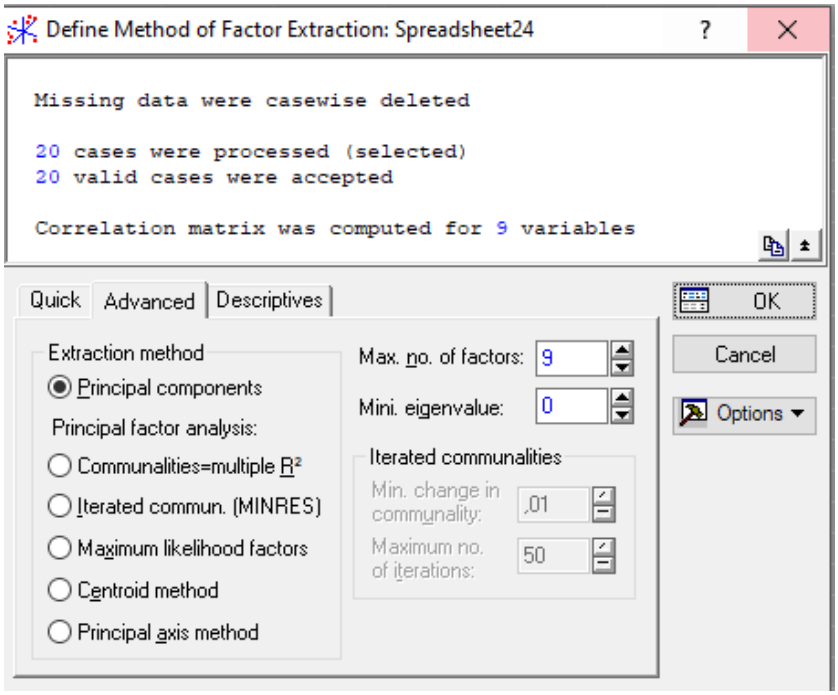

Рисунок 3.2 –Вікно налаштування методу дослідження

Результати факторного аналізу зображено на (рис. 3.3).

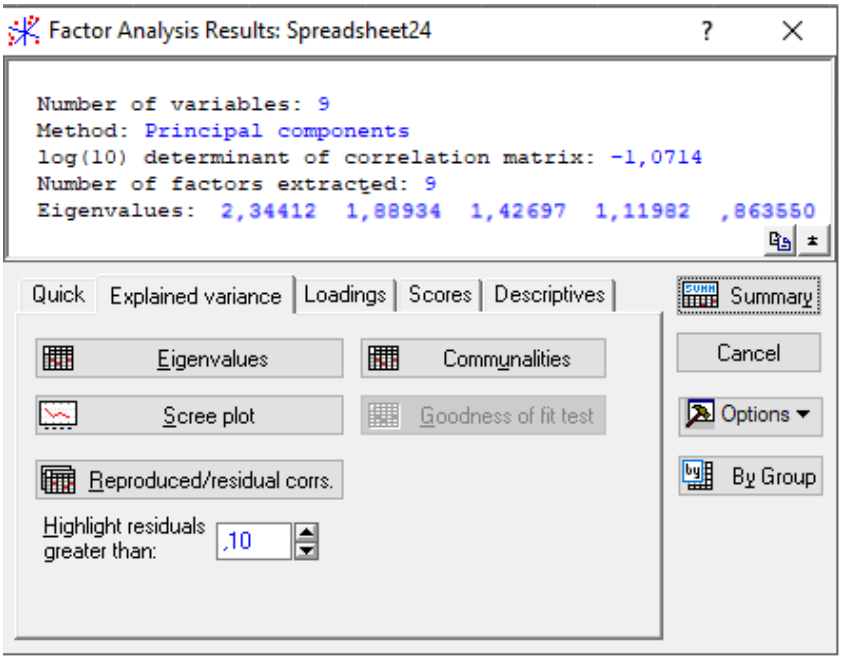

Рисунок 3.3 – Результати факторного аналізу

У рядках отримуємо інформацію про відповідний номер виділеного чинника, у стовпцях – власне значення, відсоток загальної дисперсії, який вираховується самим чинником; накопичена дисперсія – показує відсоток, який поясненюється сукупністю чинників. Результат зображено в табличній формі на (рис. 3.4).

Значен.	Собств. Знач.	% общей дисперс.	Кумулятивн. Собств. Знач.	Кумулятивн. %
1	2,344118	26,04576	2,344118	26,0458
2	1,889340	20,99266	4,233458	47,0384
3	1,426975	15,85528	5,660433	62,8937
4	1,119822	12,44246	6,780254	75,3362
5	0,863550	9,59500	7,643805	84,9312
6	0,524862	5,83180	8,168667	90,7630
7	0,347828	3,86476	8,516495	94,6277
8	0,305656	3,39618	8,822151	98,0239
9	0,177849	1,97610	9,000000	100,0000

Рисунок 3.4 – Результати факторного аналізу

З даних факторів визначаються ті, які мають більший вплив на інформаційну безпеку. Відповідно до критеріїв Кайзера (the Kaiser criterion), потрібні лише ті фактори, власні значення котрих перевищує одиницю. Це підтверджується на графіку створений по критерію відсіювання за яким можливо отримати важливі фактори (рис. 3.5).

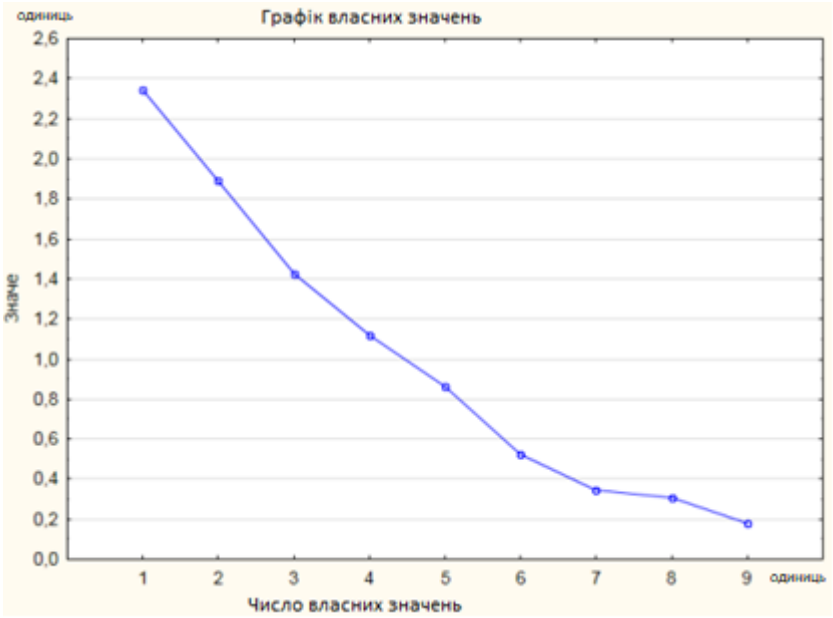

Рисунок 3.5 – Графік критерію відсіювання

Для з'ясування чинників, що мають знайчний вплив на пояснення дисперсії, користуємся дослідженням факторних навантажень. Отримаємо матрицю кореляції між змінними та виділеними чинниками. Результат представлено на таблиці факторних навантажень (рис 3.6).

	Фактор 1	Фактор 2	Фактор 3	Фактор 4	Фактор 5	Фактор 6	Фактор 7	Фактор 8	Фактор 9
Порушення конфіденційності	0,526335	0,560720	0,198213	-0,523029	0,083393	0,016505	0,083480	-0,135851	-0,251128
Втрата цілісності	-0,331718	0,587815	0,455440	0,023101	-0,464067	-0,038484	0,311299	0,120758	0,090267
Порушення доступності	0,336530	0,215951	0,279118	0,803672	-0,230836	0,016814	-0,130522	-0,175753	-0,121752
Порушення роботи системи	0,768281	0,229855	-0,088529	0,042948	0,081609	-0,567654	-0,020611	0,066816	0,115969
Крадіжка	-0,289505	0,841732	-0,059009	-0,059933	0,048842	0,087359	-0,382735	0,209100	0,019315
Фальсифікація	0,179320	-0,352269	0,743595	-0,375676	-0,218706	0,008514	-0,253739	-0,136521	0,136964
Знищення	0,750523	0,276231	0,102887	0,134953	0,348089	0,399106	0,114189	-0,000829	0,195249
Віруси	0,721557	-0,416370	-0,054121	-0,040813	-0,374931	0,151525	-0,031418	0,355061	-0,103967
Збої	0,231618	0,218318	-0,724283	-0,182737	-0,518976	0,103177	-0,039938	-0,220987	0,101488
Общ дис.	2,344118	1,889340	1,426975	1,119822	0,863550	0,524862	0,347828	0,305656	0,177849
Доля общ	0,260458	0,209927	0,158553	0,124425	0,095950	0,058318	0,038648	0,033962	0,019761

Рисунок 3.6 – Таблиця факторних навантажень

Зображено ступінь впливу кожного з факторів на вхідні дев’ять ризиків моделі. Можна спостерігати ступінь впливу кожного чинника. Початкові чотири є суттєвими і пояснюють велику частку залежності та загальної дисперсії.

Значення факторних оцінок по кожному спостереженню зображено на (рис.3.7).

Коефіцієнти відповідають ступеню впливу прихованих чинників по кожному ризику. Цей вплив зумовлює відповідну варіацію ознак.

Набл.	Фактор 1	Фактор 2	Фактор 3	Фактор 4	Фактор 5	Фактор 6	Фактор 7	Фактор 8	Фактор 9
1	-0,17283	0,23102	-0,84313	-1,20044	-1,11656	-0,39817	-0,21618	-0,57480	-1,97391
2	-1,48159	-0,58874	0,02290	-1,84729	-0,07582	0,29154	-0,57746	-0,50931	1,15367
3	-0,96649	-0,16165	0,08641	-0,99699	-2,35247	0,81735	-0,24226	-0,28960	0,73715
4	-0,36271	0,99526	1,30243	0,54150	0,56910	1,93386	1,59760	-0,93940	-1,08676
5	-2,22206	0,49031	-0,23548	0,81088	0,10929	0,16224	0,11947	2,59291	0,31210
6	-0,68659	0,00337	0,26016	-0,00033	1,13431	-0,31567	0,22470	0,28723	0,68020
7	-1,22937	-1,54989	0,00088	1,54438	0,60550	-0,03293	-0,62847	-1,63194	-1,31503
8	0,89321	-1,59452	0,38788	-0,40751	0,49748	-1,06483	-0,61202	1,37878	0,24301
9	1,02017	0,93288	1,16541	-0,00711	-0,71762	-0,13666	0,31461	-0,38355	1,41618
10	0,34476	-0,79329	1,55484	0,65177	-1,36400	0,12846	1,16182	1,25916	-0,28792
11	-0,13928	1,54486	-0,73961	-0,33733	1,45513	1,07635	0,23962	0,31878	-0,06692
12	1,20162	-1,26712	0,25895	0,55935	-0,21009	1,45868	-0,82405	-0,56456	0,41665
13	-0,38463	1,67039	0,33958	0,08563	-0,78570	-2,12173	-0,95141	-0,30302	-1,34386
14	0,46267	-0,54127	0,48123	1,12951	0,26101	-1,47634	0,96871	0,18690	-0,37047
15	-0,10303	-0,39611	-1,89032	1,66182	-0,29686	0,55643	-1,25360	-0,15733	0,61809
16	0,01412	0,04869	-1,56188	0,15851	0,11279	-1,44045	2,26363	-1,46467	1,69340
17	0,21614	-1,24271	0,41188	-2,10298	1,42668	-0,08460	0,44820	-0,04556	-0,77923
18	1,58632	0,63845	-0,50288	0,14952	-0,93745	0,50664	-0,15354	0,23637	-0,21929
19	0,55028	1,27163	1,33383	0,12532	1,24214	-0,39204	-2,04865	-0,53010	0,97253
20	1,45931	0,30843	-1,83307	-0,51821	0,44316	0,53187	0,16927	1,13371	-0,79959

Рисунок 3.7 – Значення факторних оцінок по кожному спостереженню

Перший фактор є головним у моделі, та відображає об'єднання трьох ознак, і впливає найбільше відносно інших. Тобто ризики X1, X7 та X8 можна замінити фактором 1. Фактор 2 має сильний вплив ризик X5, фактор 3 на X6 та X9, а фактор 4 на – ризик X3, і тому можлива їх заміна. Всі навантаження більші за 0,7. Відповідно до факторного аналізі, моделі МГК визначальних факторів, виглядають наступним чином:

$$R_1 = 0{,}77 \cdot Z_4 + 0{,}75 \cdot Z_7 + 0{,}72 \cdot Z_8\,, \tag{3.1}$$

$$R_2 = 0{,}84 \cdot Z_5\,, \tag{3.2}$$

$$R_3 = 0{,}74 \cdot Z_6 - 0{,}72 \cdot Z_9\,, \tag{3.3}$$

$$R_4 = 0{,}8 \cdot Z_3\,, \tag{3.4}$$

де Z_i – стандартизовані значення змінних X_i .

Для побудови моделей використовувались ваги навантаження, тому необхідно нормалізувати змінні Z, за формулою (2.5). Вигляд моделі в інших змінних:

$$R_1 = 0{,}77 \cdot X_4 + 0{,}75 \cdot X_7 + 0{,}72 \cdot X_8 - 5{,}46, \tag{3.5}$$

$$R_2 = 0{,}84 \cdot X_5 - 2{,}08, \tag{3.6}$$

$$R_3 = 0{,}74 \cdot X_6 - 0{,}72 \cdot X_9 - 0{,}43, \tag{3.7}$$

$$R_4 = 0{,}8 \cdot X_3 - 2{,}82\,, \tag{3.8}$$

де R_1, R_2, R_3, R_4 – нормалізовані моделі МГК визначальних факторів.

3.2 Перевірка адекватності побудованих моделей

Моделі оцінки ризиків інформаційної безпеки, розроблені за допомогою факторного аналізу, повинні пройти перевірку на адекватність. Незалежно від типу або методу побудови моделі, придатність її застосування для оцінки ризиків інформаційної безпеки може бути визначена лише шляхом встановлення її адекватності. Однак повна відповідність між моделями і реальним процесом або

об'єктом неможлива, що робить адекватність дещо умовним поняттям. Модель може бути точною, але неадекватною, або навпаки. Це може дати результати, які відповідають дійсності, але не відповідають певним критеріям адекватності.

Адекватність регресійних моделей можна оцінити за допомогою статистичного аналізу залишкової послідовності. Для оцінки точності регресійних моделей використовуватимуться статистичні критерії Фішера та Стьюдента. Стандартна помилка рівняння, яка представляє емпіричну дисперсію залишків, вказує на абсолютний розкид випадкової складової рівняння. З поправкою на ступені свободи він забезпечує неупереджену оцінку залишкової дисперсії (3.9). Моделі з меншою стандартною помилкою рівняння є кращими перед іншими, оскільки вони демонструють більшу точність.

$$\sigma_z^2 = \frac{1}{n-m-1}\sum_{i-1}^{n}\varepsilon_i^2. \quad (3.9)$$

Перевірка значущості регресійної моделі проводиться з використанням F-критерію Фішера. Розрахунковим значенням F-критерію є відношення дисперсії вихідної серії спостережень досліджуваного показника до незміщеної оцінки дисперсії залишкової послідовності для моделі. Щоб визначити значущість моделі, порівнюється розраховане значення з табличним значенням на заданому рівні значущості, враховуючи ступені свободи k1 = (m) і k2 = (n - m - 1).

Початкове припущення полягає в тому, що нульова гіпотеза стверджує, що рівняння в цілому є статистично незначущим. У подальшому визначається фактичне значення F-критерію (3.10), і якщо воно перевищує табличне значення, модель вважається значимою.

$$F = \frac{R^2}{1-R^2} \cdot \frac{n-m-1}{m}. \quad (3.10)$$

Табличне значення визначається за допомогою таблиць розподілу Фішера для певного рівня значущості. У лінійній регресії кількість ступенів свободи для загальної

суми квадратів (більша дисперсія) дорівнює 1, а кількість ступенів свободи для залишкової суми квадратів (менша дисперсія) дорівнює n-2.

Табличне значення, позначене як F_{tabl} представляє максимально можливе значення критерію під впливом випадкових факторів, заданих ступенями свободи та рівнем значущості α. Рівень значущості α являє собою ймовірність відхилення правильної гіпотези, коли вона насправді вірна. Зазвичай α вибирається рівним 0,05. Якщо розраховане значення F-критерію менше табличного значення, це означає, що немає достатніх доказів для відхилення нульової гіпотези. І навпаки, якщо розраховане значення перевищує значення таблиці, нульова гіпотеза відхиляється, а альтернативна гіпотеза щодо статистичної значущості рівняння в цілому приймається з імовірністю (1-α).

Для оцінки статистичної значущості коефіцієнтів регресії та кореляції використовується t-критерій Стьюдента. Нульова гіпотеза припускає, що коефіцієнти є випадковими і істотно не відрізняються від нуля. Методи перевірки гіпотез використовуються, щоб визначити, чи є параметри статистично значущими, що вказує на значущу різницю від нуля в популяції.

Основна гіпотеза сформульована на основі припущення про відсутність суттєвої різниці від нуля параметра або статистичної характеристики в генеральній сукупності. Поряд з основною гіпотезою пропонується альтернативна гіпотеза, яка передбачає нерівність до нуля параметра або статистичної характеристики в генеральній сукупності. Для оцінки основної гіпотези щодо рівності коефіцієнтів регресії проведемо перевірку значущості на обраному рівні значущості α = 0,05. Якщо основна гіпотеза виявиться невірною, приймається альтернативна гіпотеза. Для перевірки цієї гіпотези використовується t-критерій Стьюдента (3.11).

$$t = \frac{R\sqrt{n-m-1}}{\sqrt{1-R^2}} \qquad (3.11)$$

Отримане значення t-критерію з даних спостережень порівнюється з критичним (табличним) значенням, яке визначається на основі рівня значущості (α) і ступенів свободи. Якщо абсолютне значення розрахованого t-критерію перевищує табличне

значення, основна гіпотеза відхиляється. Це вказує на те, що з імовірністю (1-α) параметр або статистична характеристика в генеральній сукупності істотно відрізняється від нуля. З іншого боку, якщо абсолютне значення розрахованого t-критерію менше табличного значення, немає достатніх доказів, щоб відхилити основну гіпотезу. У цьому випадку можна зробити висновок, що параметр або статистична характеристика в генеральній сукупності істотно не відрізняється від нуля при обраному рівні значущості α.

Для проведення перевірки відповідності для чотирьох моделей використаєм програмний пакет Statistica.

Визначимо параметри нелінійної функції для моделі R_1 (рис 3.8)

N=20	Результат регресії для залежних змінних: У1 (Ризики) R=1.00000 R2=1.00000 F(3.16)=240E14 p<0.0000 Бета	Ст. Ош. Бета	B	Ст. Ош. B	t(16)	p-знач.
Св. член			-5,46000	0,000000	-508516139	0,00
Порушення роботи системи	0,442733	0,000000	0,77000	0,000000	166977666	0,00
Знищення	0,438051	0,000000	0,75000	0,000000	167519774	0,00
Віруси	0,424569	0,000000	0,72000	0,000000	170670283	0,00

Рисунок 3.8 – Таблиця регресії для моделі R_1

На основі даних моделі R_1 визначено коефіцієнт детермінації рівним 1, що свідчить про те, що 100% варіації показника можна пояснити варіаціями показників несправності системи, знищення інформації та вірусів.

Значимість коефіцієнта множинної кореляції оцінюють за допомогою таблиці F-критерію Фішера. У цьому випадку табличне значення F-тесту Фішера з 16 ступенями свободи (20 спостережень мінус 4) і рівнем значущості α 0,05 становить 3,24. Однак розраховане значення становить 240, що значно перевищує табличне значення. Це означає, що знайдені значення є статистично значущими. Зазвичай вважається прийнятним для практичного використання, коли розраховане значення F-тесту принаймні в 4 рази перевищує табличне значення (F_{tabl}). Ця умова в нашому випадку виконується.

На рисунку 3.8 показано значення параметрів b_0 і b_1 рівняння регресії в стовпці B. Значущість цих параметрів оцінюється за допомогою таблиці t-критерію

Стьюдента. Розраховані значення t-критерію Стьюдента для кожного параметра (показані в стовпці t(16)) порівнюються з табличним значенням t-критерію для 16 ступенів свободи.

Табличне значення (F_{tabl}) на рівні значущості α 0,05 становить 2,12. Обидва розраховані значення t-критерію для параметрів b_0 і b_1 вищі за табличне значення, що вказує на значущість цих знайдених значень.

Подібні розрахунки будуть виконані для моделей R_2, R_3 і R_4. На рисунку 3.9 представлені результати множинної регресії для моделі R_2.

Результат регресії для залежних змінних: У2 (Ризики)
R1=1.000000000 R2=1.000000000
F(1,18)=-.0408 p<0.0053

N=20	БЕТА	Ст.Ош. БЕТА	B	Ст.Ош. B	t(18)	p-знач.
Св.член			-2,08000	0,0000	0,01	0,0053
Крадіжка	1,000000	0,0020	0,84000	0,0000	1,03	0,0040

Рисунок 3.9 – Таблиця регресії для моделі R_2

Згідно з даними моделі R_2, коефіцієнт детермінації визначено рівним 1, що свідчить про те, що 100% варіації показника можна пояснити варіацією показника крадіжки інформації.

Значимість коефіцієнта множинної кореляції оцінюють за допомогою таблиці F-критерію Фішера. У цьому випадку табличне значення F-критерію Фішера з 18 ступенями свободи та рівнем значущості α 0,05 становить 4,41. Однак розрахункове значення становить 0,04, що значно менше табличного значення. Це свідчить про статистичну незначущість знайдених значень.

На малюнку 3.9, в стовпці B відображаються значення параметрів b_0 і b_1 рівняння регресії. Значущість цих параметрів оцінюється за допомогою таблиці t-критерію Стьюдента. Розраховані значення t-критерію Стьюдента для кожного параметра (відображені в стовпці t(18)) порівнюються з табличним значенням t-критерію для 18 ступенів свободи.

Табличне значення (F_{tabl}) на рівні значущості α 0,05 становить 2,10. Обидва розрахункові значення t-критерію для параметрів b_0 і b_1 менші за табличне значення, що свідчить про незначущість цих знайдених значень.

На рисунку 3.10 представлені результати множинної регресії для моделі R_3.

Згідно з даними моделі R_3, коефіцієнт детермінації визначено рівним 1, що свідчить про те, що 100% варіації показника можна пояснити варіацією показників фальсифікації інформації та програмно-технічних збоїв.

Результат регресії для залежних змінних: УЗ (Ризики)
R=1.000000000 R2=1,000000000
F(2,17)=1.5532 p<0.0025

N=20	БЕТА	Ст.Ош. БЕТА	B	Ст.Ош. B	t(17)	p-знач.
Св.член			-0,430000	0,0106	0,40	0,00029
Фальсифікація	0,597290	0.0016	0,740000	0,0003	1,18	0,00000
Збої	-0,625742	0.0030	-0,720000	0,0009	2,01	0,00008

Рисунок 3.10 – Таблиця регресії для моделі R_3

Достовірність коефіцієнта множинної кореляції оцінюють за допомогою таблиць F-критерію Фішера. У цьому випадку табличне значення для F-критерію Фішера з 17 ступенями свободи та рівнем значущості α 0,05 становить 3,59. Однак розраховане значення становить 1,55. Оскільки фактичне значення F менше табличного значення (F < F_{tabl}), оцінене рівняння регресії вважається статистично ненадійним.

На малюнку 3.10, в стовпці B відображаються значення параметрів b_0 і b_1 рівняння регресії. Значущість цих параметрів оцінюється за допомогою таблиці t-критерію Стьюдента. Розраховані значення t-критерію Стьюдента для кожного параметра (відображені в стовпці t(17)) порівнюються з табличним значенням t-критерію для 17 ступенів свободи.

Табличне значення (F_{tabl}) на рівні значущості α 0,05 становить 2,10. Обидва розрахункові значення t-критерію для параметрів b_0 і b_1 менші за табличне значення, що свідчить про незначущість цих знайдених значень.

На рисунку 3.11 представлені результати множинної регресії для моделі R_4.

Результат регресії для залежних змінних: У4 (Ризики)
R=1.000000000 R2=1.000000000
F(1.18)=3.084 p<0.0000

N=20	БЕТА	Ст.Ош. БЕТА	B	Ст.Ош. B	t(18)	p-знач.
Св.член			-2,82000	0,000000	0,430	0,00
Порушення доступності	1,000000	0,000000	0,80000	0,000000	1,273	0,00

Рисунок 3.11 – Таблиця регресії для моделі R_4

Відповідно до моделі R_4, коефіцієнт детермінації дорівнює 1, що свідчить про те, що 100% варіації показника можна пояснити варіацією показника порушення доступності.

Щоб оцінити значущість коефіцієнта множинної кореляції, звернемося до таблиці F-критерію Фішера. Для випадку з 18 ступенями свободи та рівнем значущості α 0,05 табличне значення F-тесту Фішера становить 4,41. Однак розрахункове значення становить 3,08. Оскільки фактичне значення F менше табличного значення (F < F_{tabl}), можливо зробити висновок, що оцінене рівняння регресії є статистично ненадійним.

На малюнку в стовпці B відображаються значення параметрів b_0 і b_1 рівняння регресії. Значущість цих параметрів оцінюється за допомогою таблиці t-критерію Стьюдента. Розраховані значення t-критерію Стьюдента для кожного параметра (відображені в стовпці t(17)) порівнюються з табличним значенням t-критерію для 17 ступенів свободи.

При рівні значущості α 0,05 табличне значення (F_{tabl}) дорівнює 2,10. Обидва розрахункові значення t-критерію для параметрів b_0 і b_1 менші за табличне значення, що свідчить про незначущість цих знайдених значень. Таким чином, з огляду на перевірку адекватності створеної моделі оцінки ризиків інформаційної безпеки, лише модель R_1 вважається придатною для подальшої роботи та точного аналізу.

3.3 Інтерпретація отриманих результатів

Після розрахунку моделі R_1 значення R_a служить оцінкою ризику інформаційної безпеки. Вищі значення R_a вказують на більші ризики для

інформаційної безпеки. Цей показник знаходиться в діапазоні від -r до r. Щоб оцінити ризик, його порівнюють із заздалегідь визначеною якісною шкалою ризику.

Якісна шкала ризику визначається таким чином:

1. Зона прийнятного (мінімального) ризику (-r; -1): Ця зона характеризується рівнем збитків, що не перевищує чистого прибутку. Ризики в цій зоні вважаються прийнятними.

2. Зона допустимого (підвищеного) ризику (-1; 1): У цій зоні збитки обмежені розрахунковим прибутком. У цій зоні ризику працюють обережні менеджери.

3. Зона катастрофічного (неприйнятного) ризику (1; r): У межах цієї зони очікувані збитки можуть досягати величини, що дорівнює всьому майновому стану підприємства. До цієї зони також відносяться ризики, пов'язані із загрозою життю людей або екологічними катастрофами. Встановлення потенційних зон ризику передбачає порівняння потенційних фінансових втрат з очікуваним прибутком, доходом і капіталом.

У діяльності конкретного суб'єкта господарювання можна використовувати таку класифікацію зон ризику: зона відсутності ризику, зона допустимого ризику, зона критичного ризику, зона катастрофічного ризику (рис 3.12). Ці класифікації допомагають оцінити серйозність ризиків і керувати рішеннями щодо управління ризиками.

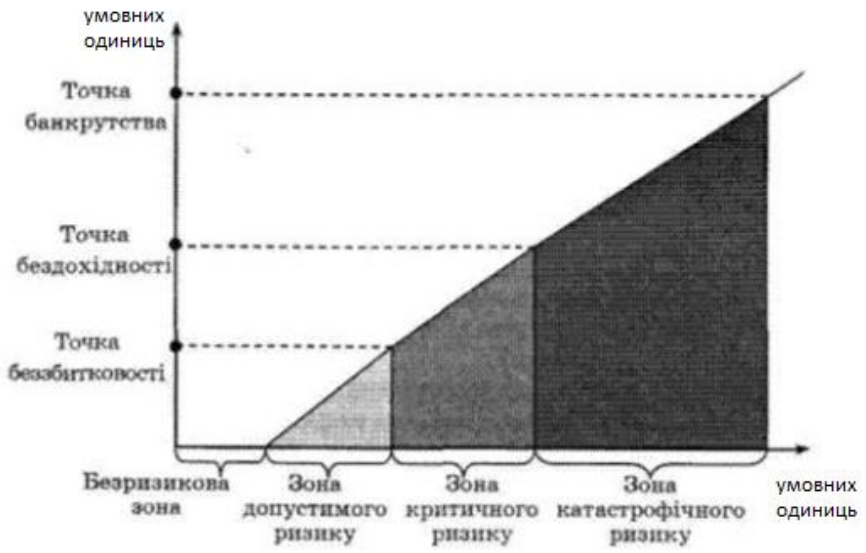

Рисунок 3.12 – Зони ризику

Оцінка ризику служить спрощеним відображенням реальності. Незважаючи на проведення профілактичних заходів, показники свідчать про те, що рівень небезпеки для підприємств залишається значним. Однак завдяки розрахункам стає можливим встановити уніфіковану шкалу, де всі ризики ранжуються відповідно. У цьому контексті конкретне значення індексу не має вирішального значення; швидше, це відносне положення кожного ризику, яке має важливе значення.

Однією з істотних переваг цієї моделі є скорочення часу, необхідного для розрахунку оцінки ризику. Раніше, за початкових умов, отримання найточнішої оцінки ризику вимагало участі мінімум 5 експертів. Проте за нинішньої моделі можливо досягти надійних результатів, залучивши лише 3 експертів. Такий підхід забезпечує більшу надійність, мінімізуючи суб'єктивність у процесі оцінювання.

Для продовження тестування моделі, проводиться кількісний розрахунок оцінки ризику відключення сервера, який є одним із ризиків інформаційної безпеки на підприємстві.

Для початку зберемо оцінки начальника відділу інформаційної безпеки, начальника відділу інформаційних технологій та співробітника відділу інформаційних технологій. Отримаєм від них оцінки ризиків за вербальною шкалою (1 – низький ризик, 2 – середній ризик, 3 – високий ризик).

Зібравши оцінки, видно значні відмінності в рейтингах через такі причини:

Начальник відділу інформаційної безпеки оцінює ризики відключення серверів як високі, оскільки їх реалізація призведе до порушення робочого процесу.

Керівник відділу інформаційних технологій, натомість, оцінює ризики відключення серверів як низькі, оскільки існують процедури регулярного архівування та резервного копіювання даних.

Співробітник відділу інформаційних технологій оцінює ризик як помірний, оскільки вимагатиме залучення серверів, розташованих в інших офісах.

Отже, є експертні оцінки: $X_1 = 3$, $X_2 = 1$, $X_3 = 2$.

Введемо ці значення в модель (3.5), щоб оцінити ризик відключення сервера:

$$F_1 = 0{,}77 \cdot 3 + 0{,}75 \cdot 1 + 0{,}72 \cdot 3 - 5{,}46 = -0{,}96. \quad (3.12)$$

У результаті підраховано, що оцінка ризику для вимкнення системи R_a = -0,96. Виходячи з цього значення, можна зробити висновок, що даний ризик потрапляє в зону допустимого (підвищеного) ризику (-1;1), що характеризується потенційними збитками, які не перевищують розрахунковий прибуток.

Розроблена модель в першу чергу матиме безпосередній вплив на внутрішній стан підприємства. Це пояснюється тим, що методологія дозволяє оцінювати та зменшувати ризики всередині підприємства шляхом удосконалення окремих компонентів. Однак важливо відзначити, що віруси є одним із ризиків, тому вони також можуть впливати на зовнішній стан підприємства, хоча й у меншій мірі.

При оцінці ефективності впровадження моделі зазвичай враховуються наступні компоненти:

- Технічна ефективність: це стосується здатності моделі виконувати функції, для яких вона розроблена. Модель має ефективно оцінювати та аналізувати ризики, надаючи цінну інформацію та рекомендації щодо зменшення ризиків.
- Економічна ефективність: Економічна ефективність вступає в дію, коли обґрунтовуються інформаційні потреби керівництва та вибирається модель вирішення конкретних проблем. Модель має пропонувати економічно ефективні рішення та забезпечувати явну вигоду щодо зменшення ризику порівняно з інвестованими ресурсами.
- Соціальна ефективність: соціальна ефективність пов’язана із заохоченням збільшення інтелектуальної праці серед працівників. Модель має заохочувати проактивний підхід до ризиків інформаційної безпеки, що веде до підвищення обізнаності та залучення працівників до заходів зі зменшення ризиків.

Також складається перелік основних ефектів впровадження моделі оцінки ризиків інформаційної безпеки:

- Зменшення інформаційного ризику: модель дозволяє ідентифікувати та оцінювати ризики інформаційної безпеки, що призводить до ефективних стратегій зменшення ризику та зниження загального рівня інформаційного ризику всередині підприємства.

- Зменшення втрат, пов’язаних із ризиком: шляхом активного виявлення й усунення потенційних ризиків модель допомагає звести до мінімуму виникнення інцидентів безпеки та пов’язаних з ними фінансових втрат.
- Вивільнення додаткового капіталу: завдяки зниженню ризику модель дозволяє оптимізувати розподіл капіталу шляхом мінімізації потреби в надмірних інвестиціях у заходи зі зменшення ризику.
- Збільшення прибутку від фондів: зі зниженими ризиками підприємство може досягти вищих прибутків від інвестованих коштів, оскільки ресурси можуть розподілятися ефективніше.
- Збільшення доходу за рахунок вивільненого капіталу: шляхом перерозподілу капіталу зі зменшення ризиків на діяльність, що приносить дохід, підприємство може потенційно збільшити свій дохід і прибутковість.
- Зменшення внутрішніх і зовнішніх крадіжок: модель допомагає визначати вразливі місця та впроваджувати превентивні заходи, що призводить до зменшення як внутрішніх, так і зовнішніх випадків крадіжок або несанкціонованого доступу.
- Удосконалення командної роботи. Спільний характер моделі сприяє міжвідомчому співробітництву та комунікації, сприяючи міцнішій культурі командної роботи на підприємстві.
- Технічні оновлення та оновлення програмного забезпечення: модель висвітлює потенційні сфери для вдосконалення, заохочуючи впровадження оновлених технологій і програмних рішень для підвищення інформаційної безпеки.
- Удосконалення управління виробництвом: розглядаючи ризики інформаційної безпеки, модель сприяє кращому управлінню виробництвом, забезпечуючи безпечний і ефективний робочий процес.
- Підвищення довіри клієнтів до підприємства: за допомогою надійної моделі оцінки ризиків інформаційної безпеки клієнти отримують впевненість у здатності підприємства захистити їхні конфіденційні дані, тим самим зміцнюючи їхню довіру та лояльність.

- Підвищення прозорості в роботі: модель сприяє прозорості, надаючи чітку структуру для оцінки та управління ризиками інформаційної безпеки, дозволяючи зацікавленим сторонам краще розуміти практику безпеки підприємства.
- Поліпшення фінансового стану: Завдяки зниженню ризику та підвищенню операційної ефективності фінансовий стан підприємства може покращитися, що призведе до більш стабільного та сталого фінансового становища.
- Та інші ефекти: впровадження моделі також може мати додаткові позитивні наслідки, такі як покращення дотримання нормативних вимог, підвищення репутації та краща відповідність найкращим галузевим практикам.

Важливо враховувати, що проведення експрес-оцінки ризиків інформаційної безпеки та зручності використання демонструє технічну ефективність моделі. Крім того, впровадження моделі може опосередковано сприяти більшій зацікавленості працівників у результатах своєї роботи, оскільки вона стає більш інтелектуально захоплюючою та різноманітною, підкреслюючи аспект соціальної ефективності.

Висновки за розділом 3

Для реалізації використано пакет аналізу даних STATISTICA.

Моделі оцінки ризиків інформаційної безпеки, розроблені за допомогою факторного аналізу, повинні пройти перевірку на адекватність. Незалежно від типу або методу побудови моделі, придатність її застосування для оцінки ризиків інформаційної безпеки може бути визначена лише шляхом встановлення її адекватності. Однак повна відповідність між моделями і реальним процесом або об'єктом неможлива, що робить адекватність дещо умовним поняттям. Модель може бути точною, але неадекватною, або навпаки. Це може дати результати, які відповідають дійсності, але не відповідають певним критеріям адекватності.

З огляду на перевірку адекватності створеної моделі оцінки ризиків інформаційної безпеки, лише модель R_1 вважається придатною для подальшої роботи та точного аналізу.

Створена модель оцінювання була інтерпретована для перевірки розподіленої системи на підприємстві.

У результаті роботи підраховано, що оцінка ризику для вимкнення системи $R_a = -0{,}96$. Виходячи з цього значення, можна зробити висновок, що даний ризик потрапляє в зону допустимого (підвищеного) ризику (-1;1), що характеризується потенційними збитками, які не перевищують розрахунковий прибуток.

Розроблена модель в першу чергу матиме безпосередній вплив на внутрішній стан підприємства. Це пояснюється тим, що методологія дозволяє оцінювати та зменшувати ризики всередині підприємства шляхом удосконалення окремих компонентів. Однак важливо відзначити, що віруси є одним із ризиків, тому вони також можуть впливати на зовнішній стан підприємства, хоча й у меншій мірі.

ВИСНОВКИ

Розподілені системи стають все більш популярними завдяки своїй високій доступності, масштабованості та відмовостійкості. Однак вони також створюють певні проблеми, які необхідно вирішити. Розуміючи характеристики та проблеми розподілених систем, розробники можуть проектувати та впроваджувати ефективні розподілені системи, які відповідають потребам їхніх користувачів.

Моделі оцінки ризиків інформаційної безпеки, розроблені за допомогою факторного аналізу, повинні пройти перевірку на адекватність. Незалежно від типу або методу побудови моделі, придатність її застосування для оцінки ризиків інформаційної безпеки може бути визначена лише шляхом встановлення її адекватності. Однак повна відповідність між моделями і реальним процесом або об'єктом неможлива, що робить адекватність дещо умовним поняттям. Модель може бути точною, але неадекватною, або навпаки. Це може дати результати, які відповідають дійсності, але не відповідають певним критеріям адекватності.

Створена модель оцінювання була інтерпретована для перевірки розподіленої системи на підприємстві.

Розроблена модель в першу чергу матиме безпосередній вплив на внутрішній стан підприємства. Це пояснюється тим, що методологія дозволяє оцінювати та зменшувати ризики всередині підприємства шляхом удосконалення окремих компонентів. Однак важливо відзначити, що віруси є одним із ризиків, тому вони також можуть впливати на зовнішній стан підприємства, хоча й у меншій мірі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cost of a data breach 2022. A million-dollar race to detect and respond. Access: https://www.ibm.com/reports/data-breach

2. What Is Information Security Risk? Definition and Explanation. Luke Irwin. 20th January 2022. Access: https://www.vigilantsoftware.co.uk/blog/what-is-information-security-risk-definition-and-explanation

3. DEFINITION OF A DISTRIBUTED SYSTEM. Access: https://wachemo-elearning.net/courses/introduction-to-distributed-systemitec3102/lessons/chapter-1-introduction-to-distributed-systems-2/topic/1-2-definition-of-a-distributed-system/

4. P.C. Meunier and E.H. Spafford, “Running the free vulnerability notification system Cassandra,” Proc. 14th Annual Computer Security Incident Handling Conference, Hawaii, Jan. 2002.

5. G. Stoneburner, A. Goguen, and A. Feringa, “Risk Management Guide for Information Technology Systems,” NIST Special Publication 800-30, Washington, DC, 2001.

6. W.A. Arbaugh, et al., “Windows of Vulnerability: A Case Study Analysis,” IEEE Computer, pp. 52-59, Vol. 33 (12), Dec. 2000.

7. M. Dacier, Y. Deswarte, and M. Kaâniche, “Quantitative Assessment of Operational Security: Models and Tools,” Technical Report, LAAS Report 96493, May 1996.

8. The American Heritage Dictionary of the English Language, Fourth Edition, Houghton Mifflin, 2000.

9. B. Bhargava and Y. Zhong, “Authorization Based on Evidence and Trust,” Proc. Intl. Conf. on Data Warehousing and Knowledge Discovery DaWaK-2002, Aix-en-Provence, France, Sep. 2002.

10. Y. Zhong, Y. Lu, and B. Bhargava, “Dynamic Trust Production Based on Interaction Sequence,” Tech. Rep. CSD-TR 03-006, Dept. Comp. Sciences, Purdue Univ., Mar.2003.

11. C. Meadows, “Applying the Dependability Paradigm to Computer Security,” Proc. Workshop on New Security Paradigms, Sep. 1995, pp. 75-81.

12. E. Jonsson et al., “On the Functional Relation Between Security and Dependability Impairments,” Proc. 1999 Workshop on New Security Paradigms, Sep. 1999, pp. 104-111.

13. G. Song et al., “CERIAS Classic Vulnerability Database User Manual,” Technical Report 2000-17, CERIAS, Purdue University, West Lafayette, IN, 2000.

14. N.R. Mead, R.J. Ellison, R.C. Linger, T. Longstaff, and J. McHugh, “Survivable Network Analysis Method,” Tech. Rep. CMU/SEI-2000-TR-013, Pittsburgh, PA, Sep. 2000.

15. P. Ammann, S. Jajodia, and P. Liu, “A Fault Tolerance Approach to Survivability,” in Computer Security, Dependability, and Assurance: From Needs to Solutions, IEEE Computer Society Press, Los Alamitos, CA, 1999.

16. Determining Key Risks for Modern Distributed Information Systems, Dmytro Palko, Hrygorii Hnatienko, Tetiana Babenko, Andrii Bigdan, Taras Shevchenko National University of Kyiv 64/13, Volodymyrska Street, Kyiv, 01601, Ukraine, 2021.

17. 2019 Global Cyber Risk Perception Survey // Marsh, Microsoft. - 2019. Access: https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf

18. Konev I. Informatsyonnaya bezopasnost predpriyatiya. / I. Konev, A. Beliaev SPb.:BKhVPeterburg, 2003.

19. Chang, L.-Y. Applying fuzzy expert system to information security risk Assessment - A case study on an attendance system [Text] / L.-Y. Chang, Z.-J. Lee // 2013 International Conference on Fuzzy Theory and Its Applications (iFUZZY). - 2013. doi: 10.1109/ifuzzy.2013.6825462.

20. Xin Y. et al. Machine learning and deep learning methods for cybersecurity //IEEE access. – 2018.– Vol. 6. – P. 35365-35381.

21. Архипов А.Є., Архипова С.А. Применения мотивационностоимостных моделей для описания вероятностных соотношений в системе «атака-защита».

Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 1(16) вип., 2008р.

22. Шапорін, В.О. Моделі та методи аналізу ризиків безпеки інформаційних систем: дис. канд. техн. наук : 05.13.06 — Інформаційні технології - Одеса, 2016. – 178 с.

23. ISO 31000 Risk Management. Brien Posey. Access: https://www.techtarget.com/searchsecurity/definition/ISO-31000-Risk-Management

24. Understanding the Differences between the COSO ERM Framework and ISO 31000 Risk Management Standards. Lisanne Sison, Jim Doran. Access: https://www.ajg.com/us/news-and-insights/2020/oct/coso-iso-3100-risk-management-plans/

25. What Is ISO 27001:2013? A Guide for Businesses. Adam Nunn. Access: https://auth0.com/blog/what-is-iso-27001-2013-a-guide-for-businesses/

26. ISO/IEC 27005 Information Security Risk Management - Training Courses. Access: https://pecb.com/en/education-and-certification-for-individuals/iso-iec-27005

27. ISO/IEC 17799:2005. Access: https://www.iso.org/standard/39612.html

28. NIST SP 800-30 standard for technical risk assessment: An evaluation. Dharshan Shanthamurthy. 05 Aug 2011. Access: https://www.computerweekly.com/tip/NIST-SP-800-30-standard-for-technical-risk-assessment-An-evaluation

29. What is BSI Standard 200-3? // March 7, 2022 by Information Security Asia. Access: https://informationsecurityasia.com/what-is-bsi-standard-200-3/

30. What is COBIT? // Access: https://www.forcepoint.com/cyber-edu/cobit

31. TIBCO Statistica Enterprise. Access: https://www.tibco.com/resources/datasheet/tibco-statistica-enterprise

32. Technical Standard Risk Taxonomy ISBN 1-931624-77-1 Document Number: C081 Published by The Open Group, January 2009.

33. Whitman, Michael E.; Mattord, Herbert J. Management of Information Security. Cengage Learning. ISBN 978-1-305-15603-6. 18 October 2013.

34. «An Introduction to Factor Analysis of Information Risk (FAIR)», Risk Management Insight LLC, November 2006. Access: https://web.archive.org/web/20150924091313/http://www.riskmanagementinsight.com/media/docs/FAIR_introduction.pdf

35. Freund, Jack; Jones, Jack (2015). Measuring and Managing Information Risk. Waltham, MA: Butterworth-Heinemann. ISBN 9780127999326.

36. Smith, John 2022. Information Security Risk Assessment in Distributed Systems. XYZ Publishing House.

37. Johnson, Sarah. 2021. Managing Information Security Risks in Distributed Environments. ABC Press.

38. Brown, Michael. 2020. Risk Management for Distributed Information Systems. DEF Publishers.

39. Anderson, Lisa. 2019. Assessing Information Security Risks in Distributed Networks. GHI Publications.

40. Wilson, David. 2018. Information Systems Risk Assessment and Management in Distributed Environments. JKL Books.

ДОДАТОК А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Тези наукових доповідей:

1. Гальміз Максим, Бабенко Тетяна. Вирішення проблем оцінки ризиків інформаційної безпеки в розподілених інформаційних системах. Міжнародна науково-практична конференція «Наукоємні технології в інфокомунікаціях», 2023, Харків – Кам’янець-Подільський, Україна.