Міністерство освіти і науки України
Сумський державний університет
Навчально-науковий інститут бізнес-технологій «УАБС»
Кафедра економічної кібернетики

КВАЛІФІКАЦІЙНА МАГІСТЕРСЬКА РОБОТА

на тему: «МОДЕЛЮВАННЯ ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

Виконав студент 2 курсу, групи ЕК.м-61а
(номер курсу) (шифр групи)
Спеціальності 051 «Економіка («Економічна кібернетика»)»
Ропаєва А. Г.
(прізвище, ініціали студента)
Керівник ст. викл., к.е.н. Яременко Н.С.
(посада, науковий ступінь, прізвище, ініціали)

Суми – 2018 рік

РЕФЕРАТ

кваліфікаційної магістерської роботи на тему

«МОДЕЛЮВАННЯ ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

студента _____Ропаєвої Анни Геннадіївни_____
(прізвище, ім'я, по батькові)

Актуальність кваліфікаційної магістерської роботи визначається чутливістю телекомунікаційних компаній до надійної і безпечної роботи інформаційних систем, швидкими темпами появи та модифікації нових загроз інформаційній безпеці.

Метою кваліфікаційної магістерської роботи є розробка моделі оцінювання ризиків інформаційної безпеки для телекомунікаційних компаній.

Об'єктом дослідження виступають ризики інформаційної безпеки компанії.

Предметом є методи та моделі, що можуть бути використані для оцінювання ризиків інформаційної безпеки.

Методи дослідження: порівняння та теоретичного узагальнення, аналізу та синтезу, експертний метод, метод факторного аналізу.

Інформаційна база кваліфікаційної магістерської роботи: дослідження українських та закордонних науковців та інформація по ризикам інформаційної безпеки на ТОВ «Неткрекер».

В результаті проведення дослідження було запропоновано модель оцінювання ризиків інформаційної безпеки, яка ґрунтується на використанні факторного аналізу та є придатною для проведення експрес-оцінювання стану інформаційної безпеки підприємства.

Розроблена модель може бути використана керівництвом та фахівцями інформаційної безпеки телекомунікаційних підприємств для ефективного управління ризиками інформаційної безпеки.

Результати, отримані при виконанні кваліфікаційної магістерської роботи, були апробовані на ІІ Міжнародній науково-практичній конференції «Теорія і практика розвитку наукових знань» (28-29 грудня 2017 року), м. Київ. В результаті чого були опубліковані тези доповіді:

– Ропаєва А. Г. Сучасний стан інформаційної безпеки підприємств та організацій в Україні / А. Г. Ропаєва // Теорія і практика розвитку наукових знань (ч. ІІ): матеріали ІІ Міжнародної науково-практичної конференції м. Київ, 28-29 грудня 2017 року. – Київ. : МЦНД, 2017. – С. 22-23.

Ключові слова: ризики, факторний аналіз, інформаційна безпека, оцінка ризиків, метод головних компонент.

Основний зміст кваліфікаційної магістерської роботи викладено на 80 сторінках, зокрема список використаних джерел із 46 найменувань, розміщений на 6 сторінках. Робота містить 4 таблиці, 18 рисунків, а також 2 додатки, розміщені на 3 сторінках.

Рік виконання кваліфікаційної роботи – 2017 рік

Рік захисту роботи – 2018 рік

Міністерство освіти і науки України

Сумський державний університет

Навчально-науковий інститут бізнес-технологій «УАБС»

Кафедра економічної кібернетики

ЗАТВЕРДЖУЮ
Завідувач кафедри
д.е.н., доцент
_____ О.В. Кузьменко
“__” _____2017 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ МАГІСТЕРСЬКУ РОБОТУ
(спеціальність 051 «Економіка («Економічна кібернетика»)»)
студенту 2 курсу, групи ЕК.м-61а

Ропаєвій Анні Геннадіївні
(прізвище, ім’я, по батькові студента)

1. Тема роботи Моделювання оцінювання ризиків інформаційної безпеки затверджена наказом по університету від «08» грудня 2017 року № 2748-III

2. Термін подання студентом закінченої роботи «12» січня 2018 року

3. Мета кваліфікаційної роботи розробка моделі оцінювання ризиків інформаційної безпеки для телекомунікаційних компаній

4. Об’єкт дослідження ризики інформаційної безпеки компанії

5. Предмет дослідження методи та моделі, що можуть бути використані для оцінювання ризиків інформаційної безпеки

6. Кваліфікаційна робота виконується на матеріалах досліджень українських та закордонних науковців з даної тематики та ТОВ «Некрекер».

7. Орієнтовний план кваліфікаційної роботи, терміни подання розділів керівникові та зміст завдань для виконання поставленої мети

Розділ 1 Огляд сучасних економіко-математичних методів та можливості їх використання для оцінювання ризиків інформаційної безпеки – 13 листопада 2017 р.
(назва – термін подання)

У розділі 1 необхідно розглянути сутність ризиків інформаційної безпеки як об’єкта моделювання, провести огляд існуючих підходів до моделювання оцінювання ризиків інформаційної безпеки, виявити найбільш вагомі характеристики об’єкта та дослідити їх взаємозв’язок, сформулювати постановку задачі
(зміст конкретних завдань до розділу, які повинен виконати студент)

Розділ 2 Розробка математичної моделі оцінювання ризиків інформаційної безпеки – 12 грудня 2017 р.
(назва – термін подання)

У розділі 2 необхідно сформувати вимоги до моделі, описати ознаковий простір моделі та розробити математичну модель задачі
(зміст конкретних завдань до розділу, які має виконати студент)

Розділ 3 Перевірка адекватності моделі та пропозиції щодо її використання – 04 січня 2018 р.
(назва – термін подання)

У розділі 3 провести програмну реалізацію побудованої моделі, здійснити апробацію моделі та інтерпретацію отриманих результатів, провести перевірку адекватності моделі.
(зміст конкретних завдань до розділу, які повинен виконати студент)

8. Консультації з роботи:

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1			
2			
3			

9. Дата видачі завдання: «10» жовтня 2017 року

Керівник кваліфікаційної роботи _____ Н.С. Яременко
(підпис) (ініціали, прізвище)

Завдання до виконання одержав _____ А.Г. Ропаєва
(підпис) (ініціали, прізвище)

ЗМІСТ

ВСТУП

З розвитком Internet-технологій і електронної комерції з кожним днем з'являється все більше загроз безпеки інформації. Сьогодні організації все частіше використовують інформацію в бізнес-процесах, для полегшення управлінських рішень і ведення бізнесу. Залежність від інформації в бізнес-середовищі вкрай велика, адже безліч торгових операцій здійснюється в електронному вигляді через Internet. Така інформаційна залежність привела до істотного збільшення впливу рівня безпеки інформаційних систем на успіх, а іноді і просто можливість ведення бізнесу. Тому безпека інформаційних систем є одним з найважливіших питань, яке привертає велику увагу з боку аналітиків, інженерів та інших фахівців в області інформаційно безпеки.

Телекомунікаційні компанії – одні з найбільш чутливих до надійної і безпечної роботи інформаційних систем, так як надані ними послуги практично повністю створюються на основі IT-рішень. Особливу важливість представляють питання боротьби з шахрайством і гарантування доходів. У зв'язку з цим зростає актуальність завдання збереження стабільності роботи компанії.

Мета оцінювання ризиків в інформаційній безпеці – прогнозування можливого збитку, пов'язаного з реалізацією загроз, і відповідно оцінка необхідного обсягу інвестицій на побудову систем захисту інформації.

На практиці застосовуються кількісний і якісний підходи для оцінки ризиків інформаційної безпеки.

При кількісному підході всіх елементів оцінки ризиків привласнюють конкретні і реальні кількісні значення. Об'єктом оцінки може бути цінність активу в грошовому вираженні, ймовірність реалізації загрози, збитки від реалізації загрози, вартість захисних заходів та інше.

При якісному підході до об'єкта оцінки присвоюється показник, проранжований за трибальною, п'ятибальною або десятибальною шкалою. Аналіз ризиків інформаційної безпеки якісним методом повинен проводитися із залученням співробітників, що мають досвід і компетенції в тій області, в якій розглядаються загрози.

Чіткої методики кількісного розрахунку величин ризиків досі не існує. Це пов'язано, в першу чергу, з відсутністю достатнього обсягу статистичних даних про ймовірності реалізації тієї чи іншої загрози. В результаті найбільшого поширення набула якісна оцінка інформаційних ризиків.

Складність бізнес-процесів, їх постійна зміна, а також наявність великого числа розрізнених інформаційних систем призводять до того, що традиційні способи управління правами доступу до IT-систем, наявні в телекомунікаційних компаніях, стають неефективними з точки зору безпеки і витрат ресурсів.

Таким чином, можна помітити, що, з одного боку, оцінка ризиків інформаційної безпеки відіграє важливу роль в стабільному функціонуванні телекомунікаційних компаній, але, з іншого боку, більшість методів і моделей такої оцінки мають недоліки. Деякі з них є тільки якісними методами аналізу, деякі – тільки кількісними, громіздкими для реалізації. Ці традиційні методи оцінки мають масу суб'єктивних проблем і неточностей, тому вони досить складні в застосуванні.

Метою даного дослідження є розробка моделі оцінювання ризиків інформаційної безпеки для телекомунікаційних компаній.

Досягнення поставленої мети передбачає вирішення наступних завдань:

– аналіз сутності інформаційної безпеки як об’єкта моделювання;

– огляд існуючих підходів до моделювання оцінювання ризиків інформаційної безпеки;

– виявлення найбільш вагомих параметрів об’єкта та дослідження їх взаємозв’язку;

– постановка задачі дослідження;

– формування вимог до моделі оцінювання ризиків інформаційної безпеки;

– характеристика вхідних даних, необхідних для модельних розрахунків;

– побудова моделі оцінювання ризиків інформаційної безпеки;

– реалізація побудованої моделі на ЕОМ;

– перевірка адекватності побудованої математичної моделі;

– апробація моделі та інтерпретація отриманих результатів;

– формування пропозицій щодо подальшого використання розробленої моделі.

Об'єктом дослідження є ризики інформаційної безпеки компанії.

Предметом є методи та моделі, що можуть бути використані для оцінювання ризиків інформаційної безпеки.

Результати, отримані при виконанні дипломної роботи, були апробовані на II Міжнародній науково-практичній конференції «Теорія і практика розвитку наукових знань» (28-29 грудня 2017 року), м. Київ. В результаті чого були опубліковані тези доповіді:

– Ропаєва А. Г. Сучасний стан інформаційної безпеки підприємств та організацій в Україні / А. Г. Ропаєва // Теорія і практика розвитку наукових знань (ч. II): матеріали II Міжнародної науково-практичної конференції м. Київ, 28-29 грудня 2017 року. – Київ. : МЦНД, 2017. – С. 22-23.

РОЗДІЛ 1 ОГЛЯД СУЧАСНИХ ЕКОНОМІКО-МАТЕМАТИЧНИХ МЕТОДІВ ТА МОЖЛИВОСТІ ЇХ ВИКОРИСТАННЯ ДЛЯ ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Сутність ризиків інформаційної безпеки як об’єкта моделювання.

Розвиток нових інформаційних технологій і загальна комп'ютеризація привели до того, що інформаційна безпека не тільки стає обов'язковою, вона ще й одна з характеристик інформаційних систем. Існує досить великий клас систем обробки інформації, при розробці яких фактор безпеки відіграє першорядну роль.

Комплексний характер актуальних загроз національній безпеці в інформаційній сфері потребує визначення інноваційних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації [42].

На сьогодні інформація, виступає як однин із факторів (ресурсів) виробництва. Обсяг, достовірність, цілісність, якість обробки інформації визначає ефективність дій менеджменту підприємства, а, отже, актуалізує використання інформаційних технологій в управлінні грошово-кредитними, фінансовими, соціально-економічними процесами даного підприємства. «Без необхідного обсягу та якості інформації неможливо забезпечити розвиток суб’єкта господарювання на основі високотехнологічного виробництва, ефективних методів організації праці» [41].

В умовах економіки постіндустріального суспільства, інформація, що стосується усіх напрямків діяльності підприємства, стає найбільш цінним і дорогим ресурсом, а проблеми інформаційної безпеки – усе більш складними і практично значущими. Інформаційна безпека є однією із

складових частин економічної безпеки, яка формує модель захищеності підприємства.

Глобальні процеси інформатизації суспільства держав світу та широке запровадження інформаційних технологій (як характерні риси нинішнього століття), їх вплив на всі сфери розвитку цих держав, висуває на перший план питання забезпечення інформаційної безпеки. Від виваженої політики інформаційної безпеки, від ступеня захищеності, повноти і достовірності інформації у сучасному світі залежить стабільність соціально-економічної ситуації держави, збереження правопорядку, забезпечення прав її громадян.

Проаналізуємо термінологію щодо інформаційної безпеки. Основні визначення сутності інформаційної безпеки продекларовано у численних нормативно-правових актах центральних органів законодавчої та виконавчої влади.

Інформаційну безпеку можна поділити на такі поняття щодо забезпечення стану захищеності:

– особистості, суспільства, держави від впливу неякісної інформації;

– інформації та інформаційних ресурсів від несанкціонованого впливу сторонніх осіб;

– інформаційних прав і свобод людини і громадянина.

Так, в Законі України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 рр.» цей термін набуває такого трактування: «інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» [36].

Численні дослідники пропонують наступні точки зору щодо аналізованого терміну:

– інформаційна безпека – це стан захищеності потреб інформації особистістю, суспільством і державою, при якому забезпечується їхнє існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз [23];

– під інформаційною безпекою підприємства пропонуємо розуміти суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності [41];

– інформаційна безпека – стан інформації, у якому забезпечується збереження визначених політикою безпеки властивостей інформації [40];

– інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави [20];

– інформаційна безпека – представляє собою стан захищеності потреб в інформації особистості, суспільства і держави, при якому забезпечується їхнє існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз [17];

– під інформаційною безпекою слід розуміти одну із сторін розгляду інформаційних відносин у межах інформаційного законодавства з позицій захисту життєво важливих інтересів особистості, суспільства, держави та акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами [40].

Інформаційна безпека виступає як характеристика стабільного, стійкого стану системи, яка при впливі внутрішніх та зовнішніх загроз та небезпек зберігає суттєво важливі характеристики для власного існування.

Основні характеристики інформаційної безпеки:

– доступність – можливість за прийнятний час отримати шукану інформаційну послугу будь-яким суб'єктом;

– цілісність – актуальність і несуперечливість інформації, її захищеність від руйнування і несанкціонованої зміни;

– конфіденційність – захист від несанкціонованого ознайомлення.

Під інформаційною безпекою будемо розуміти захищеність інформації і підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати неприйнятного збитку суб'єктам інформаційних відносин, в тому числі власникам і користувачам інформації, а також підтримуючої інфраструктури. Захист інформації – це комплекс заходів, спрямованих на забезпечення інформаційної безпеки.

Таким чином, правильний з методологічної точки зору підхід до проблем інформаційної безпеки починається з виявлення суб'єктів інформаційних відносин та інтересів цих суб'єктів, пов'язаних з використанням інформаційних систем (ІС).

Загрози інформаційної безпеки – це зворотній бік використання інформаційних технологій. З цього положення можна вивести два важливих наслідки:

– трактування проблем, пов'язаних з інформаційною безпекою, для різних категорій суб'єктів може істотно різнитися.

– інформаційна безпека не зводиться тільки до захисту від несанкціонованого доступу до інформації, це принципово ширше поняття. Суб'єкт інформаційних відносин може постраждати (зазнати збитків і / або отримати моральну шкоду) не тільки від несанкціонованого доступу, а й від поломки системи, що викликала перерву в роботі. Більш того, для багатьох відкритих організацій (наприклад, навчальних) власне захист від несанкціонованого доступу до інформації стоїть за важливістю аж ніяк не на першому місці.

Вибіркова і безсистемна реалізація заходів, спрямованих на підвищення рівня ІТ-безпеки, не зможе забезпечити необхідного рівня захисту. Щоб сформувати розуміння пріоритетності заходів щодо

підвищення рівня безпеки, необхідно розробити механізм управління ризиками ІТ-безпеки, що дозволить спрямувати всі зусилля на захист від найбільш небезпечних загроз і мінімізацію витрат [25].

Під ризиком, в загальному розумінні цього слова, розуміють можливість або ймовірність настання подій з негативними або позитивними наслідками в результаті певних рішень або дій [28].

Всі ризики є випадковими подіями, що найчастіше обумовлено недоліком якісної інформації про них. Отримання всієї необхідної інформації обмежується відсутністю відповідних інструментальних засобів, часу на збір і обробку даних, дією зовнішніх сил, а також відсутністю повних наукових знань про сутність ризикових процесів або явищ.

Ризик притаманний будь-якій сфері людської діяльності, що зумовлена великою кількістю умов і факторів, що впливають на результат прийнятих людьми рішень. Найбільшого поширення оцінка ризиків отримала в економічній, природній, політичній, військовій сферах діяльності.

Про ризики в області інформаційної безпеки всерйоз заговорили в кінці XX століття, що зумовлено значним вдосконаленням засобів обчислювальної техніки і збільшенням обсягів оброблюваної і переданої інформації. Управління ризиками в області інформаційної безпеки має свої специфічні особливості. Однак варто зазначити, що багато положень теорії ризиків ІБ беруть свій початок із загальної теорії ризиків.

У нормативних документах і методичній літературі часто зустрічаються розбіжності в використовуваній термінології, складі типових процедур оцінки ризиків і наборі оцінюваних параметрів. Це робить необхідним проведення аналізу предметної області оцінки ризиків безпеки інформаційних систем (ІС).

В даний час термін «ризик інформаційної безпеки» або «інформаційний ризик» знайшов широке застосування. Однак поки що не

існує прийнятої більшістю вчених і практиків трактування цього поняття [21]. Наведемо лише деякі з них:

– «можливість настання випадкової події в інформаційній системі підприємства, що приводить до порушення її функціонування, зниження якості інформації, в результаті яких завдається шкода підприємству» [11];

– «небезпека виникнення збитків або шкоди в результаті застосування інформаційних технологій» [16];

– «невизначеність, що припускає можливість втрат (Збитку)» [25];

– «невизначеність, що припускає можливість збитків, які пов'язані з порушенням інформаційної безпеки» [37];

– «потенційна загроза експлуатації уразливості активу, що викликає, таким чином, шкоду для організації» [47].

Далі в роботі під ризиком розуміється ризик інформаційної безпеки, що представляє собою комбінацію ймовірності виникнення ризикової події (наприклад, реалізації загрози) і викликаної при цьому шкоди.

Оцінка ризику розглядається як процес ідентифікації інформаційних ресурсів системи і загроз цих ресурсів, а також можливих втрат, заснований на оцінці частоти виникнення подій і розмір збитку. Кількісна оцінка ризику інформаційної безпеки відкриває можливість більш оптимально розподіляти існуючи обмежені ресурси запобігання виникненню ризикових ситуацій та планувати подальші заходи їх запобігання. Процес оцінки повинен бути адаптований до індивідуальних особливостей організації, але в той же час узгоджений з кращими стандартами та провідними практиками.

Після проведення оцінки ризику, необхідно прийняти рішення: прийняти ризик, знизити ризик або перенести ризик:

– прийняти ризик – значить усвідомити його, змиритися з його можливістю і продовжити діяти як раніше. Стосується загроз з малим збитком і малою вірогідністю виникнення;

– знизити ризик – значить ввести додаткові заходи та засоби захисту, провести навчання персоналу і т д. Тобто провести цілеспрямовану роботу щодо зниження ризику. При цьому необхідно зробити кількісну оцінку ефективності додаткових заходів і засобів захисту. Всі витрати, які несе організація, починаючи від закупівлі засобів захисту до введення в експлуатацію (включаючи установку, настройку, навчання, супровід та ін.), не повинні перевищувати розміру збитку від реалізації загрози;

– перенести ризик – значить перекласти наслідки від реалізації ризику на третю особу, наприклад за допомогою страхування.

1.2 Огляд існуючих підходів до моделювання оцінювання ризиків інформаційної безпеки

Строгої класифікації для методів аналізу ризиків не існує, однак існують відмінності в підходах до аналізу ризиків, способах подання елементів ризику, функціональних можливостях та ін. На основі таких відмінностей можна виділити три основні групи – графічні, математичні та лінгвістичні методи.

Графічні методи – методи, які передбачають візуалізацію об'єктів аналізу і процесів взаємодії між ними. При цьому будуються графи, дерева або діаграми, що дозволяють різним способом відображати інформацію про досліджувані об'єкти. У більшості випадків ці методи дозволяють здійснити лише ідентифікацію елементів ризику і способи взаємодії між ними.

Математичні методи – методи, які передбачають визначення властивостей об'єктів і їх взаємодії за допомогою деяких формальних мов опису, що визначають закони функціонування, зміни властивостей і ін. Дані методи дозволяють не тільки ідентифікувати елементи, але і аналізувати їх поведінку, зміну їх властивостей і вплив на інші елементи.

Лінгвістичні методи є найбільш популярними і простими у використанні, проте не завжди здатні привести до адекватної оцінки ситуації. Дані методи не передбачають будь-яких інструментальних засобів і програм, і вимагають лише наявності команди осіб, відповідальних за аналіз ризику. При цьому всі етапи оцінки ризику, на скільки це можливо, припускають тільки усне спілкування між групою осіб, в ході якого ідентифікуються елементи ризику, будуються припущення про їх поведінку і здійснюється приблизна оцінка можливостей і збитків.

Одне з перших трактувань підходу до вимірювання ризику запропонував Мільтон Фрідмен. Він розглядав проблему розрахунку (оцінки) рівня ризику крізь призму теорії корисності. Фрідмен зазначав, що в умовах спадної корисності і наявності ризику звичайні принципи максимізації не можуть бути використані, оскільки необхідна певна податкова плата у вигляді компенсації за фактор ризику. Рішення, пов’язані з ризиком Фрідмен класифікував так: невеликий ризик, пов’язаний із заздалегідь відомим результатом; помірний ризик без великих доходів і витрат; великий ризик, пов’язаний із великими доходами або збитками. Фрідмен виходив із припущення, що економічна одиниця має певну систему переваг, яка може бути описана функцією, що дає чисельні значення різним альтернативам.

На жаль, сама сутність методології ризиків обумовлює певні труднощі у своєму практичному застосуванні, бо вимагає обчислення високоточних оцінок інформаційних ризиків, оперування з ними й передбачає необхідність певної індивідуалізації, винятковості отриманих в рамках цього підходу рішень.

Для того, щоб отримати більш-менш чітке уявлення про ситуацію, пов’язану з можливостями практичного застосування методології ризиків в сфері інформаційної безпеки, розглянемо численні рекомендації та приклади застосування цієї методології, описані у міжнародних

стандартах, національних нормативних документах та настановах з інформаційної безпеки.

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

Практично всі сучасні стандарти в області безпеки відображають спільний підхід до організації управління ризиками, що склався у міжнародній практиці. При цьому управління ризиками представляться як базова частина системи менеджменту якості організації. Стандарти носять відверто концептуальний характер, що дає змогу експертам з інформаційної безпеки реалізовувати будь-які методи, засоби та технології оцінювання, обробки та управління ризиками.

Вважається, що міжнародні стандарти, створені на основі аналізу та узагальнення найкращих методів, апробованих, як великими групами професіоналів так і провідними організаціями на практиці, в більшості випадків визначають найкращі варіанти дій при виникненні інцидентів в

інформаційній безпеці. Використання стандартів збільшує цінність створюваної інформаційної системи або технології, але немає таких стандартів, які б охопили всі аспекти управління, безпеки та якості.

Методи експертних оцінок є комплексом логічних і математико-статистичних методів і процедур по обробці результатів опитування групи експертів, причому результати опиту є єдиним джерелом інформації. В цьому випадку виникає можливість використання інтуїції, життєвого і професійного досвіду учасників опиту [22].

Методи експертної оцінки ризику історично виникли першими. Вони мають ту істотну перевагу над іншими методами, що експертна оцінка може використовуватися в умовах дефіциту і навіть браку інформації. Головна умова досконалої експертної оцінки – виключення взаємного впливу експертів один на одного (так звана дельфійська процедура). Легкість експертної оцінки і недостатність інформації про оцінювані процеси сприяли появі в Україні величезної кількості фахівців і спеціалізованих видань, які пропонують розроблені ними прогнози. Далеко не завжди це робиться на достатньо професійному рівні. Необхідно розуміти, що будь-яка, навіть і непрофесійна, оцінка, особливо якщо вона повторюється засобами масової інформації, формує у населення певні сподівання і відповідно впливає на поведінку суб’єктів ринку, а ця справа далеко не безпечна. Поведінка експертів в умовах значного браку інформації про об’єкт оцінки підкоряється певним закономірностям. Оцінка економічних явищ мало залежить від якості існуючих економічних прогнозів і дуже добре корелює з дохідністю, яка може бути реально досягнута на даний момент на ринку за чисто об’єктивних, технічних причин.

Найпопулярніший метод експертної оцінки ризику ґрунтується на ідеї обговорення проблеми кількома особами, які вважаються спеціалістами у цьому питанні. Проблема, яка виникає при цьому, полягає в тому, що в результаті прийняття рішення ймовірність правильної оцінки

знижується. Парадоксальність цього явища випливає з самого процесу обговорення. У переважній більшості випадків погляд експертів-аналітиків відрізняється від погляду практиків. Ця розбіжність може бути формалізована через так званий коефіцієнт розбіжності. Задавши цьому коефіцієнту декілька практичних значень, можна одержати ряд можливих ймовірностей розробки точної оцінки.

На сьогодні існують різні підходи і методи оцінки ризиків, запропоновані різними виробниками. Наведемо найбільш поширені методики.

Методика "Facilitated Risk Analysis Process (FRAP)" [12], запропонована компанією Peltier and Associates, дозволяє компаніям віднайти баланс між витратами на засоби захисту й отримуваним ефектом. Оцінка визначається за правилами, що задаються матрицею ризиків, яка виділяє чотири рівні ризиків:

– рівень A – дії, пов'язані з ризиком, повинні бути виконані обов'язково й негайно;

– рівень B – пов'язані з ризиком дії повинні бути виконані;

– рівень C – попередження, що потрібен моніторинг ситуації;

– рівень D – ніяких дій на цей час здійснювати не потрібно.

Компанія RiskWatch розробила методику аналізу ризиків для проведення різних видів аудиту безпеки і сімейство програмних засобів, які її реалізують.

У методі RiskWatch [10] як критерії для оцінки і управління ризиками використовуються очікувані річні втрати і оцінка повернення інвестицій. RiskWatch орієнтована на точну кількісну оцінку співвідношення втрат від загроз безпеки і витрат на створення системи захисту. На виході отримується значення M – це оцінка очікуваних втрат для одного конкретного активу від реалізації однієї загрози.

Коли всі активи і дії ідентифіковані і зібрані разом, то з'являється можливість оцінити загальний ризик інформаційної системи як суму всіх окремих значень.

В основу методу CRAMM [15] покладено комплексний підхід до оцінки ризиків, що поєднує кількісні і якісні методи аналізу і проводиться у три стадії. Для кожного інформаційного процесу будується дерево зв'язків використовуваних ресурсів. Побудована модель дозволяє виділити критичні елементи. Цінність фізичних ресурсів в CRAMM визначається вартістю їх відновлення в разі руйнування, дається оцінка збитків за шкалою зі значеннями від 1 до 10. При низькій оцінці за всіма використовуваними критеріями (3 бали і нижче) вважається, що дана система вимагає базового рівня захисту (без докладної оцінки загроз інформаційної безпеки).

На другій стадії оцінюються залежність призначених для користувача сервісів від певних груп ресурсів і існуючий рівень загроз і уразливостей, обчислюються рівні ризиків і аналізуються результати. Ресурси групуються за типами загроз і уразливостей.

Програмне забезпечення CRAMM для кожної групи ресурсів і кожного типу загроз генерує список питань, що допускають однозначну відповідь. Рівень загроз оцінюється, залежно від відповідей, як дуже високий, високий, середній, низький і дуже низький. Рівень уразливості оцінюється, залежно від відповідей, як високий, середній і низький. На основі цієї інформації розраховуються рівні ризиків від 1 до 7.

Проте оцінка ризиків на якісному рівні не дозволяє однозначно порівняти витрати на забезпечення інформаційної безпеки і одержувану від них віддачу (у вигляді зниження сумарного ризику). Тому переважними є кількісні методики, а вони вимагають наявності оцінок імовірності виникнення для кожної загрози безпеки.

Методологія OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) [5] була розроблена в Інституті програмної

інженерії при Університеті Карнегі-Меллона і передбачає активне залучення власників інформації в процес визначення критичних інформаційних активів і асоційованих з ними ризиків.

Ключові елементи OCTAVE:

– ідентифікація критичних інформаційних активів;

– ідентифікація загроз для критичних інформаційних активів;

– визначення вразливостей, асоційованих з критичними інформаційними активами;

– оцінка ризиків, пов'язаних з критичними інформаційними активами.

OCTAVE передбачає високу ступінь гнучкості, що досягається шляхом вибору критеріїв, які підприємство може використовувати при адаптації методології під власні потреби. Методологія розроблена для застосування у великих компаніях, а її зростаюча популярність призвела до створення версії OCTAVE-S для невеликих підприємств. Крім того є комерційні програмні продукти, що реалізують положення OCTAVE [5].

Методологія CORAS [1] розроблена в рамках програми Information Society Technologies. Її суть полягає в адаптації, уточненні і комбінуванні таких методів проведення аналізу ризиків, як Event-Tree-Analysis, ланцюги Маркова, HazOp і FMECA. CORAS використовує технологію UML і базується на австралійському / новозеландському стандарті AS / NZS 4360: 1 999 Risk Management і ISO / IEC 17799-1 2000 Code of Practice for Information Security Management. У цьому стандарті враховані рекомендації, викладені в документах ISO / IEC TR 13335-1: 2001 Guidelines for the Management of IT Security і IEC 61508 2000 Functional Safety of Electrical / Electronic / Programmable Safety Related.

Відповідно до CORAS інформаційні системи розглядаються не тільки з точки зору використовуваних технологій, але з кількох сторін, а саме як складний комплекс, в якому враховано і людський фактор. Правила цієї методології реалізовані у вигляді Windows- і Java-додатків.

В рамках даного питання варто розглянути економіко-вартісні моделі, запропоновані для кількісного оцінювання параметрів інформаційних ризиків.

Для визначення ймовірнісних параметрів ризику в [19, 18, 17] використовуються певні характеристики мотиваційно-вартісних та економіко-фінансових відносин, характерних для ситуації «атака-захист» в інформаційній сфері. На виході, розраховані коефіцієнти дають вартісну характеристику ситуації «атака-захист». На базі цих відомостей можна побудувати логіко-евристичну схему експертного оцінювання ймовірнісних характеристик, що використовуються для обчислення інформаційних ризиків.

Модель на основі побудови «Матриці системи управління інформаційною безпекою (СУІБ)». Дана модель призначена для дослідження вже існуючої інформаційної системи і системи захисту інформації з метою модернізації системи захисту і підвищення захищеності інформаційних ресурсів.

Методичні та практичні рекомендації щодо організації захисту інформації за допомогою інформаційно-методичного інструменту управління інформаційною безпекою «Матриця СУІБ» було розроблено Домарєвим В.В. та Домарєвим Д.В. [25]. Для дослідження інформаційної системи запропонований метод, заснований на побудові системи управління інформаційною безпекою (СУІБ). При цьому СУІБ може являти собою базу знань про дану інформаційну систему і систему захисту інформації. Дані, отримані в результаті аналізу інформаційної системи, дозволять визначити оптимальні заходи щодо забезпечення захисту інформації.

Модель оцінки ризиків інформаційної безпеки на основі нечітких множин будується з використанням нечітких когнітивних карт (НКК) [27]. Нечіткі когнітивні карти представляють собою простий граф з вузлів і зважених дуг, де вузли – концепти предметної області (наприклад: безліч

порушників, безліч способів подолання системи захисту), а дуги причинно-наслідкові зв'язки між ними (наприклад: ймовірність наявності певного виду порушників, ймовірність реалізації атаки і ін.).

У загальному випадку при розрахунку ризику використовують співвідношення:

$$R_{ij} = P_i^u \cdot P_{ij}^v \cdot A_j , \qquad (1.1)$$

де R_{ij} – ризик j-го ресурсу по відношенню до i-ої загрози;

P_{ui} – ймовірність i-ої загрози;

P_{ijv} – вразливість захисту j-го ресурсу по відношенню до i-ої загрози;

A_j – цінність j-го ресурсу.

Вага зв'язків в нечітких когнітивних картах задається в нечіткому вигляді: з допомогою лінгвістичних терм або інтервальних оцінок.

За допомогою НКК обчислюється повний ефект впливу сукупності загроз на деякий інформаційний ресурс системи або ж на безліч ресурсів інформаційної системи.

На основі отриманих даних потім обчислюється ризик [27]. У роботі пропонуються моделі з лінгвістичною і бальною шкалами для оцінки рівня захищеності інформаційної системи на підставі експертних оцінок (еталонних значень) і результатів опитування користувачів, які здійснюють оцінку прийнятих в інформаційних системах заходів захисту.

Перспективною є можливість проведення пробіт-аналізу, ідея якого належить американському ентомологу Ч. Блісс [2]. Суть пробіт-аналізу полягає в спеціальному відображенні S-подібних кривих залежності втрат від характеристик реалізованих загроз в прямі лінії, які в подальшому можуть бути оброблені методами лінійного аналізу. Зворотне перетворення здійснюється шляхом перетворення значень лінійних пробіт-функцій в значення характеристик ймовірності [7].

Відомо, що пробіт-функція є математичною залежністю, яка пов'язує специфічні особливості негативного впливу на деякий об'єкт (в нашому випадку – інформаційний актив) з розміром можливих втрат. Вираз для визначення значень пробіт-функції в загальному випадку, має такий вигляд:

$$\Pr(D) = a + b + \ln D + \gamma \ln \tau, \qquad (1.2)$$

де a, b, γ – коефіцієнти, які характеризують ступінь уразливості інформаційного активу щодо конкретної загрози або класу загроз;

D – оцінка негативного впливу;

τ – період часу від початку до кінця негативного впливу.

Для сфер, в яких можна знехтувати часовим періодом актуальності загрози, а саме це і характерно для більшості випадків загроз безпеці інформації, використовується наступна форма подання пробіт-функції:

$$\Pr(D) = a + b + \ln D. \qquad (1.3)$$

На основі аналогії з функціями розподілу ймовірностей втрат від реалізації сценаріїв загроз безпеки інформації з *S*-подібними кривими слід припустити, що використання підходу на основі пробіт-аналізу може виявитися результативним.

При цьому необхідно зазначити, що рішення задачі визначення імовірнісних характеристик для кожної пари (загроза, вразливість) виконується в два етапи:

1) визначення значень елементів пробіт-функції *Pr(D)*, що входять в праву частину виразу (1.3);

2) розрахунок пробіт-функції *Pr(D)* і визначення за відомими значеннями пробіт-функції значень імовірнісних характеристик.

Вибір одного з двох способів визначення значень величини *D* залежить від обраної методики аналізу ризиків [3]. Якщо методика пріоритетно орієнтована на аналіз втрат, то слід вибирати перший спосіб. Якщо ж методика віддає пріоритет аналізу загроз і вразливостей, то слід віддати перевагу другому способу.

Пробіт аналіз забезпечує єдину методологічну базу обліку особливостей пар загроза/наслідок для різних інформаційних активів і створює основу для вирішення завдання кількісної оцінки ризиків у сфері безпеки інформації. Недоліком даного аналізу є недостатність практичних прикладів. Відомі приклади таких досліджень в гідротехніки, будівельної механіки, пожежної безпеки та інших сферах, відмінних від інформаційної безпеки.

Методика ISRAM (кількісний аналіз ризиків інформаційної безпеки) передбачає проведення двох незалежних експертних опитувань для встановлення величин двох атрибутів ризику – ймовірності та наслідків подій [12]. Модель ризику описується наступною формулою:

$$R = P \cdot C, \tag{1.4}$$

де R – величина ризику;

P – ймовірність настання ризикової події ;

C – наслідки настання ризикової події.

Модель ризику, в якій відображаються обидві основні частини формули (1.5), представлена формулою:

$$R = \left(\frac{\sum_m T_1(\sum_i w_i p_i)}{m} \right) \left(\frac{\sum_n T_2(\sum_j w_j p_j}{n} \right), \tag{1.5}$$

де i – число питань, заданих експертам в ході опитування про ймовірність настання ризикової події;

m – кількість експертів, які взяли участь в опитуванні по ймовірності настання ризикової події;

j – кількість коштів для виявлення і оцінки наслідків настання ризикової події;

n – кількість експертів, які взяли участь в опитуванні по ймовірності настання ризикової події;

w_i і w_j – ваги питань i і j, відповідно;

p_i і p_j – чисельні значення відповідей на питання i і j, відповідно;

T_1 і T_2 – табличні ризики дослідження ймовірності і наслідків настання ризикової події, відповідно.

Експерти здійснюють вибір табличних значень, а наведена формула дозволяє формалізувати їх вибір і отримати достовірні оцінки.

Таблиця 1.2 – Основні переваги та недоліки існуючих моделей оцінювання ризиків інформаційної безпеки

Підходи	Переваги	Недоліки
Модель на основі побудови «Матриці СУІБ»	- повнота опису інформаційної системи, її ресурсів і уразливостей; - можливість виділити найбільш уразливі ресурси; - можливість оцінки існуючої системи захисту інформації.	- наявність суб'єктивної думки щодо визначення важливості активів і частоти реалізації загроз.
Модель оцінювання ризиків інформаційної безпеки на основі нечітких множин	- застосування апарату нечіткої логіки; - можливість розрахувати ймовірність реалізації загрози; - визначає ризики реалізації відповідної загрози.	- неможливо розрахувати час, що витрачається зловмисником на реалізацію загрози, а також час виявлення атаки.
Пробіт-аналіз	- забезпечує єдину методологічну базу обліку особливостей пар загроза/наслідок; - основа для вирішення завдання кількісної оцінки у сфері безпеки інформації.	- замало практичних прикладів.

Продовження таблиці 1.2

Підходи	Переваги	Недоліки
Кількісний аналіз ризиків інформаційної безпеки	- відносна простота впровадження; - зрозумілість для менеджерів; - є приклади успішного застосування.	- відносно дорогий; - краще застосовується до існуючих інформаційних активів.
Стандарти ISO	- спільний підхід до організації управління ризиками.	- концептуальний характер стандартів.
Методи експертних оцінок	- відносна простота; - можливість якісні оцінювання	- суб'єктивність думок експертів; - обмеженість суджень.
Методологія "Facilitated Risk Analysis Process (FRAP)"	- надає кількісний аналіз ризиків; - забезпечує симуляційну модель системи.	- занадто “науковий” метод; - тільки для відносно великих підприємств.
Методологія RiskWatch	- відносна простота впровадження; - зрозумілість для менеджерів; - можливість створення своїх профілів захищеності	- відносно дорогий; - краще застосовується до існуючих інформаційних активів.
Методологія CRAMM	- є універсальною і підходить для організацій як державного, так та комерційного сектору; - використовує кількісні і якісні способи оцінки ризиків; - розроблені комерційні програмні продукти, що реалізовують положення CRAMM.	- використання методики потребує спеціальної підготовки і високої кваліфікації спеціаліста; - довготривалий процес аналізу; - програмний інструментарій генерує велику кількість паперової документації, яка не завжди виявляється корисною практиці; - не дає змоги створювати власні шаблони звітів або модифікувати наявні.
Методологія OCTAVE	- швидко впроваджується; - можливе застосування для організацій різного розміру та галузей зайнятості; - є комерційні програмні продукти, що реалізовують положення методики; - високий рівень гнучкості.	- не дає кількісної оцінки ризиків; - припускає використання як способів зниження ризиків лише його зниження і прийняття; - важкість реалізації окремих етапів.
Методологія CORAS	- простота у використанні ; - підходить для нових проектів; - прийнятна вартість.	- проводиться тільки разова оцінку рівня ризику.

Розглянувши описані вище підходи, можна зробити висновок, що жоден з методів не дає докладних рекомендацій з приводу складання розкладу проведення повторних оцінок ризиків, і в методологіях не приділено уваги оновленню величин ризиків. У разі якщо потрібно виконати тільки разову оцінку рівня ризиків в компанії будь-якого розміру, доцільно застосовувати методологію CORAS. Для управління ризиками на базі періодичних оцінок на технічному рівні найкраще підходить CRAMM. Методологія OCTAVE краща для використання у великих компаніях, де передбачається впровадження управління ризиками на базі регулярних оцінок на рівні не нижче організаційного і потрібна розробка обґрунтованого плану заходів щодо їх зниження.

Хоча з розглянутих літературних джерел можна виділити ряд нових, цікавих для реалізації ідей, найчастіше введення складних математичних теорій погіршує прозорість підсумкової оцінки для експерта, вимагає від нього достатньої математичної підготовки. Тому при проведенні аналізу розглянутих методів та моделей зайва математична складність оцінювання параметрів інформаційної безпеки відзначалася як недолік.

З огляду на це, для розробки моделі візьмемо за основу факторний аналіз заснований на виявленні факторів, які з певною ймовірністю ведуть до реалізації загроз і тих або інших негативних наслідків. Методами факторного аналізу вирішують три основні групи проблем:

– пошук передбачуваних неявних закономірностей, що визначаються впливом зовнішніх або внутрішніх чинників на інформаційну безпеку;

– виявлення та вивчення статистичного зв’язку ознак з факторами або головними компонентами;

– стискування інформації шляхом подання процесу оцінювання за допомогою узагальнених факторів або головних компонент, кількість яких є меншою за кількість обраних спочатку ознак (параметрів), але

достатньою для забезпечення відтворення кореляційної матриці з потрібною точністю.

1.3 Виявлення найбільш вагомих параметрів об’єкта та дослідження їх взаємозв’язку

При визначенні актуальних ризиків, експертно-аналітичним методом визначаються об'єкти захисту, схильні до дії тієї чи іншої загрози, характерні джерела цих загроз і вразливості, що сприяють реалізації ризиків. На сьогодні, даний процес є досить специфічним і унікальним для кожної сфери. В рамках даного дослідження, був виокремлений список ризиків, який притаманний підприємствам в сфері телекомунікаційних технологій так як для них інформаційна безпека, є не тільки гарантом отримання прибутку, а й важливою складовою іміджевого показника в загальному рейтингу по сфері інформаційних технологій.

В загальному, предметна область оцінки ризиків безпеки інформаційних систем може бути представлена діаграмою класів в нотації Unified Modeling Language (UML), як показано на рис. 1.1.

Під ризиком розуміється ризик інформаційної безпеки, що представляє собою комбінацію ймовірності виникнення ризикової події (наприклад, реалізації загрози) і завдання при цьому шкоди.

Ризики, як правило, пов'язують з активами, під якими розуміється «що небудь, що має цінність для організації і, отже, потребує захисту». В ISO / IEC 27005: 2011 активи поділяються на первинні та вторинні. До первинних активів відносять інформацію і бізнес-процеси, а до вторинних - технічні засоби (ТЗ), програмне забезпечення (ПЗ), мережа, персонал, місця функціонування і організаційну структуру .

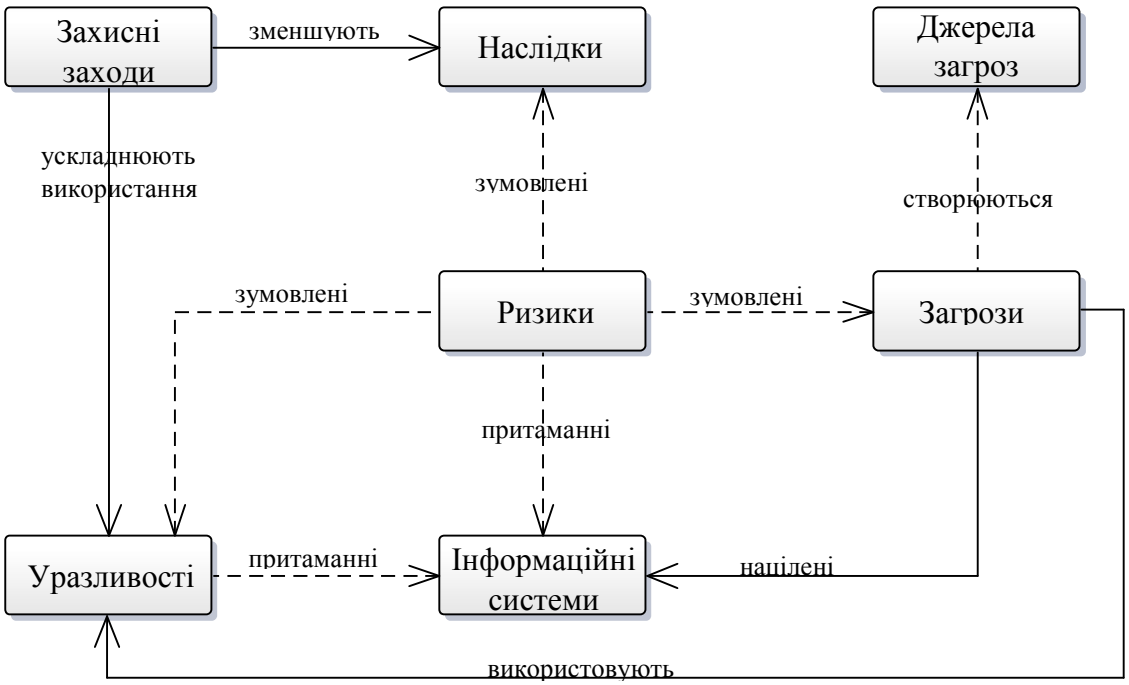

Рисунок 1.1 – Предметна область оцінки ризиків безпеки інформаційних систем

Інформаційна система – це сукупність взаємопов’язаних компонентів, які визначають різні сторони інформаційної діяльності об’єкта. При цьому під ІС може розумітися як окрема прикладна система, так і вся інформаційна інфраструктура підприємства. Найчастіше під ІС розуміється одна або кілька прикладних систем, необхідних для реалізації одного або декількох пов'язаних бізнес-процесів підприємства.

Під загрозою (безпеки інформації) розуміється сукупність умов і факторів, що створюють потенційну або реально існуючу небезпеку порушення безпеки інформації.

Поняття «загроза» тісно пов'язане з поняттям «інцидент інформаційної безпеки». У нормативних документах наводяться наступні визначення терміну «інцидент інформаційної безпеки»:

1. поява однієї або декількох небажаних або несподіваних подій інформаційної безпеки, з якими пов'язана значна ймовірність компрометації бізнес-операцій і створення загрози інформаційній безпеці;

2. будь-яка непередбачена або небажана подія, яка може порушити діяльність або інформаційну безпеку.

Загроза безпеки ІС може виникнути при наявності уразливості, під якою розуміється «властивість інформаційної системи, що обумовлює можливість реалізації загроз безпеки оброблюваної в ній інформації». Уразливості поділяються на технічні (слабкості коду і конфігурації ПО та інші) і організаційні (уразливості, пов'язані з персоналом, слабкості нормативно-документаційного забезпечення, контролю та інші).

Під джерелом загроз розуміється суб'єкт доступу, матеріальний об'єкт або фізичне явище, що є причиною виникнення загрози безпеки інформації, а також сутність, яка негативно впливає на активи. За характером походження загроз джерела загроз поділяються на природні та антропогенні. Опис існуючих загроз безпеки інформації, їх актуальності, можливості реалізації і наслідків називається моделлю загроз.

Під наслідками розуміються різні матеріальні і нематеріальні втрати, які може понести підприємство в результаті ризикового події (реалізації загрози). Якісна або кількісна (вартісна) оцінка всіх наслідків ризикової події називається рівнем збитків.

Захисні заходи – це дії, процедури і механізми, здатні забезпечити безпеку від виникнення загрози, зменшити вразливість, обмежити вплив інциденту в системі безпеки, виявити інциденти і полегшити відновлення активів. Захисні заходи можуть бути спрямовані як на зменшення ймовірності реалізації загроз (за рахунок усунення або утруднення використання уразливостей), так і на зниження величини наслідків (збитків) від реалізації загроз.

Сукупність захисних заходів, а також діяльність на їх основі, спрямовану на виявлення, відображення і ліквідацію наслідків реалізації загроз безпеки ІС, називають системою захисту інформації.

1.4 Постановка задачі

Мета даного дослідження полягає в розробці моделі оцінювання ризиків інформаційної безпеки. При цьому проведений в попередньому розділі аналіз дозволяє зробити висновок, що розроблювана модель має бути придатною для проведення експрес-оцінки ризиків інформаційної безпеки, простою у використанні та доступною для невеликих підприємств. При цьому отримана оцінка має давати як кількісну так і якісну характеристику ризиків інформаційної безпеки.

Задля досягнення поставленої мети в ході виконання кваліфікаційної магістерської роботи необхідно розробити модель, яка б на основі математичного апарату дала змогу оцінити ризики інформаційної безпеки підприємства.

Вхідними даними для реалізації моделі будуть результати анкетного експертного оцінювання основних загроз інформаційній безпеці, оскільки подібна статистична інформація на підприємстві, як правило, відсутня. Оцінки експертів збираються у якісному вигляді, формалізуються, обробляються методами факторного аналізу, що дозволяє визначити фактори, які найбільше впливають на ризики інформаційної безпеки підприємства та отримати його оцінку.

Таблиця 1.3 – Постановка проблеми оцінювання ризиків інформаційної безпеки

Елементи	Опис
Проблема	оцінювання ризиків інформаційної безпеки.
Впливає на	фінансовий стан підприємства.
Результатом чого є	можливі збитки від реалізації ризикової ситуації.
Переваги від	моделі оцінювання ризиків інформаційної безпеки
Можуть бути такими	- вчасне виявлення та попередження загроз інформаційній безпеці через проведення експрес-оцінки ризиків інформаційної безпеки підприємства; - зменшення збитків від реалізації ризикових ситуацій; - доступність та простота використання роблять розроблену модель доступною для невеликих підприємств.

РОЗДІЛ 2 РОЗРОБКА МАТЕМАТИЧНОЇ МОДЕЛІ ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 Формування вимог до моделі

В основу оцінки ризику було покладено метод факторного аналізу, який є найбільш адекватним в умовах невизначеності, конфліктності та нечіткої оцінки впливу окремих чинників, та дозволяє поєднати якісну і кількісну складові аналізу.

Для забезпечення правдоподібності побудованої моделі і використанні її в подальшому вона повинна відповідати ряду вимог. Запропонована модель оцінювання ризику інформаційної безпеки має відповідати таким вимогам:

– модель має бути адекватною стосовно досліджуваного процесу та давати результати, схожі з реальними;

– давати характеристику сучасного стану інформаційної безпеки підприємства;

– повинна надавати кількісну і якісну оцінку ризиків інформаційної безпеки;

– має дозволяти виділити найбільш небезпечні фактори ризику і їх ймовірність настання.

– давати можливість використання даної моделі для прийняття управлінських рішенн щодо інформаційної безпеки.

Вхідні дані моделі, а саме експертні оцінки вимагають достатньої підготовки експертів, а саме:

– чітке визначення мети і завдань опитування;

– набір достатньо компетентних незалежних експертів в досліджуваній області;

– вибір оптимально підходящих методів обробки оцінок експертів.

Для більш ефективного аналізу загроз інформаційній безпеці підприємства і їх обробки необхідно встановити існуючі зв'язки між факторами уразливостей, які впливають на підсумковий рівень ризиків інформаційної безпеки.

Після розробки моделі оцінки ризиків інформаційної безпеки у працівників відділу інформаційної безпеки і керівників структурних підрозділів буде можливість з легкістю проводити моніторинг, оцінювати ризик інформаційної безпеки, як окремого підрозділу, так і всього підприємства в цілому.

Успішна розробка даної моделі дасть змогу спростити роботу усім вищевказаним працівникам, щоб надалі здійснювати свою діяльність більш точніше, приділяти більше уваги тим ризикам, які більше сприяють виникненню ризикових ситуацій та швидше попереджати, реагувати на їх виникнення.

2.2 Формування ознакового простору моделі

На основі досліджень [19, 44, 30], можна виділити ризики інформаційної безпеки, представлені в табл. 2.1.

Таблиця 2.1 – Опис вхідних змінних

Ім’я змінної	Зміст змінної	Роль змінної	Тип	Допустимі значення
Порушення конфіденційності (X_1)	Отримання несанкціонованого доступу до інформації.	вхідна	інтервальний	1…3
Втрати цілісності (X_2)	Втрата актуальності і несуперечливості інформації.	вхідна	інтервальний	1…3
Порушення доступності (X_3)	Збої доступу до інформації.	вхідна	інтервальний	1…3
Порушення роботи системи (X_4)	Незадовільна робота по організації роботи всіх елементів системи.	вхідна	інтервальний	1…3
Крадіжка інформації (X_5)	Передача інформації третім особам.	вхідна	інтервальний	1…3

Продовження таблиці 2.1

Ім’я змінної	Зміст змінної	Роль змінної	Тип	Допустимі значення
Фальсифікація інформації (X_6)	Дублювання даних або введення завідома неправильних даних.	вхідна	інтервальний	1…3
Знищення інформації (X_7)	Цілеспрямоване або випадкове видалення інформації.	вхідна	інтервальний	1…3
Віруси (X_8)	Вплив шкідливих програм на безпеку.	вхідна	інтервальний	1…3
Апаратні та програмні збої (X_9)	Порушення роботи апаратних та програмних засобів.	вхідна	інтервальний	1…3

Окремо для показників будуємо таблицю, у якій зазначимо шкали вимірювання показників, допустимі значення кожного елемента масиву вихідних даних.

Таблиця 2.2 – Опис проміжних та вихідних змінних

Ім’я змінної	Зміст змінної	Роль Змінної	Тип	Допустимі значення
Стандартизовані значення змінних X_i (Z_i)	Нормалізація X_i за рахунок математичного перетворення	проміжна	інтервальний	-6…6
Оцінка ризику (R_a)	Отримання кількісної оцінки ризику інформаційної безпеки.	вихідна	інтервальний	-6…6

Вибірка даних склала 20 спостережень, узятих на прикладі оцінок експертів на підприємстві ТОВ «НЕТКРЕКЕР», які заповнили анонімну анкету оцінювання (рис. 2.1), всі питання анкети представлені в Додатку Б.

Оцінка ризиків визначалась вербальним показником небезпеки, який має три значення:

1) низька небезпека – якщо реалізація ризику може призвести до незначних негативних наслідків;

2) середня небезпека – якщо реалізація ризику може призвести до негативних наслідків;

3) висока небезпека – якщо реалізація ризику може призвести до значних негативних наслідків.

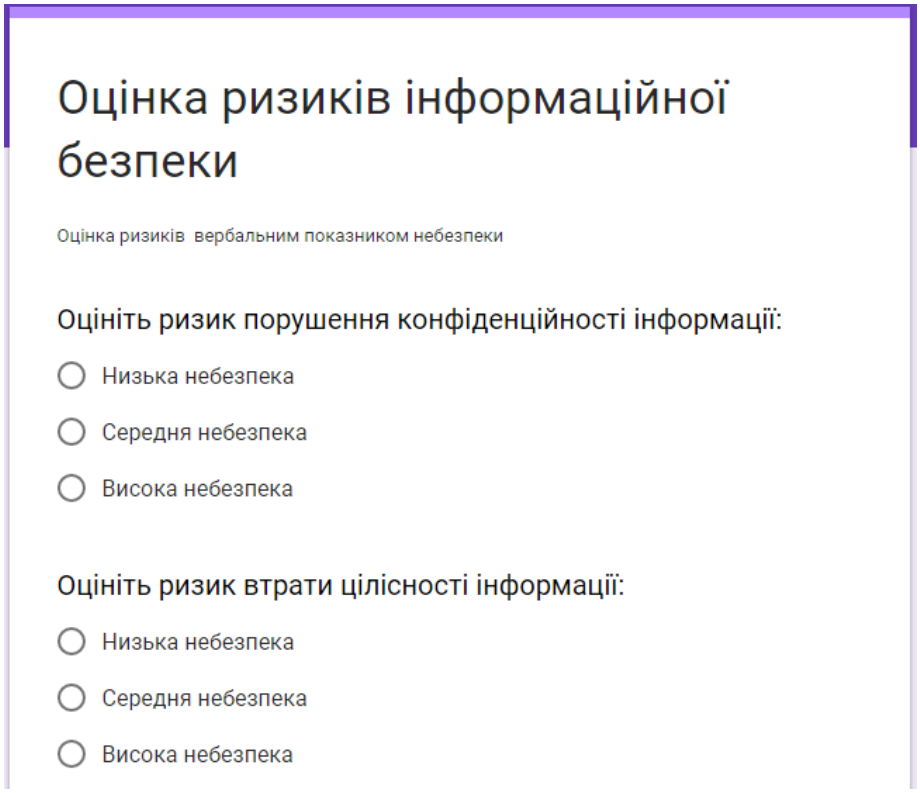

Рисунок 2.1 – Приклад питань з анкети анонімного оцінювання експертів

Функціональну модель методу головних компонент визначальних факторів оцінки ризиків інформаційної безпеки представлено на (рис. 2.2).

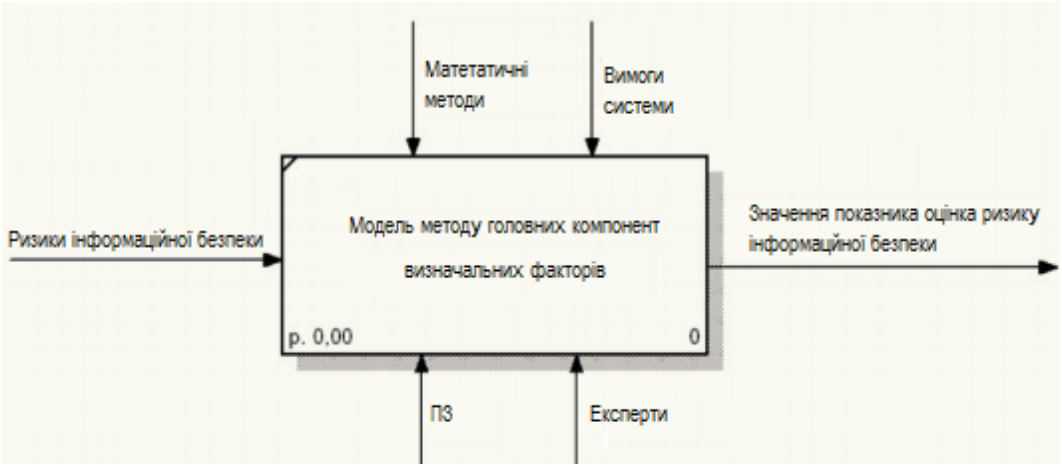

Рисунок 2.2 – Функціональна модель методу головних компонент визначальних факторів оцінки ризиків інформаційної безпеки

2.3 Розробка математичної моделі

Існують ситуації, коли із різних причин, значною мірою в зв'язку з відсутністю достовірної інформації, використання статистичних чи розрахунково-аналітичних методів не надається можливим. У таких випадках широко застосовуються методи, що використовують результати досвіду й інтуїцію, тобто евристичні чи методи експертних оцінок.

Особливістю даного методу є відсутність строгих математичних доказів оптимальності рішень. Загальною спрямованістю цього методу є використання людини як "вимірювального" приладу для одержання кількісних оцінок процесів і суджень, що через неповноту і невірогідність наявної інформації не піддаються безпосередньому виміру.

Загальна схема експертних опитувань включає наступні основні етапи:

1) підбір експертів і формування експертних груп;
2) формування питань і складання анкет;
3) робота з експертами;
4) формування правил визначення сумарних оцінок на основі оцінок окремих експертів;
5) аналіз і обробка експертних оцінок.

У практичній діяльності застосовуються як індивідуальні, так і групові (колективні) експертні оцінки.

Цілі індивідуальних експертних оцінок:

– прогнозування ходу розвитку подій і явищ у майбутньому, а також оцінка їх у сьогоденні.

– аналіз і узагальнення результатів, представлених іншими експертами;

– складання сценаріїв дій;

– видача висновків іншим фахівцям і організаціям (рецензії, відзиви, експертизи тощо).

Позитивною особливістю індивідуальної експертизи є оперативність одержання інформації для ухвалення рішення і відносно невеликі витрати. Як недолік варто виділити високий рівень суб'єктивності і, як наслідок, відсутність впевненості у ймовірності отриманих оцінок. Зазначений недолік покликаний усунути чи послабити групові експертні оцінки.

Для проведення анкетного опитування був складений анонімний оцінювальний лист та шкала оцінки. При цьому обов'язково окрім самого ризику або ймовірності появи ризикової ситуації, передбачається оцінка ваги впливу кожного фактору на показники ризику.

При дослідженні складних систем часто немає можливості безпосередньо вимірювати величини, що визначають їх властивості (фактори). Більше того, нерідко є невідомими кількість та зміст цих факторів. Але можуть вимірюватися інші величини, що залежать від них. Якщо невідомий фактор впливає на декілька вимірюваних ознак, останні виявляють певний зв’язок, наприклад корельованість, між собою. Тому загальна кількість факторів може бути значно меншою, ніж кількість вимірюваних ознак. Для виявлення таких факторів використовують факторний аналіз. Зменшення кількості факторів може бути необхідним також для забезпечення збіжності алгоритмів подальшого аналізу даних, скорочення ресурсів пам’яті ЕОМ та часу, потрібних для їх обробки, бажанням візуалізувати отримані результати тощо.

В основу оцінки ризику було покладено метод факторного аналізу, який є найбільш адекватним в умовах невизначеності, конфліктності та нечіткої оцінки впливу окремих чинників, та дозволяє поєднати якісну і кількісну складові аналізу.

Запропонований факторний підхід є універсальним і може бути використаний для оцінювання ризику на різних стадіях розвитку підприємства та етапах вибору й обґрунтування напрямів мінімізації ризиків інформаційної безпеки.

Обов’язковими умовами факторного аналізу є такі:

– всі досліджувані ознаки мають бути кількісними;

– кількість ознак має бути принаймні вдвічі більшою, ніж кількість змінних;

– вибірка має бути однорідною.

Нехай на підприємстві, для оцінки інформаційної безпеки виділено N експертів. Кожен з яких проставляє значення K ризикам, і на виході отримуємо значення випадкових багатовимірних нормально розподілених величин:

$$X_t = (X_{1t}, X_{2t}, ..., X_{kt}), \qquad (2.1)$$

де $t = 1,2,...,N.$

Значення випадкових багатовимірних величин обумовлені якимись об'єктивними причинами, які будемо називати факторами. Передбачається, що число цих факторів завжди менше, ніж число K вимірюваних ризиків інформаційної безпеки. Ці чинники є прихованими, їх не можна безпосередньо виміряти і тому вони представляються гіпотетичними. Однак є методи їх виявлення, які і складають сутність факторного аналізу.

Нехай в інформаційній безпеці ми виділили чотири ризики, які обумовлені дією двох чинників (факторів) F_1 і F_2. Фактор F_1 пояснює вплив всіх ризиків на інформаційну безпеку, в свою чергу F_2 описує вплив лише X_2 і X_3.

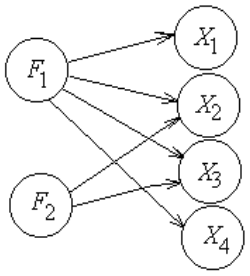

Рисунок 2.3 – Взаємозв’язок факторів і ризиків інформаційної безпеки

Отже, значення ризиків X_1 і X_4 визначаються тільки фактором F_1, а ризики X_2 і X_3 визначаються сукупною дією факторів F_1 і F_2. Але все це, поки що нам не відомо, і перед нами стоїть завдання оцінити інтенсивність впливу факторів F_1 і F_2 на ризики X_i і виділити в X_i ті частини, які обумовлені дією кожного з факторів F_1 і F_2 окремо.

Для вирішення цього завдання припускають, що X_i лінійно залежить від F_m, $(m=1,2)$. Для нашого випадку маємо:

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

де $i = 1,2,3,4$;

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

З даної гіпотези, можемо отримати дві моделі факторного аналізу:

1) метод головних компонент (МГК), в якому значення оцінки кожного з ризиків представляються у вигляді лінійних комбінацій факторних навантажень a_{ij} і факторів Z_j, де $j = 1,2,\ldots,m$.

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

де m – число факторів.

2) модель власне факторного аналізу (ФА), коли спостережувані ризики визначаються не тільки факторами, але і дією локальних випадкових причин.

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

У факторному аналізі вихідні значення ознак вибіркової сукупності центруються і нормуються за допомогою перетворення:

$$Z_i = \frac{X_i - \overline{X}_i}{\sigma_i}, \qquad (2.5)$$

де $\overline{X_i}$ – середнє значення *i*-ї змінної;

σ_i – середньоквадратичне відхилення *i*-ї змінної.

На основі обчислених головних компонент можна побудувати більш просту і разом з тим найбільш інформативну систему опису ризиків, оцінити силу причинно-наслідкового зв'язку між факторами і виділеними головними компонентами, досліджувати можливості зміни аналізованих чинників під впливом головних компонент.

Крім того, результати групування по головних компонентах можна використовувати для проведення порівняльного аналізу факторів, за рахунок яких підприємство домоглося найкращих результатів у збільшенні безпеки. Це дозволяє виявити прогресивні тенденції підвищення ефективності використання виробничих ресурсів.

Метод головних компонент виявляє *k*-компоненти - фактори, що пояснюють всю дисперсію і кореляції вихідних *k* випадкових величин; при цьому компоненти будуються в порядку спадання частки сумарної дисперсії вихідних величин, які пояснюються ними, що дозволяє часто обмежитися декількома першими компонентами.

Перша головна компонента F_1 визначає такий напрямок в просторі вихідних ознак, за яким сукупність об'єктів (точок) має найбільший розкид (дисперсію).

Друга головна компонента F_2 будується з таким розрахунком, щоб її напрямок був ортогональний напрямку F_1 і вона пояснювала якомога більшу частину залишкової дисперсії і так до *k*-ї головної компоненти F_k.

Так як виділення головних компонент відбувається в порядку спадання з точки зору частки, дисперсії, що пояснюється ними, то ознаки,

що входять в першу головну компоненту з великими коефіцієнтами, надають максимальний вплив на диференціацію досліджуваних об'єктів.

Таке перетворення дозволяє знижувати інформацію шляхом відкидання координат, відповідних напрямках з мінімальною дисперсією.

У факторному аналізі використовують також інші міри інформативності, що дають змогу визначити кількість істотних факторів.

Критерій Кайзера, або критерій власних чисел, запропонований американським психологом Генрі Феліксом Кайзером, передбачає, що до моделі включають тільки фактори, для яких власні числа є не меншими, ніж одиниця. За змістом це означає, що таким факторам відповідає дисперсія, еквівалента принаймні дисперсії одної змінної. У протилежному випадку виокремлення фактору не має сенсу. Цей критерій іноді залишає в моделі занадто багато факторів.

Критерій кам’янистого осипу (критерій відсіювання) передбачає побудову графіка, де по осі абсцис відкладають порядковий номер власного числа, а по осі ординат – його значення.

Згідно з Р. Кеттелом необхідно знайти точку найбільшого уповільнення спадання власних значень і враховувати лише фактори, яким відповідають власні числа, розташовані лівіше цієї точки.

На відміну від попереднього цей критерій статистично необґрунтований і часто залишає в моделі не всі істотні фактори. Втім у випадках, коли істотних факторів небагато, а кількість змінних є великою, обидва критерії є придатними для практичного застосування.

На практиці часто здійснюють розрахунки, використовуючи різні критерії, а потім обирають модель, що містить найбільшу кількість факторів, яким можна надати змістову інтерпретацію.

Усі загальні фактори, кількість яких дорівнює кількості параметрів, пояснюють 100% дисперсії. Якщо сума відсотків за факторами перевищує 100%, це свідчить про отримання від’ємних власних значень і, відповідно, комплексних власних векторів, що може бути наслідком некоректної

редукції вихідної кореляційної матриці. Доцільно здійснювати двохетапну процедуру аналізу. На першому етапі максимальну кількість факторів не задають. Після його проведення аналізують дисперсії, оцінюють приблизну кількість факторів і проводять повторний аналіз.

Схема опису моделі методу головних компонент визначальних факторів оцінки ризиків інформаційної безпеки представлена на рис. 2.4:

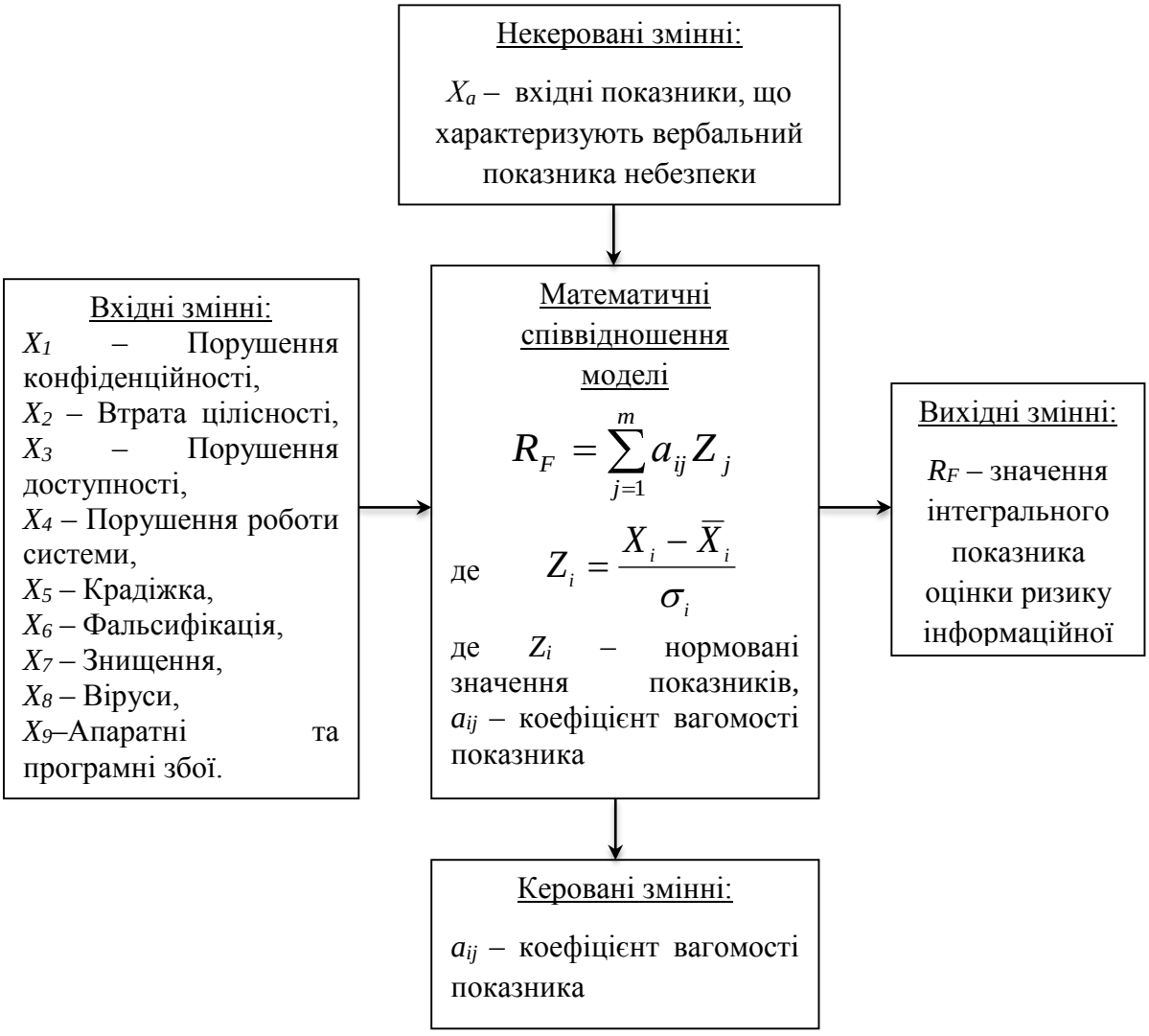

Рисунок 2.4 – Схема опису моделі методу головних компонент визначальних факторів

Оцінка ризику є досить спрощеним відображенням реальності. Показник свідчить про те, що, незважаючи на вжиття всіх

попереджувальних заходів, рівень небезпеки для підприємств залишається суттєвим. Проте його розрахунки дають можливість побудувати єдину шкалу, де в ранжируваному порядку розміщуються всі ризики. Конкретне значення R_a в цьому випадку не є визначальним, а важливим є лише місце, що займає кожний ризик.

РОЗДІЛ 3 ПЕРЕВІРКА АДЕКВАТНОСТІ МОДЕЛІ ТА ПРОПОЗИЦІЇ ЩОДО ЇЇ ВИКОРИСТАННЯ

3.1 Програмна реалізація побудованої моделі

Сутність факторного аналізу полягає в переході від опису деякої множини досліджуваних об’єктів заданої великим набором вимірюваних ознак до їх опису меншим число, що відображає найбільш істотні властивості явища. Для реалізації використано пакет аналізу даних STATISTICA.

Програма STATISTICA містить вичерпний набір аналітичних процедур в галузі вивчення бізнесу, здобуття даних, науки і промислового виробництва. Вона дозволяє будувати різні графіки, ефективно керувати даними і розробляти власні програми. STATISTICA не тільки включає в себе універсальні статистичні, графічні процедури та засоби керування даними, але також реалізує спеціалізовані методи аналізу даних. Всі аналітичні інструменти STATISTICA доступні як окремі компоненти єдиного інтегрованого пакета.

Для проведення факторного аналізу початкових заданих даних, скористаємося пунктом меню Аналіз / Багаторівневий розвідувальний аналіз/ Факторний аналіз.

На вкладці швидких опцій потрібно вказати змінні. Натискуємо на кнопку «Змінні» і вибираємо за умовою всі 9 факторних ознак для дослідження. Головною метою аналізу чинників є редукція даних та класифікація змінних. А також – виявлення загальних для факторних ознак латентних (прихованих) чинників, впливом яких обумовлені варіації та коваріації ознак ризиків. Діалогове вікно початкового задання змінних буде мати вигляд (рис. 3.1).

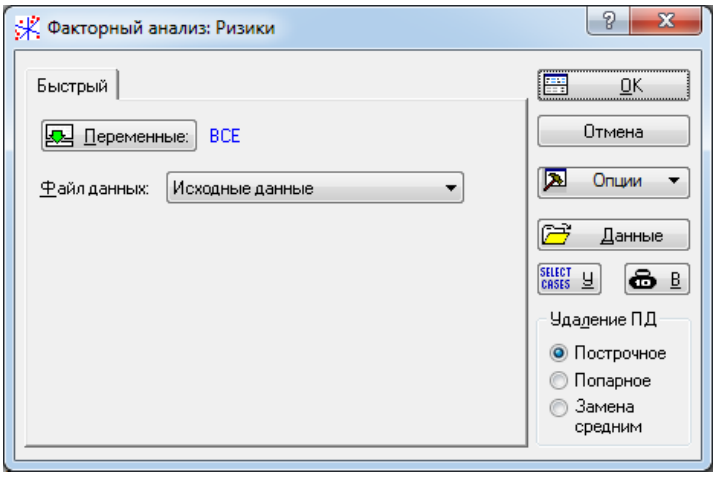

Рисунок 3.1 – Діалогове вікно вибору змінних для проведення факторного аналізу

Після натиснення на кнопку «ОК» програма переходить до вікна визначення методу виділення факторів. Вкладка «Додатково» дозволяє встановити максимальну кількість нових чинників у моделі та метод обчислення таких чинників.

Вкладка описових статистик дозволяє переглянути кореляції, дисперсію та стандартне відхилення для ризиків, а також побудувати регресійну модель між даними ознаками. Можна натиснути на кнопку перегляду основних статистик і перейти до діалогового вікна, де обираємо кнопку «Кореляції». Отримаємо таку таблицю коефіцієнтів кореляції для досліджуваних ознак (рис. 3.2). Отже можна зробити попередній висновок про наявність взаємодії між ризиками, як в прямій, так і в оберненій направленості залежності.

Корреляции (Ризики)
Построчное удаление ПД
N=20

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 3.2 – Кореляційна матриця

Повернувшись до вікна вибору методу, обираємо метод головних компонентів. У полі мінімального власного значення встановлюється рівень для власних значень чинників. Якщо значення буде менше за цей рівень, то воно до аналізу братись не буде. Також у методі головних компонентів максимально можлива кількість чинників буде дорівнювати кількості змінних. Кожному чиннику буде відповідати рівень дисперсії, який пояснюється цим чинником (мінливість). Відповідно її прийнято називати власним значенням, що відповідає чинникам.

Для того, щоб визначити потрібну кількість чинників, на вкладці «Додатково» отриманого діалогового вікна вкажемо максимальну кількість факторів 9, а мінімальне власне значення на рівні 0.

Маємо такі початкові вхідні параметри дослідження для моделі (рис. 3.3).

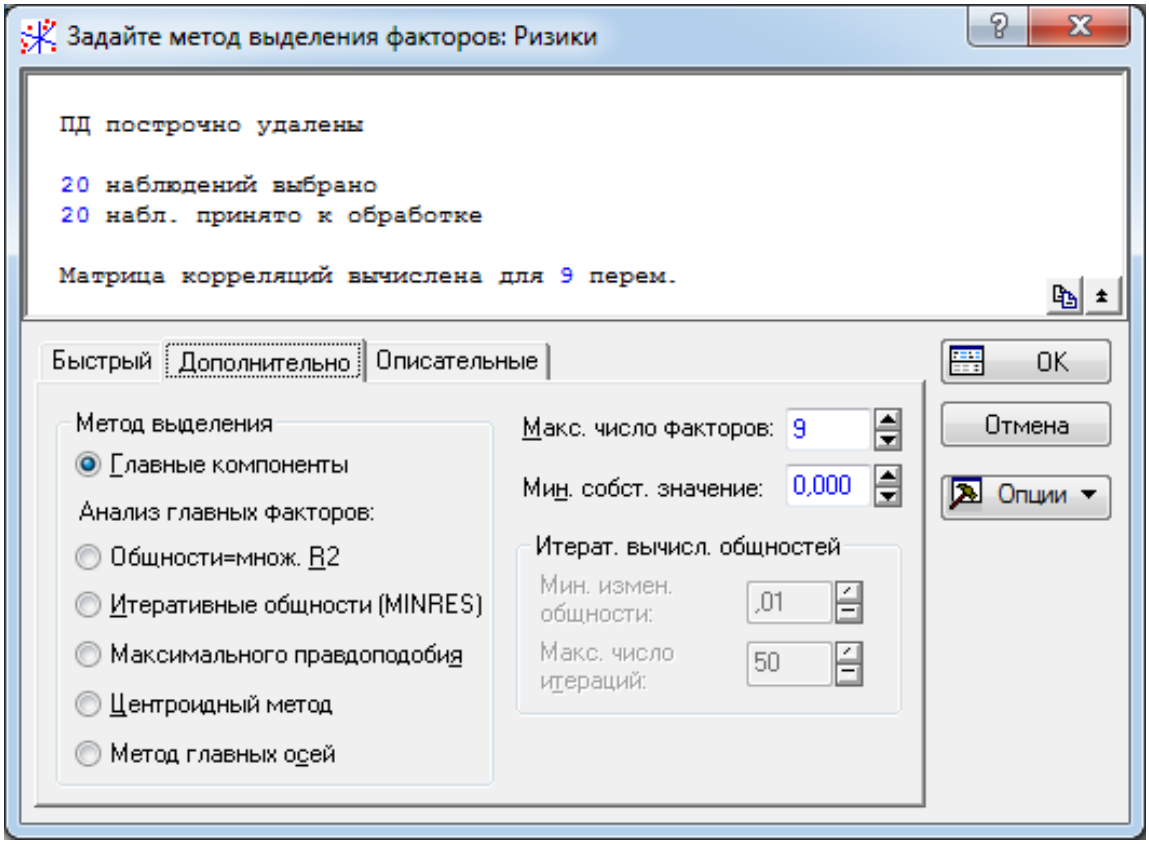

Рисунок 3.3 – Діалогове вікно вибору методу дослідження

Після натиснення на кнопку «ОК» переходимо до вікна результатів факторного аналізу. Діалогове вікно матиме такий вигляд (рис. 3.4). Вкладка «Пояснена дисперсія», кнопка «Власні значення» дозволяє отримати таблицю власних значень.

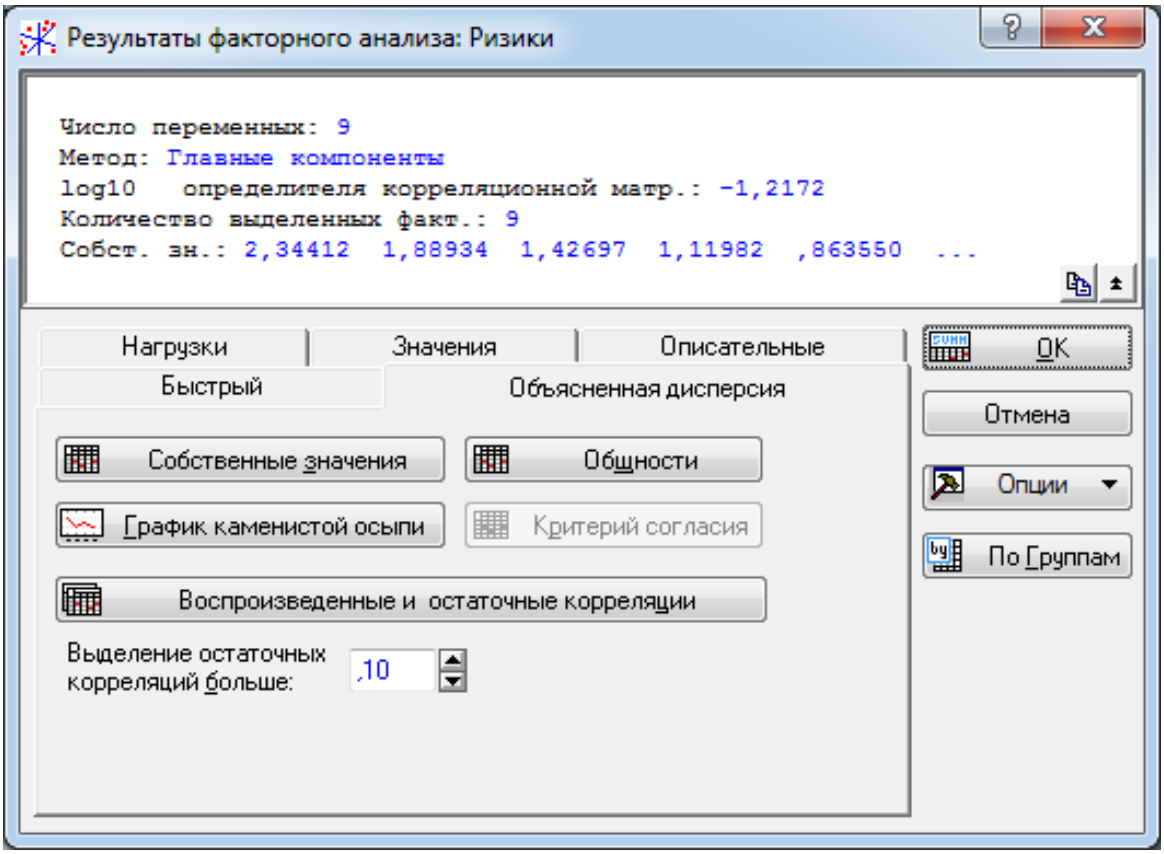

Рисунок 3.4 – Результати факторного аналізу

Відкривши «Власні значення» ми отримуємо інформацію у рядках про відповідний номер виділеного чинника, у стовпцях – власне значення для чинника, відсоток загальної дисперсії, що пояснюється саме цим чинником; накопичена дисперсія – показує загальний відсоток, що має бути пояснений множиною чинників. Табличне представлення цих даних має вигляд (рис. 3.5).

Значен.	Собст.значения (Ризики) Выделение: Главные компоненты			
	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 3.5 – Власні значення по дисперсіях досліджуваних факторів

З представлених факторів необхідно обрати ті, які найбільше впливають на інформаційну безпеку. Згідно з критерієм Кайзера (the Kaiser criterion), необхідно залишити ті фактори, власні значення яких більше 1. Що також підтверджує побудову графіка по методу «Каменистого осипу» за допомогою якого можемо визначити найбільш значущі фактори (рис. 3.6).

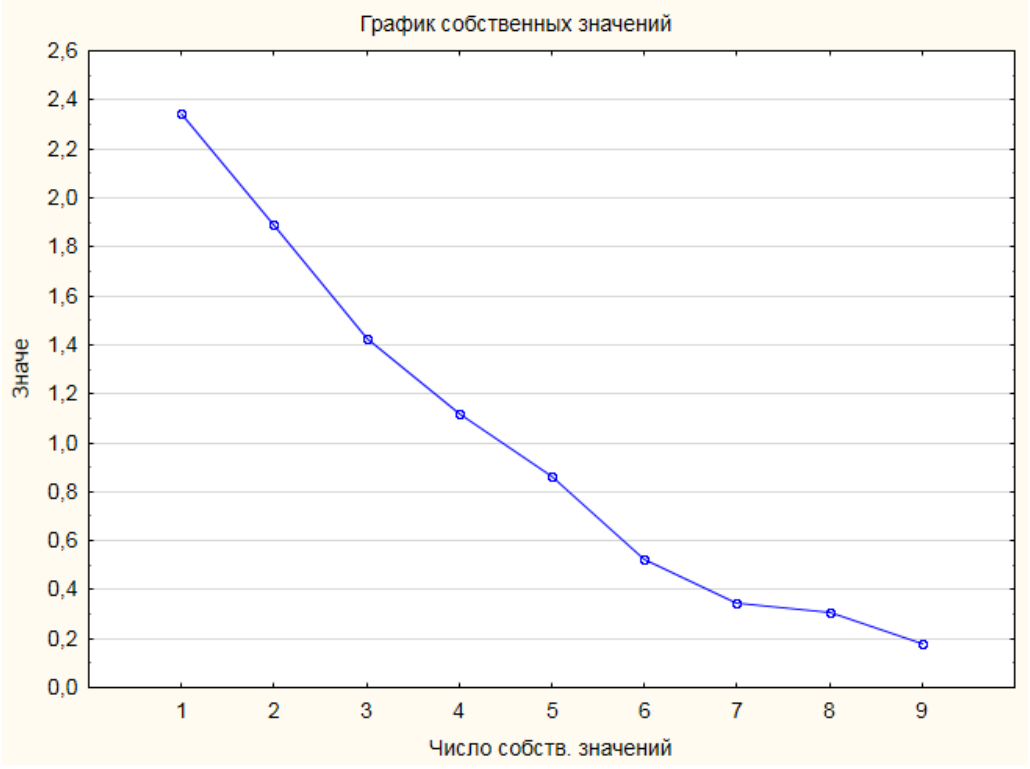

Рисунок 3.6 – Графік каменистого осипу

Для з'ясування того, які саме чинники мають такий вплив на пояснення дисперсії, необхідно скористатися дослідженням факторних навантажень. На вкладці «Навантаження» діалогового вікна результатів факторного аналізу потрібно натиснути на кнопку «Факторні навантаження». Отримаємо матрицю кореляції між змінними та виділеними чинниками. Таблиця факторних навантажень представлена наступним чином (рис. 3.7):

Перемен.	Фактор.нагрузки (Без вращ.) (Ризики) Выделение: Главные компоненты (Отмечены нагрузки >,700000) **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 3.7 – Таблиця факторних навантажень для досліджуваних факторів

Таблиця показує нам ступінь впливу кожного з факторів на вхідні 9 ризиків моделі. Червоним кольором показано значущу статистику.

Можна спостерігати ступінь впливу кожного з чинників на кожну із досліджуваних ознак. А результуюча ознака залежить від ступеня впливу цих факторів. При чому перші 4 є досить суттєвими і можуть пояснити значну частину залежності та загальної дисперсії при дослідженні факторних ознак.

Статистика дозволяє перегляд усіх значень, які приймають різні фактори для кожного спостереження. Це можливе за допомогою переходу до вкладки «Значення» та натиснення кнопки «Значення факторів». Будуть розраховані такі відповідні дані (рис. 3.8).

По цим даним можна судити про значення кожного фактору по кожному ризику. Коефіцієнти показують відповідний ступінь впливу латентних (прихованих) чинників на модель по кожному ризику. І цим впливом якраз і зумовлена відповідна варіація ознак.

Значения факторов (Ризики)
Вращение: Без вращ.
Выделение: Главные компоненты

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 3.8 – Значення факторних оцінок по кожному спостереженню

Знову ж перший фактор є основним у даній моделі, він відображає синтез 3 досліджуваних ознак, пояснює їх і має найбільший вплив серед інших. Тобто ризики порушення роботи системи, знищення інформації та віруси можна замінити фактором 1. Фактор 2 має сильний вплив ризик крадіжки інформації, фактор 3 на фальсифікацію інформації в програмні та апаратні збої, а фактор 4 на – ризик порушення доступності тому можна говорити про можливість їх заміни. Всі факторні навантаження перевищують значення 0,7.

За отриманими даними можна судити про великий вплив першого фактору та про менший вплив другого, третього та четвертого.

Провівши факторний аналіз, моделі методу головних компонент визначальних факторів, мають наступний вигляд:

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

$$R_2 = 0{,}84 \cdot Z_5, \quad (3.2)$$

$$R_3 = 0{,}74 \cdot Z_6 - 0{,}72 \cdot Z_9, \quad (3.3)$$

$$R_4 = 0{,}8 \cdot Z_3, \quad (3.4)$$

де Z_i – стандартизовані значення змінних X_i.

Оскільки, для побудови цих моделей використовувались ваги навантаження, нам необхідно нормалізувати змінні Z, по формулі (2.5).

Отримаємо моделі в звичайних змінних:

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

$$R_2 = 0{,}84 \cdot X_5 - 2{,}08, \quad (3.6)$$

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

$$R_4 = 0{,}8 \cdot Z_3 - 2{,}82, \quad (3.8)$$

де R_1, R_2, R_3, R_4 – нормалізовані моделі методу головних компонент визначальних факторів.

3.2 Перевірка адекватності побудованих моделей

Створені моделі оцінки ризиків інформаційної безпеки на основі факторного аналізу потрібно перевірити на адекватність. Незалежно від

виду і способу побудови моделей питання про можливість їх застосування з метою використання оцінювання ризиків інформаційної безпеки може бути вирішено тільки після встановлення адекватності моделей. В нашому випадку повної відповідності моделей реальному процесу чи об'єкту не може бути, тому адекватність певною мірою умовне поняття. Модель може бути точною, проте неадекватною і навпаки, бути не точною, але адекватною відносно критеріїв дослідження, може давати результат, що відповідає дійсності, проте в цей же час не задовольняти деякі критерії адекватності.

Адекватність регресійних моделей може бути визначена на основі статистичного аналізу залишкової послідовності. Для оцінки точності регресійних моделей використовуватимемо статистичні критерії Фішера та Стьюдента.

Стандартна похибка рівняння (точкова оцінка емпіричної дисперсії залишків) характеризує абсолютну величину розкиду випадкової складової рівняння і з поправкою на кількість ступенів свободи дає незміщену оцінку дисперсії залишків (3.9). Перевага надається моделям, у яких стандартна похибка рівняння менша порівняно з іншими моделями.

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

Перевірка значущості моделі регресії проводиться з використанням F-критерію Фішера, розрахункове значення якого знаходиться як відношення дисперсії вихідного ряду спостережень досліджуваного показника і незміщеної оцінки дисперсії залишкової послідовності для даної моделі. Якщо розрахункове значення з $k_1 = (m)$ і $k_2 = (n\text{-}m\text{-}1)$ ступенями свободи більше табличного при заданому рівні значущості, то модель вважається значущою.

На початку висувається нульова гіпотеза про те, що рівняння в цілому статистично незначуще. Далі визначають фактичне значення F-критерію (3.10).

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

Табличне значення визначається за таблицями розподілу Фішера для заданого рівня значущості, беручи до уваги, що число ступенів свободи для загальної суми квадратів (більшою дисперсії) дорівнює 1 і число ступенів свободи залишкової суми квадратів (меншою дисперсії) при лінійної регресії одно *n-2.*

$F_{табл.}$ – це максимально можливе значення критерію під впливом випадкових чинників при даних ступенях свободи і рівні значущості α. Рівень значущості α – ймовірність відкинути правильну гіпотезу за умови, що вона вірна. Зазвичай α приймається рівною 0,05. Якщо фактичне значення *F*-критерію менше табличного, то кажуть, що немає підстави відхиляти нульову гіпотезу. В іншому випадку, нульова гіпотеза відхиляється і з ймовірністю (1-α) приймається альтернативна гіпотеза про статистичної значущості рівняння в цілому.

Для оцінки статистичної значущості коефіцієнтів регресії і кореляції розраховуються *t*-критерій Стьюдента. Була висунута нульова гіпотеза про випадкову природу показників, тобто про незначну їх відмінність від нуля. Щоб перевірити, чи значимі параметри, тобто чи значимо вони відрізняються від нуля, для генеральної сукупності використовують статистичні методи перевірки гіпотез.

В якості основної (нульової) гіпотези висувають припущення про незначну відмінність від нуля параметра або статистичної характеристики в генеральній сукупності. Поряд з основною гіпотезою висувають альтернативну гіпотезу про нерівність нулю параметра або статистичної

характеристики в генеральній сукупності. Перевіримо основну гіпотезу про рівність коефіцієнтів регресії на рівні значущості $\alpha = 0.05$. У разі якщо основна гіпотеза виявиться невірною, ми приймаємо альтернативну. Для перевірки цієї гіпотези використовується *t*-критерій Стьюдента (3.11).

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

Знайдене за даними спостережень значення t-критерію порівнюється з табличним (критичним) значенням, що визначається за таблицями розподілу Стьюдента. Табличне значення визначається в залежності від рівня значущості (α) і числа ступенів свободи.

Якщо фактичне значення t-критерію більше табличного (по модулю), то основну гіпотезу відкидають і вважають, що з імовірністю (1-α) параметр або статистична характеристика в генеральної сукупності значимо відрізняється від нуля.

Якщо фактичне значення t-критерію менше табличного (по модулю), то немає підстав відкидати основну гіпотезу, тобто параметр або статистична характеристика в генеральної сукупності незначимо відрізняється від нуля при рівні значущості α.

Проведемо перевірку на адекватність для 4-х моделей (3.5-3.8) використавши програмний пакет Statistica.

Для того щоб визначити параметри нелінійної функції перейдемо на вкладку Анализ / Углубленные методы анализа/ Множественная нелинейная регрессия/ Результат множественной регрессии (рис. 3.9).

N=20	Итог регрессии для зависимой переменной: У1 (Ризики) R=1,00000 R2=1,00000 Скоррект.R2=1,00000 F(3,16)=240E14 p<0,0000 Станд.ошибка оценки: -,00000					
	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 3.9 – Підсумкова таблиця регресії моделі R_1

За даними моделі R_1 коефіцієнт детермінації вийшов рівним 1, таким чином, 100% варіації показника пояснюється варіацією показників порушення роботи системи, знищення інформації та вірусів.

Значущість множинного коефіцієнта кореляції перевіряється по таблиці F-критерію Фішера. У нашому випадку табличне значення *F*-критерію Фішера для мір свободи 16 (20 спостережень мінус 4 рівно 16) при рівні значущості α = 0,05 рівно 3,24, а розраховане значення рівне 240.

Розрахункове значення значно більше табличного, тому признається статистична значущість знайдених значень. Як правило, вважається, що рівняння придатне для практичного використання, якщо $F_{розр} > F_{табл}$ мінімум в 4 рази. У нашому випадку ця умова дотримується.

На рисунку 3.9, в стовпці B відбиті значення параметрів b_0 і b_1 регресійного рівняння. Значущість параметрів b_0 і b_1 перевіряється по таблиці *t*-критерію Стьюдента. Розрахункові значення *t*-критерію Стьюдента для кожного параметра, відбиті в стовпці *t*(16), порівнюємо з табличним значенням *t*-критерію для числа ступенів свободи, рівного 16. $t_{табл}$ = 2,12 при рівні значущості α=0,05. Розраховані значення t-критерію для обох параметрів більше табличного, що свідчить про значущість знайдених значень.

Проведемо аналогічні розрахунки для моделей R_2, R_3, R_4. На рисунку 3.10 представлені результати множинної регресії для моделі R_2.

	Итоги регрессии для зависимой переменной: У2 (Ризики) R=1,00000000 R2=1,00000000 Скоррект. R2=1,00000000 F(1,18)=-,0408 p<0,0053 Станд.ошибка оценки: -,00020						
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 3.10 – Підсумкова таблиця регресії моделі R_2

За даними моделі R_2 коефіцієнт детермінації вийшов рівним 1, таким чином, ми можемо зробити припущення, що 100% варіації показника пояснюється варіацією показника крадіжка інформації.

Значущість множинного коефіцієнта кореляції перевіряється по таблиці F-критерію Фішера. У нашому випадку табличне значення *F*-критерію Фішера для мір свободи 18 при рівні значущості α = 0,05 рівно 4,41, а розраховане значення рівне 0,04.

Розрахункове значення значно менше табличного, тому признається статистична незначущість знайдених значень.

На рисунку 3.10, в стовпці B відбиті значення параметрів b_0 і b_1 регресійного рівняння. Значущість параметрів b_0 і b_1 перевіряється по таблиці t-критерію Стьюдента. Розрахункові значення t-критерію Стьюдента для кожного параметра, відбиті в стовпці $t(18)$, порівнюємо з табличним значенням *t*-критерію для числа ступенів свобода, рівного 18. $t_{табл}$ = 2,10 при рівні значущості α=0,05. Розраховані значення t-критерію для обох параметрів менше табличного, що свідчить про незначущість знайдених значень.

На рисунку 3.11 представлені результати множинної регресії для моделі R_3.

За даними моделі R_3 коефіцієнт детермінації вийшов рівним 1, таким чином, ми можемо зробити припущення, що 100% варіації показника пояснюється варіацією показників фальсифікація інформації та програмні і апаратні збої.

N=20	Итоги регрессии для зависимой переменной: У3 (Ризики) R=1,00000000 R2=1,00000000 Скоррект. R2=1,00000000 F(2,17)= 1,5532 p<0,0025 Станд.ошибка оценки: -,00032					
	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 3.11 – Підсумкова таблиця регресії моделі R_3

Значущість множинного коефіцієнта кореляції перевіряється по таблиці *F*-критерію Фішера. У нашому випадку табличне значення *F*-критерію Фішера для мір свободи 17 при рівні значущості α = 0,05 рівно 3,59, а розраховане значення рівне 1,55. Оскільки фактичне значення $F < F_{табл}$, то знайдена оцінка рівняння регресії статистично ненадійна.

На рисунку 3.11, в стовпці B відбиті значення параметрів b_0 і b_1 регресійного рівняння. Значущість параметрів b_0 і b_1 перевіряється по таблиці t-критерію Стьюдента. Розрахункові значення t-критерію Стьюдента для кожного параметра, відбиті в стовпці t(17), порівнюємо з табличним значенням t-критерію для числа ступенів свобода, рівного 17. $t_{табл}$ = 2,10 при рівні значущості α=0,05. Розраховані значення *t*-критерію для обох параметрів менше табличного, що свідчить про незначущість знайдених значень.

На рисунку 3.12 представлені результати множинної регресії для моделі R_4.

N=20	Итоги регрессии для зависимой переменной: У4 (Ризики) R=1,00000000 R2=1,00000000 Скоррект. R2=1,00000000 F(1,18)=3,084 p<0,0000 Станд. ошибка оценки: ,00000					
	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 3.12 – Підсумкова таблиця регресії моделі R_4

За даними моделі R_4 коефіцієнт детермінації вийшов рівним 1, таким чином, ми можемо зробити припущення, що 100% варіації показника пояснюється варіацією показника порушення доступності.

Значущість множинного коефіцієнта кореляції перевіряється по таблиці F-критерію Фішера. У нашому випадку табличне значення *F*-критерію Фішера для мір свободи 18 при рівні значущості α = 0,05 рівно 4,41, а розраховане значення рівне 3,08. Оскільки фактичне значення $F < F_{табл}$, то можемо зробити висновок, що знайдена оцінка рівняння регресії статистично ненадійна.

На рисунку 3.12, в стовпці В відбиті значення параметрів b_0 і b_1 регресійного рівняння. Значущість параметрів b_0 і b_1 перевіряється по таблиці *t*-критерію Стьюдента. Розрахункові значення *t*-критерію Стьюдента для кожного параметра, відбиті в стовпці *t*(17), порівнюємо з табличним значенням *t*-критерію для числа ступенів свобода, рівного 17. $t_{табл}$ = 2,10 при рівні значущості α=0,05. Розраховані значення t-критерію для обох параметрів менше табличного, що свідчить про незначущість знайдених значень.

Отже, беручи до уваги перевірку на адекватність створених моделі оцінки ризиків інформаційної безпеки, для подальшої роботи і точного аналізу підходить тільки модель R_1. Саме її і візьмемо за основу, для загальної оцінки ризиків інформаційної безпеки і подальшої апробації.

3.3 Апробація моделі та інтерпретація отриманих результатів

В результаті розрахунку моделі R_1, величина R_a виступає оцінкою ризиків інформаційної безпеки. Чим більший показник R_a, тим небезпечнішими вони є для інформаційної безпеки. Даний показник знаходиться в межах, від -*r* до *r*. В результаті, проходить зіставлення оцінки ризиків із заздалегідь визначеною якісною шкалою ризику.

Якісна характеристика має такий вигляд:

1. Зона прийнятного (мінімального) ризику (-*r*;-1) характеризується рівнем втрат, який не перевищує розмір чистого прибутку.

2. Зона допустимого (підвищеного) ризику (-1;1) характеризується рівнем втрат, які не перевищують розміри розрахункового прибутку. Обережні управлінці діють у межах такої зони ризику.

3. Зона катастрофічного (недопустимого) ризику (1;*r*) характеризується тим, що в межах цієї зони очікувані втрати можуть досягти величини, рівної всьому майновому стану підприємства. До цієї зони також відноситься ризик, пов'язаний з виникненням загрози для життя людей або екологічної катастрофи.

Встановлення потенційних зон ризику полягає у порівнянні можливих фінансових втрат із розрахунковою сумою прибутку, доходу, власного капіталу (рис. 3.13). У рамках діяльності певного суб'єкта господарювання може бути використана така класифікація зон ризику: без ризикова зона, зона допустимого ризику, зона критичного ризику, зона катастрофічного ризику.

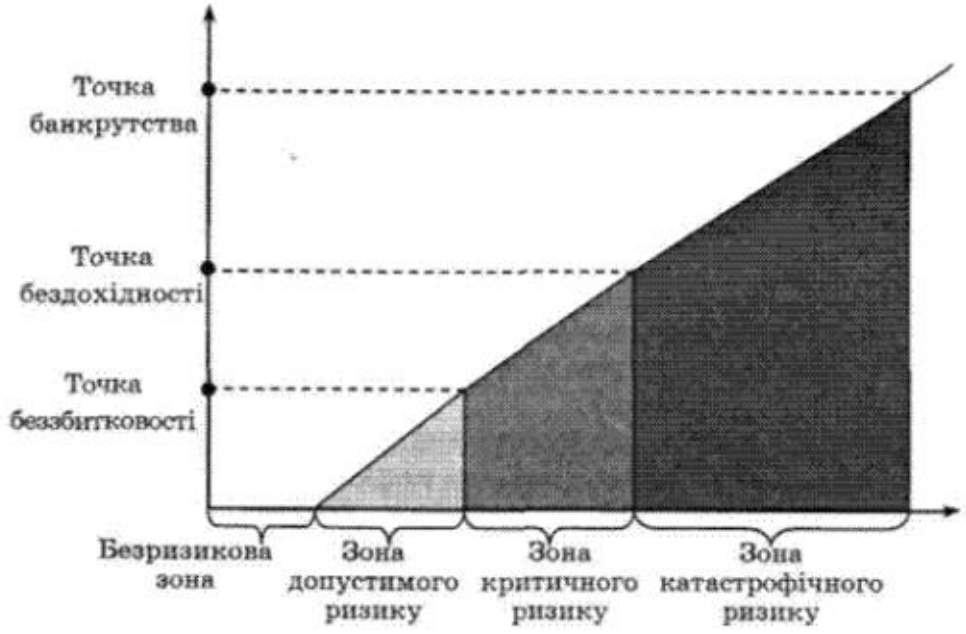

Рисунок – 3.13. Виділення зон ризику

Оцінка ризику є досить спрощеним відображенням реальності. Показники свідчать про те, що, незважаючи на вжиття всіх

попереджувальних заходів, рівень небезпеки для підприємств залишається суттєвим. Проте його розрахунки дають можливість побудувати єдину шкалу, де в ранжируваному порядку розміщуються всі ризики. Конкретне значення індексу в цьому випадку не є визначальним, а важливим є лише місце, що займає кожний ризик.

Дана модель в першу чергу, дозволить скоротити час розрахунку оцінки ризику. Якщо за початкових умов, для отримання максимально точної оцінки ризику необхідно було отримати оцінку щонайменше від 5 експертів, то на сьогодні, цю кількість можемо звести до 3-х експертів. Це зумовить достовірність і знизить суб'єктивізм оцінки.

Проведемо апробацію моделі (3.5). Одним з ризиків інформаційної безпеки на підприємстві ТОВ «НЕТКРЕКЕР» є відключення серверів. Проведемо кількісний розрахунок оцінки ризику відключення серверів.

Для початку, керівнику відділу інформаційної безпеки, керівнику відділу інформаційних технологій і працівнику відділу інформаційних технологій підприємства було запропоновано оцінити ризик за вербальним показником (1 – низька небезпека ризику, 2 – середня небезпека ризику, 3 – висока небезпека ризику).

За результатами ми отримали, що оцінки сильно відрізняються, адже:

– керівник відділу інформаційної безпеки оцінив ризик відключення серверів, як високу небезпеку, тому що реалізація цього ризику призведе до зупинки процесу роботи;

– керівник відділу інформаційних технологій оцінив ризик відключення серверів, як низьку небезпеку, тому що на регулярній основі проводиться архівування і копіювання інформації з серверів;

– працівник відділу інформаційних технологій підприємства оцінив ризик відключення серверів, як середню небезпеку, тому що у разі реалізації цього ризику необхідне буде залучення серверів, які знаходяться в інших офісах.

Отже, в результаті ми отримали експерті оцінки $X_1=3$, $X_2=1$, $X_3=2$. Підставимо ці значення в нашу модель (3.5), для оцінки ризику відключення серверів:

$$R_1 = 0{,}77 \cdot 3 + 0{,}75 \cdot 1 + 0{,}72 \cdot 3 - 5{,}46 = -0{,}96. \quad (3.12)$$

В результаті ми отримали, що для ризику відключення серверів оцінка складає $R_a = -0.96$. З цього можемо зробити висновок, що даний ризик відноситься до зона допустимого (підвищеного) ризику (-1;1), який характеризується рівнем втрат, які не перевищують розміри розрахункового прибутку.

На підприємстві ТОВ «НЕТКРЕКЕР», ризик відключення серверів, також знаходиться в зоні допустимого ризику, що підтверджує правильність наших розрахунків.

Оцінка ефективності є важливим показником для використання, чи не використання обраної моделі. Якщо впровадження системи є більш затратним ніж ефекти від впровадження, то необхідність в таких змінах автоматично відпадає.

На справді ситуація на українському ринку впровадження технологія набагато складніше ніж за кордоном. В розвинених країнах вже досить давно зрозуміли необхідність інновацій. І розуміють, що ефект може одразу ж не виявитись.

Оцінка ефективності для даної моделі є досить важкою, і підприємства, які не мають якогось фонду для зменшення ризику інформаційної безпеки не будуть її використовувати.

В багатьох дослідженнях, досить велика увага приділяється оцінці ризиків. Але при цьому всі оцінки виступають в ролі рекомендацій, а не обов’язків. Отже можна прогнозувати, що майже всі підприємства опиняться перед вибором методу оцінки ризиків інформаційної безпеки, і тоді вони вже будуть змушені шукати найбільш ефективні моделі.

Оцінка ефективності від впровадження даної моделі не розглядається однобічно. Це явище багатогранне. По-перше, ефект від впровадження очікується та отримується в системі за рахунок підвищення продуктивності праці персоналу, що виражається в скороченні часу на виконання основних функціональних обов'язків персоналу та зменшенні витрат на підтримання функціональності всієї системи, а у виробничій системі – за рахунок підвищення ефективності якості управлінських рішень, тобто після впровадження даної моделі, управлінські рішення, що приймаються керівником, спираються не тільки на його досвід та освіченість, але й на об'єктивні оцінки ризиків.

Перейдемо до безпосередньої моделі оцінки ризиків інформаційної безпеки. Щоб краще оцінити ефект від впровадженої моделі слід відповісти на наступні питання:

- де буде проявлятись ефект?
- на скільки довго даний ефект буде приносити користь?
- який характер наслідків?
- як проявиться ефект?
- коли почнеться ефект?
- яким буде вплив позитивним, чи ні?

Тепер послідовно будемо відповідати на ці поставлені тим самим визначаючи ефект від впровадження системи.

Розроблена модель буде на пряму впливати в першу чергу, на внутрішній стан підприємства. Це можна пояснити тим, що завдяки методиці оцінюються ризики та підприємство може скоротити їх, тобто удосконалюючи якусь складову. Але не слід забувати, що одним з ризику є віруси, тому можна говорити про вплив і на зовнішній стан підприємства та намагання зменшити ризики з зовні, хоча і в меншій мірі.

Оцінка ефективності впровадження моделі зазвичай включає наступні складові:

- технічну ефективність – здатність моделі виконувати ті функції, для яких вона призначена;
- економічну ефективність – необхідність якої виникає в ситуації обґрунтування інформаційних потреб управління, вибору моделі рішення окремих задач тощо;
- соціальну ефективність – сприяння збільшенню інтелектуальності роботи працівників.

Ефективність даної моделі, як вже зазначалась, принесе свою користь через достатній період часу. Через декілька періодів, підприємство побачить ефект від впровадження даної моделі і він буде проявлятись в зменшені ризиків. Але тільки через декілька років буде досягнутий максимальний ефект, тому можна говорити про довготривалий ефект від впровадження моделі.

Характер наслідків є економічним, бо на підприємстві будуть зменшуватись витрати на покриття інцидентів.

Всі зміни пов’язані з моделлю будуть носити прямий характер, бо впливають безпосередньо на становище підприємства. Можна знайти деякі риси і опосередкованого впливу, але вони набагато менш значущі. Модель почне приносити плоди тільки після впровадження її, в процесі ефектів майже не помічається. В цілому після впровадження даної моделі, можна очікувати позитивний вплив на становище підприємства, і прогнозувати покращення його фінансових показників.

Тепер сформуємо список основних ефектів від впровадження моделі оцінки ризику інформаційної безпеки:

– зниження інформаційного ризику;
– зменшення втрат пов’язаних з ризиками;
– вивільнення додаткового капіталу;
– підвищення фондовіддачі;

– збільшення доходу за рахунок вивільненого капіталу;
– зменшення внутрішніх та зовнішніх крадіжок;
– покращення роботи в колективі;
– оновлення технічного та програмного забезпечення;
– покращення менеджменту на виробництві;
– збільшення довіри клієнтів до підприємства;
– підвищення прозорості в роботі;
– покращення фінансового стану;
– та інші ефекти.

Проведення експрес-оцінки ризиків інформаційної безпеки і простота у використанні є проявом технічної ефективності.

Також слід враховувати й непрямий ефект від впровадження моделі, який полягає у більшій зацікавленості працівників у результатах своєї роботи, оскільки вона стає більш інтелектуальною та різноманітною. Даний аспект є проявом соціальної ефективності.

Спрогнозуємо ймовірний обсяг доходів та витрат підприємства від впровадження моделі оцінювання ризиків.

За 2017 рік ТОВ «НЕТКРЕКЕР», мав збитки у розмірі 87 тис. грн.

Розрахуємо можливий розмір збільшення доходу підприємства від впровадження моделі. За рахунок завчасної оцінки ризиків, будуть використані запобіжні заходи, щодо їх реалізації. В результаті чого, підприємством буде отримано дохід, за рахунок скорочення витрат на усуненя наслідків реалізації ризиків на 1%, в розмірі (3.13):

$$D_1 = 87000 \cdot 0{,}01 = 870(грн). \qquad (3.13)$$

За 2017 рік ТОВ «НЕТКРЕКЕР», отримав прибуток у розмірі 12 млн. грн. на основі цієї інформації розрахуємо можливий розмір доходу від збільшення кількості нових клієнтів

$$D_2 = 12000000 \cdot 0{,}01 = 120000(грн). \quad (3.14)$$

Отже, загальна сума річної економії (S) для підприємства «НЕТКРЕКЕР» становитиме (3.15):

$$S = D_1 + D_2 = 8710 + 120000 = 120870(грн). \quad (3.15)$$

На основі розрахунків вище, проведемо розрахунок суми капітальних витрат (C) на впровадження моделі оцінювання ризиків інформаційної безпеки, якщо витрати на заробітну плату розробників становитимуть 60 тис. грн., амортизаційні витрати – 15 тис. грн., витрати на обслуговування – 50 тис. грн. (3.16):

$$C = 60000 + 15000 + 50000 = 125000(грн). \quad (3.16)$$

Далі, розрахуємо річний економічний ефект (Ey), беручи до уваги, що нормативний коефіцієнт окупності капітальних вкладень (rn) становить 0,33 (3.17):

$$Ey = S - C \cdot rn = 120870 - 125000 \cdot 0{,}33 = 79620(грн). \quad (3.17)$$

На основі отриманих значень, розрахуємо коефіцієнт ефективності (Rce) капітальних вкладень (3.18):

$$Rce = \frac{S}{C} = \frac{120870}{125000} = 0{,}97. \quad (3.18)$$

Отже, річний економічний ефект становитиме 79620 грн. Визначимо термін окупності (To) витрат на впровадження моделі (3.19):

$$To = \frac{1}{Rce} = \frac{C}{S} = \frac{125000}{120870} = 1{,}03\,(\text{років}). \qquad (3.19)$$

Отже, термін окупності витрат на впровадження моделі буде складати – 1 рік та 3 дні.

Оскільки показники ефективності моделі є досить високими, можемо зробити висновок, що дана модель може практично застосовуватись на підприємстві «НЕТКРЕКЕР».

Для мінімізації інформаційних ризиків необхідним є забезпечення належного контролю за доступом до інформації через використання адміністративних та технічних засобів захисту. Удосконалення інформаційної системи обліку передбачає організацію контролю несанкціонованого використання інформації та попередження її фальсифікації обліковим персоналом. З метою мінімізації негативного економічного результату діяльності, який пов’язаний з фінансовими та часових втратами на виправлення організаційних ризиків, необхідна детальна їх класифікація на етапах автоматизації обліку. Належний та своєчасний контроль проблем впровадження інформаційних систем допоможе знайти шляхи побудови ефективного моніторингу виникнення можливих ризиків та мінімізації їх наслідків.

ВИСНОВКИ

У дипломній роботі було розкрито сутність оцінювання ризиків інформаційної безпеки, в результаті реалізації яких, телекомунікаційні підприємства можуть понести, як фінансовий, так і іміджевий збиток.

Інформаційна безпека виступає як характеристика стабільного, стійкого стану системи, яка при впливі внутрішніх та зовнішніх загроз та небезпек зберігає суттєво важливі характеристики для власного існування, які завжди пов’язана з певним ризиком. Ґрунтовний аналіз наукових праць з проблем ризику дав можливість узагальнити основні положення, що визначають сутність його оцінки й окреслюють основні підходи до управління ним. У процесі дослідження виявлено неоднозначність тлумачення поняття «ризик», що зумовило необхідність формування власного бачення сутності «ризик» та його місця у системі економічних категорій.

Розглянувши існуючі методи оцінювання ризиків можна побачити, що основними проблемами в їх застосуванні є:

– високі фінансові витрати на здійснення аналізу ризиків;

– необхідність залучення великої кількості експертів;

– відсутність у багатьох методів можливості проведення швидкого повторного циклу оцінки ризиків;

Недосконалість та обмеженість методик оцінки ризику інформаційної безпеки, врахування їх переваг і недоліків обумовили доцільність використання експертних оцінок для виявлення ризиків, що мають місце на телекомунікаційних підприємствах. Для подальшої оцінки був обрний факторний аналіз, для побудови моделі методу головних компонент визначального фактору.

Сформульовані ризики, які формують інформаційні ризики, які характерні для різних структурних підрозділів в телекомунікаційних

підприємствах. Основою для побудови моделі було обрано дев’ять вхідних змінних, які на сьогодні є визначеними ризиками для діючого підприємства в сфері телекомунікацій.

Факторний аналіз вхідних даних та побудова моделей проводилася з використанням програмного пакету Statistica.

Побудовані моделі пройшли перевірку на адекватність та якість, було проаналізовано їх результати. В результаті аналізу і перевірки на якість, було встановлено, що усі 4 побудовані моделі майже однаково точно описують вхідні дані, проте за усіма показниками перевірки на адекватність найкращою виявилась перша модель. Що і підтвердила апробація моделі.

Застосування даної моделі працівникам підприємства дозволить завчасно оцінювати загрози і загальний стан інформаційної безпеки, тим самим попереджуючи виникнення можливих збитків, при реалізації загроз.

Не зважаючи, на високу якість і точність даної моделі, вона потребує постійного оновлення та удосконалення у зв’язку з появою нових загроз. З певною періодичністю, необхідно оновлювати вибірку даних актуальною інформацією про існуючі загрози.

Використання моделі на телекомунікаційних підприємствах призведе до отримання соціального та економічного ефектів. Проведення оцінки ризиків інформаційної безпеки дозволить сконцентрувати увагу на найбільш актуальних проблемах і запобігти нанесенню шкоди компанії. Аналіз ефективності моделі підтвердив, що модель придатна для практичного застосування.

Проблеми ризиків інформаційної безпеки і знаходження шляхів зниження шкоди постають з кожним роком все гостріше. Однак не всі власники і користувачі інформаційних ресурсів можуть самостійно забезпечити надійний захист інформації та гарантоване покриття можливих втрат від ризиків.

Можливі рішення з управління ризиками:

– застосування належних контролів для зниження ризиків;

– об'єктивне прийняття рішень щодо ризиків, які задовольняють політику організації та критерії оцінки ризиків;

– уникнення дій, які можуть спричинити виникнення ризиків;

– перерозподіл ризиків між іншими сторонами;

– страхування ризиків.

Для забезпечення їх поінформованості й зацікавленості необхідно чітко розподілити ролі й відповідальність у процесі керування ризиками, наприклад, відповідальність за контроль над ризиками ІБ, пов'язаними з бізнес-процесом, покласти на власника процесу. При цьому він здійснює оцінку можливих збитків у разі реалізації загрози й повідомляє про зміни, що відбуваються в бізнес- процесі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Bjorn, AG. CORAS, A Platform for Risk Analysis on Security Critical Systems - Model-based Risk Analysis Targeting Security [Электронный ресурс]. – Режим доступа: www.nr.no/coras

2. Bliss C. I. The Method of Probits / C. I. Bliss // Science. – 1934. – Vol. 79. – № 2053. – P. 409–410.

3. BS 7799-3:2006 Information security management systems. Guidelines for information security risk management.

4. Information technology — Security techniques — Information security management systems — Overview and vocabulary: ISO/IEC 27000:2009. — [Чинний від 01-05-2009]. — Женева: [б.в.], 2009. — 26 с. — (Міжнародні стандарти ISO/IEC).

5. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process / Richard A. Caralli, James F. Stevens, Lisa R. Young, William R. Wilson. − Carnegie Mellon University, 2008. – 154 p.

6. International standard BS ISO/IEC 27005:2008, 2008-06-15.

7. ISO / IEC 27005 - Information security risk management.

8. James J. Cebula A Taxonomy of Operational Cyber Security Risks / James J. Cebula, Lisa R. Young. – Hanscom AFB, MA: Carnegie Mellon University. – 47 p.

9. Maria Garnaeva. Kaspersky Security Bulletin 2015. Overall statistics for2015 / [Maria Garnaeva, Jornt van der Wiel, Denis Markushin and etc.]. – Kaspersky Lab, 2015. – 86p.

10. RiskWatch International. Global Leader in Risk Assessment Solutions [Электронный ресурс]. – Режим доступа: www.riskwatch.com.

11. Sanjay Goel, Vicki Chen. Анализ рисков информационной безопасности – матричный подход [Електронний ресурс] / University at Albany, 2009. – Режим доступу: http://www.docstoc.com/

12. Thomas R. Peltier. Facilitated Risk Analysis Process (FRAP) [Электронный ресурс]. – Режим доступа: www.ittoday.info/AIMS/DSM/85-01-21.pdf.

13. Visintine V. An Introduction to Information Risk Assessment / Visintine V. – Bethesda, Maryland: SANS Institute, 2009. – 13 p.

14. Wayne Jansen. Directions in Security Metrics Research , NISTIR 7564, April 2009 [Електронний ресурс] // NIST.gov - Computer Security Division - Computer Security Resource Center [сайт] / Wayne Jansen ; Computer Security Division , Information Technology Laboratory , National Institute of Standards and Technology — Режим доступу: http://csrc.nist.gov/publications/nistir/ir7564/nistir7564_metrics-research.pdf

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

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

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

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

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

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

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

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

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

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

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

26. Информационная безопасность [Электронный ресурс]. – Режим доступа: http://inf-bez.ru.

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

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

29. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах

персональных данных [Электронный ресурс]. – ФСТЭК России, 2008. – Режим доступа: http://securitypolicy.ru.

30. Нурдинов Р.А. Модель количественной оценки рисков безопасности корпоративной информационной системы на основе метрик: дис. канд. техн. наук : 05.13.19 – Методы и системы защиты информации, информационная безопасность / Нурдинов Руслан Артурович – Санкт-Петербург, 2016. – 209 с.

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

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

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

34. Про Концепцію Національної програми інформатизації: [закон України: офіц. текст: за станом на 9 січня 2007р., із змінами, внесеними Законом України від 7 серпня 2011р.] // Відомості Верховної Ради України (ВВР). – 2012. – № 7. – ст. 53.

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

36. Про основні засади розвитку інформаційного суспільства в Україні на 2007 2015 р.р.: [закон України: офіц. текст: за станом на 9 січня 2007р.] // Відомості Верховної Ради України (ВВР). – 2007. – № 12. – ст. 102.

37. Ропаєва А. Г. Сучасний стан інформаційної безпеки підприємств та організацій в Україні / А. Г. Ропаєва // Теорія і практика розвитку наукових знань (ч. II): матеріали II Міжнародної науково-практичної конференції м. Київ, 28-29 грудня 2017 року. – Київ. : МЦНД, 2017. – С. 22-23.

38. Сабанов А.Г. Анализ применимости методов оценки рисков к процессам аутентификации при удалённом электронном взаимодействии // Электросвязь. 2014. No 5. С. 43-44

39. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки / Г. Сащук: [Електронний ресурс].– Режим доступу: http:// journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php.

40. Світлична В.Ю., Інформаційна безпека: багатогранність сутності, види загроз та шляхи забезпечення http://economy.kname.edu.ua/images/files/publishing/360-369_%D0%A1%D0%B2%D1%96%D1%82%D0%BB%D0%B8%D1%87%D0%BD%D0%B0_2.pdf

41. Сороківська О.А. Інформаційна безпека підприємства: нові загрози та перспективи / О.А. Сороківська, В.Л. Гевко // Економічні науки: Вісник Хмельницького національного університету 2010. – № 2. – Т. 2. – С.32-35.

42. Указ Президента України №47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»

43. Цирлов В. Л. Основы информационной безопасности: краткий курс. — Ростов н/Д: Феникс, 2008. – 253, [1]с.-(Профессиональное образование).

44. Шапорин, В.О. Модели и методы анализа рисков безопасности информационных систем: дис. канд. техн. наук : 05.13.06 —

Информационные технологии / Шапорин Владимир Олегович - Одеса, 2016. – 178 с.

45. Шапорин, В.О. Модели и методы анализа рисков безопасности информационных систем: дис. канд. техн. наук : 05.13.06 — Информационные технологии / Шапорин Владимир Олегович – Одеса, 2016. – 178 с.

46. Щербина В.М. Інформаційне забезпечення економічної безпеки підприємств та установ / В.М. Щербина // Актуальні проблеми економіки. – 2008. – № 10. – С. 220-225.

47. Язов, Ю.К. Парадигма предельного ущерба и ее использование при оценке рисков нарушений безопасности информации в компьютерной системе [Текст] / Ю.К. Язов, Т.В. Григорьева // Известия Южного федерального университета. Технические науки. – 2008. – Т. 85. – №8. – С. 81-87.

ДОДАТОК А

SUMMARY

Ropaieva A. G. The modeling of information security risk estimation - Qualification master degree work. Sumy State University, Sumy, 2018.

The work studies theoretical and methodological basis of information security risk estimation. It gives the analysis of currently existing ways of the modeling of information security risk estimation. The main goal of this study is the creating of mathematical model of information security risk estimation and its real-life approbation (with the use “Statistica” application package).

Key words: risks, factor analysis, information security, risk estimation, the method of main components.

АНОТАЦІЯ

Ропаєва А. Г. Моделювання оцінювання ризиків інформаційної безпеки. – Кваліфікаційна магістерська робота. Сумський державний університет, Суми, 2018 р.

У роботі досліджено теоретико-методологічні основи оцінювання ризиків інформаційної безпеки. Проведено аналіз існуючих підходів до моделювання оцінювання ризиків інформаційної безпеки. Основною метою проведеного дослідження є побудова математичної моделі оцінювання ризиків інформаційної безпеки та її практична реалізація за допомогою пакету «Statistica».

Ключові слова: ризики, факторний аналіз, інформаційна безпека, оцінка ризиків, метод головних компонент.

ДОДАТОК Б

Анкета анонімного оцінювання ризиків інформаційної безпеки ТОВ «НЕТКРЕКЕР»

Оцінка ризиків інформаційної безпеки

Оцінка ризиків вербальним показником небезпеки

Оцініть ризик порушення конфіденційності інформації:

- ◯ Низька небезпека
- ◯ Середня небезпека
- ◯ Висока небезпека

Оцініть ризик втрати цілісності інформації:

- ◯ Низька небезпека
- ◯ Середня небезпека
- ◯ Висока небезпека

Оцініть ризик порушення доступності інформації:

- ◯ Низька небезпека
- ◯ Середня небезпека
- ◯ Висока небезпека

Оцініть ризик порушення роботи системи:

- ◯ Низька небезпека
- ◯ Середня небезпека
- ◯ Висока небезпека

Оцініть ризик крадіжки інформації:

- Низька небезпека
- Середня небезпека
- Висока небезпека

Оцініть ризик фальсифікації інформації:

- Низька небезпека
- Середня небезпека
- Висока небезпека

Оцініть ризик знищення інформації:

- Низька небезпека
- Середня небезпека
- Висока небезпека

Оцініть ризик вірусного зараження інформації:

- Низька небезпека
- Середня небезпека
- Висока небезпека

Оцініть ризик апаратних та програмних збоїв:

- Низька небезпека
- Середня небезпека
- Висока небезпека

ОТПРАВИТЬ