

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА**

**Навчально-науковий інститут
«Інститут інформаційних технологій в економіці»
Кафедра системного аналізу та кібербезпеки**

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Системний аналіз»

СПЕЦІАЛЬНІСТЬ

124 «Системний аналіз»

Форма навчання: очна (денна)

КВАЛІФІКАЦІЙНА МАГІСТЕРСЬКА РОБОТА

на тему «Системний аналіз в управлінні інформаційними ризиками підприємств»

здобувача Галіцина Володимира Євгеновича

(підпис)

**Науковий керівник: кандидат фізико-математичних наук,
доцент, Гладка Ю.А.**

(підпис)

**Робота допущена до захисту перед екзаменаційною
комісією з атестації здобувачів вищої освіти (ЕК)**

**Завідувач кафедри: доктор фізико-математичних наук,
професор Джалладова Ірада Агаверді-кизи**

(підпис)

Київ 2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА
Навчально-науковий інститут
«Інститут інформаційних технологій в економіці»
Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
СПЕЦІАЛЬНІСТЬ

«Системний аналіз»
124 «Системний аналіз»

ПОГОДЖЕНО

Керівник проектної групи (гарант)
освітньо-професійної програми
д.фіз.–мат.н., проф.Джалладова Ірада
Агаверді-кизи

(підпис)
_____ 2024 р.

ЗАТВЕРДЖУЮ

Завідувач кафедри
д.фіз.–мат.н., проф.Джалладова Ірада
Агаверді-кизи

(підпис)
_____ 2024 р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ
здобувача вищої освіти Галіцина Володимира Євгеновича
очної (денної) форми навчання

на підготовку кваліфікаційної магістерської роботи
на тему «Системний аналіз в управлінні інформаційними ризиками підприємств»
Тему затверджено наказом ректора Університету від " _____ " _____ 2024 р. № _____

Кваліфікаційна магістерська робота виконується на нормативно-правових документах,
фінансових звітах підприємства.

Розділ 1	СИСТЕМНИЙ АНАЛІЗ ІНФОРМАЦІЙНИХ РИЗИКІВ У ДІЯЛЬНОСТІ ПІДПРИЄМСТВА
Розділ 2	НЕЧІТКІ ПРОДУКЦІЙНО-БАЄСОВІ ІНСТРУМЕНТИ УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РИЗИКАМИ ПІДПРИЄМСТВА
Розділ 3	РЕКОМЕНДАЦІЇ З КОМП'ЮТЕРИЗОВАНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РИЗИКАМИ НА ПІДПРИЄМСТВІ
Об'єкт дослідження:	Інформаційні процеси підприємства

Предмет дослідження:	Фактори невизначеності зовнішнього та внутрішнього інформаційного середовища, інформаційні ризики підприємства
Мета кваліфікаційної магістерської роботи:	Аналіз і оцінка інформаційних ризиків підприємства з використанням комбінованих нечітких баєсових моделей для управління даними ризиками з метою визначення можливості настання несприятливих подій різних типів та нечітко-логічних процедур прогнозування збитків від ризиків для підвищення обґрунтованості управлінських рішень щодо забезпечення інформаційної безпеки та ефективності підприємства

Конкретні завдання, які здобувач повинен виконати для досягнення поставленої мети:

Розділ 1	Визначити вплив управління інформаційними ризиками на ефективність підприємства. Виконати аналітичний огляд сучасних методів та інструментів управління інформаційними ризиками підприємства. Розглянути логіко-інформаційну модель формування інформаційних ризиків підприємства.
Розділ 2	Надати характеристику об'єкту дослідження. Розглянути методику побудови комбінованих нечітких баєсових мереж оцінки можливості настання інформаційного ризику. Дослідити нечітко-продукційну процедуру розрахунку збитків від настання інформаційних ризиків підприємства.
Розділ 3	Оцінити методику організації комп'ютеризованих бізнес-процесів управління інформаційними ризиками підприємства. Визначити архітектуру та режими функціонування комп'ютеризованої системи управління інформаційними ризиками підприємства. Надати рекомендації щодо розробки комп'ютеризованої системи управління інформаційними ризиками підприємства.

Завдання підготував науковий керівник	Ю. А. Гладка (підпис) (ініціали, прізвище) «_____» _____ 2024 р.
Завдання одержав здобувач	В. Є. Галіцин (підпис) (ініціали, прізвище) «_____» _____ 2024 р.

Реферат

Кваліфікаційна магістерська робота містить 91 сторінку, 4 таблиці, 18 рисунків та перелік джерел з 35 найменувань.

«Системний аналіз в управлінні інформаційними ризиками підприємств»

Об'єктом дослідження є інформаційні процеси підприємства.

Предметом дослідження є фактори невизначеності зовнішнього та внутрішнього інформаційного середовища, інформаційні ризики підприємства.

Мета кваліфікаційної магістерської роботи - аналіз і оцінка інформаційних ризиків підприємства з використанням комбінованих нечітких баєсових моделей для управління даними ризиками з метою визначення можливості настання несприятливих подій різних типів та нечітко-логічних процедур прогнозування збитків від ризиків для підвищення обґрунтованості управлінських рішень щодо забезпечення інформаційної безпеки та ефективності підприємства.

Відповідно до поставленої мети були визначені такі *завдання*:

- Виконати організаційно-економічний аналіз впливу інформаційних ризиків на ефективність та конкурентоспроможність підприємства.
- Проаналізувати джерела виникнення ризикових ситуацій, класифікацію інформаційних ризиків підприємства.
- Розглянути структурну модель управління інформаційними ризиками на основі використання міжнародних та національних стандартів у галузі інформаційної безпеки та ризиків.
- Розглянути логіко-інформаційну модель виникнення інформаційних ризиків та розвитку ризикових ситуацій на підприємстві.
- Дослідити методики побудови комбінованих нечітких баєсових мереж для оцінки можливості настання інформаційних ризиків.
- Застосувати процедури логічного висновування для комбінованих нечітких баєсових мереж.
- Застосувати нечітко-логічні процедури розрахунку збитків від настання інформаційних ризиків на підприємстві.
- Застосувати архітектури комп'ютеризованої системи управління інформаційними ризиками на підприємстві.

Практичне значення отриманих результатів. Застосовані логіко-інформаційна модель виникнення інформаційних ризиків, комбінована нечітка баєсова мережа та нечітко-логічна процедура для оцінки ризиків на підприємстві мають практичне значення для створення та модернізації існуючих на підприємствах систем управління ІР та можуть бути практично використані для вирішення завдань управління ІР підприємства.

Рік виконання кваліфікаційної магістерської роботи 2024.

Рік захисту роботи 2024.

Ключові слова: системний аналіз, інформаційні ризики, нечітко-логічна процедура прогнозування збитків, мережі Баєса, система управління інформаційними ризиками.

В і д г у к
про кваліфікаційну магістерську роботу
здобувача навчально-наукового інституту «Інститут інформаційних технологій в економіці»
освітньо-професійної програми «Системний аналіз»

Галіцина Володимира Євгеновича

на тему: **«Системний аналіз в управлінні інформаційними ризиками підприємств»**

Актуальність теми. В умовах глобалізації та високої динаміки зміни інформаційного простору, невизначеності зовнішнього та внутрішнього середовища складність завдань управління інформаційними потоками у соціально-економічних системах постійно зростає. Саме аналізу і оцінці інформаційних ризиків підприємства з використанням комбінованих нечітких баєсових моделей для управління даними ризиками з метою підвищення обґрунтованості управлінських рішень щодо забезпечення інформаційної безпеки та ефективності підприємства присвячена ця робота.

Позитивні риси кваліфікаційної роботи. В основу КМР покладено системний підхід до розв'язання проблем, що розглядаються, з використанням методів теорії нечітких множин, методів штучного інтелекту та теорії прийняття рішень в умовах невизначеності, застосовані логіко-інформаційна модель виникнення інформаційних ризиків, комбінована нечітка баєсова мережа та нечітко-логічна процедура для оцінки ризиків на підприємстві.

Наявність самостійних розробок автора. В ході роботи розглянуті логіко-інформаційна модель управління інформаційними ризиками, комбіновані нечіткі баєсові мережі та нечітко-логічна процедура для оцінки ризиків на підприємстві; проведено оцінку доцільності застосування нечітко-продукційної процедури розрахунку збитків від настання інформаційних ризиків підприємства; описано архітектуру комп'ютеризованої системи управління інформаційними ризиками "InformRM 1.0"; запропоновано науково-обґрунтовані рекомендації щодо управління інформаційними ризиками на підприємстві. Надані рекомендації та проєктні рішення базуються на результатах дослідження предметної області, виконаного автором самостійно.

Цінність теоретичних висновків та практичних рекомендацій. У роботі вирішено завдання комп'ютеризованого аналізу та управління інформаційними ризиками на основі використання нечітко-логічних та баєсових методів, що має важливе значення для досягнення конкурентоспроможності, інформаційної безпеки та ефективності підприємства.

Наявність недоліків. Суттєвих недоліків не виявлено, але є окремі зауваження до стилю викладу, що не впливає на позитивну оцінку роботи.

Загальна оцінка кваліфікаційної магістерської роботи та її допущення до захисту перед ЕК. В роботі переконливо обґрунтовано актуальність завдання, яке вирішилося в повному обсязі. Робота виконана на сучасному рівні та показує, що автор добре орієнтується у даному питанні. Результати проведеного дослідження викладено в роботі професійно.

Кваліфікаційна магістерська робота Галіцина В.Є. може бути рекомендована до захисту в ЕК. Робота відповідає вимогам, що висуваються до кваліфікаційних робіт на здобуття освітнього ступеня магістр, заслуговує високої оцінки, а її автор, Галіцин Володимир Євгенович, заслуговує на присвоєння йому освітнього ступеня магістр зі спеціальності 124 «Системний аналіз», галузі знань 12 «Інформаційні технології».

Науковий керівник
доцент кафедри системного аналізу та кібербезпеки
Інституту інформаційних технологій в економіці
канд. фіз.-мат.наук, доцент



Гладка Ю.А.

20 травня 2024 р.

Рецензія

на кваліфікаційну магістерську роботу
здобувача вищої освіти Галіцина Володимира Євгеновича

Тема "Системний аналіз в управлінні інформаційними ризиками
підприємств"

Актуальність теми кваліфікаційної роботи і доцільність її розроблення обумовлені необхідністю вирішення проблем управління інформаційними ризиками підприємства на основі їх аналізу та оцінки, прогнозування збитків від їх можливого настання. Вирішення цих питань дозволить забезпечити безпеку інформації та підвищити ефективність підприємства. Оцінка можливості настання інформаційних ризиків та процедури розрахунку збитків від їх настання на підприємстві потребують застосування спеціальних інструментів, таких як комбіновані нечітко-логічні процедури. Комп'ютеризована система управління інформаційними ризиками, здатна мінімізувати витрати та максимізувати продуктивність підприємства, стає однією з гарантій ефективного управління виробництвом.

Якість проведеного дослідження. Методи системного економічного аналізу, економіко-математичного моделювання, логіко-ймовірнісні методи, методи теорії нечітких множин та теорії прийняття рішень в умовах невизначеності, методи Басса зумовили високу якість проведеного дослідження.

Позитивні риси кваліфікаційної бакалаврської роботи. Робота виконана якісно. Дослідження виконані комплексно та об'єктивно описують реальний стан проблеми в Україні та світі. Усі аналітичні дані і висновки добре структуровані та проілюстровані. Для здійснення аналізу кваліфіковано використаний системний аналіз та управління на основі сучасних наукових методик.

Зауваження. Доцільним було б розширити виконане дослідження одночасним використанням статистичних, квазістатистичних та нестатистичних факторів для комбінованої нечіткої мережі Басса.

Практична значимість висновків і рекомендацій. Застосована автором логіко-інформаційна модель виникнення інформаційних ризиків, комбіновані нечіткі багатовимірні мережі та нечітко-логічна процедура для оцінки ризиків на підприємстві мають практичне значення для створення та модернізації існуючих на підприємствах систем управління інформаційними ризиками для максимального підвищення ефективності підприємства.

Державний торговельно-економічний університет
Доцент кафедри цифрової економіки
та системного аналізу, к.е.н., доцент

Ірина СТОЛЕТОВА



Підпис Ірини Столетової засвідчую

44470674

Начальник відділу кадрів

Н. Шевченко

ЗМІСТ

ВСТУП.....	4
РОЗДІЛ 1 СИСТЕМНИЙ АНАЛІЗ ІНФОРМАЦІЙНИХ РИЗИКІВ У ДІЯЛЬНОСТІ ПІДПРИЄМСТВА.....	7
1.1 Вплив управління інформаційними ризиками на ефективність підприємства.....	7
1.2 Аналітичний огляд сучасних методів та інструментів управління інформаційними ризиками підприємства.....	16
1.3 Логіко-інформаційна модель формування інформаційних ризиків підприємства.....	32
РОЗДІЛ 2 НЕЧІТКІ ПРОДУКЦІЙНО-БАЄСОВІ ІНСТРУМЕНТИ УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РИЗИКАМИ ПІДПРИЄМСТВА .	40
2.1 Характеристика об'єкта дослідження.....	40
2.2 Методика побудови комбінованих нечітких баєсових мереж оцінки можливості настання інформаційного ризику	46
2.3 Нечітко-продукційна процедура розрахунку збитків від настання інформаційних ризиків підприємства	55
РОЗДІЛ 3 РЕКОМЕНДАЦІЇ З КОМП'ЮТЕРИЗОВАНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РИЗИКАМИ НА ПІДПРИЄМСТВІ.....	65
3.1 Методика організації комп'ютеризованих бізнес-процесів управління інформаційними ризиками підприємства.....	65
3.2 Архітектура та режими функціонування комп'ютеризованої системи управління інформаційними ризиками підприємства.....	72
3.3 Рекомендації щодо розробки комп'ютеризованої системи управління інформаційними ризиками підприємства.....	81
ВИСНОВКИ	87
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ.....	89

ВСТУП

Актуальність теми. Нині інформація, як один із найважливіших ресурсів підприємств, забезпечує досягнення успіху у конкурентній боротьбі, дозволяючи знизити ступінь невизначеності під час ухвалення рішень та підвищити ефективність управління підприємством. У зв'язку з цим однією з тенденцій розвитку всіх соціально-економічних систем є створення єдиного інформаційного середовища та комплексна інформатизація бізнес-процесів.

У той самий час інформація є самостійним об'єктом управління. В умовах глобалізації та високої динаміки зміни інформаційного простору, невизначеності зовнішнього та внутрішнього середовища складність завдань управління інформаційними потоками у соціально-економічних системах постійно зростає.

Щоб забезпечити оптимальний рівень продуктивності підприємств, інформація має бути актуальною, достовірною, повною та добре захищеною. Виникнення несприятливих ситуацій у зовнішньому та внутрішньому інформаційному середовищі підприємства призводить до зниження показників якості інформації, прийняття нераціональних управлінських рішень і, як наслідок, до економічних збитків. Таким чином, ефективне управління інформаційними ризиками (ІР) багато в чому визначає ефективність та конкурентоспроможність підприємств.

Аналіз останніх досліджень та публікацій. Різні аспекти управління ризиками в соціально-економічних системах розглянуті в працях як зарубіжних вчених Akerlof G., Barkley B., Barton T., Bernstein P., Crockford N., Crouhy M., Duncan R., Fragniere E., Frenkel M., Friedman M., Redhead K., Walker P., так і вітчизняних науковців Амоша О.І., Геєць В.М., Вітлінський В.В., Галіцин В.К., Матвійчук А.В., Герасимчук В.Г. та ін.

У цих роботах вивчено природу виникнення ризиків, наведено їх класифікацію та різні методи якісної та кількісної оцінки, запропоновано рекомендації щодо організації ризик-менеджменту та прийняття рішень в умовах невизначеності на підприємствах.

Управління ІР на підприємствах є відокремленою проблемою ризик-менеджменту, при вирішенні якої необхідно враховувати специфічні особливості джерел ІР, а також високу динаміку зміни інформації про невизначені фактори зовнішнього та внутрішнього середовища.

Аналіз сучасних наукових праць показав, що для оцінки ІР найчастіше використовуються статистичні методи, до яких належать баєсові мережі - ефективний інструмент графічного уявлення причинно-наслідкових відносин між безліччю змінних. У той же час, існуючі та застосовувані на практиці методи та інструменти управління ІР підприємства не повною мірою дозволяють враховувати різні види факторів невизначеності інформації та аналізувати кількісні та якісні характеристики ризиків, а, отже, і здійснювати оцінку та управління ІР з урахуванням стану та особливостей внутрішнього та зовнішнього середовища підприємства.

У зв'язку з цим розробка ефективних інструментів аналізу та управління ІР на основі нечітко-логічних методів та баєсових моделей є актуальною та має суттєве значення для підвищення конкурентоспроможності, економічної ефективності та інформаційної безпеки підприємства.

Мета і завдання дослідження. Аналіз і оцінка інформаційних ризиків підприємства з використанням комбінованих нечітких баєсових моделей для управління даними ризиками з метою визначення можливості настання несприятливих подій різних типів та нечітко-логічних процедур прогнозування збитків від ризиків для підвищення обґрунтованості управлінських рішень стосовно забезпечення безпеки інформації та оптимізації продуктивності підприємства.

Для досягнення поставленої цілі потрібно вирішити взаємопов'язані завдання:

1. Виконати організаційно-економічний аналіз впливу ІР на ефективність та конкурентоспроможність підприємства.
2. Проаналізувати джерела виникнення ризикових ситуацій, класифікацію

ІР підприємства.

3. Розглянути структурну модель управління ІР на основі використання міжнародних та національних стандартів у галузі інформаційної безпеки та ризиків.

4. Розглянути логіко-інформаційну модель виникнення ІР та розвитку ризикових ситуацій на підприємстві.

5. Дослідити методики побудови комбінованих нечітких баєсових мереж для оцінки можливості настання ІР.

6. Застосувати процедури логічного висновування для комбінованих нечітких баєсових мереж.

7. Застосувати нечітко-логічні процедури розрахунку збитків від настання ІР на підприємстві.

8. Застосувати архітектури комп'ютеризованої системи управління ІР на підприємстві.

Об'єкт дослідження: інформаційні процеси підприємства.

Предмет дослідження: фактори невизначеності зовнішнього та внутрішнього інформаційного середовища, інформаційні ризики підприємства.

Методи дослідження: методи системного аналізу соціально-економічних об'єктів; методи економіко-математичного моделювання; логіко-ймовірнісні методи; методи ризик-менеджменту; методи теорії нечітких множин; методи штучного інтелекту та теорії прийняття рішень в умовах невизначеності.

Теоретична, методична та практична значущість отриманих результатів. Застосовані логіко-інформаційна модель виникнення ІР, комбінована нечітка баєсова мережа та нечітко-логічна процедура для оцінки ризиків на підприємстві мають практичне значення для створення та модернізації існуючих на підприємствах систем управління ІР та можуть бути практично використані для вирішення завдань управління ІР підприємства.

Інформаційна база дослідження. Інформаційну базу роботи становлять наукові праці вітчизняних та зарубіжних науковців, нормативно-правові документи, статистичні дані, фінансові звіти підприємства, дані офіційних сайтів.

РОЗДІЛ 1

СИСТЕМНИЙ АНАЛІЗ ІНФОРМАЦІЙНИХ РИЗИКІВ У ДІЯЛЬНОСТІ ПІДПРИЄМСТВА

1.1 Вплив управління інформаційними ризиками на ефективність підприємства

На сьогоднішній день операційна діяльність підприємств відбувається в умовах невизначеності та нестабільності зовнішніх та внутрішніх факторів, що спричиняє збільшення вірогідності виникнення різноманітних та значних за обсягом ризиків.

У сучасних умовах управління ризиками є актуальним завданням і самостійною галуззю стратегічного та оперативного менеджменту. Мета ризик-менеджменту - виявити та оцінити головні для підприємства ризики, а також проаналізувати адекватність застосовуваних методів та засобів контролю для збільшення показників ефективності діяльності підприємства.

Коли мова йде про ризики, в першу чергу йдеться про можливість понести певні збитки з відповідною ймовірністю.

Внаслідок впливу факторів ризику на підприємство можливі фінансові, матеріальні, трудові та інші види втрат. Матеріальні втрати можуть виражатися у втратах майна, устаткування, продукції, енергоресурсів чи у вигляді додаткових витрат.

Фінансові втрати можуть виникнути внаслідок непередбачених витрат, неотримання запланованих доходів, сплати штрафів, а також додаткових податків, зниження виручки через зменшення ціни на продукцію тощо. Втрати часу виникають найчастіше через незаплановане збільшення тривалості виробничого циклу. Прикладом специфічних втрат є завдання збитку навколишньому

середовищу, заподіяння збитку здоров'ю працівників підприємства.

Некоректна оцінка ризиків є фундаментальною причиною виникнення глобальних і локальних криз. У зв'язку з цим впровадження ризик-менеджменту є актуальним з погляду запобігання спаду ділової активності підприємства. У період кризового стану відзначається істотне падіння виробничих та збутових показників, з'являються складнощі, пов'язані з інвестуванням у формування стабільного економічного середовища. Глобалізація не тільки надає додаткові можливості суб'єктам світового економічного простору, а й є відокремленим джерелом ризиків [2].

Цілеспрямоване і ефективне управління ризиками на підприємствах дозволяє подолати труднощі та зменшити ймовірність виникнення ситуацій, спричинених ризиками, до мінімуму.

Ефективне управління ризиками сприяє досягненню мети, підвищенню результативності бізнес-процесів і допомагає виявити прихований потенціал підприємства в умовах невизначеності. Аналіз світового досвіду підтверджує, що комплексне управління ризиками є ключовою складовою успішної діяльності великих компаній.

На підприємствах часто приділяють увагу невизначеності як зовнішнього, так і внутрішнього середовища, що призводить до виникнення ризиків. При цьому термін "ризик" має різні визначення залежно від контексту. За теорією статистики, ризик - це ймовірність настання події, яка може призвести до змін в передбачуваному тренді. З точки зору впливу на ефективність комерційних операцій, ризик розглядається як можливість неочікуваних збитків від події, що повністю змінює умови угоди. У загальному розумінні, ризик - це можливість виникнення небезпечної події.

Таким чином, ризик – виникнення небезпечної ситуації, збитки – наслідки ризику. Терміни «ризик» та «збитки» використовуються лише в контексті опису об'єкта та (або) суб'єкта. У науковій літературі зустрічаються також інші визначення ризиків. Так, під ризиками слід розуміти розмір фінансових втрат, які

виражаються у можливості не досягти поставленої мети внаслідок невизначеності запланованого результату та суб'єктивності його оцінки [20]. Можлива інтерпретація ризику як ступеня варіабельності доходів підприємства, які можна отримати завдяки володінню активами.

Ризик можна розглядати як діяльність, пов'язану з подоланням невизначеності при прийнятті необхідних рішень, коли наявна можливість кількісної та якісної оцінки ймовірності отримання бажаного результату та відхилення від мети.

Найбільш точним визначенням поняття ризик є таке: ризик - економічна категорія, яка описує здатність природної або соціально-економічної системи (явища, процесу) призводити у разі виникнення в процесі функціонування даної системи або поза нею деякої небезпечної події (ризикової ситуації) до появи збитку (збитків, втрат), що завдається або системі, або її навколишньому природному, економічному чи соціальному середовищу [3].

Перехід на інноваційну модель розвитку супроводжується інтенсивним застосуванням новітніх інформаційних технологій в усіх сферах діяльності: фінанси, промисловість, енергетика, транспорт та зв'язок, державне управління, оборона, наука та освіта, культура, охорона здоров'я та багато інших. Однак, широке та повсюдне застосування інформаційних технологій неможливе без розв'язання проблем забезпечення їхньої безпеки. Інформаційні технології стають одним із головних інструментів управління бізнесом та найважливішим засобом підвищення ефективності виробництва.

Проте активне використання інформаційних технологій у діяльності підприємств має і негативні наслідки, які полягають у значному збільшенні ролі ризиків, пов'язаних із цими технологіями, а саме інформаційних ризиків, що своєю чергою призводить до необхідності пошуку ефективних методів управління ними. Оскільки будь-яке підприємство є організаційною системою, механізми управління інформаційними ризиками повинні бути частиною загальної системи корпоративного управління.

Інформація — це ресурс, який, подібно до інших ресурсів організацій (матеріальних, фінансових, людських), має цінність. Наявність на підприємстві інформації високої якості (що відповідає таким показникам, як конфіденційність, цілісність, доступність) є необхідною умовою для забезпечення безперервності бізнес-процесів, підвищення конкурентоспроможності підприємств та підвищення ефективності їхньої інвестиційної політики, реалізації потенційних ринкових можливостей [30].

У процесі експлуатації інформаційних систем та обчислювальних мереж підприємства стикаються з різними видами загроз: шпигунство, стихійні лиха та надзвичайні події (пожежі, вибухи), диверсія, шахрайство, вандалізм та інші. Фактори ризиків, такі як комп'ютерні віруси і трояни, мережеві зломи та атаки хакерів, зустрічаються все частіше, стають все більш складними і адресними. Залежність бізнесу від безперебійної роботи інформаційних систем передбачає, що вразливість підприємств до загроз інформаційної безпеки невпинно зростає. При цьому організація інформаційного обміну між мережами загального доступу та приватними мережами, а також колективне використання інформації значно ускладнює керування доступом. Прагнення розподіленої обробки даних знижує ефективність процесів централізованого контролю.

Виникнення ризикових ситуацій в інформаційному середовищі підприємства призводить до збитків. У зв'язку з цим, інформаційні ризики можуть розглядатися як складова частина економічних ризиків. При цьому необхідно оцінити взаємний вплив інформаційних та економічних ризиків, їх причинно-наслідкові, функціональні та часові зв'язки. Проведений аналіз описаних у літературних джерелах класифікацій ризиків дозволив дійти висновку, що взаємозв'язок між поняттями інформаційний та економічний ризик полягає в тому, що різні інформаційні ризики можуть бути зараховані одночасно до кількох видів економічних ризиків.

У табл. 1.1 наведено приклади ризиків підприємства та відповідні їм інформаційні загрози [7].

Таблиця 1.1 - Види інформаційних загроз та відповідні бізнес-ризики

Вид ризику	Інформаційні загрози	Можливі наслідки
Ризик недотримання законодавства (стягнення правоохоронних органів влади)	- Недотримання законодавства у сфері захисту інформації; - відсутність ліцензій	Штрафи, пені, втрата репутації, призупинення чи припинення діяльності
Ризик зміни ринкової кон'юнктури (посилення конкуренції, дефолт, ревальвація, девальвація, валютна інтервенція тощо)	- Витік конфіденційної інформації; - несвоєчасне надходження інформації; - хибне прогнозування; - спотворення інформації у фінансовій звітності	Втрати фінансових ресурсів, повна втрата бізнесу
Інвестиційний ризик (помилкові рішення щодо інвестування коштів)	- Нестача інформації, на підставі якої приймаються рішення; - несвоєчасне надходження даних	Втрати фінансових ресурсів
Фінансовий ризик (помилки в процесах планування та обліку, неефективне управління фінансовими активами, розкрадання готівки, шахрайство тощо)	- Фінансове шахрайство із застосуванням комп'ютерних систем; - атаки на банківські рахунки; - шахрайства із пластиковими картками; - умисне викривлення фінансової звітності	Втрати фінансових ресурсів, падіння репутації підприємства
Репутаційні ризики (негативний вплив різних подій на репутацію та імідж підприємства)	- Крадіжка конфіденційних даних; - невиконання договірних зобов'язань через відсутність доступу до інформаційних сервісів	Зменшення кількості клієнтів
Природні надзвичайні ситуації (пожежі, повені, землетруси тощо)	- Втрата важливої та конфіденційної інформації на різних носіях; - неможливість доступу до інформаційних сервісів	Втрати фінансових та матеріальних ресурсів, порушення безперервності діяльності підприємства, повна чи часткова втрата бізнесу
Ризики техногенних катастроф (збої та відмови обладнання та програмного забезпечення)	- Втрата критичної інформації; - втрата підсумків роботи	Втрати фінансових та матеріальних ресурсів, простої у роботі підприємства, невиконання договірних зобов'язань
Фізичні ризики (крадіжка, пограбування, саботаж тощо)	- Втрата критичної інформації; - порушення конфіденційності даних; - неможливість доступу до інформаційних сервісів	Погіршення репутації, втрати фінансових та матеріальних ресурсів, порушення безперервності роботи підприємства, простої обладнання та людських ресурсів

Джерело: розроблено автором на основі [9]

Обов'язковим елементом всіх економічних ризиків є інформаційний ризик. Це пояснюється насамперед тим, що процес прийняття рішень здійснюється в умовах невизначеності зовнішнього та внутрішнього середовища.

Окремі категорії економічних ризиків (наприклад інвестиційний) є підвидами інформаційних ризиків.

До складу інформаційних ризиків включаються: банківський, валютний, процентний ризики, ризики підприємств, діяльність яких полягає у наданні інформаційних послуг, та інші ризики, пов'язані з прийняттям управлінських рішень, отриманням та виробництвом інформації [3].

З вищесказаного можна дійти висновку, що першорядним завданням з погляду досягнення інформаційної безпеки підприємства, є обґрунтування термінологічного значення поняття «інформаційний ризик».

На сьогодні не склалося загальноприйнятого тлумачення цієї категорії.

Вважається, що небезпеку становлять нерозмежований доступ персоналу до корпоративної інформації, технічні неполадки та збої, суперечливість даних у інформаційних системах.

У зв'язку з цим інформаційні ризики виникають на всіх етапах інформаційних процесів (збір, обробка, передача, зберігання, захист та використання інформації).

Для забезпечення ефективного управління інформаційною безпекою та ризиками в даний час активно застосовуються різноманітні міжнародні стандарти, такі як ISO 15408, ISO 17799 (BS7799), серія ISO 27000, а також стандарти національних провайдерів, наприклад, BSI (Великобританія), *NIST 80030 (США)*, нормативно-рекомендаційні бібліотеки та стандарти (*COSO, ITIL, SAS 55/78*) та інші.

У стандарті *ISO 17799* використовується широке трактування ризику як поєднання ймовірності несприятливої події та наслідків її появи. На відміну від комерційних ризиків, внаслідок яких може бути отриманий і певний позитивний ефект (вивільнення додаткових коштів через зниження валютного курсу), події, що

характеризують стан інформаційної безпеки, мають лише негативні наслідки.

Стандарт ISO 27005 розглядає складові поняття «інформаційного ризику» як активи, загрози, вразливості та потенційні збитки. Так, відповідно до ISO 27005:

«Ризик інформаційної безпеки полягає у можливості експлуатації вразливостей у системі або групі систем за дії певних загроз, що може негативно вплинути на діяльність організації» [9].

Усі загрози, які негативно впливають на наявні на підприємстві інформаційні ресурси, а також на інформаційні системи та програмно-технічні засоби, вимагають ретельного аналізу, контролю та вирішення завдання захисту інформації. Такі несприятливі чинники є загрозою інформації.

У той самий час інформаційна діяльність будь-якого підприємства не є кінцевою метою, а слугує для забезпечення безперервності господарської діяльності. Дані, що є частиною інформаційних ресурсів підприємства, їх зміст та якість, правила отримання можуть містити додаткові загрози, оскільки на підставі їх аналізу та обробки здійснюється прийняття рішень щодо управління виробничими та організаційними процесами підприємства. Таким чином, інформаційне середовище є джерелом різноманітних загроз для підприємства. Такі загрози називаються інформаційними загрозами. Існування інформаційних загроз визначає необхідність розв'язання проблеми безпеки інформації. З погляду виявлення інформаційних загроз та загроз інформації системою інформаційної безпеки є набір засобів, інструментів і заходів, спрямованих на забезпечення високого ступеня захищеності інформації та мінімізації інформаційних загроз з боку інформаційного середовища.

Інформаційний ризик є несприятливою подією в інформаційному середовищі, реалізація якого призводить до збитків як для самого інформаційного середовища, так і для всього підприємства. Імовірність виникнення цієї події є параметром ризику, що оцінюється, проте на практиці обчислити його аналітично або на підставі статистики дуже складно. У зв'язку з цим ймовірність найчастіше визначається Складові автоматизованих інформаційних систем (AIC), систем

управління (АСУ), телекомунікаційні системи та мережі (ТКС), інформаційні ресурси (ІР), що збираються та обробляються цими системами є об'єктами аналізу та управління в галузі забезпечення інформаційної безпеки. В контексті системного підходу до аналізу інформаційної безпеки підприємства, необхідно здійснити більш ретельну класифікацію ІТ-ризиків.

Виділяють велику кількість різних підходів до розробки даних класифікацій. Так, наприклад, ІТ-ризики за критерієм «джерело виникнення» поділяються на три групи [10]:

- ризики відмови обладнання (технологічні);
- ризики відмови програмного забезпечення (програмні);
- ризики помилок персоналу, зокрема через відсутність єдиних корпоративних стандартів (організаційні).

Виділяються комбіновані ризики, наприклад, коли технічний збій у роботі сервера є причиною порушення цілісності та несуперечності бази даних (програмний рівень).

За рівнем впливу на діяльність підприємства виділяють критичні та некритичні ризики; за джерелом виникнення - зовнішні та внутрішні.

Зовнішній інформаційний ризик визначається процесами, які безпосередньо і опосередковано впливають на стан інформаційного середовища підприємства і протікають поза ним. Джерела появи такого ризику: дії конкурентів чи шахраїв, виникнення нових технологій порушення інформаційної безпеки систем, проблеми фінансового та організаційного характеру, надзвичайні події та стихійні лиха, заворушення тощо. [10]. Прояв зовнішнього ризику може бути прямим (перехоплення повідомлення через телекомунікаційні мережі та потоки документів) та непрямим (електромагнітні випромінювання, спеціалізована техніка, шпигунство).

Інформаційна активність усередині підприємства здійснюється за рахунок елементів: АІС, АСУ, ТКС, інформаційно-аналітична підтримка бізнес-процесів (у

тому числі у вигляді методик та технологій роботи та використання паперових документів). Визначення внутрішньої складової інформаційного процесу можна трактувати як синонім інформаційної системи підприємства (ІС), коли вона з'єднує всі складові інформаційної діяльності (телекомунікаційні системи та мережі, документообіг, інформаційно-аналітична підтримка бізнес-процесів тощо.). Таким чином, внутрішній інформаційний ризик належить до внутрішніх процесів підприємства та викликаний такими факторами, як, наприклад, неефективна оргструктура ІТ-підрозділу, низька кваліфікація персоналу, помилки проектування та побудови ІТ-інфраструктури або ІС, тощо.

Вихідною точкою поширення загроз інформації в основному є зовнішнє оточення підприємства, проте джерелами може бути і внутрішнє інформаційне середовище. Такі інформаційні загрози переважно виникають як результат існування недоліків в організації внутрішнього інформаційного середовища, у тому числі у технологіях інформаційно-аналітичної підтримки бізнес-процесів на основі зовнішніх ІР, але зустрічаються і спрямовані зовнішні джерела інформаційних загроз.

Втрата інформаційного активу призводить до прямих збитків для підприємства. Найчастіше вони стикаються зі спамом та шкідливими програмами (віруси, черв'яки, шпигунське програмне забезпечення), зі зломом корпоративних комп'ютерів та телекомунікаційних мереж, шпигунством, цільовими та *DDoS*-атаками.

На сьогодні серед аналітиків та експертів поширена думка, що найбільш серйозні наслідки для сучасних підприємств мають спам та поширення вірусів через електронну пошту, *DDoS*-атаки, фішинг, черв'яки, аномалії у протоколах. У корпоративному секторі також з'являється потреба вводити обмеження та посилювати контроль за діями персоналу в мережі, наприклад, блокувати сайти та доступ до соціальних мереж з метою запобігання можливим витокам конфіденційних даних.

Зовнішні загрози інформації є дуже актуальними, що спричинено великою

кількістю атак на системи інтернет-банкінгу та подій, пов'язаних із крадіжкою корпоративних конфіденційних даних. Наприклад, потенційна можливість крадіжки фінансових коштів із рахунків у банках визначається отриманням автентифікаційних даних до системи клієнт-банк. Інформація може бути вкрадена зовнішніми зловмисниками, які виявляють та експлуатують існуючі вразливості в захисті підприємства.

Таким чином, управління інформаційними ризиками є актуальним завданням у сучасних умовах використання інформаційних технологій у всіх сферах діяльності підприємства.

Водночас у зв'язку з тісним взаємозв'язком інформаційних ризиків з іншими видами бізнес-ризиків інформаційний ризик-менеджмент має стати окремим елементом корпоративної системи управління ризиками, що враховує специфіку інформації як об'єкта управління.

1.2 Аналітичний огляд сучасних методів та інструментів управління інформаційними ризиками підприємства

Однією з актуальних проблем підприємства є управління інформаційними ризиками. У зв'язку з цим спостерігається посилення залежності успішності бізнесу від організаційно-технічних заходів і засобів контролю та зменшення ризику, що використовуються. Оскільки інформаційні ризики мають різний ступінь значущості для різних підприємств, виділяють три підходи до ризик-менеджменту у сфері інформаційної безпеки, які відрізняються одна від одної глибиною та рівнем формалізації [8].

Для систем, несприйнятливих до ризику, коли інформаційні ресурси є допоміжними для функціонування підприємства, а рівень інформатизації бізнес-процесів невеликий, виникає мінімальна потреба в аналізі та оцінці ризиків. У

таких підприємствах існує певний базовий рівень інформаційної безпеки, що задається стандартами у сфері ІБ та кращими практиками, досвідом інших організацій.

Міжнародні стандарти, крім визначення необхідних механізмів і інструментів для впровадження та супроводу безпеки, також враховують вимоги щодо оцінки ризиків та економічної ефективності застосування різних методів управління для вибору оптимальних для конкретної організації. При цьому достатньо скористатися якісними підходами до вирішення цього завдання.

Для систем, сприйнятливих до ризиків, у яких інформаційні процеси не належать до основних бізнес-процесів підприємства, проте ступінь його інформатизації високий, а інформаційні ризики можуть вплинути на економічну діяльність, процеси аналізу та оцінки інформаційних ризиків є обов'язковими елементами корпоративного управління. Рекомендується використовувати комбіновані якісні та кількісні підходи до оцінки ризиків, приділяючи особливу увагу максимально критичним системам та процесам.

Коли діяльність підприємства орієнтована на надання інформаційних послуг і передбачає використання інформаційних активів для реалізації основних бізнес-процесів, ризики інформаційної безпеки належать до найважливіших, для їх оцінки необхідно використовувати формальні підходи та різноманітні кількісні методи на основі статистики та інтелектуальних алгоритмів.

Водночас для більшості підприємств раціональним є використання підходу до побудови системи інформаційної безпеки, який полягає у високорівневій оцінці ризиків для визначення видів інформаційних загроз та загроз інформації, що мають критичне значення для здійснення виробничих та бізнес-процесів, з подальшою більш детальною оцінкою ризиків для виділених підсистем.

Розроблено спеціальні методи управління ризиками в інформаційній сфері, опис яких міститься у міжнародних, національних та інших стандартах та документах, таких як ISO 15408, ISO 17799 (BS7799), серії стандартів ISO 27000, BSI, NIST. 80030, САК, КОСО, САС 55/78.

Підсумовуючи, можна відзначити, що управління інформаційними ризиками включає наступні етапи:

1. Формулювання цілей та методів захисту інформації підприємства.
2. Розробка та впровадження ефективної системи оцінки та управління ІТ-ризиками.
3. Визначення якісних та кількісних оцінок ІТ-ризиків, що впливають на досягнення бізнес-цілей.
4. Використання спеціального набору інструментів та методів оцінки та управління ІТ-ризиками.

Проаналізуємо обрані міжнародні стандарти в сфері інформаційної безпеки. У Великобританії був розроблений стандарт BS 7799 Частина 3: «Системи управління інформаційною безпекою – Практичні правила управління ризиками інформаційної безпеки». Після доопрацювання він був переданий до міжнародних організацій зі стандартизації (ISO та IEC) і наразі є стандартом ISO/IEC 27001.

BS 7799-3 описує процеси оцінки та управління ІТ-ризиками як одну з підсистем комплексної системи управління промисловим підприємством, застосовуючи при цьому процесну модель, що включає 4 категорії (планування, реалізація, перевірка, дії). Ці процеси відображають стандартний цикл будь-яких процесів керування (рис. 1.1).



Рисунок 1.1 – Процеси оцінки та контролю ризиків відповідно до стандарту BS 7799-3

Джерело: розроблено автором на основі [20]

На етапі планування відбувається встановлення стратегії та вибір методології управління ризиками, оцінка рівня ризиків, проведення інвентаризації інформаційних активів, розробка профілів загроз та вразливостей, оцінювання ефективності прийнятих заходів та визначення допустимого рівня ризиків.

Етап впровадження включає аналіз ризиків та впровадження контрольних механізмів для їх зменшення. Керівництво приймає рішення стосовно кожного виявленого ризику: зберігати, уникати, переносити або мінімізувати. Після цього розробляється і впроваджується план заходів щодо управління ризиками.

Етап перевірки дозволяє відстежувати роботу механізмів та інструментів контролю. Здійснюється аналіз змін стану джерел ризику (загроз, вразливостей), проводяться аудиторські перевірки та контролюючі процедури.

Етап дій виконується на основі результатів моніторингу та перевірок. Включає в себе проведення коригувальних заходів, таких як переоцінка ризиків, внесення змін до стратегії та методології управління ризиками ІТ, а також розробку плану обробки ризикових подій.

На основі британських стандартів BS створена серія стандартів ISO/IEC 27000, яка була опублікована спільно Міжнародною Організацією зі Стандартизації (ISO) та Міжнародною Електротехнічною Комісією (IEC).

Міжнародні стандарти ISO 27002 та ISO 27001 є серед найбільш поширених в сфері інформаційної безпеки.

ISO 27002 (раніше відомий як ISO 17799) містить опис основних рекомендацій для ефективних систем управління інформаційною безпекою на підприємствах, зосереджуючись на всіх ключових аспектах, включаючи [21]:

- створення стратегії інформаційної безпеки;
- інформаційну безпеку професійної діяльності персоналу;
- забезпечення безпеки зв'язку;
- забезпечення фізичного захисту даних та обладнання;
- управління доступом до інформації;
- розробка процедур опрацювання інцидентів;

- забезпечення відповідності законодавчим вимогам щодо інформаційної безпеки.

У табл. 1.2 подано список та короткий опис основних стандартів даної серії [9].

Таблиця 1.2 – Опис основних стандартів інформаційної безпеки серії ISO 27000

Стандарт ISO/IEC	Опис
27000	Огляд та словник
27001	Інформаційні технології. Методи забезпечення безпеки. Системи управління інформаційною безпекою. Вимоги.
27002	Інформаційні технології. Методи забезпечення безпеки. Практичні правила управління інформаційною безпекою.
27003	Посібник із впровадження системи управління інформаційною безпекою.
27004	Вимірювання ефективності системи управління інформаційною безпекою.
27005	Методи забезпечення безпеки. Управління ризиками інформаційної безпеки.
27006	Методи забезпечення безпеки. Вимоги до органів аудиту та сертифікації систем управління інформаційною безпекою.
27007	Керівництво для аудитора СУІБ.
27008	Посібник з аудиту механізмів контролю СУІБ.
27032	Посібник із забезпечення кібербезпеки.
27033	Основні концепції управління мережевою безпекою.

Джерело: [9]

Міжнародні стандарти ISO 27002 та ISO 27001 є серед найбільш поширених в сфері інформаційної безпеки.

ISO 27002 (раніше відомий як ISO 17799) містить опис основних рекомендацій для ефективних систем управління інформаційною безпекою на підприємствах, зосереджуючись на всіх ключових аспектах, включаючи [21]:

- створення стратегії інформаційної безпеки;
- інформаційну безпеку професійної діяльності персоналу;
- забезпечення безпеки зв'язку;
- забезпечення фізичного захисту даних та обладнання;
- управління доступом до інформації;
- розробка процедур опрацювання інцидентів;

- забезпечення відповідності законодавчим вимогам щодо інформаційної безпеки.

Стандарт інформаційної безпеки ISO 27001 включає критерії, які використовуються для оцінки та аналізу системи управління, результатом якої є видача сертифіката відповідності акредитованим центром, який потім вноситься до реєстру. ISO 27001 описує систему управління інформаційної безпеки (СУІБ), спрямовану на розробку та впровадження програм для підвищення безпеки підприємств. У СУІБ використовується цикл розробки, аналізу та перегляду, який відомий як модель PDCA (Plan-Do-Check-Act, Цикл Демінга).

Перші ітерації даного циклу значно відрізнятимуться від наступних, оскільки цикл запускається «з нуля», без достатньої кількості вихідних корпоративних даних і узагальнює практики, що застосовуються сьогодні в рамках упорядкованої СУІБ. По закінченні реалізації першої ітерації циклу здійснюється безперервне його повторення для збереження стійкого та ефективного функціонування СУІБ.

Бібліотека інфраструктури інформаційних технологій *ITIL* є методом використання кращого світового досвіду в інформаційних процесах. *ITIL* є набором публікацій, що включають рекомендаційні поради у сфері надання високоякісних ІТ-послуг та реалізації підтримуючих процесів. Головна мета *ITIL* – надання та обмін найбільш сучасними знаннями та досвідом. Відмінна риса *ITIL* – реалізація управління ІТ-послугами у вигляді набору процесів.

ITIL включає сім книг, що описують сім процесів: підтримка послуг, надання послуг, планування впровадження управління послугами, управління інформаційно-комунікаційною інфраструктурою, управління програмами, перспективи бізнесу, безпека. Підприємствам, які прагнуть використати *ITIL*, необхідно організувати ефективну систему менеджменту ІТ. Це обов'язкова умова успішної реалізації *ITIL*.

Міжнародна організація ISACA, що спеціалізується на аудиті та контролі інформаційних систем, адаптувала стандарт COBIT 5, включивши в нього

найбільш ефективні методи управління та стратегічного керівництва в галузі ІТ.

COBIT є синтезом практичного досвіду компаній з усього світу, міжнародної та національної нормативної бази різного роду, а також стандартів у галузі інформаційної безпеки та ризиків. Розроблення COBIT здійснювалося командою експертів з різних секторів, включаючи державні та комерційні організації, а також освітні установи, що спеціалізуються на інформаційній безпеці та управлінні ІТ.

Основна мета COBIT полягає у подоланні розриву між топ-менеджментом, який визначає стратегічні цілі бізнесу, та департаментом інформаційних технологій, що забезпечує підтримку інформаційної інфраструктури та основних бізнес-процесів. COBIT 5 включає 5 принципів, які дозволяють забезпечити ефективне керівництво та управління, враховуючи сім факторів впливу. Ці принципи є основою для практичних заходів у сфері управління ІТ.

1. Принцип відповідності вимогам зацікавлених сторін. COBIT 5 визначає широку систему цілей, яка декомпозує інтереси зацікавлених сторін в організаційні цілі, потім у цілі топ-менеджменту та управління ІТ та, нарешті, у цілі відокремлених елементів СМІБ.

2. Принцип комплексного підходу до підприємства являє собою системний підхід, коли управління ІТ розглядається як невід'ємна частина корпоративної системи управління.

3. Принцип використання єдиної інтегрованої методології. У COBIT інтегруються елементи найбільш популярних міжнародних та національних стандартів, зведення знань, а також інших підходів.

4. Принцип забезпечення цілісності підходу. COBIT 5 використовує спеціальні елементи, «чинники впливу», такі як політика, принципи та підходи, щоб забезпечити цілісність управління ІТ.

5. Принцип поділу керівництва та управління. Модель керівництва та управління у COBIT включає 5 з 32 процесів керівництва та управління, які об'єднуються в групи відповідно до їх призначення. Процеси управління об'єднані

в групи *EDM* (Оцінка, вибір напрямку та спостереження), *АРО* (Забезпечення відповідності, планування та організація), *BAI* (Створення, придбання та впровадження), *DSS* (Обслуговування, експлуатація та супровід), *MEA* (Відстеження, вимірювання та оцінка).

COBIT пропонує користувачам нормативну базу для управління ІТ, що включає необхідні інструкції з досягнення більшої відповідності вимогам бізнесу. *COBIT* також надає механізм для вимірювання потенціалу організації (люди, процеси та технології), що дозволяє їй успішно задовольняти потреби бізнесу та механізм для вимірювання продуктивності.

Хоча стандарт *COBIT* орієнтований на ІТ-процеси, до нього не включені відповідні процедури та завдання. Він більш сфокусований на тому, що підприємству необхідно зробити, а не на те, як цього досягти. Процеси *COBIT* звертаються до потреб бізнесу та містять інструкції щодо визначення адекватних засобів для їх задоволення.

COBIT і *ITIL* спільно формують комбінацію рекомендацій, які допомагають підприємствам управляти ІТ, виходячи з бізнес-завдань, тобто, застосовувати на практиці стратегію, відому як Управління бізнес-послугами (*Business Service Management - BSM*). *ITIL* пропонує інструкції щодо здійснення процесів ІТ відповідно до передової практики та у параметрах узгодження ІТ із потребами бізнесу. *COBIT* допомагає адаптувати процеси *ITIL* до потреб конкретного бізнесу та цілей організації. Він допомагає організації визначити відправну та кінцеву точки, тобто, зрозуміти, де організація зараз і де вона хотіла б бути. Знаючи цілі, ІТ-організація може активувати бізнес-цілі [4].

Таким чином, на підприємстві доцільно використовувати різні стандарти, при цьому консолідуючим стандартом виступає *COBIT* (рис. 1.2).

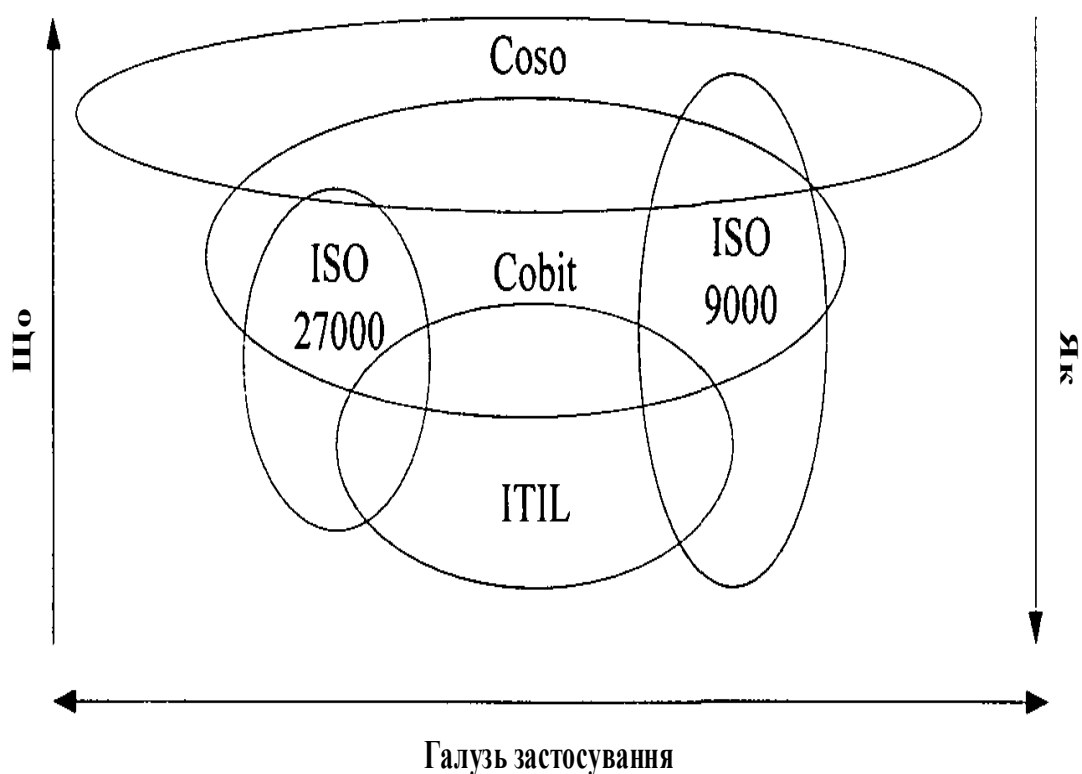


Рисунок 1.2- Взаємозв'язок стандартів, які регламентують управління інформаційними технологіями в організації
Джерело: складено автором

Переваги застосування стандартів полягають у зниженні витрат матеріальних, фінансових, людських ресурсів, що витрачаються на розробку управлінської стратегії. У той самий час жоден стандарт докладно не описує весь процес управління з урахуванням специфіки конкретного об'єкта. У зв'язку з цим доцільно вивчити всі основні стандарти з метою адаптації їх ідей та змісту для конкретної ситуації. Таким чином, побудова системи управління має бути заснована на кращому з відповідних стандартів (рис. 1.3.)

Методології управління інформаційними ризиками (ІР) у міжнародних стандартах

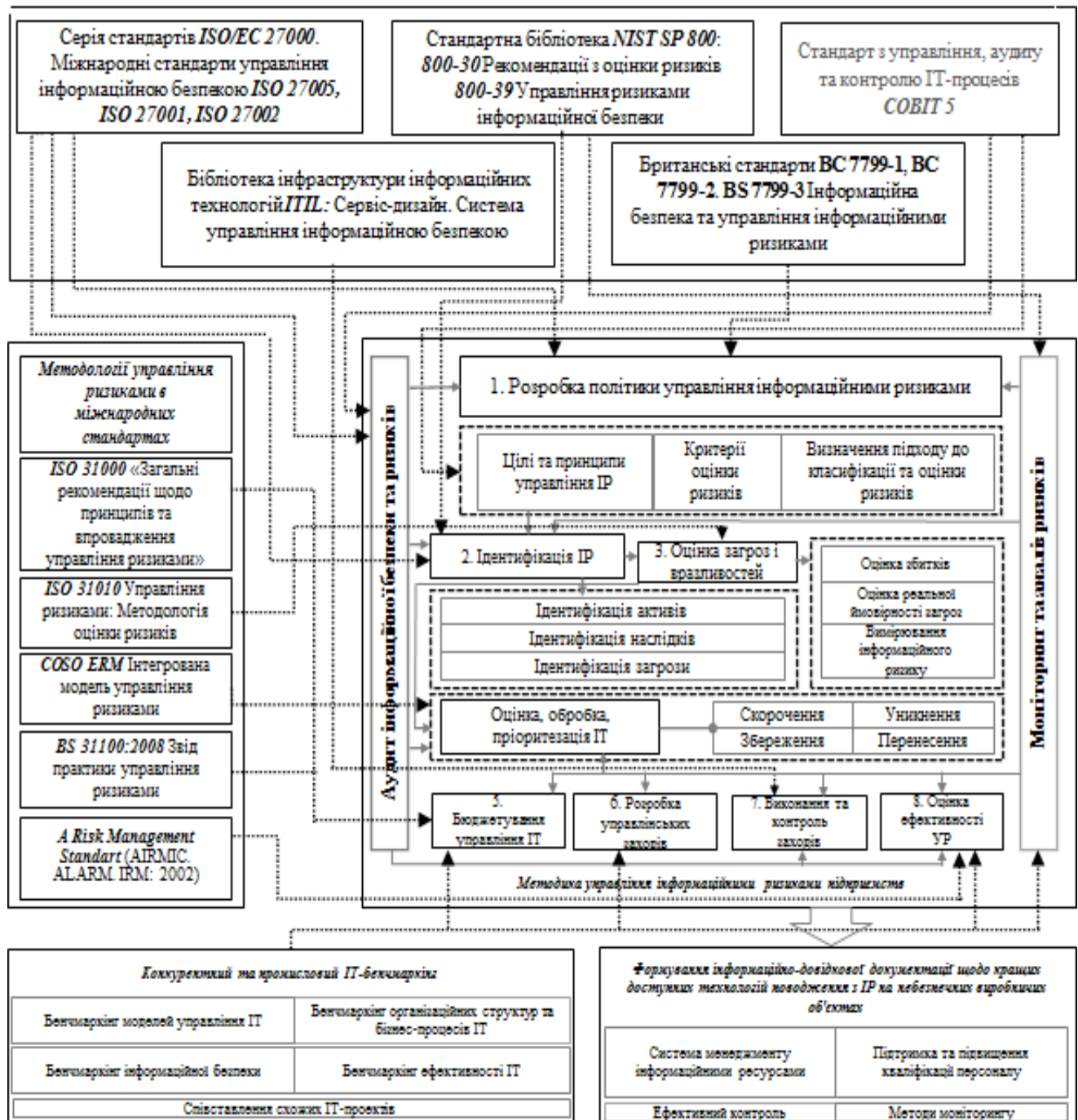


Рисунок 1.3 – Модель управління інформаційними ризиками підприємства згідно з міжнародними стандартами

Джерело: розроблено автором на основі [20]

На рисунку 1.3 показано на якому етапі методики управління ризиками який стандарт використовувати найбільш раціонально. На практиці це виражається у наступному. Наприклад, стандарт ISO 27001 наголошує на важливості аудиту ІТ-

безпеки, проте не містить обґрунтованих рекомендацій та правил його виконання. Стандарт *COBIT* включає опис основних принципів проведення аудиту. Процес управління інформаційною безпекою докладно описаний у стандарті *BS 7799*, повний перелік процедур оцінки, розробки заходів, контролю та управління ІТ-безпекою представлений у спеціальній книзі бібліотеки *ITIL*.

Стандарти, які наразі використовуються в галузі інформаційної безпеки та ризиків, такі як *ISO 15408*, *ISO 17799*, *ISO 9001*, *NIST 800-30*, *BSI*, *BS 7799*, *COBIT*, *ITIL* і інші, не охоплюють всі принципові аспекти, які слід враховувати при розробці методик управління інформаційними ризиками. Урахування цих аспектів залежить від рівня зрілості підприємства, його специфіки та інших факторів. Таким чином, неможливо розробити універсальну методику управління інформаційними ризиками, яка підходила б усім вітчизняним підприємствам і забезпечувала економічно обґрунтовану безпеку. В кожному окремому випадку рекомендується адаптувати її до потреб конкретного підприємства з урахуванням його особливостей.

Одним із необхідних етапів управління інформаційними ризиками є проведення ІТ-бенчмаркінгу. Бенчмаркінг є порівняльним аналізом однієї бізнес-системи з аналогічними їй. З одного боку, це науковий метод, з іншого боку повною мірою практичний, як і експеримент чи аналіз. У процесі бенчмаркінгу важливо визначити, за якими параметрами буде проведено зіставлення, як і з чим. З'являється велика кількість питань. Наприклад, як порівнювати та визначати порівняльну базу. Зазвичай зіставляються значення по цілій сукупності параметрів, причому критерії і вага параметрів, а також варіант їх обробки обумовлюються цілями аналізу. Порівнювати можна спосіб організації бізнес-систем, їх ефективність. Таким чином, аналіз може бути як кількісним, так і якісним.

Незважаючи на існування великої кількості стандартів та методик управління інформаційними ризиками та безпекою, дослідження показує, що, хоча практично у кожній другій компанії є документально оформлений підхід до управління ризиками, існує об'єктивна необхідність подальшої стандартизації

процедур та політик.

Найбільш складним і неоднорідним з погляду алгоритмів і методів, що застосовуються, етапом управління інформаційними ризиками є оцінка ризиків. На сьогодні єдиної методики оцінки інформаційних ризиків немає. Насправді найбільшого поширення набула якісна оцінка інформаційних ризиків.

Для нормативного регулювання процесів оцінки різних видів ризиків стандартом ISO 31010 «Методи оцінки ризику» визначено відповідні підходи. Згідно з цим стандартом, процес оцінки ризику включає в себе ідентифікацію, аналіз та порівняльну оцінку ризиків.

Ідентифікація ризику - це процес виявлення основних елементів ризику, формування їх переліку та опис кожного з них.

Методи ідентифікації ризику:

- методи, що базуються на документованих даних (аналіз контрольних листів, експериментальних даних, ретроспективний аналіз);
- підхід, який передбачає, що група експертів виконує регламентований процес ідентифікації ризику з використанням підказок чи питань;
- індуктивні методи (наприклад, HAZOP вивчення небезпеки та дійсності).

Для підвищення точності та повноти процесів ідентифікації ризику можуть застосовуватись допоміжні способи, наприклад, метод Дельфі та мозкового штурму.

Аналіз ризику складається з наступних етапів: аналіз даних про ризик, ймовірність (можливість) та наслідки настання виявлених небезпечних ситуацій з урахуванням ефективності використовуваних методів управління. Інформація про ймовірність ризикових ситуацій та їх наслідки застосовується для оцінки рівня ризику.

Розглянуті методи аналізу ризиків можна розділити на якісні, кількісні або змішані. Якісне оцінювання включає в себе опис наслідків ризиків, їх ймовірність та значимість, виражену за шкалою «високий», «середній» та «низький». У цьому

випадку порівняльна оцінка ризиків базується на якісних критеріях.

У змішаних методах застосовується чисельна шкала аналізу наслідків, ймовірності, і, навіть, їх поєднання, виявлення величини ризику за спеціальною формулою. Виділяються лінійні, логарифмічні та інші види шкал. Відповідно, формули розрахунку можуть значно відрізнятися.

При проведенні кількісного аналізу ризиків визначається значущість та грошова оцінка можливих наслідків та ймовірності їх виникнення. В цьому випадку значення ризику вимірюється в одиницях, встановлених для відповідної області застосування управління ризиками. Однак повний кількісний аналіз ризиків може бути нездійсненним у зв'язку з недостатньою кількістю даних про систему, що аналізується, впливом людського фактору та інших аспектів, а також через великі витрати праці на його проведення. У таких ситуаціях простого впорядкування ризиків кваліфікованими фахівцями може бути достатньо.

Порівняльна оцінка ризиків полягає у порівнянні кількісних значень ризику з критеріями, визначеними для конкретної області застосування управління ризиками, з метою визначення класу ризику та його важливості.

Стандарт ISO 31010 визначає основні методи оцінки ризиків, що використовуються на різних етапах процедури оцінки. Ці методи включають мозковий штурм, метод Delphi, метод контрольних списків, аналіз небезпек та критичних контрольних точок, аналіз сценаріїв, аналіз дерева відмов, аналіз причин і наслідків, аналіз дерева рішень, марківський аналіз, моделювання Монте-Карло, байєсовський аналіз та байєсовські мережі, криві FN, індекси ризику, матриця наслідків та ймовірностей, багатокритеріальний аналіз рішень (MCDA) та інші.

Вибір конкретних методів оцінки залежить від доступності ресурсів, рівня невизначеності, а також відповідності поставленим цілям, відповідальності за прийняття рішень та інших факторів.

Найбільш поширеними методами кількісної оцінки ризиків є статистичний метод, метод експертних оцінок, дерево рішень, дерево подій, метод аналогій,

метод індексів небезпеки та інші. Розглянемо деякі з них [9].

1. Метод експертних оцінок використовується для визначення величини ризикових подій. Часто метод експертних оцінок реалізується за допомогою SWOT- аналізу, методу Дельфі та інших аналогічних методів.

2. Статистичний метод. Він використовується, якщо є необхідність визначити ризик підприємства, використовуючи при цьому ретроспективну інформацію та статистичні дані щодо аналогічних підприємств. Перевага методу полягає у його простоті, недолік – необхідність великої кількості статистичних даних.

3. Сценарний метод - метод, який ґрунтується на імітації різних варіантів розвитку аналізованої системи. Зазвичай враховуються три варіанти - ймовірний, оптимістичний та песимістичний. За кожним варіантом визначаються та оцінюються можливі ризики. Перевагою методу є те, що він дозволяє отримати інформацію про можливі відхилення цільових показників з урахуванням взаємодії ризикових факторів. Недоліком методу є спрямованість дослідження на зміну одного результуючого показника, тобто метод не дозволяє провести комплексний аналіз ризиків.

4. Метод списків джерел ризиків. Цей метод полягає у використанні історичних даних та заснований на застосуванні переліку ризиків та їх джерел для підприємства за проектами. Мінусами способу є втрата керованості списку ризиків у процесі його збільшення і можливість використання способу тільки на етапі ідентифікації ризиків.

5. Метод «дерево рішень» - метод оцінки ризику, що пов'язаний з необхідністю вибору одного з альтернативних варіантів розвитку системи. Різні сценарії розвитку аналізованої системи визначаються прийнятими альтернативними рішеннями.

6. Метод «дерева подій». Даний метод дозволяє визначити наслідки вихідних подій та розрахувати найбільшу ймовірність настання головного наслідку. Важливо враховувати максимальну кількість початкових подій та

проміжних ланок «дерева подій».

7. Імітаційне моделювання. Використання модельного підходу забезпечує багатоваріантність проектних розрахунків.

8. Метод «дерев відмов». Побудова дерева подій можливе і в напрямку від наслідків до причин, коли відправним пунктом при формуванні дерева є сукупність ймовірних причин, що викликають головну подію. Цей метод «дерево відмов» доповнює «дерево подій». Формування «дерева відмов» дає можливість знайти маршрути, якими деякі події за їх сукупним впливом можуть викликати небезпечні (ризикові) ситуації.

9. Метод «події-наслідки». Цей метод є підвидом «дерева подій», у якому не розраховуються ймовірності виникнення подій. В основу методу закладено розподіл складних систем на складові, які піддаються глибокому аналізу з метою виявлення всіх ризиків. Прикладом методу «події-наслідки» на підприємствах є аналіз працездатності підприємства з урахуванням несправностей, аварій та відмов обладнання на етапі проектування.

10. Метод індексів безпеки. Цей метод дозволяє отримати інтегральну оцінку (індекс) ступеня потенційної безпеки системи (підприємства). Недоліком методу є те, що він не дозволяє ідентифікувати окремі ризики. Одна з переваг методу полягає в тому, що індекси потенційної безпеки можна розраховувати не тільки для системи в цілому, але і для окремих її елементів, що дозволяє здійснювати оперативний контроль за рівнем безпеки виробництва.

Оцінка ризиків включає в себе оцінку ймовірності виникнення ризикових ситуацій і визначення розміру збитків для підприємств у разі настання цих подій. Під час оцінки слід враховувати як прямі, так і непрямі збитки. Прямі збитки включають безпосередні збитки здоров'ю третіх осіб, майну самого підприємства. Непрямі збитки виникають через неможливість нормального функціонування підприємства протягом певного періоду (втрата доходів, витрати на юридичне врегулювання справ, сплата штрафів і неустойок контрагентам за невиконання зобов'язань та інше).

Розмір непрямих збитків, зазвичай, набагато перевищує розмір прямих, проте єдиної загальноприйнятої методики оцінки збитків від настання ризикових подій нині немає, а результати розрахунків з допомогою різних методик можуть істотно відрізнятись.

Огляд сучасних досліджень з оцінки та управління ризиками показав, що в чинному методичному апараті управління ризиками найбільш широко використовується ймовірнісний ризик-аналіз, коли розраховуються статистичні оцінки ймовірностей можливих небезпечних подій. При пошуку рішень з управління ризиками, як правило, використовуються методи на основі «дерев рішень», «дерев подій», «дерев відмов», «платіжних матриць», різні ігрові методи і т. д. Однак практика функціонування підприємства показує, що часто рішення щодо розвитку підприємств приймаються за наявності небезпечних ситуацій з високою невизначеністю вихідної інформації, складністю та недетермінованістю виробничо-технологічних процесів, а також унікальністю конкретних інвестиційних проектів.

Для оптимізації процедур прийняття рішень з управління ризиками в умовах невизначеності необхідно використовувати теорію експертних оцінок, теорію штучного інтелекту, теорію нечітких множин, методи нечітких логічних міркувань. Ці методи дозволяють за допомогою безлічі лінгвістичних змінних, нечітких значень факторів та змін оцінити величину впливу різних факторів ризику на цільові показники діяльності підприємств і виявити найзначніші з них. Проте, відомі експертні методи аналізу ризиків не забезпечують повністю можливість використання добре розробленого апарату імітаційного моделювання небезпечних ситуацій. Це обмежує гнучкість алгоритмічного та програмно-інформаційного забезпечення сучасних систем підтримки прийняття рішень, що базуються на цих методах. Така ситуація призводить до зниження обґрунтованості рішень з управління ризиками підприємств в умовах невизначеності.

1.3 Логіко-інформаційна модель формування інформаційних ризиків підприємства

Побудова системи управління інформаційними ризиками підприємства починається з ідентифікації ризиків. Метою ідентифікації ризику є визначення того, що могло б статися, щоб завдати потенційних втрат, та отримання уявлення про те, як, де і чому могли мати місце ці втрати. Для проведення ідентифікації ризиків доцільно використовувати системний підхід, який передбачає розгляд інформаційної системи підприємства як відкритої системи, що взаємодіє із зовнішнім інформаційним середовищем та здійснює перетворення вхідних ресурсів у вихідні.

Інформаційна система підприємства включає різні складові підсистеми, призначені для пошуку, збору, обробки, зберігання і передачі даних, що є однією з умов нормального безперервного її функціонування. Розглядаючи загальний інформаційний процес, як допоміжний бізнес-процес підприємства, у ньому виділяються механізми (персонал підприємства, матеріально-технічні засоби), управлінська документація (стандарти та методики, що регламентують виконання кожного виду операцій), об'єкти перетворення (інформаційні ресурси, у тому числі ті, що надходять з зовнішнього середовища). Інформаційне середовище підприємства поділяється на зовнішнє та внутрішнє. Об'єкти та суб'єкти, а також процеси та події зовнішнього середовища впливають на внутрішню інформацію підприємства та інформацію у зовнішньому середовищі.

Ризик - парне поєднання ймовірної (або можливої) несприятливої події (або подій) та її наслідків. Як міра інформаційного ризику далі розуміємо добуток можливості настання несприятливої події у зовнішньому чи внутрішньому інформаційному середовищі підприємства, що призводить до зниження якості корпоративної інформації, на величину втрат від даної події. При цьому враховуються всі події, що відбуваються на всіх етапах інформаційного процесу –

від пошуку та збору інформації до її передачі та захисту.

На рисунку 1.4 представлено логіко-інформаційну модель формування інформаційного ризику на підприємствах.

Інформаційні потоки підприємства у внутрішньому та зовнішньому середовищі є джерелами отримання інформаційних ресурсів. Інформаційні процеси включають пошук, збирання, обробку, зберігання, передачу та захист інформації та дозволяють перетворити вхідні ресурси у внутрішні дані (бази даних) підприємства. При цьому зовнішнє та внутрішнє інформаційні середовища є джерелами виникнення різних загроз - факторів ризику (невизначених ситуацій). Кожен фактор є дискретною випадковою величиною з кінцевим набором станів. Водночас, однією з основних проблем аналізу та оцінки ризику є необхідність урахування невизначеності. Невизначеність факторів ризику пов'язана з тим, що значна частина інформації про них представлена у вигляді експертних даних. Інший аспект невизначеності пов'язаний з неясністю чи нечіткістю виділення та опису змінних або окремих станів, а також вхідних та вихідних впливів. На підставі аналізу різноманітних інформаційних ризиків на підприємствах були виділені такі види невизначених факторів:

1. Статистичні чинники виникають за наявності достатнього обсягу статистичної інформації. Однак, щодо більшої частини інформаційних ризиків, отримати статистичну інформацію не вдається.

2. Квazістатистичні чинники. Для опису їх станів використовується «квazістатистика» або несувора статистика, яка ґрунтується на комбінуванні частотного визначення ймовірності випадкових величин та експертних оцінок.

3. Нестатистичні чинники. Вони характеризуються неповним знанням поведінки фактору ризику. Побудова оцінок ґрунтується на використанні суб'єктивної експертної думки.

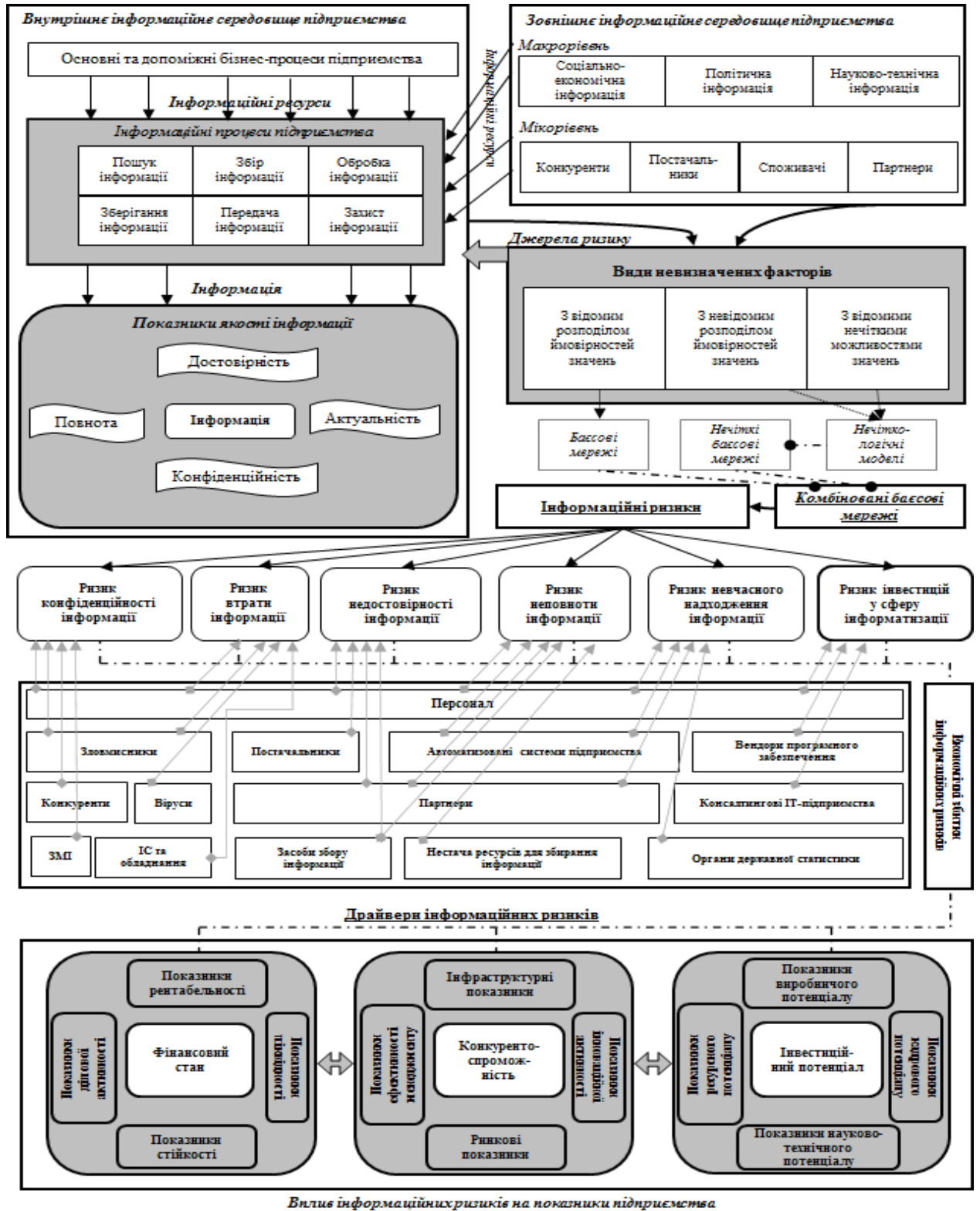


Рисунок 1.4 – Логіко-інформаційна модель формування інформаційних ризиків на підприємстві

Джерело: складено автором

В основу запропонованої класифікації факторів ризику покладена описана класифікація видів невизначеності (рис. 1.5).

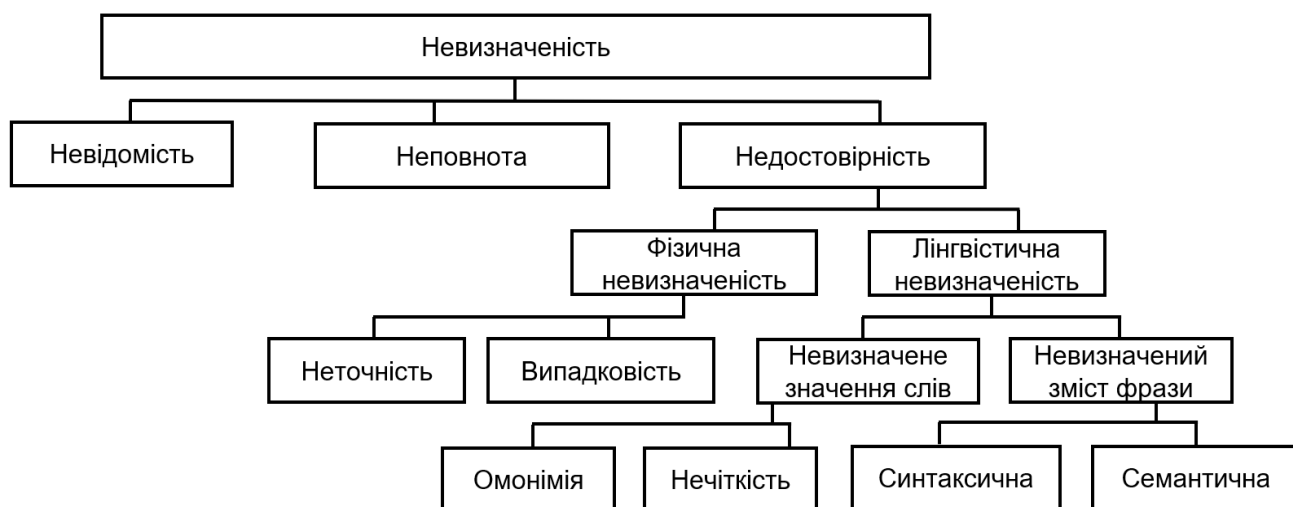


Рисунок 1.5 - Класифікація видів невизначеностей

Джерело: розроблено автором

Невизначеність - непереборна якість інформаційної системи, обумовлена тим, що на її функціонування одночасно впливає незмірна кількість чинників різноманітної природи, оцінити які разом неможливо. Але й у випадку, коли різні фактори впливу, були враховані (що недосяжно), зберіглася б непереборна невизначеність реакції системи на певні впливи.

Невизначеність інформаційної системи підприємства, обумовлена впливом різних факторів зовнішнього та внутрішнього середовища, не має статистичної природи. Враховуючи, що роль інформації, як ресурсу, полягає у відображенні сукупності знань про стан зовнішнього оточення підприємства, можна зробити висновок, що вона перебуває під впливом умов функціонування підприємства, що постійно змінюються, циклічних економічних явищ, при цьому цикли не відтворюються, оскільки циклічні зміни економічних факторів корелюються з динамікою науково-технічного прогресу. На підставі зазначеного вище можна дійти невтішного висновку, що отримання вибірки статистично однорідних подій, що спостерігаються у постійних умовах довкілля, є неможливим.

Таким чином, з практичної точки зору системи знаходяться під впливом

факторів, що характеризуються нестатистичною невизначеністю, коли необхідна для підтвердження конкретного закону розподілу кількість спостережень відсутня. При цьому об'єкти спостереження є неоднорідними, тому класичної статистичної вибірки не існує.

Лофті Заде (засновник теорії нечіткої логіки) представив широку класифікацію розподілів, використання яких дозволяє розв'язувати проблему лінгвістичної невизначеності [27]. Вона включає такі основні елементи:

- Розподіли, побудовані на можливостях. Можна навести наступний приклад її використання: вираз «Людина *молода*» у неявній формі включає у своєму описі нечітку множину $A_1 = \text{«Молодий вік»}$, визначений на $X = \text{«Тривалість людського життя»}$; на X задана функція приналежності, що визначає можливість того, що деяке зафіксоване значення $X = u$ відповідає змісту визначення «молодий» (в іншому трактуванні, можливість, що людині рівно $X = u$ років);
- Імовірнісні розподіли (невизначеність статистичного характеру);
- Нечітко-імовірнісні розподіли. Наприклад: «Здається, що людина *молода*». Тут у неявній формі описується лінгвістична змінна $A = \text{«Ступінь впевненості»}$, що задається на інтервалі $[0,1]$ і що передбачає аксіологічну ймовірність (ступінь довіри, психологічна категорія), виражену природною мовою;
- Розподіл випадкових нечітких множин із зафіксованим імовірнісним значенням;
- Розподіли на основі нечітких граф. Наприклад, розглядаються дві нечіткі класифікації. Тоді функціонал, який задається на декартовому добутку цих двох класифікацій, має сенс розподілу, побудованого на можливостях.

Для багатьох невизначених факторів, для яких відсутня необхідна кількість спостережень, можна припускати, що вони підпорядковані певному закону розподілу. Визначити точні параметри цього закону неможливо, проте можна дотримуватися гіпотези про вигляд закону і про можливий діапазон значень його характеристик. Для опису цих чинників застосовується квазістатистика.

Квазістатистика - це вибірка спостережень, яка є недостатньою для визначення виду і параметрів імовірнісного закону розподілу, але достатньою для

суб'єктивного уявлення закону спостережень у імовірнісної чи іншій формі.

Таке тлумачення квазістатистики дає найбільш широке розуміння ймовірності, коли вона має не тільки статистичний, а й суб'єктивний аксіологічний зміст. Здійснюється комбінація теорії ймовірності у її класичному вигляді та ймовірності, що описує ступінь впевненості у тому чи іншому судженні експерта-дослідника.

Квазістатистика підносить на новий рівень проблему визначення достатнього обсягу вибірки спостережень. Наприклад, експерт, аналізуючи величину ризиків підприємства, розуміє, що будь-яке підприємство унікальне, має власну ринкову частку тощо. У зв'язку з цим статистичної інформації (у класичному розумінні) немає, незважаючи на те, що вибірка може охоплювати сотні компаній. У той же час експерт, вивчаючи вибірку окремого параметру, зазначає, що для більшої частини підприємств його значення варіюються в рамках певного діапазону, ближче до деяких прогнозованих значень. Ця закономірність дозволяє експерту стверджувати, що існує закон розподілу випадкової величини, якому можна надати імовірнісну або нечітко-множинну форму.

Квазістатистика дозволяє застосовувати нечіткі описи для законів, за якими проявляється певна вибірка спостережень. Загалом, без використання квазістатистичного підходу не можна науково-обґрунтовано описувати неоднорідні та обмежені за кількістю спостережень процеси, що протікають в інформаційному просторі та в економіці в цілому в умовах невизначеності, яка супроводжує прийняття рішень.

Якщо порівняти ймовірнісні, нечітко-множинні та експертні уявлення з точки зору ефективності вирішення завдань управління інформаційними ризиками, то можна зробити такий висновок. Вочевидь, зі збільшенням невизначеності статистичні ймовірнісні моделі програють як суб'єктивним (експертним) ймовірностям, а так і ймовірностям, заданим якісно (приблизно). В останньому випадку точкові оцінки ймовірностей замінюються інтервальними (для експертних методів) та нечіткими числами (для методів теорії нечіткої логіки та множин).

Якщо потік спостережень випадкової величини описаний стандартними статистичними методами, то краще проводити дослідження з урахуванням імовірнісних моделей. У випадку, якщо статистики немає, експерт вибирає один із таких варіантів:

- 1) відмова від використання ймовірностей (перехід до використання інтервальних підходів, які є одним із найбільш широко застосовуваних напрямів експертних методів). Експерт вважає, що об'єкт спостереження, що його цікавить, може випадковим чином змінюватися в межах певного інтервалу дійсної осі. Усі наступні висновки експерт отримує на підставі цієї інтервальної оцінки;
- 2) використання аксіологічних ймовірностей та розподілів. Даний підхід не має частотного (статистичного) змісту і є результатом віртуального парі по Севіджу, або ймовірність щодо свідчення в сенсі Кайберга, або точкову оцінку, засновану на принципі мінімуму ентропії Гіббса-Джеймса. Відокремлено від цієї теорії постає питання про обґрунтованість вибору цих оцінок, вирішення якого здійснюється у спеціальній експертній моделі;
- 3) облік невизначеності з урахуванням застосування нечітких висловлювань.

Виділяється 3 варіанти:

- а) перехід від класичних ймовірностей до ймовірностей із нечіткими параметрами;
- б) заміщення кількісних ймовірностей якісними (лінгвістичними змінними);
- в) визначення стану системи з урахуванням застосування нечітких класифікаторів.

У перелічених випадках найважливішим етапом є визначення функцій приналежності нечітких множин застосовуваних лінгвістичних змінних, що задані на відповідному вхідному інтервалі.

Як приклад статистичних факторів можна навести SYN- флуд-атаки на комп'ютерний сервер, які, відповідно до дослідження, характеризуються імовірнісним розподілом Пуассона.

Прикладом квазістатистичних факторів другого типу є втрата ноутбука, в

пам'яті якого зберігається конфіденційна корпоративна інформація.

До нестатистичних факторів третього виду належить витік інформації на паперових носіях. Дана подія є рідкісною і не дозволяє передбачити можливість її виникнення будь-якими методами, за винятком експертного оцінювання.

Вплив невизначених факторів зовнішнього та внутрішнього середовища на перебіг інформаційних процесів призводить до зниження показників якості інформації підприємства (достовірність, актуальність, повнота, конфіденційність), що, своєю чергою, викликає виникнення інформаційних ризиків.

Наслідки інформаційних ризиків на підприємстві виражаються у вигляді прямих та непрямих втрат, заподіяних бізнесу в результаті інцидентів, що відбулись. У загальному випадку сукупний збиток реалізації інформаційних ризиків на підприємстві призводить до значного погіршення фінансового стану, зниження конкурентоспроможності підприємства та його інвестиційного потенціалу.

Непрямі збитки виражаються у тому, що внаслідок виникнення інформаційних ризиків на підприємствах погіршується фінансовий стан, знижується конкурентоспроможність та інвестиційний потенціал.

РОЗДІЛ 2

НЕЧІТКІ ПРОДУКЦІЙНО-БАЄСОВІ ІНСТРУМЕНТИ УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РИЗИКАМИ ПІДПРИЄМСТВА

2.1 Характеристика об'єкта дослідження

Проведений системний аналіз інформаційних процесів підприємства показав, що найважливішими джерелами інформаційних ризиків є ненавмисні та навмисні помилки персоналу, відмови програмного забезпечення, пошкодження та руйнування обладнання, програмні атаки на доступність даних, втрата даних на різних носіях, впровадження шкідливого програмного забезпечення, перехоплення конфіденційної інформації, крадіжка резервних носіїв, спотворення інформації та інші. На підприємстві виділено шість основних видів ІР:

1. Ризик порушення конфіденційності інформації - настання подій, пов'язаних з тим, що конфіденційну або іншу вразливу інформацію буде розкрито.
2. Ризик втрати інформації - настання подій, що призводять до втрати інформації чи доступу до неї.
3. Ризик недостовірності інформації - отримання інформації, яка не є правильною, що відображає реальну ситуацію.
4. Ризик неповноти інформації - інформація про об'єкт не відбиває всю сукупність відомостей про його стан.
5. Ризик несвоєчасного надходження інформації – ризик того, що отримана інформація є застарілою.
6. Ризик інвестицій у сферу інформатизації - інвестиції в ІТ не принесуть очікуваної віддачі або виділені на ІТ кошти будуть витрачені даремно.

На підставі аналізу джерел інформаційного ризику підприємства та класифікації інформаційних ризиків побудовано модель ризику підприємства (рис.

2.1), яка є основою для оцінки можливості настання ризиків з метою підвищення якості та обґрунтованості прийнятих управлінських рішень.

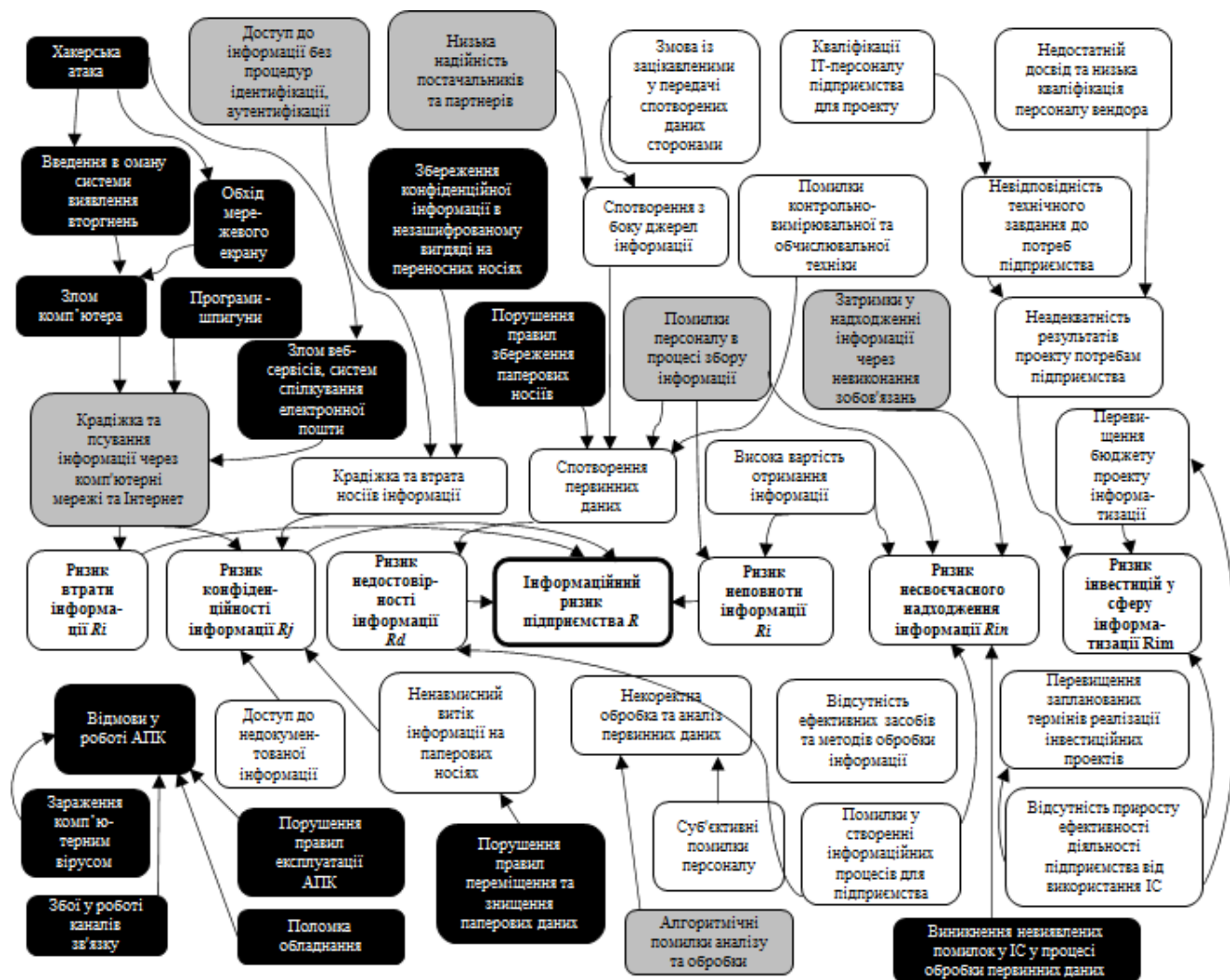


Рисунок 2.1 - Топологія комбінованої нечіткої базової мережі оцінки можливості настання інформаційного ризику

Джерело: розроблено автором на основі [9]

Стратегія управління підприємством орієнтована на підвищення якості виробленої продукції та на досягнення високих показників конкурентоспроможності, підвищення інвестиційної привабливості підприємства на міжнародному ринку. Особлива увага у цій стратегії приділяється інформаційним процесам, створенню інтегрованого інформаційного простору підприємства, автоматизації його бізнес та виробничих процесів.

Для виконання розробленої на підприємстві стратегії, орієнтованої на досягнення високих показників якості та конкурентоспроможності виробленої продукції та зміцнення інвестиційної привабливості, керівництво підприємства ініціювало масштабний проект з модернізації системи стратегічного та оперативного управління, що включає, у тому числі, організацію інтеграційних процесів підприємства.

Найважливіші вимоги до цієї системи включають:

1. Побудова оптимальних інформаційних потоків за дотримання правила одиничного введення первинних даних.
2. Гармонізація з вимогами стандартів бухгалтерського та податкового обліку, відповідність різним міжнародним стандартам та внутрішнім корпоративним нормам.
3. Існування механізмів та інструментів внутрішнього аудиту, контролінгу та розподіл відповідальності за результати функціонування бізнес-процесів.
4. Швидке реагування на будь-які зміни оргструктури та модифікацію бізнес-процесів корпорації.
5. Формування та розвиток єдиної системи нормативно-довідкової інформації та аналітичних даних.
6. Створення форм та атрибутів корпоративної звітності, що відповідають вимогам законодавства та керівництва підприємств.

Інтеграція діяльності підприємства визначила вибір та вимоги до нової інформаційної системи, яка має забезпечити високу автоматизацію реалізації наскрізних бізнес-процесів діяльності підприємств у загальному інформаційному просторі.

До цього моменту для підприємства застосовувалося кілька різних програмних рішень, не об'єднаних між собою, що викликало необхідність багаторазового введення інформації та призводило до зменшення ефективності функціонування. Відсутність загального інформаційного середовища призводила також до непрозорого обліку та знижувала оперативність процесу прийняття

рішень у галузі управління.

Територіально розподілена структура підприємства значно ускладнювала передачу інформації.

Розрізненість інформаційного простору корпорації зумовила факт високої складності оновлення інформації у довідниках та класифікаторах, що є частиною функціонування підприємств. Дані, зібрані в одному підрозділі, дублювалися у довідковій документації інших відділів вручну. Ці та інші процеси, наприклад, управління продажами, вимагали величезних часових витрат і були причинами неможливості проведення об'єктивної оцінки ефективності діяльності корпорації.

На підприємстві використовується система *Microsoft Dynamics AX*, яка забезпечує автоматизацію наступних основних завдань: планування, контроль та розподіл ресурсів, фінансове управління, управління витратами, запасами та матеріально-технічним постачанням, виробництво готової продукції та контроль якості, управління збутом, дебіторами та кредиторами, інвестиціями та основними фондами, управління нормативно-довідковою документацією, бухгалтерський та податковий облік, складання фінансово-управлінської звітності. Це дозволяє підвищити прозорість бізнес-процесів підприємств, а також оптимізувати їхні бази даних.

Інформаційні потоки для підприємства є досить складними, що зумовлює актуальність запровадження системи управління інформаційними ризиками. Виявлення чинників інформаційних ризиків починається з побудови принципової схеми інформаційних потоків підприємства.

На рис. 2.2 представлена інформаційна система управління виробництвом та якістю продукції на підприємстві.



Рисунок 2.2 - Інформаційна система управління виробництвом та якістю
Джерело: розроблено автором за даними [22]

На рис. 2.3 представлено функціональну структуру інформаційної системи оперативного обліку на підприємстві.



Рисунок 2.3 Функціональна структура інформаційної системи оперативного обліку підприємства
Джерело: розроблено автором

Аналіз поточного стану підприємства з використанням запропонованих комбінованої нечіткої баєсової мережі оцінки можливості настання інформаційного ризику та нечітко-продукційної процедури розрахунку збитків від його настання показав, що для підприємства характерні можливості виникнення інформаційних ризиків, подані в табл. 2.1.

Таблиця 2.1 - Можливості та збитки від настання інформаційних ризиків на підприємстві

Інформаційний ризик	Можливість настання інформаційного ризику		Збитки від настання інформаційного ризику, тис. грн.		Розмір інформаційного ризику, тис. грн.	
	ДЗ	ПЗ	ДЗ	ПЗ	ДЗ	ПЗ
Ризик недостовірності інформації	0,54	0,43	1750	1550	945	666,5
Ризик неповноти інформації	0,42	0,34	1400	1200	588	408
Ризик невчасного надходження інформації	0,37	0,29	650	580	240,5	168,2
Ризик конфіденційності інформації	0,25	0,14	2100	1850	525	259
Ризик втрати інформації	0,23	0,13	2600	2400	598	312
Ризик інвестицій у сферу інформатизації	0,13	0,09	1900	1700	247	153
					3143,5	1966,7

Джерело: розроблено автором

З отриманих даних можна дійти висновку, що у першу чергу необхідно знизити ризик недостовірності інформації.

2.2 Методика побудови комбінованих нечітких баєсових мереж оцінки можливості настання інформаційного ризику

На підставі побудованої мережевої структури здійснено оцінку можливості виникнення інформаційних ризиків на підприємстві.

Одним із найефективніших інструментів аналізу ризиків, що базуються на використанні ймовірнісного підходу, є використання баєсових мереж. Вони є ефективним інструментом як для графічного уявлення відносин між безліччю змінних, так і для обліку невизначеності цих змінних. На відміну від підходу до аналізу та моделювання ризиків, що базується на продукційних правилах, баєсові мережі орієнтовані на реалізацію істотних особливостей правдоподібних міркувань на основі послідовного та добре математично обґрунтованого методу прийняття рішень. При цьому для баєсової мережі характерним є те, що поява нової інформації про значення змінних-нащадків змінює уявлення про значення змінних-причин.

Використання баєсових мереж забезпечує досягнення максимального ефекту, оскільки вони засновані на ймовірнісному підході і здатні застосовувати найбільший обсяг інформації з навколишнього середовища. Баєсове висновування є статистичною процедурою, що використовує апіорний розподіл даних для оцінки ймовірності результатів [Вік]. Точність результатів баєсового аналізу залежить від точності апіорного розподілу. Баєсова мережа моделює причинно-наслідкові зв'язки, опираючись на аналіз ймовірнісних взаємозв'язків між вхідними даними та результатами.

Отже, баєсові мережі довіри (БМД) використовуються для створення моделей конкретних ситуацій, які містять елемент невизначеності. БМД також називають причинно-наслідковими мережами, в яких випадкові події поєднані причинно-наслідковими зв'язками.

В основі БМД лежить формула Баєса для розрахунку апостеріорних

ймовірностей несумісних подій Y_i на основі заданих апіорних ймовірностей [20]:

$$P(Y_i|X) = \frac{P(Y_i) \cdot P(X|Y_i)}{P(X)} \quad (2.1)$$

Умовна залежність двох вершин визначається сукупністю ребер, які описують всі маршрути між цими вершинами.

Переваги баєсових мереж для аналізу та обробки інформації:

оскільки модель містить опис взаємозалежностей між усіма змінними, легко враховуються ситуації, коли значення окремих чинників невідомі;

баєсові мережі легко інтерпретуються і дозволяють легко виконувати сценарний аналіз «що, якщо...» на етапі прогнозного моделювання;

БМД забезпечують можливість поєднати закономірності, виявлені в результаті проведеного аналізу даних, і знання в фактичному вигляді, наприклад, надані експертами;

застосування БМД дозволяє уникнути проблем додаткового припасування (*overfitting*), тобто зайвого ускладнення моделей, виникнення якого можливо при використанні таких методів як дерева рішень, висновування на основі продукційних правил при дослідженні «зашумлених» даних.

Баєсові мережі довіри є визнаним спільнотою дослідників штучного інтелекту методом прийняття рішень в умовах невизначеності, заснованим на використанні графової структури для подання причинно-наслідкових зв'язків та розрахунків ймовірностей для кількісного відображення даних зв'язків.

Баєсова мережа довіри – спрямований ациклічний граф. Під словом «ациклічний» тут розуміється відсутність спрямованих циклів – ненаправлені цикли дозволені. У вузлах задаються випадкові змінні, ребра – спрямовані відносини підпорядкування між змінними. Теоретично, змінні можуть бути як дискретними, так і неперервними, у роботі розглядаються мережі з дискретними змінними. У зв'язку з цим, можна зробити висновок, що вузли є дискретними випадковими змінними з двома або більше станами. Наприклад, булева змінна, що

відображає стан працездатності обладнання, приймає одне з двох значень: 0 або 1.

Вузли, які не мають батьків, мають назву кореневі вузли та характеризуються ступенем апіорного ймовірнісного розподілу. Для кожного вузла, що має батьків, формується таблиця умовних ймовірностей, що визначає ймовірності станів цієї вершини для кожної можливої комбінації значень її батьків.

Однією з ключових концепцій використання БМД є пропagaція свідчень: інформація про те, що події, що відповідають певним вузлам, відбулися або не відбулися, вводиться в систему. Механізми обробки, що покладені в основу цього підходу, повинні враховувати можливість надходження свідчень.

У БМД зв'язок (відповідно до термінології теорії ймовірностей та ймовірнісної логіки, залежність) існує не тільки між вершинами, безпосередньо з'єднаними ребром. Закони, якими поширюється цей зв'язок, мають практичну природу, тобто походять із вимог здорового глузду. Вимоги ці формалізовані у понятті d -розділеності.

Дві вершини спрямованого графа x і y є d -розділеними, якщо для кожного шляху з x в y (в даному випадку не береться до уваги напрямок ребер) є проміжна вершина z (не збігається з x , y), така, що або зв'язок в цій вершині послідовний, або розбіжний і відомо значення z , або зв'язок, що сходиться, при цьому ні вузол z , ні жоден з його нащадків значення не отримав. В іншому випадку вузли називаються d -пов'язаними.

Аналіз існуючих підходів до оцінки ризиків виявив ряд обмежень, які мають нечітке логічне висновування і мережі Баєса при моделюванні та аналізі ризиків, незважаючи на широке застосування, яке отримали інструменти на основі нечіткої логіки. Головним обмеженням у застосуванні методів нечіткого логічного висновування при моделюванні та аналізі ризиків є складність отримання результатів зворотного висновування. Хоча цей підхід дозволяє визначити значення вихідних змінних на основі відомих значень вхідних, він не дає можливості провести обернену операцію. Наприклад, часто постає завдання, коли вихідними даними для аналізу є ймовірні наслідки ризику, а результатом -

ймовірність відповідної небажаної події, що призводить до негативних наслідків.

Однак, обмеження баєсових мереж при аналізі ризиків пов'язані з особливостями ймовірнісного підходу для оцінки невизначеності, що вимагає значної кількості експериментальних даних у вигляді таблиць умовних ймовірностей. Ці дані часто складно або навіть неможливо зібрати. До того, навіть для експертів важко оцінити ймовірності значень вхідних змінних, які призводять до різних ймовірностей значень вихідних змінних. У таких випадках використання підходу, заснованого на нечіткій логіці та теорії можливостей, якісних характеристик або інтервальних величин є більш доцільним.

Вимоги, що пред'являються до ймовірнісних дерев рішень, утруднюють використання баєсових мереж для аналізу ризиків прийнятих рішень, який є багато в чому суб'єктивним процесом, в ході якого враховуються не тільки кількісні, а й якісні змінні, що погано піддаються формалізації. Крім того, ці змінні є суттєво взаємозалежними

Разом з тим, унікальність та складність типізації оцінюваних ситуацій, неможливість отримання достатніх статистичних даних, нечіткість значень, спричинену експертним характером інформації, наслідки ризику, які залежать як від моменту, коли ризик виявлено, так і від можливої тяжкості його наслідків обумовлюють невизначеність при аналізі ризиків прийнятих рішень і неможливість використання при цьому ймовірнісного підходу.

Вищесказане зумовлює доцільність використання методів теорії нечітких множин та нечітких обчислень у баєсових мережах. Це дозволяє врахувати і кількісні та якісні змінні. Водночас, уявлення як дискретних, так і безперервних змінних на основі нечітких множин дозволяє реалізувати апроксимаційне уявлення гібридних баєсових мереж і забезпечити, таким чином, ефективне вирішення завдань нечіткого висновування по мережі та навчання.

Визначення нечіткої баєсової мережі:

$$HBC = (U, E, P), \quad \text{де} \quad (2.2.)$$

U - множина змінних нечіткої баєсової мережі;

E - множина спрямованих зв'язків між змінними мережами (від батьків до нащадків),

P - ймовірнісний розподіл змінних мережі за їх змінними батьками з U .

Доступні такі методи введення нечіткості в байєсовську мережу:

1. Розширення байєсовського правила з використанням функцій належності відповідних значень змінних;
2. Заміна ймовірностей значень змінних у байєсовських мережах нечіткими множинами (лінгвістичними термінами змінних), а операцій над різними значеннями операціями S- та T-норм з нечіткими множинами;
3. Заміна ймовірностей значень у мережі Байєса нечіткими числами, а звичайних операцій операціями з нечіткими числами.

Цей метод введення нечіткості в баєсову мережу можна описати так: ймовірності прийняття конкретних значень змінних баєсової мережі довіри виражаються у вигляді нечітких чисел; замість стандартних арифметичних операцій додавання, віднімання, множення та ділення ймовірностей прийняття змінними окремих значень застосовуються розширені (як правило, за принципом узагальнення Лофті Заде) операції додавання, віднімання, множення та ділення нечітких чисел.

Методи виконання операцій з нечіткими числами можуть різнитися. Наприклад, при використанні інтервального арифметичного методу для операцій з нечіткими числами обчислення проводяться для всього діапазону значень цих чисел.

Методика побудови комбінованих нечітких баєсових мереж оцінки можливості настання інформаційних ризиків дозволяє враховувати невизначені фактори ризику трьох видів:

1. Виділити види інформаційного ризику та позначити їх як цільові змінні. Загальна структура дерева показана на рисунку 2.1. При цьому вершини, що відповідають статистичним факторам ризику, виділяються темно-сірим кольором, квазістатистичним - світло-сірим, нестатистичним - білим.

2. Визначити чинники ризику, які впливають на цільові змінні, вказати тип кожної змінної з погляду природи її невизначеності. Описати стосунки «причина-слідство» у вигляді орієнтованих дуг і побудувати графічне уявлення нечіткої комбінованої баєсівської мережі.

3. Для вузлів мережі, які не мають вхідних ребер, необхідно визначити ймовірність безумовного виникнення змінних першого типу, а для змінних другого і третього типів - нечітку безумовну можливість прийняття кожного значення з їх діапазону значень.

Ймовірності для статистичних величин встановлюються на підставі аналізу ретроспективних даних. Так, дискретна випадкова величина N має можливі значення $n_0 = 0, n_1, n_2, \dots, n_k$, кожне з яких величина N може прийняти з ймовірністю $p_0, p_1, p_2, \dots, p_k$.

З імовірнісної точки зору, дискретна випадкова величина N вважається повністю описаною, якщо діє закон розподілу випадкової величини, представлений у вигляді таблиці ряду розподілу.

Аналіз статистичних даних розглянутого в якості прикладу фактору «Ddos – атака» свідчить про вирогідність підпорядкування закону розподілу Пуассона розглянутого виду атак на сервери. Для доведення цієї гіпотези може бути використаний критерій Пірсона.

Хоча вихідна формула закону Пуассона визначає, що всі атаки, що виникають з інтенсивністю λ , будуть реалізовані на 100% рівні. Проте на практиці часто стикаються з ситуацією, коли лише певна частина атак, позначена як m , фактично реалізується, і це число (k) менше загальної кількості атак (m) $k < m$.

Основна задача полягає у визначенні закону розподілу ймовірностей p (p_i, k, m), де p_i - ймовірність успішної реалізації атаки, k - кількість успішно реалізованих атак, m - загальна кількість атак, що виникли, зі знайденою ймовірністю.

$$p_m = \frac{\lambda_i^m}{m!} e^{-\lambda_i}, \quad (2.3)$$

для кожного $m > k$. У цьому випадку використовується відповідна формула, яка відтворює схему Бернуллі, і відповідно до цієї формули

$$p_{k,m} = C_m^k p_i^k (1 - p_i)^{m-k} \quad (2.4)$$

тоді загальна ймовірність реалізації k атак є сумою за всіма $m > k$ (з урахуванням ймовірності того, що на даному інтервалі часу при інтенсивності λ_i виникло саме m атак):

$$p_k = \sum_{m>k} C_m^k p_i^k (1 - p_i)^{m-k} \frac{\lambda_i^m}{m!} e^{-\lambda_i} \quad (2.5)$$

Причому такий облік ймовірності реалізації атаки еквівалентний множенню інтенсивності виникнення атак λ_i на цю ймовірність p_i

$$\sum_{m>k} C_m^k p_i^k (1 - p_i)^{m-k} \frac{\lambda_i^m}{m!} e^{-\lambda_i} = \frac{p_i \lambda_i^m}{m!} e^{-\lambda_i}; p_k(p_i, \lambda) = \frac{p_i \lambda_i}{m!} e^{-p_i \lambda_i} \quad (2.6)$$

Квазістатистичні фактори невизначеності характеризуються обмеженою статистичною базою.

Тому, при визначенні їхньої потенційної можливості виникнення подій, використовується процес згладжування чіткої множини на основі статистичних даних щодо ймовірності.

Для визначення можливості виникнення таких факторів використовуються трикутні нечіткі числа з параметрами $\{\alpha, a, \beta\}$, де модальне значення збігається з обчисленою ймовірністю $a=p$.

При цьому коефіцієнти розмиття праворуч та ліворуч задаються фахівцем. Для нестатистичних чинників можливості прийняття значень встановлюються з урахуванням експертних оцінок.

Для опису можливості виникнення таких факторів використовуються трапецеїдальні функції належності типу $\{\alpha, a, b, \beta\}$, де нижнє і верхнє модальне значення являють собою інтервал, отриманий в результаті опитування експертів.

На рисунках 2.4 та 2.5 представлені приклади графічного та аналітичного завдання трикутної та трапецеїдальної функцій належності нечітких ймовірностей цих значень.

4. Для кожного вузла графа, який є змінною першого типу та має вхідні ребра того ж типу, потрібно вказати умовні чіткі ймовірності для різних значень цього вузла, залежно від комбінацій значень його батьківських змінних у графі.

5. Для вершин другого та третього типу, а також для вузлів першого типу, які мають батьків другого чи третього типу, необхідно визначити нечіткі умовні можливості прийняття різних значень змінної вузла в залежності від комбінацій значень його батьківських змінних у графі.

$$\mu(x) = \begin{cases} 0, & x < a, \\ \frac{x-a}{b-a}, & a \leq x < b, \\ \frac{x-c}{c-b}, & b \leq x < c, \\ 0, & c \leq x. \end{cases}$$

*Рисунок 2.4 - Приклад завдання трикутної функції належності
Джерело: складено автором на основі [9]*

$$\mu(x) = \begin{cases} 0, & x < a, \\ \frac{x-a}{b-a}, & a \leq x < b, \\ 1, & b \leq x < c, \\ \frac{x-d}{c-d}, & c \leq x < d, \\ 0, & d \leq x. \end{cases}$$

*Рисунок 2.5 - Приклад завдання трапецеїдальної функції належності
Джерело: складено автором на основі [9]*

Для полегшення розрахунків у комбінованій нечіткій баєсовій мережі, коли вузол має батьків як першого, так і другого або третього типу, умовні або безумовні ймовірності задані для вузла-батька першого типу замінюються нечіткими можливостями події, що представлені як точки на площині, що визначається за осями значень змінної події та функції належності. Наприклад, точне значення ймовірності настання події 0,4 в результаті фазифікації замінюється неточним трикутним числом з параметрами (0.4; 0.4; 0.4).

6. Виконати аналіз структури побудованої комбінованої баєсової мережі, якщо виявляються циклічні зв'язки, проводиться модифікація структури відповідно до розробленого алгоритму:

Метод обробки циклічних зв'язків змінних у комбінованій нечіткій баєсовій мережі включає наступні етапи:

1) Побудова різноманітних ланцюжків кон'юнкцій подій, отриманих виходячи з послідовного розриву зв'язків циклічної структури (рис. 2.6).

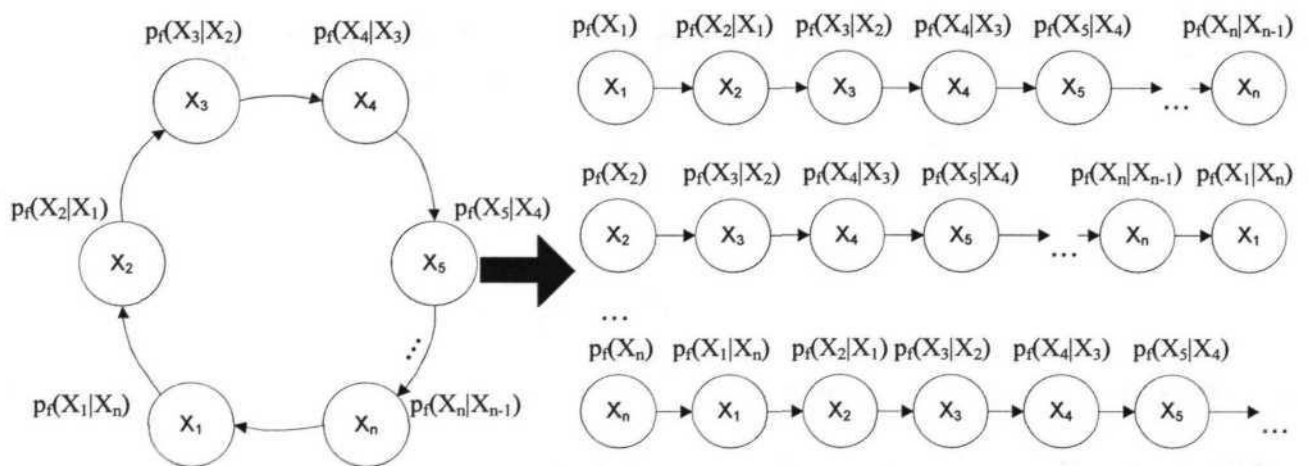


Рисунок 2.6 - Перетворення циклічної структури комбінованої нечіткої баєсової мережі на безліч ланцюжків кон'юнкцій факторів ризику
Джерело: складено автором на основі [9]

2) За допомогою експертної оцінки для кожного ланцюжка встановлюється безумовна нечітка можливість настання події-вузла, що не має батьків.

3) Обчислення загальної можливості настання сукупності подій для кожного виявленого ланцюжка здійснюється за допомогою нечітких баєсових правил:

$$\begin{aligned} P_f^1 (X_1, X_2, X_3, X_4, X_5 \dots X_n) \\ P_f^2 (X_2, X_3, X_4, X_5 \dots X_n, X_1) \\ P_f^3 (X_3, X_4, X_5 \dots X_n, X_1, X_2) \\ \dots P_f^n (\dots X_n, X_1, X_2, X_3, X_4, X_5) \end{aligned}$$

4) Визначення ланцюжка подій, якому відповідає найбільше значення можливості спільного наступу всіх подій – вузлів графа.

5) Модифікація структури комбінованого нечіткого дерева Баєса полягає в зміні циклічної структури на обраний кон'юнктивний ланцюжок подій.

7. Розрахувати спільні нечітких апіорні можливості виникнення будь-якої комбінації подій за допомогою процедури логічного висновування для комбінованих нечітких баєсових мереж оцінки можливості настання інформаційного ризику.

2.3 Нечітко-продукційна процедура розрахунку збитків від настання інформаційних ризиків підприємства

Оцінка рівня інформаційного ризику враховує аналіз двох основних показників: ймовірність виникнення ризику та масштаб збитків.

Під час оцінки масштабу збитків доцільно використовувати нечітко-логічний підхід, який також враховує індивідуальні фактори збитків.

Так, наприклад, до втрати конфіденційності інформації можуть призвести різні обставини (зламування пошти, крадіжка ноутбука тощо), проте при

розрахунку наслідків ці фактори враховувати недоцільно. У зв'язку з цим для оцінки величини збитків від настання інформаційних ризиків підприємства використовується наступна нечітко-продукційна процедура:

1. Необхідним є побудувати так звані «дерева збитків» для обраного підприємства. Структура такого «дерева збитків» показана рис. 2.7.

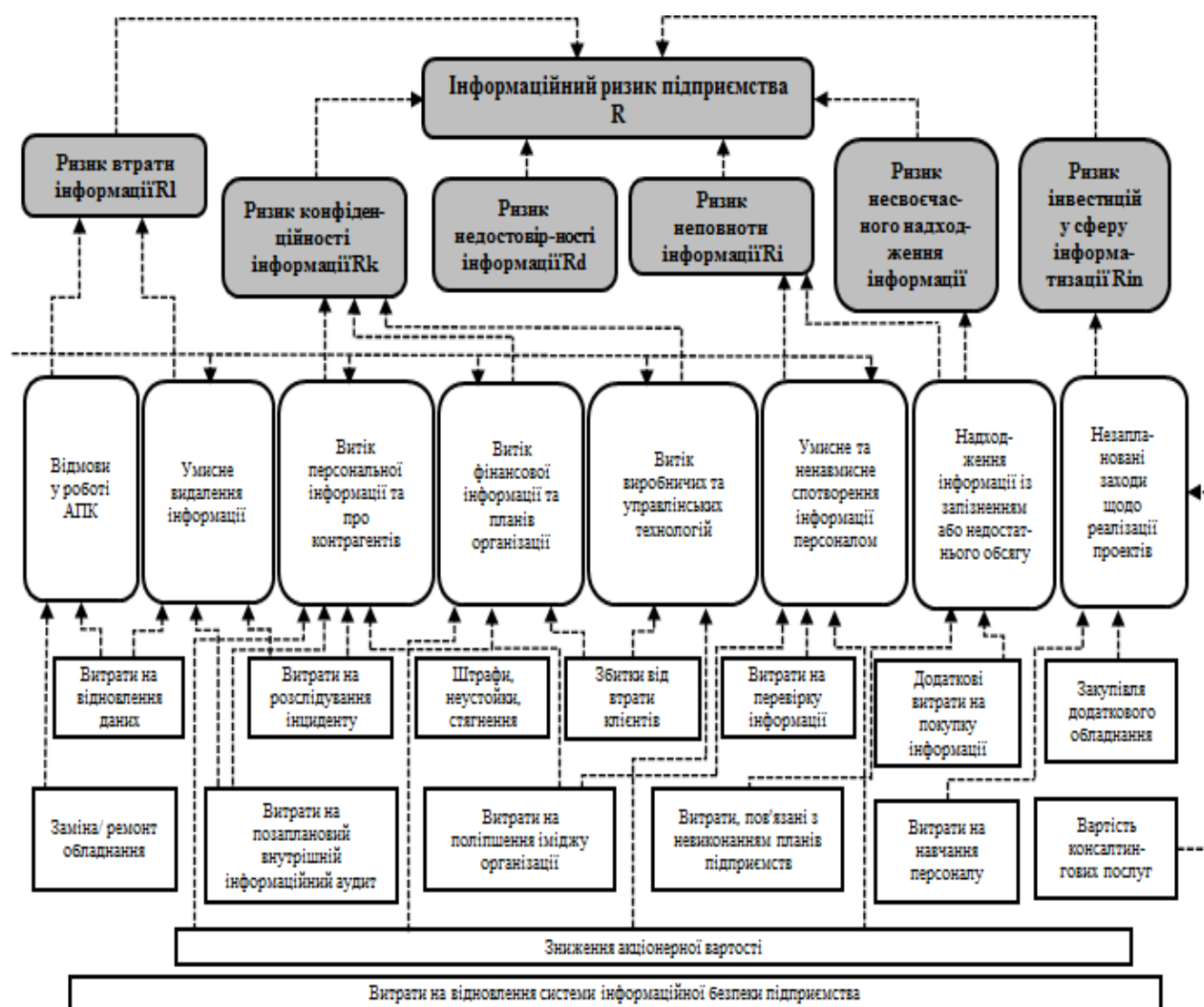


Рисунок 2.7 – Дерево збитків від настання інформаційних ризиків на підприємстві

Джерело: розроблено автором

Під час формування дерева збитків рівні наповнюються елементами, які відібрані з доступної бази знань за допомогою експертної оцінки. Комбінація відомих елементів є творчим етапом. Проте безліч елементів створює труднощі

подальшого аналізу, тому доводиться спрощувати структуру. Для скорочення кількості елементів доцільно проводити їх групування на кожному рівні за подібними ознаками чи ранжувати за рівнем значущості.

2. Опис лінгвістичних змінних кожного вузла дерева збитків.

Опис функцій належності нечітких множин показника збитку кожного рівня всіх видів інформаційних ризиків. На рис. 2.8 представлено класифікацію існуючих методів.



Рисунок 2.8 - Класифікація методів побудови функцій належності
Джерело: складено автором на основі [28]

Прямими методами побудови функцій належності припускається, визначення експертом правил завдання значень функції належності $A(x)$ самостійно, що описує елемент x .

Значення безпосередньо вибираються експертом на безлічі елементів X відповідно до наступних правил:

1. Для $\forall x_1, x_2 \in X$ співвідношення їх функцій належності визначається

нерівністю $\mu_A(x_1) < \mu_A(x_2)$ коли x_2 віддається перевага перед x_1 , тобто більшою мірою описується властивістю A .

2. Для $\forall x_1, x_2 \in X$ співвідношення їх функцій належності визначається рівністю $\mu_A(x_1) = \mu_A(x_2)$ коли x_1 і x_2 однакові щодо властивості A .

Зазвичай, для кількісно вимірних змінних чи у випадках, коли можна виділити протилежні значення, застосовуються прямі методи визначення функцій належності.

Підкласом прямих методів є прямі групові методи, які передбачають, що досліджуваний об'єкт пред'являють групі експертів, кожен з яких має вирішити, чи належить даний об'єкт до заданої множини. Тоді значення функції належності об'єкта до заданої нечіткої множини дорівнює кількості позитивних відповідей, розділеної на сукупну кількість експертів.

Прямі методи включають у себе завдання функції належності графічним чи табличним способом, а також у вигляді формул.

Дослідження показали, що прямі методи ефективно використовуються у випадках, коли випадкові помилки експертів є дуже рідкими та їх опитування стосовно значення функції належності може бути проведено безпосередньо. Однак слід враховувати можливість спотворень, таких як суб'єктивне відхилення оцінок об'єктів до крайніх точок використовуваної шкали. Тому прямі методи рекомендується використовувати лише тоді, коли експертні помилки малоймовірні.

Непрямі методи визначення функції належності об'єкта використовуються, коли відсутні вимірні властивості, що визначають нечіткі множини [59].

Непрямі методи визначення функції належності є більш складними на практиці, але вони мають перевагу в стійкості до спотворень.

Для непрямих методів можна задати умову екстремуму: безліч об'єктів, що вивчаються, повинно включати, щонайменше, два об'єкти, функції належності яких приймають відповідно значення 0 і 1.

У непрямих методах визначення функцій належності потрібно, щоб вони

відповідали заздалегідь встановленим умовам.

Інформація, отримана від експертів, є вихідними даними для подальшої обробки. За допомогою допоміжних умов можуть бути визначені вид отриманої інформації та механізми її перетворення. Такі методи, як статистичний, парних порівнянь, експертних оцінок належать до непрямих методів.

У роботі для визначення функцій належності до нечітким множин використовуються методи статистичних даних, з урахуванням експертних оцінок, з урахуванням параметричного підходу.

Метод статистичних даних ґрунтується на проведенні аналізу статистичних даних з метою встановлення ступеня належності об'єкта до нечіткої множини. Цей ступінь належності визначається як оцінка частоти використання лінгвістичного терміна, який описує нечітку множину, для характеристики даного об'єкта. Застосування спеціалізованих матриць підказок дозволяє отримати плавні функції належності.

Функція належності $\mu_S(x)$ призначає число з інтервалу $[0, 1]$ кожному елементу x з множини X , яке відображає ступінь належності елемента X до множини A . Під час сприйняття інформації експерт користується лінгвістичними термінами для опису значень, замість конкретних чисел, і ці терміни є індивідуальними для кожного експерта.

При виконанні аналізу стану об'єкта протягом певного часу, n разів фіксується інформація про настання факту A . Оцінною є подія, що полягає в n перевірках настання факту A . Якщо факт A зафіксований у k перевірках, то експертом визначається частота $p = k/n$ настання факту A та описується, використовуючи слова «часто», «рідко» та інших.

При оцінці частоти p , експерт враховує свій досвід про частоту настання факту A в минулих подіях, подібних до розглянутої. До того експерт використовує інформацію про сторонні дослідження настання факту A , користується суспільними знаннями. Така інформація фіксується з урахуванням різної ваги в залежності від рівня довіри до джерела інформації.

Шкала $[0, 1]$ визначає значення лінгвістичної змінної. Розрахунок належності конкретного значення нечіткій множині є відношенням загальної кількості експериментів, в яких це значення зафіксоване в названому інтервалі шкали, до максимального значення кількості розглянутих експериментів по всім можливим інтервалам. Використання статистичного методу передбачає умову, про настання рівної кількості експериментів в кожному інтервалі шкали, що використовується. Проте це не завжди виконується. В емпіричній таблиці, побудованій на реальних даних, експерименти можуть бути нерівномірно розподілені між інтервалами.

Підсумовуючи, відзначимо, що тільки наявність повної статистичної інформації дозволяє, при використанні розглянутого методу, отримувати достовірні та адекватні оцінки функцій належності.

Метод побудови функції належності, що базується на експертних оцінках. Метод побудови функції належності, що базується на експертних оцінках, використовує нечіткі числа, які приблизно рівні чітким числам, а також наближені інтервальні оцінки, що відображають думки експертів з аналізованого питання. Основне завдання полягає у визначенні параметрів конкретної експоненційної функції, для чого використовуються результати опитування експертів.

Під час застосування *параметричного методу* для створення функції належності, використовуються модифіковані нечіткі терміни, що базуються на наявних даних.

Описаний метод отримання функцій належності ґрунтується на припущенні, що експерт з мінімальними витратами може визначити три точки на універсальній шкалі - A , B , C - для відображення лінгвістичного значення певної ознаки. Дві з цих точок, B та C , можуть або ще не відповідати, або вже не відповідати лінгвістичному значенню, що описується. Точка A однозначно відповідає цьому значенню (рис. 2.9).

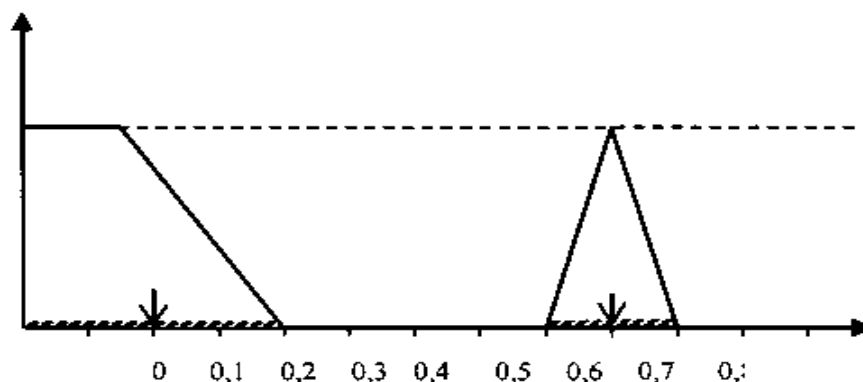


Рисунок 2.9 – Ілюстрація параметричного методу

Джерело: складено автором на основі [28]

Алгоритм побудови функції належності:

- Точка на прямій $\mu = 1$ встановлюється проти значення носія x_1 , яке чітко відповідає даному терму (точки A та D).
- Точки на прямій $\mu = 0$ визначаються проти найближчих значень, розташованих ліворуч і праворуч від x_1 на носії (осі X), які однозначно не відповідають даному терміну (точки B, C та E).
- Побудовані точки на прямих $\mu = 1$ і $\mu = 0$ з'єднуються лініями.
- Частина носія, що входить до побудованого опису, позначається штрихуванням.

Метод побудови функцій належності з використанням інтервальних оцінок використовується при відсутності меж між припустимим та неприпустимим, ідеальним та неідеальним станами для формалізованого опису завдань вибору.

Вибір методу побудови функцій належності залежить від класу завдання, складності збору статистичної інформації та експертних оцінок, ступеня достовірності зібраних даних, тескладністю алгоритмів аналізу та обробки інформації при визначенні цих функцій.

3. Формується продукційна база знань, що задана у вигляді набору продукційних правил та описує вплив станів вузлів-батьків графа на величину

вузлів-нащадків. Для моделі збитків управління використовуються наступні правила:

$$\begin{aligned} & \Pi_i: \text{якщо } x_1 \in A_{i1} \text{ I } \dots \text{ I } x_j \in A_{ij} \text{ I } \dots \text{ I } x_m \in A_{im}, \\ & \text{то } y_1 \in B_{i1} \text{ I } \dots \text{ I } y_k \in B_{ik} \text{ I } \dots \text{ I } y_p \in B_{ip}, i = 1, \dots, n \end{aligned}$$

4. Будуються ієрархічні системи нечітко-логічного висновування з нечіткими вхідними змінними на основі нечіткої імплікації Ларсена та композиції *max-prod* для одержання сумуючого значення збитку кожного виду інформаційного ризику.

Процес нечітко-логічного виснову здійснюється за допомогою нечіткої імплікації Ларсена, використовуючи формулу:

$$\mu_R(x, y) = \mu_A(x) \cdot \mu_B(y) \quad (2.7)$$

Операцію множення використовують як операцію згортання. В основі нечіткого висновування лежить використання *max-prod* композиції:

$$\mu_{B'}(y) = \max_{x \in X} \{ \mu_{A'}(x) \cdot \mu_R(x, y) \} \quad (2.8)$$

Простота реалізації та велика чутливість до змін вхідних змінних у передумовах нечітких продукційних правил зумовлює вибір даного композиційного правила.

Так зване приведення до чіткості (*defuzzification*) засновано на перетворенні нечітких значень визначених вихідних змінних у чіткі значення. При цьому всі методи отримання чіткого значення вихідної змінної поділяються на дві групи:

- методи дефазифікації, які використовують акумульовані на попередньому етапі (з активізованих висновків усіх правил бази) вихідні змінні;
- методи дефазифікації, що працюють з вихідною змінною без попереднього акумулювання висновків правил.

До першої групи належать такі методи дефазифікації:

1. Метод центру тяжіння. Цей метод дефазифікації може бути використаний лише для моделей, що базуються на нечітких лінгвістичних продукційних правилах, де консеквенти є нечіткими висловлюваннями. Чітке значення y' вихідної змінної визначається як центр тяжіння отриманої функції належності $\mu_{B'}(y)$ і обчислюється за формулою:

$$y' = \frac{\int_{Y_{min}}^{Y_{max}} y \mu_{B'}(y) dy}{\int_{Y_{min}}^{Y_{max}} \mu_{B'}(y) dy} \quad (2.9)$$

де

Y_{min} і Y_{max} - межі інтервалу носія нечіткої множини вихідний змінної y .

2. Метод центру площі. За цим підходом, чітке значення вихідної змінної y' визначається з наступного рівняння:

$$\underbrace{\int_{Y_{min}}^{y'} \mu_{B'}(y) dy}_{S1} = \underbrace{\int_{y'}^{Y_{max}} \mu_{B'}(y) dy}_{S2} \quad (2.10)$$

3. Максимум функції належності.

Чітке значення вихідної змінної розраховується за такою формулою:

Точне значення вихідної змінної обчислюється за наступною формулою:

$$y' = \underset{y}{rgsup}(\mu_{B_1}(y)) \quad (2.11)$$

де $\mu_{B'}(y)$ - унімодальна функція, форма якої може мати будь-яку форму.

4. Перший максимум або лівий максимум. Чітке значення y' визначається як найменше значення, при якому досягається максимум підсумкової нечіткої множини:

$$y' = \min\{y_{max} | \mu_{B'}(y_{max}) = \max | \mu_{B'}(y)\} \quad (2.12)$$

5. Найправіший максимум. Чітке значення змінної y' визначається як найбільше значення, при якому досягається максимум підсумкової нечіткої множини:

$$y' = \max\{y_{max} | \mu_{B'}(y_{max}) = \max_y |\mu_{B'}(y)|\} \quad (2.13)$$

6. Середній максимум. Чітке значення y' знаходиться відповідно до виразу:

$$y' = \frac{\int_{G_{max}} y \, dy}{\int_{G_{max}} dy} \quad (2.14)$$

де

G_{max} - інтервал носія нечіткої множини B' (підмножина його елементів), в якому $\mu_{B'}(y)$ приймає максимальне значення.

7. Висотна дефазифікація. Елементи носія нечіткої множини B' , для якого значення функції належності менше, ніж деякий заданий рівень $\lambda \mu_{B'}(y) < \lambda$ до уваги не приймаються, і дефазифіковане значення вихідної змінної y' розраховується відповідно до виразу:

$$y' = \frac{\int_{G_\lambda} y \mu_{B'}(y) \, dy}{\int_{G_\lambda} \mu_{B'}(y) \, dy} \quad (2.15)$$

де

G_λ - інтервал носія нечіткої множини B' , в якому $\mu_{B'}(y) < \lambda$.

Перевагою ієрархічного (багатошарового) уявлення дерева збитків є зменшення складності системи нечітко-логічного висновування з великою кількістю входів.

РОЗДІЛ 3

РЕКОМЕНДАЦІЇ З КОМП'ЮТЕРИЗОВАНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РИЗИКАМИ НА ПІДПРИЄМСТВІ

3.1 Методика організації комп'ютеризованих бізнес-процесів управління інформаційними ризиками підприємства

Управління інформаційними ризиками підприємства є безперервний бізнес-процес, що передбачає необхідність повної регламентації з метою підвищення його ефективності. Опис управління інформаційними ризиками як відокремленого бізнес-процесу необхідне для подальшого аналізу та реорганізації.

Найважливішим завданням аналізу та реорганізації процесу управління інформаційними ризиками є впровадження на підприємстві системи ризик-менеджменту в інформаційному середовищі, підвищення економічної ефективності функціонування підприємства, формування докладних посадових обов'язків для співробітників відділу інформаційної безпеки та різних категорій користувачів інформаційних систем тощо.

Логіко-інформаційна модель бізнес-процесу управління ІР має описувати такі аспекти:

1. Основні роботи, необхідні для досягнення кінцевої мети.
2. Послідовність їх виконання.
3. Механізми та інструменти управління ІТ-ризиками.
4. Співробітники, залучені у процес управління.
5. Вхідні дані та документи, необхідні для управління.
6. Вихідні дані та документи, які є результатом реалізації робіт з управління інформаційними ризиками.

7. Ресурси, необхідні для виконання кожної роботи бізнес-процесу.
8. Документи, що регламентують виконання робіт бізнес-процесу.
9. Параметри реалізації робіт та бізнес-процесу в цілому.

Регламентація бізнес-процесів реалізується на основі використання нотації та інструментального середовища, які дають змогу брати до уваги всі зазначені вище аспекти. У цьому випадку логіко-інформаційна модель бізнес-процесу буде ефективною для підприємства, оскільки її можна буде надалі проаналізувати та виконати реорганізацію з урахуванням виявлених недоліків. Моделювання бізнес-процесів управління інформаційними ризиками підприємства складає основу технології структурно-функціонального моделювання.

Технологія моделювання *SADT (Structured Analysis & Design Technique)*, а також її нотація для представлення бізнес-процесів підприємства, яка називається *IDEF0*-діаграмами (*Integration definition for function modeling*), є на сьогодні одним з найбільш ефективних та поширених методів опису функціонування складних систем та процесів. Ця технологія дозволяє здійснювати моделювання бізнес-процесів управління інформаційними ризиками з використанням графічного представлення. На першому етапі моделювання будується контекстна діаграма, яка є описом бізнес-процесу, а також показує взаємодії системи, що реалізує даний процес, із зовнішнім середовищем. На наступному етапі проводиться декомпозиція (розбиття функції на підфункції) – бізнес-процес поділяється на складові і кожен із них аналізується самостійно (діаграми декомпозиції) [11].

Кожна діаграма, побудована в нотації *IDEF0*, складається з двох основних елементів: дуг і блоків. Блоки використовуються для відображення функцій бізнес-процесу. Дуги з'єднують блоки та описують існуючі між ними взаємозв'язки.

У *IDEF0* існують п'ять видів дуг (стрілок):

Вхід - ресурси, що перетворюються функцією задля досягнення результату (виходу). Допустима ситуація, при якій функція не містить жодного входу. З графічного погляду стрілка входу входить у ліву грань роботи.

Управління - інформація, що регламентує виконання робіт конкретного

бізнес-процесу. Найчастіше стрілки управління вказують на інформацію, що описує, що має реалізовувати практично конкретна робота і підставі яких правил. Кожна процедура, як правило, має не менше однієї стрілки управління, які в графічному зображенні входять у верхню грань.

Вихід - ресурси, отримані як наслідок перетворення входів. Кожна функція повинна включати хоча б одну стрілку цього типу, що відображається як вихід із правої грані роботи.

Механізм - ресурси, що реалізують роботу. Стрілка механізму входить у нижню грань. Аналітик на власний розсуд може не використовувати стрілки механізму для робіт моделі.

Виклик –стрілка, яка спрямована на іншу модель. Графічне зображення стрілки виклику відображається як вихід з нижньої частини робочого процесу. Це свідчить про те, що конкретна робота виконується за межами системи.

Методологія *IDEF0* описує п'ять видів взаємодій між блоками: управління, вхід, зворотний зв'язок з управління, зворотний зв'язок з входу, вихід-механізм.

Для моделювання бізнес-процесу управління інформаційними ризиками у нотації *IDEF0* використовується програмний продукт *ERwin Process Modeler*. Він являє собою потужний *CASE* -засіб для моделювання бізнес-процесів.

ERwin Process Modeler дозволяє не тільки будувати діаграми, але й здійснювати оцінку цілісності та узгодженості моделі. *ERwin Process Modeler* здійснює перевірку відображення діаграм, зв'язків між окремими діаграмами. Даний інструментальний засіб коригує помилки, які часто зустрічаються при моделюванні, наприклад, «втрата» зв'язків при пересуванні між діаграмами, порушення асоціативних зв'язків і т.п. Крім того, *ERwin Process Modeler* дозволяє призначати користувацькі властивості до відокремлених елементів діаграм для уявлення специфічних особливостей, властивих конкретному елементу.

ERwin Process Modeler містить також генератор звітів. Вони зазвичай будуються після закінчення процесу моделювання та містять інформацію, відображення якої на моделі ускладнило б її сприйняття користувачами. Так,

наприклад, звіт може містити докладне уявлення всіх основних елементів діаграми, що сприяє розумінню ролі кожного елемента моделі без додаткових пояснень аналітика, який розробив цю діаграму. Крім того, існують звіти, які призначені саме для системного аналітика, як, наприклад, звіт щодо аналізу та оцінки цілісності побудованої моделі.

На рис. 3.1 представлено логіко-інформаційну модель бізнес-процесів управління інформаційними ризиками підприємства. На основі даної логіко-інформаційної моделі можна виділити основні функціонально-технічні вимоги щодо подальшої розробки допоміжних інструментальних засобів, а саме інформаційної системи управління інформаційними ризиками підприємства.

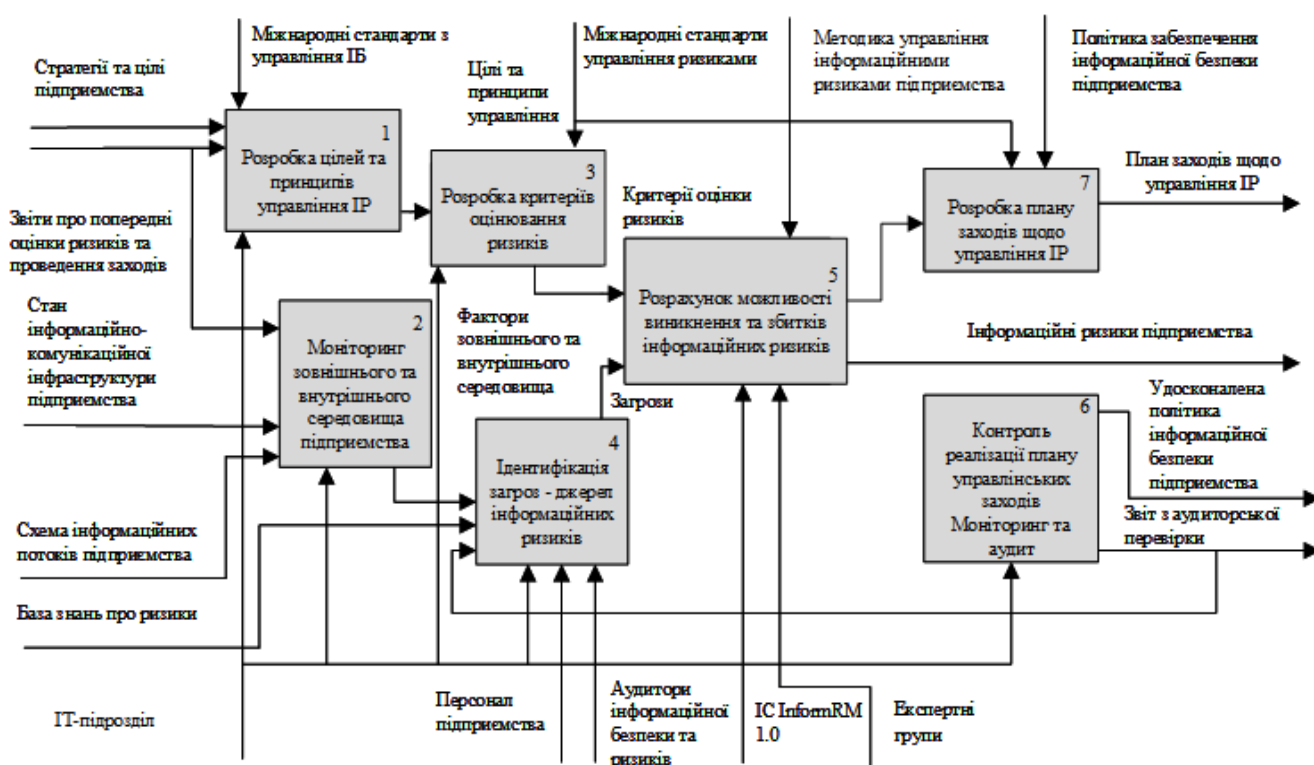


Рисунок 3.1 – Узагальнена логіко-інформаційна модель бізнес-процесів управління інформаційними ризиками підприємства в умовах невизначеності

Джерело: складено автором

Автоматизація процесу управління інформаційними ризиками підприємства дозволить збільшити ефективність його діяльності за рахунок організації

оперативного надходження даних про виникнення ризикових ситуацій, аналізу ефективності управлінських заходів, автоматизації діяльності з побудови планів та програм з управління інформаційними ризиками (складання та розсилання опитувальних листів, формування планів заходів, заповнення бази даних щодо ризиків, підготовка звітів). Інформаційна система управління ІР має працювати у режимі реального часу, у зв'язку з цим система має відображати такі процеси, як статус виконання заходів щодо управління ризиками, налаштування системи повідомлень для відповідальних осіб та ін.

На першому етапі методики управління інформаційними ризиками здійснюється розробка цілей та принципів управління. Багато в чому вони залежать від специфічних особливостей конкретного підприємства. Цілі управління інформаційними ризиками визначають у подальшому глибину аналізу ризиків, критичні значення, що зумовлюють прийняття чи вплив на ризики.

Далі здійснюється визначення критеріїв оцінювання ризиків.

Кожна організація повинна визначити критерії для прийняття ризиків, що встановлюють максимально прийнятний рівень залишкового ризику, а також можливі винятки для певних ризиків у конкретних обставинах.

Ризики, що перевищують встановлений керівництвом організації допустимий рівень, - це ризики, які є неприйнятними для бізнесу, а пов'язана з ними діяльність - занадто ризикованою. Всі інші ризики нижче цього рівня є допустимими та можуть бути прийняті без подальшої обробки.

Моніторинг зовнішнього та внутрішнього середовища підприємства дозволяє виділити ті ключові процеси та фактори інформаційної взаємодії, які надалі дозволять визначити потенційні загрози. Складність інформаційного середовища підприємства передбачає необхідність використання різних видів моніторингу:

- 1) Епізодичний моніторинг. Проводиться нечасто через встановлені проміжки часу, як правило, не частіше одного-двох разів на місяць. Цей вид моніторингу проводиться, наприклад, для контролю технічного стану обладнання,

споруд.

2) Від регулярного до частого (від кількох разів на тиждень до 3-4 разів на місяць). Висока періодичність проведення моніторингу дозволяє своєчасно виявляти джерела ризику та вчасно здійснювати реалізацію коригуючих заходів.

3) Інтенсивний (безперервне дослідження чинників ризику з частотою, що перевищує раз в день). У такому разі маєтсья на увазі, наприклад, обстеження процесів знищення важливої інформації на паперових носіях.

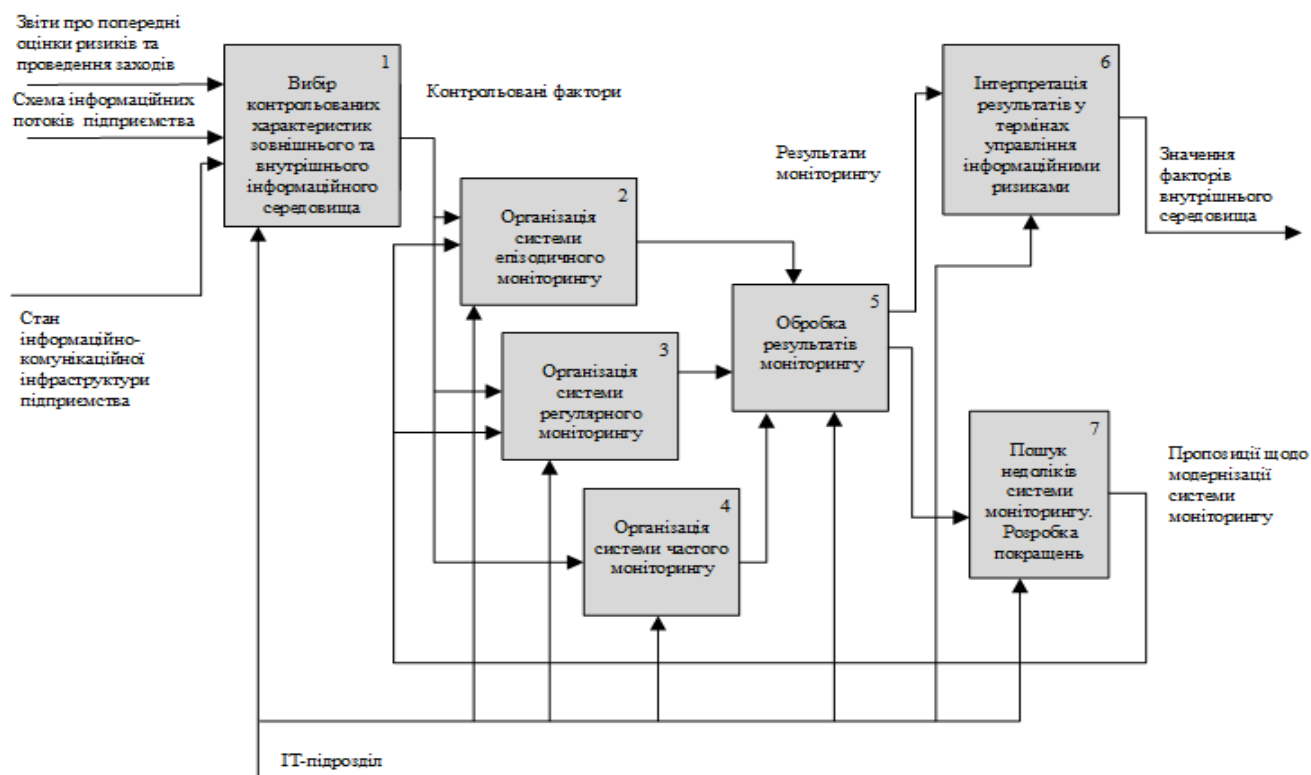


Рисунок 3.2 - Логіко-інформаційна модель процесу моніторингу зовнішнього та внутрішнього середовища підприємства

Джерело: розроблено автором

На рис. 3.2 представлено логіко-інформаційну модель процесу моніторингу зовнішнього та внутрішнього середовища підприємства.

На рис. 3.3 представлена логіко-інформаційна модель процесу оцінки інформаційних ризиків підприємства з використанням комбінованих нечітких баєсових мереж та процедури нечітко-логічного висновування.

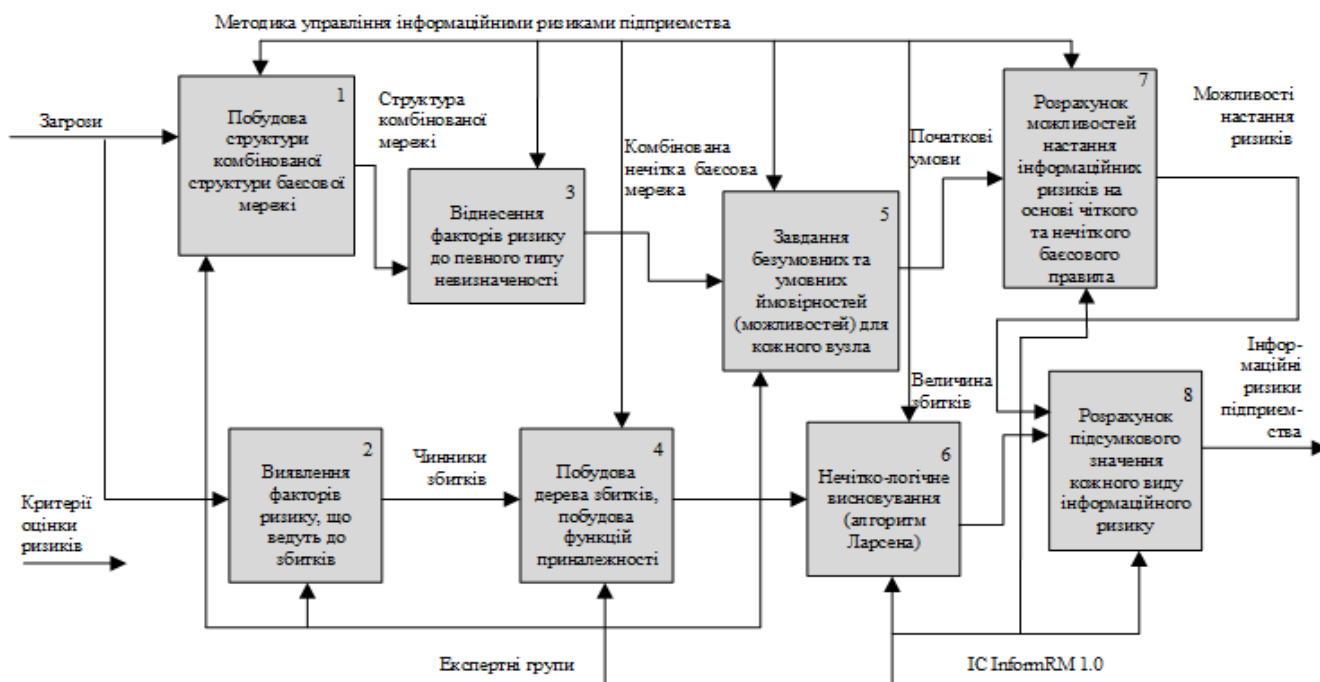


Рисунок 3.3 - Оцінка інформаційних ризиків підприємства з використанням комбінованих нечітких баєсових мереж та процедури нечітко-логічного висновування

Джерело: розроблено автором

Особливе місце в організації управління інформаційними ризиками грає становлення процесів внутрішнього контролю.

Внутрішній контроль є системою різних видів контролю, що створюється керівництвом підприємства задля досягнення й підтримки ефективності функціонування підприємства; реалізації стратегічних та інших видів планів; захисту власності підприємства; достовірності, актуальності, конфіденційності та повноти інформації; виконання договірних зобов'язань, а також для контролю пов'язаних із усіма цими процесами інформаційних ризиків.

Внутрішній контроль включає процедури, пов'язані з оцінкою поточної системи управління інформаційними ризиками та підготовкою різних проектів документів, проведенням консультацій з питань внутрішнього контролю. В його рамках передбачається навчання персоналу.

Система внутрішнього контролю підприємства та управління ІТ-ризиками здійснюється на наступних основних рівнях:

керівник ІТ-департаменту, який відповідає за розробку політики у сфері внутрішнього контролю та управління ІТ-ризиками, методологічну допомогу та координацію реалізації заходів щодо формування та функціонування системи контролю;

начальники відділів інформатизації, які відповідають за стан внутрішнього контролю на підприємстві та управління ІТ-ризиками у підконтрольних їм процесах;

ІТ-менеджери, що безпосередньо реалізують ідентифікацію, аналіз та управління ІТ-ризиками.

3.2 Архітектура та режими функціонування комп'ютеризованої системи управління інформаційними ризиками підприємства

Управління інформаційними ризиками підприємства передбачає необхідність організації безперервного моніторингу та оцінки якості стану інформаційних ресурсів. Дане завдання вирішується на підставі вбудовування комп'ютеризованої системи, що розробляється, в усі інформаційні процеси функціонування підприємства. Така інтеграція є досить складною. У зв'язку з цим побудова комп'ютеризованої системи оцінки та управління ІР має здійснюватися відповідно до наступних передумов:

1. Принцип несуперечності експертної інформації. Проектована інформаційна система оцінки інформаційних ризиків має включати різні алгоритми тестування експертних даних на несуперечність.

2. Принцип оптимальності рівня централізації та децентралізації проектованої інформаційної системи. Безперервний моніторинг великої кількості показників, що характеризують рівень інформаційного ризику, потребує організації розподіленого збору та обробки інформації.

3. Принцип безперервного вдосконалення. Інформаційна система повинна забезпечувати необхідну гнучкість та реалізовувати різні механізми самонавчання для організації більш обґрунтованого висновування внаслідок накопичення статистичної інформації.

4. Принцип інтеграції інформаційних потоків підприємства у єдиний інформаційний простір. Комп'ютеризована система, що розробляється, повинна мати можливість швидкого доступу до будь-яких інформаційних ресурсів підприємства.

5. Принцип безперервної комунікації. Ключовим фактором забезпечення успіху інструментів управління інформаційними ризиками, що впроваджуються, є постійна комунікація учасників цього процесу.

Нечітко-логічні та ймовірнісні інструменти управління інформаційними ризиками підприємства практично реалізовані як комп'ютеризована система «*InformRM 1.0*» (рис. 3.4).

На рисунку 3.4 представлено блок-схему архітектури комп'ютеризованої системи управління інформаційними ризиками на підприємстві.

Архітектура комп'ютеризованої системи управління інформаційними ризиками на підприємстві " *InformRM 1.0* " побудована за модульним принципом з використанням середовища програмування *Delphi*, пакету програм *Matlab*, СУБД *Microsoft SQL Server* для зберігання даних та різних інструментальних засобів інтеграції. Функціональний рівень, який відповідає за реалізацію основної логіки процесу аналізу та управління інформаційними ризиками, включає такі основні блоки: блок моніторингу зовнішнього та внутрішнього середовища, аналітичний блок оцінки можливості настання інформаційного ризику, аналітичний блок розрахунку збитків від настання ризику, блок підготовки звітних матеріалів.

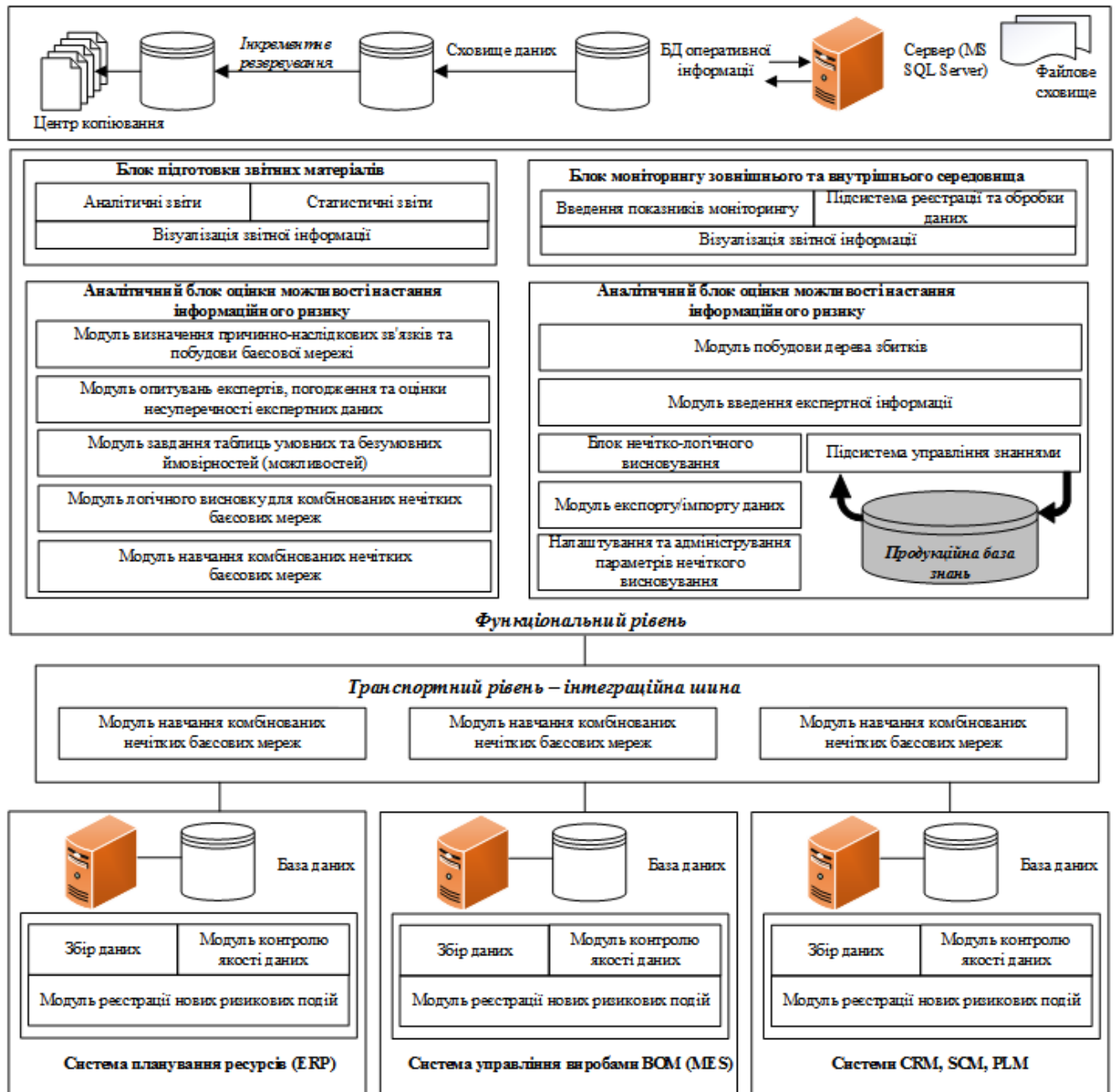


Рисунок 3.4 - Блок-схема архітектури комп'ютеризованої системи управління інформаційними ризиками на підприємстві "InformRM 1.0"

Джерело: складено автором на основі [8, 10, 28]

Основні функціонально-технічні вимоги до ІСППР були розроблені на основі аналізу наведених у пункті 3.1 логіко-інформаційних моделей бізнес-процесу управління інформаційними ризиками. Вони включають:

збирання та зберігання даних про стан та кількісні показники невизначених факторів зовнішнього та внутрішнього середовища, загроз та

вразливостей, а також їх можливих наслідків за рахунок інтеграції розроблюваної інформаційної системи в єдиний корпоративний інформаційний простір підприємства та організації процедур обміну між окремими його компонентами;

введення, запис та зберігання інформації про структуру розробленої комбінованої нечіткої баєсової мережі та дерева збитків, відстеження динаміки досягнення запланованих для підприємства цілей функціонування як в інформаційній сфері, так і пов'язаних з операційною діяльністю; виявлення факторів, що мають найбільший вплив на досягнення інформаційної безпеки;

заповнення та забезпечення можливості редагування баз знань комп'ютерної системи для реалізації аналітичних розрахунків при використанні ймовірнісно-нечітких інструментів управління інформаційними ризиками підприємства. Аналіз статистичної інформації про основні фактори невизначеності та ризику підприємства з метою автоматичного отримання нових знань, організація діалогового режиму роботи експертів для підтвердження їх введення в базу знань, або відмови від їх використання;

графічне подання комбінованої баєсової мережі взаємозв'язку причин виникнення інформаційних ризиків на підприємстві, видача рекомендацій щодо впливу на окремі концепти системи;

введення в систему вихідних значень факторів невизначеностей різного типу, побудова системи нечітко-логічного висновування з можливістю коригування основних характеристик функцій належності лінгвістичних змінних, розрахунок значень можливості виникнення та величини збитків підприємства;

забезпечення розмежування прав доступу до системи для різних категорій користувачів з метою забезпечення цілісності та збереження інформації та збільшення швидкості обробки транзакцій;

адміністрування розподілених баз даних та знань, підтримання їх цілісності, розробка алгоритмів інформаційного обміну.

Вибір середовища програмування *Delphi* пояснюється такими основними її перевагами:

а) існування засобів візуальної побудови форм, що полегшує завдання програмування інтерфейсу інформаційної системи;

б) наявність внутрішньої бібліотеки компонентів, що містить величезну кількість програмних модулів, які в результаті найпростішого налаштування та доопрацювання можна застосовувати для розробки додатків. Використання таких елементів скорочує час розробки та значно знижує ймовірність появи програмних помилок;

в) можливості та гнучкість вбудованої мови програмування *Object Pascal*. Від багатьох інших мов програмування, наприклад *Visual Basic*, мова *Pascal* відрізняється строгістю, яка дозволяє на етапі компілювання програми виявляти велику кількість помилок;

г) серед інших переваг *Delphi* можна зазначити можливості ефективної роботи з різними базами даних. Це зумовлюється трьома фактами: організація доступу до даних різного формату (*ODBC*), вбудовуванням компонентів, вкладених у функціонування у цьому середовищі.

Таким чином, можна сказати, що середовище *Delphi* - один із найпотужніших інструментів розробки різноспрямованих та складних інформаційних систем та додатків - ефективне рішення для розробки інформаційної системи управління інформаційними ризиками підприємства.

Програмна реалізація нечітко-продукційної процедури розрахунку збитків від настання інформаційних ризиків підприємства здійснюється з використанням математичного пакету *Matlab*, у тому числі вбудованого пакету розробки систем нечітко-логічного висновку *Fuzzy Logic*.

Переваги *Matlab* перед іншими математичними системами (наприклад, *MathCad*, *Mathematica*):

1. *Matlab* є відкритою системою; більшість процедур та функцій системи *Matlab* можливо коригувати та вносити до них різні зміни. *Matlab* являє собою

систему, функціональні можливості якої користувач може у разі потреби розширювати за допомогою створених ним програм та процедур;

2. У *Matlab* існує можливість використання власних процедур та функцій, водночас наявність великої кількості вбудованих компонентів у систему *Matlab* робить її ідеальним засобом для виконання наукових та інженерних розрахунків;

3. Останні версії системи *Matlab* забезпечують легкість інтеграції з текстовим редактором *Microsoft Word*, що дозволяє використовувати для складання документації обчислювальний та графічний інструментарій *Matlab*.

4. Функціональні можливості системи *Matlab* широкі, водночас за швидкістю реалізації поставлених завдань вона забезпечує набагато кращі результати, порівняно з іншими аналогічними системами.

На будь-якому підприємстві, як правило, одночасно застосовується безліч різних інформаційних систем. Базовою системою автоматизації діяльності підприємства є *ERP*-система, яка здійснює збір, обробку та аналіз інформації про стан технологічних процесів з виробничими *MES*-системами, що забезпечують безперервність виробництва. З іншого боку, для підприємства застосовуються різні аналітичні системи, створені задля рішення різних спеціальних завдань. Наприклад, система управління взаємовідносинами з клієнтами (*CRM*), інформаційна система управління транспортним процесом, ланцюгами постачання тощо. Всі перелічені інформаційні системи підприємства передбачають необхідність обміну даними з системою *ERP*. Через те, що у системі управління інформаційними ризиками проводиться аналіз зовнішнього та внутрішнього інформаційного середовища, однією з найважливіших проблем є інтеграція всіх систем підприємства з метою формування загального інформаційного простору.

Різні інтеграційні рішення, у тому числі й готові інструментальні засоби, дають можливість реалізовувати обмін даними між інформаційними системами, що розробляються та використовуються на підприємстві.

Наведена комп'ютеризована система управління інформаційними ризиками розроблена з використанням різних програмних засобів, що пов'язано з

необхідністю проведення частини розрахунків з використанням пакета *Matlab*. Інтеграція даних у систему *Matlab* здійснюється на основі технології «крапка-крапка» - результат виконання кожної операції може бути збережений у текстовому файлі або у вигляді змінної, доступної для подальшого застосування. Крім того, в системі передбачений вбудований компілятор, який перетворює *m*-файли в програмний код мовою *C* або *C++* або дозволяє згенерувати *exe*-додаток. Цей підхід дає можливість впроваджувати функції, реалізовані в *Matlab*, у практичні програми.

Широкі функціональні можливості комп'ютеризованої системи управління інформаційними ризиками підприємства, що розробляється, зберігання величезного обсягу ретроспективних даних і високі вимоги до надійності роботи зумовлюють існування певних обмежень на організацію зберігання інформації.

На підставі аналізу даних обмежень було прийнято рішення про проектування рівня зберігання даних, що складається з таких основних частин:

база даних оперативної інформації, яка призначена для тимчасового зберігання інформації про величини всіх факторів інформаційного ризику, їх динаміку, а також результати розрахунків можливості виникнення та збитку інформаційного ризику. Також у цій базі зберігається інформація, необхідна для реалізації перевірок після ухвалення рішення. Інформація з бази передається до центрального сховища після закінчення розрахунків та прийняття управлінських рішень;

сховище даних, яке застосовується для зберігання інформації про управління інформаційними ризиками, включаючи інформацію про величини ризиків, заходів з управління ними, про дати прийняття управлінських рішень та імена відповідальних осіб, які виконали ці рішення;

На підприємстві обов'язково створюються резервні копії сховища даних. Резервне копіювання баз даних сприяє забезпеченню додаткового захисту від пошкодження, випадкової втрати інформації, різних відмов та поломок обладнання та природних надзвичайних ситуацій. До службових обов'язків адміністратора баз

даних належить організація резервного копіювання та забезпечення надійного зберігання резервних копій.

Як правило, здійснюється повне копіювання існуючих баз даних - дублюються всі об'єкти, у тому числі системні таблиці та інформація. Коли починається копіювання, *SQL Server* дублює весь вміст бази, а також охоплює частини журналу транзакцій, які застосовуються під час формування резервних копій. Повну резервну копію БД можна застосовувати, щоб повністю відродити стан, який БД мала під час виконання процесу резервного копіювання.

Створення повної копії баз даних підприємства здійснюється раз на тиждень, місяць чи квартал залежно від особливостей функціонування підприємства. Зазвичай повне копіювання здійснюється щоп'ятниці або на вихідних, коли дублювання великого обсягу інформації не позначиться на роботі підприємства. Усі наступні резервні копії створюються буднями до наступного повного резервування. Вони можуть носити диференціальний або інкрементний характер, головним чином з метою збереження часу і місця на носії. Повне резервне копіювання слід виконувати не частіше ніж один раз на тиждень.

При диференційному резервному копіюванні кожен файл, змінений з часу останнього повного копіювання, записується заново. Цей вид копіювання прискорює відновлювальні процеси. Все, що потрібно для відновлення, це останні повна і диференціальна копії. Диференційне резервне копіювання стає все більш популярним, тому що всі копії окремих файлів виконуються в окремі моменти часу, що, наприклад, дуже важливо при вірусних зараженнях системи.

При інкрементному копіюванні здійснюється дублювання файлів, змінених з часу, коли востаннє здійснювалося повне чи інкрементне копіювання. За всіх наступних операцій копіювання додатково створюються лише файли, змінені з часу створення останньої копії. В середньому, інкрементне резервування даних забирає менше часу, оскільки копіюється набагато менше файлів. Однак відновлювальні процеси даних забирають більше часу, оскільки необхідно спочатку відновити дані останнього повного копіювання, а також дані всіх

інкрементних копій. Водночас на противагу диференціальному підходу, змінені, або нові файли, що змінилися, не замінюють старі, а записуються на носій незалежно.

Розроблена комп'ютеризована система управління інформаційними ризиками підприємства «*InformRM 1.0*» заснована на використанні баз даних *Microsoft SQL Server*.

У цій СУБД реалізовано можливість формування внутрішніх інструментів управління транзакціями.

Під транзакцією розуміється набір дій, які переводять базу даних з одного стану до іншого і виконуються з позиції «або все, або нічого». Доцільність використання транзакцій визначається тим, що паралельно в мережі можуть працювати багато користувачів.

Бази даних SQL-серверів спрямовані на застосування транзакцій. Це означає, що модифікації інформації не записуються безпосередньо в таблиці, як у локальної бази. Клієнтська програма посилає на сервер запит на виконання змін, а сервер реалізує пакет операцій як одну транзакцію. Для того, щоб зміна інформації була закріплена у базі даних, транзакцію необхідно завершити. Якщо якусь з операцій транзакції не буде виконано, здійснюється відкат даної транзакції, тобто транзакція обривається та повертається стан інформації, в якому вони перебували до початку виконання транзакції. У результаті формується високий рівень захисту цілісності та несуперечності інформації.

Реплікація – це процес організації та підтримки копії бази даних на іншому сервері. Доцільність застосування даного механізму полягає у необхідності постійної синхронізації кількох таблиць у процесі збирання інформації з різних корпоративних систем.

Реплікація використовується для:

- 1) поширення даних з одного сервера на кілька серверів;
- 2) збору даних із різних серверів на один сервер (наприклад, можна акумулювати звіти про платежі, реалізовані у філіях);

- 3) зниження навантаження сервера і збільшення відмовостійкості (можна використовувати додатковий сервер і через деякі проміжки часу реплікувати на нього інформацію з робочого сервера).

Комп'ютеризована система управління інформаційними ризиками на підприємстві «InformRM 1.0» може функціонувати у таких основних режимах:

1. Режим адміністрування, який передбачає виконання функцій роботи з даними (додавання, редагування та видалення інформації із системи, налаштування реплікацій баз даних та механізму управління транзакціями), розподіл прав користувачів системи (додавання нових користувачів, їх авторизація, обмеження/додавання прав як групам користувачів, так і окремим особам), індивідуальне налаштування роботи системи (зміна розмірів та типів шрифтів, гарячі клавіші та ін.).

2. Режим роботи експерта. У цьому режимі доступні модулі, пов'язані з використанням ймовірно-нечітких інструментів управління інформаційними ризиками, що дозволяють вводити, редагувати та видаляти знання у відповідні бази, налаштовувати функції належності заданих лінгвістичних змінних, інтерпретувати отримані результати системи.

3. Режим роботи ризик-менеджера. Цей режим спрямовано на використання основних функціональних можливостей системи, тобто, менеджер запроваджує фактичні значення факторів невизначеності зовнішнього та внутрішнього середовища, аналізує результати, вибираються управлінські заходи.

3.3 Рекомендації щодо розробки комп'ютеризованої системи управління інформаційними ризиками підприємства

Запропонований апарат комбінованих нечітких баєсових мереж дозволяє визначити, наскільки високий ризик недостовірності інформації спричинений

кожним із його джерел. Таким чином, за допомогою запропонованої комплексної нечіткої байєсово-продукційної системи оцінки інформаційних ризиків легко визначити напрямки розробки управлінських заходів.

Для підприємства найбільший вплив на виникнення ризиків надають суб'єктивні помилки персоналу під час роботи з інформаційними системами, помилки персоналу у процесі збору інформації, порушення правил роботи з конфіденційною інформацією, низькі фінансові та часові витрати на отримання інформації, нераціональний розподіл прав доступу між співробітниками підприємства.

В результаті запропоновано такі заходи: навчання персоналу, впровадження практики щомісячних інструктажів щодо підвищення інформаційної обізнаності співробітників підприємства, розробка нормативної документації, що регламентує перелік прав доступу для кожної категорії співробітників, розробка нової політики міжмережевої взаємодії при роботі із зовнішніми інформаційними ресурсами. Дані заходи дозволять знизити можливість настання та подальші збитки від інформаційного ризику.

Попри невисоке значення ризику втрати та порушення конфіденційності інформації, низьку можливість хакерських атак та проникнення черв'яків на підприємстві, найважливіші підсистеми слід ізолювати від глобальної мережі, а також впровадити новий регламент підключення робочих місць до мережі Інтернет та протидії *DDoS-атакам*. На підприємстві доцільно змінити існуючий підхід до інформаційного обміну із зовнішніми джерелами інформації за рахунок використання механізму завантаження/вивантаження даних через систему оперативних сховищ.

У табл. 3.1 подано комплекс заходів щодо управління інформаційними ризиками.

Таблиця 3.1 - Комплекс заходів щодо управління інформаційними ризиками

1. Розробка методики перевірки достовірності інформації.	Навчання персоналу
2. Створення регламентів опрацювання інцидентів.	
3. Впровадження системи контролю нерегламентованого використання зовнішніх пристроїв та програмного забезпечення.	
4. Розробка заходів щодо запобігання нецільовому використанню ІТ-ресурсів.	
5. Розробка системи централізованого керування доступом до інформаційних ресурсів.	

Джерело: розроблено автором

Методика перевірки достовірності інформації включає такі етапи:

1. Аналіз внутрішньої інформації підприємства, перевірка на надмірність.
2. Перевірка інформації, що надійшла з наявними аналогічними даними, або в результаті ретроспективного аналізу з використанням методів прогнозування, наприклад, статистичного прогнозу (аналіз ліній тренду).

3. Порівняння отриманих даних з даними з інших джерел. У цьому разі передбачається, якщо є потреба, залучення різних консалтингових і маркетингових компаній щодо додаткових глибших досліджень.

4. Експертний аналіз інформації, що надійшла.

Розробка регламентів реагування на інциденти інформаційної безпеки. Окремі аспекти управління інцидентами інформаційної безпеки містяться в наступних документах:

ISO/IEC 27001:2005 Information security management system. Requirements. У цьому стандарті формулюються вимоги до системи управління інформаційною безпекою та ризиками, що включають, зокрема, і окремі аспекти управління інцидентами.

ISO/IEC TR 18044 Information security incident management. Цей документ визначає інфраструктуру управління інцидентами інформаційної безпеки у контексті циклічної моделі *PDCA* (цикл Демінгу). Пропонуються окремі специфікації для етапів планування, використання, аналізу та вдосконалення

процесу. Докладно розглядаються проблеми розробки та впровадження нормативної документації, розподіл ресурсів, надаються рекомендації щодо окремих процедур.

CMU/SEI-2004-TR-015 Defining incident management processes for CISRT. Даний документ є описом методології планування, оцінки та вдосконалення процесів управління інцидентами. Багато уваги приділяється організації роботи *CISRT (Critical Incident Stress Response Team)* - підрозділу, що виконує функції запобігання, обробки та вироблення заходів у відповідь на інциденти ІБ. Використовується кілька критеріїв, виходячи з яких можна визначити ефективність функціонування даних сервісів, докладно описуються процесні карти.

NIST SP 800-61 Computer security incident handling guide. У цьому документі описані «найкращі практики» щодо організації управління інцидентами та реагування на них. Докладно розглядаються питання розробки заходів у відповідь на різні види загроз, наприклад, такі як ураження шкідливими вірусами, несанкціонований доступ і так далі.

Регламент обробки інцидентів інформаційної безпеки на підприємстві розроблений з опорою на стандарт *ISO/IEC TR 18044* і включає наступні основні етапи:

1. Повідомлення про події інформаційної безпеки, про слабкості захисту. Про інциденти порушення безпеки необхідно інформувати керівництво підприємства відповідно до певного порядку, якщо можливо, негайно.
2. Збір інформації про інцидент, попередня оцінка причин і наслідків, складання звітів.
3. Негайна реакція. Вжиття аварійних захисних заходів (відключення атакованої інформаційної системи, сервісу та (або) мережі за угодою з керівництвом) та визначення додаткових постійних захисних заходів та повідомлення співробітників організації про вжиття цих заходів.
4. Подальше реагування та антикризові заходи. На цьому етапі здійснюється відновлення уражених ділянок інформаційної системи підприємства, складання

докладних звітів. Вжиття заходів щодо запобігання повторенню інцидентів.

5. Модернізація системи управління інформаційними ризиками та безпекою: нові вимоги до інформаційної безпеки, зміни у формах звітності та базах даних.

6. Персонал повинен проходити періодичну підготовку з питань відповідальності та посадових обов'язків при реалізації заходів у відповідь на інциденти порушення ІБ. У процесі підготовки персоналу повинні моделюватись різні ситуації та події, що сприятиме у майбутньому персоналу ефективно виконувати необхідні дії у разі виникнення ризикових ситуацій.

7. Повинна проводитись періодична перевірка та оцінка ефективності реалізованих заходів щодо реагування на інциденти порушення ІБ з використанням спеціалізованих тестів (перевірочних послідовностей дій).

Впровадження системи контролю нерегламентованого використання зовнішніх пристроїв та програмного забезпечення. У рамках цієї системи фіксуються факти встановлення та застосування забороненого програмного забезпечення, несанкціонованого підключення мобільних телефонів та портативних пристроїв до службових ПК тощо. Всі дані реєструються у вигляді протоколів, і записуються в БД, весь аналіз здійснюється експертами.

Розробка системи централізованого керування доступом до інформаційних ресурсів. Зараз на підприємстві користувачі мають доступ до величезної кількості інформаційних систем. З метою забезпечення та підвищення безпеки необхідно розробити єдину систему правил доступу до інформаційних ресурсів для різних працівників підприємства.

Таким чином, умовно економічний ефект від використання нечітко-логічних та ймовірнісних інструментів оцінюється як зниження щомісячного можливого збитку від виникнення інформаційних ризиків.

Управління інформаційними ризиками підприємства передбачає необхідність організації безперервного моніторингу та оцінки якості стану інформаційних ресурсів. Дане завдання вирішується на підставі вбудовування

комп'ютеризованої системи, що розробляється, в усі інформаційні процеси функціонування підприємства.

Архітектура комп'ютеризованої системи управління інформаційними ризиками на підприємстві «*InformRM 1.0*» побудована за модульним принципом з використанням середовища програмування *Delphi*, пакету програм *Matlab*, СУБД *Microsoft SQL Server* для зберігання даних та різних інструментальних засобів інтеграції.

Функціональний рівень, який відповідає за реалізацію основної логіки процесу аналізу та управління інформаційними ризиками, включає такі основні блоки: блок моніторингу зовнішнього та внутрішнього середовища, аналітичний блок оцінки можливості настання інформаційного ризику, аналітичний блок розрахунку збитків від настання ризику, блок підготовки звітних матеріалів.

Нечітко-логічні та ймовірнісні інструменти практично використовувалися при розробці науково-обґрунтованих рекомендацій щодо створення системи управління інформаційними ризиками на підприємстві.

З використанням запропонованих комбінованої нечіткої баєсової мережі оцінки можливості настання інформаційного ризику та нечітко-продукційної процедури розрахунку збитків від його настання виконується розрахунок можливості настання різних інформаційних ризиків підприємства.

Економічний ефект від використання запропонованих нечітко-логічних та ймовірнісних інструментів оцінюється як зниження щомісячної можливої збитку від виникнення інформаційних ризиків.

ВИСНОВКИ

1. Подана логіко-інформаційна модель управління інформаційними ризиками на підприємстві висвітлює значення інформаційного ризику як імовірно-вартісного показника втрати якості інформації через вплив зовнішніх та внутрішніх факторів різного характеру. Це обґрунтовує вибір нечітких баєсових мереж для управління ризиками та підвищує обґрунтованість ухвалення управлінських рішень щодо зменшення інформаційних ризиків.

2. Розглянута комплексна нечітка баєсово-продукційна система оцінки інформаційних ризиків, що складається з двох етапів і включає в себе розрахунок імовірності виникнення ризиків та збитків від їх настання, дозволяє ідентифікувати найнебезпечніші ризики для підприємства та визначати напрями розробки управлінських рішень для їх мінімізації.

3. Розглянуто структуру, методику побудови та процедуру логічного висновування в комбінованій нечіткій баєсовій мережі для оцінки можливості настання інформаційних ризиків. Завдяки цьому можна використати циклічні зв'язки між трьома видами показників інформаційного ризику, кожен з яких може бути описаний окремо, враховуючи природу невизначеності кожного вузла.

4. Проведено оцінку доцільності застосування нечітко-продукційної процедури розрахунку збитків від настання інформаційних ризиків підприємства, що базується на поданні збитків як ієрархічного дерева та застосування операцій нечітко-логічного висновування для визначення ризиків з максимальними втратами та оперативного управління ними.

5. Описано архітектуру комп'ютеризованої системи управління інформаційними ризиками "InformRM 1.0", що ґрунтується на нечітко-продукційних та ймовірнісних методах та інструментах. Вона дозволяє приймати обґрунтовані оптимальні рішення щодо запобігання та зниження інформаційних ризиків на підприємстві.

6. Запропоновано науково-обґрунтовані рекомендації щодо управління інформаційними ризиками на підприємстві.

У роботі вирішено завдання комп'ютеризованого аналізу та управління інформаційними ризиками на основі використання нечітко-логічних та баєсових методів, що має важливе значення для досягнення конкурентоспроможності, інформаційної безпеки та ефективності підприємства.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Амоша О.І. Концепція інноваційного розвитку регіону / Амоша О.І. - Донецьк: НАН України : Ін-т економіки промисловості, 2002. -172 с.
2. Вітлінський В.В. Моделювання економіки: навчальний посібник / В.В. Вітлінський. - К.: КНЕУ, 2003. - 480 с.
3. Вітлінський В.В. Ризикологія як системотвірна складова економічної кібернетики / В.В. Вітлінський // Економічна кібернетика. - 2000. -№ 1-2.-с. 12-19.
4. Галіцин В. К. Суслов О. П., Самченко Н. К. Процес формування управлінських рішень // Стратегічні пріоритети в ХХІ столітті зб. матеріалів II Міжнар. науково-практ. конф. - Київ, 2017. с. 77-81.
5. Галіцин В. К., Суслов О. П., Самченко Н. К. Концепція дослідження і формування управлінських рішень // «Transformations in Contemporary Society: Economic Aspects». Opole: The Academy of Management and Administration in Opole, 2017- с. 155-162.
6. Галіцин В.К. Системи моніторингу / В.К. Галіцин - К.: КНЕУ. 2000. - 231 с.
7. Геєць В. Економіка України: підсумки перетворень та перспективи зростання / В. Геєць. - Харків : Фест, 2000. - 432 с.
8. Матвійчук А.В. Аналіз та прогнозування розвитку фінансово-економічних систем із використанням теорії нечіткої логіки: монографія - К.: Центр навчальної літератури, 2005. – 206 с.
9. Система управління ризиками авіаційної діяльності /Харченко В. П., Алексєєв О.М/ Под ред. Харченко В.П.: – К. : НАУ, 2018. – 312 с.
10. Згуровський М. З., Бідюк П. І., Терентьев О. М., Просянкін-Жарова Т. І. Байєсівські мережі в системах підтримки прийняття рішень — Київ : ТОВ «Видавниче Підприємство «Едельвейс», 2015. — 300 с.
11. Гур`янов А. Б., Гришко О. А. Системний підхід до стратегічного управління підприємством // Вісник економіки транспорту і промисловості. Серія Економіка підприємства. 2011. № 34. с. 274–277.

12. Демінг У. Е. Лекція перед японськими менеджерами в 1950 р // Методи менеджменту якості. - 2000. - № 10. - С. 24-29 (Пер. Ю. П. Адлера і В. Л. Шпер).
13. Ackerman, F. Using Causal Mapping with Group Support Systems до Elicit understanding of Failure in Complex Projects: Some Implications for Organizational Research / F. Ackerman // Group Decision and Negotiation. – 2003. – 14. – pp 355-376.
14. Ferat, S. A Baesian Network Approach до Self-organization and Laerning in Intellident Agents / S. Ferat //Dissertation submitted to Faculty of Virginia Politechnic and State University в fulfillment of requirements for degree of Doctor of Philosophy in Electrical and Computer Engineering, 2000 - 251 p.
15. Heckerman, D. A tutorial on learning with Bayesian networks / D. Heckerman // Technical report MSR-TR-95-06. - Microsoft Research, Redmond, WA (USA). - 1995.-57p.
16. Murphy, KP An introduction to graphical model [Електронні дані] / KP Murphy // Computer Science. - 2001 - 19 p. - Режим доступу : http://www.cs.ubc.ca/~murphyk/papers/intro_gm.pdf (дата звернення: 02.03.2024).
17. Murphy, KP Midelling Cen Expression Data за допомогою Dynamic Bayesian Networks / KP Murphy, S. Mian // Technical report. - Berkeley, CA. - 1999 - 12 p. - Режим доступу : http://www4.ncsu.edu/~smsulli2/MA810_Fall2008/SAMSIpapers/murphy99modelling.pdf (дата звернення: 02.03.2024).
18. Nahmias, S. Fuzzy Variables in Fuzzy Environment / S. Nahmias // In: Advances in fuzzy set theory. – Amsterdam: NHCP, 1979. – 254 pp.
19. Zadeh, L.A. Toward a perception-based theory of probabilistic reasoning with imprecise probabilities / L.A. Zadeh // Journal of Statistical Planning and Inference/- 2002.- 105.-P. 230-245.
20. Бідюк, П.І. Побудова та методи навчання баєсових мереж/П.І. Бідюк, О.М. Терентьєв // Таврійський вісник інформатики та математики. – 2004.-№2.-С.

139-154.

21. ISO 31000 2009 – Ризик-менеджмент. Принципи та керівництва. [Електронний ресурс] // Практичний менеджмент якості. - Режим доступу: [http://www.pqm-online.com/assets/files/standards/iso_31000-2009\(r\).pdf](http://www.pqm-online.com/assets/files/standards/iso_31000-2009(r).pdf) (дата звернення: 02.03.2024).
22. Бегун А. В., Ігнатова Ю. В., Урденко О. Г. Оцінка економічної ефективності захисту неоднорідних даних підприємств малого та середнього бізнесу. Фінансово-кредитне забезпечення інноваційної діяльності малого та середнього бізнесу / за заг. ред. М.І. Дибі. — К.: ВД «Освіта України» , 2019. — п.4.3. — С. 333–358.
23. Бегун А. В., Осипова О. І., Урденко О. Г. Ситуаційний лог менеджмент інформаційної безпеки підприємства // Моделювання та інформаційні системи в економіці. Міжвідомчий наук. збірник. Вип. № 95. — К.: КНЕУ, 2018. — С. 18–29.
24. Пугачова М.В. Статистичний моніторинг ділової активності підприємств : [підручник] / М.В. Пугачова, Н.О. Парфенова О.В. Гончар. - К.: НАСОНА, 2011. -468 с.
25. Статистичний збірник/Statistical Publication «Україна у цифрах»/"Ukraine in Figures" 2022 рік. - Режим доступу: https://ukrstat.gov.ua/druk/publicat/kat_u/2023/zb/08/zb_Ukraine_in_figures_22.pdf (дата звернення: 02.03.2024).
26. Нечітка логіка [Електронний ресурс]. — Режим доступу: URL: <http://www.victoria.lviv.ua/html/oio/html/theme11.htm> . — Назва з екрану. (дата звернення: 02.03.2024).
27. Zadeh L. Fuzzy Sets // Information and Control. — 1965. — № 8. — Р. 338–353. 197
28. А. В. Матвійчук. Штучний інтелект в економіці: нейронні мережі, нечітка логіка / КНЕУ, 2010. — 361 с.
29. Address Allocation for Private Internets [Electronic Resource]. — Mode of access:

- URL: <http://www.rfc-editor.org/rfc/rfc1918.txt> . Title from the screen. (дата звернення: 02.03.2024).
30. Шмигель О. Є. Управлінський облік та критерії його ефективності на підприємстві. Інноваційна економіка. 2020. №3-4. с. 182-187. URL: <http://inneco.org/index.php/innecoua/article/view/580/645> (дата звернення: 02.03.2024).
31. Щедріна О.І. Системний аналіз як інструмент прийняття управлінських рішень в бізнесі. 2020. с.169-183 URL: URL: https://kneu.edu.ua/userfiles/zb_mise/99/15.pdf (дата звернення: 02.03.2024).
32. Пономаренко О. І. Системні методи в економіці, менеджменті та бізнесі / О. І. Пономаренко. — К.: Либідь, 2015. — 240 с.
33. Global Management Accounting Principles. URL: <https://www.cgma.org/content/dam/cgma/resources/reports/downloadabledocument/s/global-management-accountingprinciples.pdf> (дата звернення: 02.03.2024).
34. Державна служба статистики України: офіційний сайт. URL: <http://www.ukrstat.gov.ua/> (дата звернення: 02.03.2024).
35. Міністерство економіки України: офіційний сайт. URL: <https://me.gov.ua/?lang=uk-UA> (дата звернення: 02.03.2024).



Ім'я користувача:
Комп'ютерної математики та інформаційної безпеки...

Дата перевірки:
10.05.2024 00:41:11 EEST

Дата звіту:
10.05.2024 00:46:16 EEST

ID перевірки:
1016241002

Тип перевірки:
Doc vs Internet + Library

ID користувача:
100005746

Назва документа: Диплом_Галіцин В

Кількість сторінок: 84 Кількість слів: 16499 Кількість символів: 133363 Розмір файлу: 1,006.66 KB ID файлу: 10160231

2.92%
Схожість

Найбільша схожість: 1.3% з джерелом з Бібліотеки (ID файлу: 1006101163)

2.24% Джерела з Інтернету

227

Сторінка 86

2.67% Джерела з Бібліотеки

135

Сторінка 87

0% Цитат

Вилучення цитат вимкнено

Вилучення списку бібліографічних посилань вимкнено

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи

51



УДК 004.49

[https://doi.org/10.52058/2786-6025-2024-4\(32\)-894-908](https://doi.org/10.52058/2786-6025-2024-4(32)-894-908)

Гладка Юлія Анатоліївна кандидат фізико-математичних наук, доцент, доцент кафедри системного аналізу та кібербезпеки, Київський національний економічний університет імені Вадима Гетьмана, просп. Берестейський (Перемоги), 54/1, м. Київ, 03057, тел.: (067) 440-18-37, <https://orcid.org/0000-0001-5819-7465>

Галіцин Володимир Євгенович студент 6 курсу освітньо-професійної програми «Системний аналіз» кафедри системного аналізу та кібербезпеки, Київський національний економічний університет імені Вадима Гетьмана, просп. Берестейський (Перемоги), 54/1, м. Київ, 03057, тел.: (050)410-53-56, <https://orcid.org/0009-0005-4530-6323>

ПРОТИДІЯ ВИКОРИСТАННЮ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЯК РІЗНОВИДУ КІБЕРАТАК

Анотація. В даний час дослідження поведінки шкідливого програмного забезпечення є актуальним питанням інформаційної безпеки.

Шкідливе ПЗ еволюціонує та вдосконалюється, стає дедалі ефективнішим, а кіберзлочинці впроваджують нові зразки, підходи та вектори зараження. Традиційні підходи антивірусного ПЗ, засновані на пошуку сигнатур відомих зразків в базах даних, не можуть виявляти нові екземпляри шкідливого ПЗ, що використовують невідомі раніше вразливості та способи атаки. Тому застосовуються інструменти статичного аналізу програмного забезпечення, що досліджують виконувані файли, та інструменти динамічного аналізу, що досліджують поведінку програмного забезпечення під час його роботи.

У процесі розвитку інформаційних технологій більшість держав світу виявилися не готовими до боротьби з інтернет-злочинністю на юридичному, інформаційному та технічному рівні. Через недостатню боротьбу кіберзлочинність як негативне соціально-правове явище мала негативний вплив на соціально-економічний розвиток держав.

Використання результатів досліджень розглянутої сфери дозволяють підвищити рівень антивірусного захисту, зокрема у виявленні нових зразків рекламного програмного забезпечення та потенційно небажаних програм для пристроїв на базі MacOS, та тим самим збільшити комерційну привабливість антивірусного продукту. Подальшим напрямком розвитку системи є залучення нових джерел для пошуку зразків, впровадження підтримки нових операційних систем та файлових форматів.





сЬОГОДНІ

Ключові слова: інформаційні ризики, системний аналіз, програмне забезпечення, кібератака, ефективність, комерційна привабливість.

Gladka Yuliya Anatolievna PhD, Associate Professor department of system analysis and cybersecurity Kyiv National Economic University named after Vadym Hetman, Ave. Beresteysky (Victory), 54/1, Kyiv, 03057, tel.: (067) 440-18-37, <https://orcid.org/0000-0001-5819-7465>

Galitsyn Volodymyr Evgenovich 6th year student Professional Educational Program «System analysis» by Department of System Analysis and Cybersecurity of Kyiv National Economic University named after Vadym Hetman», Kyiv, 03057, Ave. Beresteysky (Victory), 54/1, tel.: (050) 410-53-56, <https://orcid.org/0009-0005-4530-6323>

PREVENTING THE USE OF MALWARE AS A TYPE OF CYBER ATTACK

Abstract. Currently, the study of the behavior of malicious software is an urgent issue of information security.

Malware is evolving and improving, becoming more and more effective, and cybercriminals are introducing new patterns, approaches, and infection vectors. Traditional anti-virus software approaches, based on searching for signatures of known samples in databases, cannot detect new instances of malicious software using previously unknown vulnerabilities and attack methods. Therefore, static software analysis tools are used, examining executable files, and dynamic analysis tools, examining the behavior of software during its operation. In the process of development of information technologies, most of the countries of the world were not ready to fight against Internet crime at the legal, informational and technical level. Due to the insufficient fight, cybercrime as a negative socio-legal phenomenon had a negative impact on the socio-economic development of states.

The use of the results of research in the considered field allows to increase the level of antivirus protection, in particular, in the detection of new samples of advertising software and potentially unwanted programs for devices based on MacOS, and thereby increase the commercial attractiveness of the antivirus product. The further development direction of the system is the attraction of new sources for finding samples, implementation of support for new operating systems and file formats.

Keywords: information risks, system analysis, software, cyber attack, efficiency, commercial attractiveness.

Постановка проблеми. Виявлення та класифікація шкідливих програм стала однією з найважливіших проблеми в галузі кібербезпеки. Існує

895

№ 4(32)
2024

І НАУКА ТЕХНІКА

серії: право, економіка, педагогіка,
техніка, фізико-математичні науки

СЬОГОДНІ

достатньо методик виявлення невідомого шкідливого програмного забезпечення, кожна з яких має свої переваги, недоліки та особливості використання.

Статичний аналіз ускладнюється техніками захисту – пакувальниками та крипторами – які не можна обійти без динамічного аналізу та особливостями завантаження PE (наприклад, використання ApiSetSchema при дозволі імпортів). Динамічний аналіз вимагає спеціального середовища для безпечного запуску коду, що потенційно є шкідливим. Як таке середовище може виступати обмежене та контрольоване оточення (віртуальна машина, антивірусна пісочниця).

Використання таких методів, як перехоплення викликів функції та аналіз аргументів, є стандартним підходом у цій галузі, який зустрічається у багатьох рішеннях. Відомою також є техніка W xor X (write xor execute), яка заснована на модифікації прав доступу до сторінок пам'яті (за допомогою установки NX/XD біта) та застосовується для того, щоб пропустити етап розпакування коду.

Згідно з Рішенням ради національної безпеки і оборони України «Про План реалізації Стратегії кібербезпеки України», яке введене в дію Указом Президента України від 1 лютого 2022 року № 37/2022, кіберпростір визначено як один із ключових елементів воєнних дій. Основою кібероборони визначено кібервійська, які повинні забезпечувати ефективний захист критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації. Також цим нормативним документом визначено завершення до 2025 року імплементації в законодавство України положень Конвенції про кіберзлочинність. Нині у вітчизняній практиці термін «кіберзлочинність» вживається разом із терміном «комп'ютерна злочинність», під яким зазвичай розуміються злочини з допомогою комп'ютерної інформації. Термін «кіберзлочинність» зобов'язаний своєю появою виникнення та розвитку індустрії інформаційних та комп'ютерних технологій, яка поступово проникла у всі сфери життя світової спільноти.

У законі України «Про основні засади забезпечення кібербезпеки України» поняття кібербезпеки визначається як «...захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі».

Шкідливе ПЗ використовується для нападу на критичну інфраструктуру для шпигунства, крадіжки приватної інформації або для здійснення фінансових шахрайств.

За національним законодавством створення шкідливих програмних чи технічних засобів з метою протиправного використання, розповсюдження або

896

№ 4(32)
2024

НАУКА і ТЕХНІКА

серії: право, економіка, педагогіка,
техніка, фізико-математичні науки

СЬОГОДНІ

збуту, а також їх розповсюдження або збут кваліфікується за статтею 361-1 Кримінального кодексу України. Вищевказані дії караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на строк до трьох років. У разі вчинення тих самих дій повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, санкція статті передбачає позбавлення волі на строк до п'яти років.

Аналіз останніх досліджень і публікацій. Проблемам виявлення шкідливого ПЗ та захисту від нього присвячено ряд робіт як зарубіжних Barkley B., Barton T., Bernstein P., Crockford N., Crouhy M., Duncan R., Fragniere E., так і вітчизняних авторів Амоша О.І., Геєць В.М., Поляков О.М. В цих працях достатньо повно аналізуються певні напрямки, методи або засоби протидії шкідливим програмам. Як показує аналіз, на теперішній момент не існує такої методики, яка б повністю вирішувала завдання виявлення невідомого шкідливого ПЗ з прийнятною ефективністю для будь-яких видів і за будь-яких вимог до системи.

Мета статті – дослідження особливостей та визначення сучасних ефективних механізмів виявлення, протидії та блокування шпигунського та шкідливого програмного забезпечення в умовах повномасштабного вторгнення.

Виклад основного матеріалу. Після відкритої агресії рф у 2022 році з'явилися нові виклики, пов'язані з кібервійною.

Повномасштабна війна рф проти України триває майже два роки, за цей час українці змогли вистояти та пережити чимало провокацій і злочинів з боку окупантів. Один із методів сучасної війни, який активно використовують росіяни — кібератаки.

Протягом останніх місяців українці помітили значну кількість кібератак на державні та великі приватні підприємства, що забезпечують якісну життєдіяльність громадян України. За повідомленням Держспецзв'язку, кількість кібератак за минулий 2023 рік зросла на 15,9%.

Крім того, безпосередньо аналітиками безпеки було зафіксовано та оброблено 1105 кіберінцидентів, що на 62,5% більше, ніж за результатами 2022 року.

За підрахунками Держспецзв'язку, за 2023 рік було виявлено 1 516 861 підозрілих унікальних файлів, при цьому найчастіше виявляли віруси типу SmokeLoader, Agent Tesla, Snake Keylogger, Remcos, Formbook.

Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA повідомила про 347 кібератак, які здійснювали на урядові організації, ще 276 — на місцеві органи влади, 175 — на сектор безпеки та оборони та 127 випадків атак на комерційні організації.

Тому на часі вирішення проблеми контролю потоку виконання при аналізі підозрілого (потенційно шкідливого) ПЗ та маскуванню інструментів

такого контролю від виявлення. Ця проблема є частиною загальної проблеми в галузі інформаційної безпеки щодо детектування шкідливого ПЗ на основі даних моніторингу поведінки програми.

До зловмисних програмних засобів належать віруси, рекламне ПЗ, хробаки, троянці, руткіти, клавіатурні логери, дозвонювачі, шпигунські програмні засоби, здирницькі програми, шкідливі плагіни та інше зловмисне програмне забезпечення.

Шкідливим можна назвати програмне забезпечення, що створене з наміром пошкодити, використати або вивести з ладу пристрої, системи та мережі. Воно використовується для компрометації функцій пристрою, викрадення даних, обходу контролю доступу та завдання шкоди комп'ютерам та іншим пристроям і мережам, до яких вони підключені.

Незалежно від методу, усі типи шкідливого програмного забезпечення призначені для використання пристроїв користувачем на користь хакера — особи, яка розробила та/або розгорнула таке програмне забезпечення.

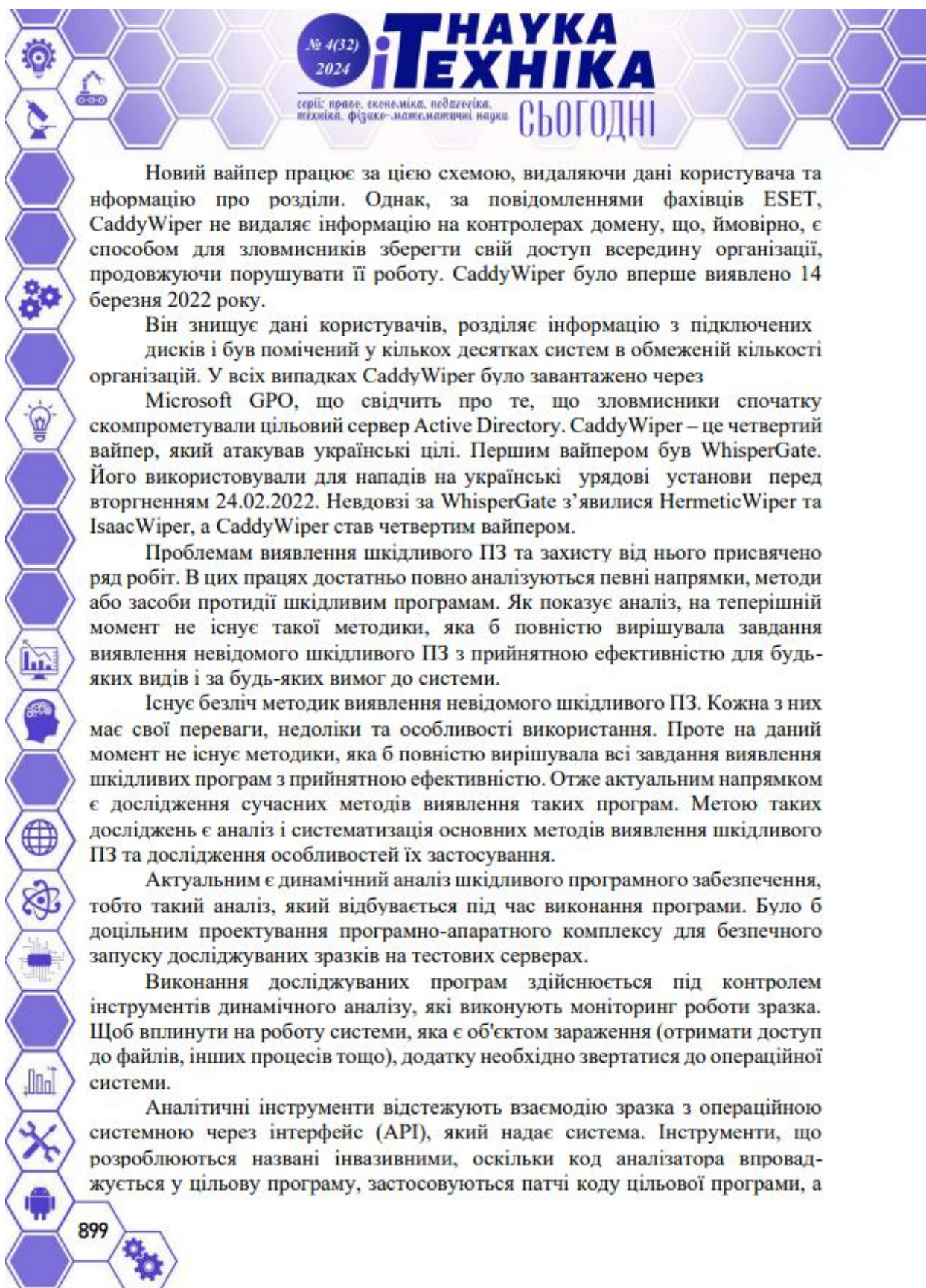
Кожен тип шкідливого програмного забезпечення має власний унікальний спосіб спричинити хаос, і більшість з них залежить від певних дій користувача. Наприклад, шкідливі програми можуть бути доставлені в систему як за допомогою USB-накопичувача, так і шляхом автоматичного завантаження без схвалення або відома особи.

Фішингові атаки є ще одним поширеним типом «доставлення» зловмисного ПЗ, коли електронні листи, замасковані під законні повідомлення, містять шкідливі посилання або вкладення, що доставляють файл зловмисного ПЗ користувачам, які нічого не підозрюють.

Нові види, так би мовити, зловмисного ПЗ включають й нові методи ухилення та обфускації, які розроблені, щоб ввести в оману не лише користувачів, а й адміністраторів безпеки та засоби захисту від ПЗ. Деякі з цих методів ухилення покладаються на просту тактику, як використання вебпроксі для приховування зловмисного трафіку або вихідних IP-адрес.

В даний час щодня з'являється велика кількість нового шкідливого ПЗ, тому класичне детектування, засноване на пошуку бази даних сигнатур антивірусних програм, відходить на другий план, поступаючись місцем підходам, заснованим на поведінковому аналізі.

У кіберпросторі до таких засобів можна віднести появу нового віруса-знищувача (вайпера) CaddyWiper. CaddyWiper – це зловмисне програмне забезпечення, зловмисний код, спеціально розроблений для пошкодження цільових систем шляхом стирання даних користувача, програм, жорстких дисків і, у деяких випадках, інформації про розділи. На відміну від програм-вимагачів, троянів та інших поширених варіантів зловмисного програмного забезпечення, вайпери не зосереджені на крадіжці чи фінансовій вигоді, вони видаляють усе на своєму шляху з чисто деструктивною метою.



№ 4(32)
2024

НАУКА і ТЕХНІКА

серії: право, економіка, педагогіка,
техніка, фізико-математичні науки

СЬОГОДНІ

Новий вайпер працює за цією схемою, видаляючи дані користувача та інформацію про розділи. Однак, за повідомленнями фахівців ESET, CaddyWiper не видаляє інформацію на контролерах домену, що, ймовірно, є способом для зловмисників зберегти свій доступ всередину організації, продовжуючи порушувати її роботу. CaddyWiper було вперше виявлено 14 березня 2022 року.

Він знищує дані користувачів, розділяє інформацію з підключених дисків і був помічений у кількох десятках систем в обмеженій кількості організацій. У всіх випадках CaddyWiper було завантажено через Microsoft GPO, що свідчить про те, що зловмисники спочатку скомпрометували цільовий сервер Active Directory. CaddyWiper – це четвертий вайпер, який атакував українські цілі. Першим вайпером був WhisperGate. Його використовували для нападів на українські урядові установи перед вторгненням 24.02.2022. Невдовзі за WhisperGate з'явилися HermeticWiper та IsaacWiper, а CaddyWiper став четвертим вайпером.

Проблемам виявлення шкідливого ПЗ та захисту від нього присвячено ряд робіт. В цих працях достатньо повно аналізуються певні напрямки, методи або засоби протидії шкідливим програмам. Як показує аналіз, на теперішній момент не існує такої методики, яка б повністю вирішувала завдання виявлення невідомого шкідливого ПЗ з прийнятною ефективністю для будь-яких видів і за будь-яких вимог до системи.

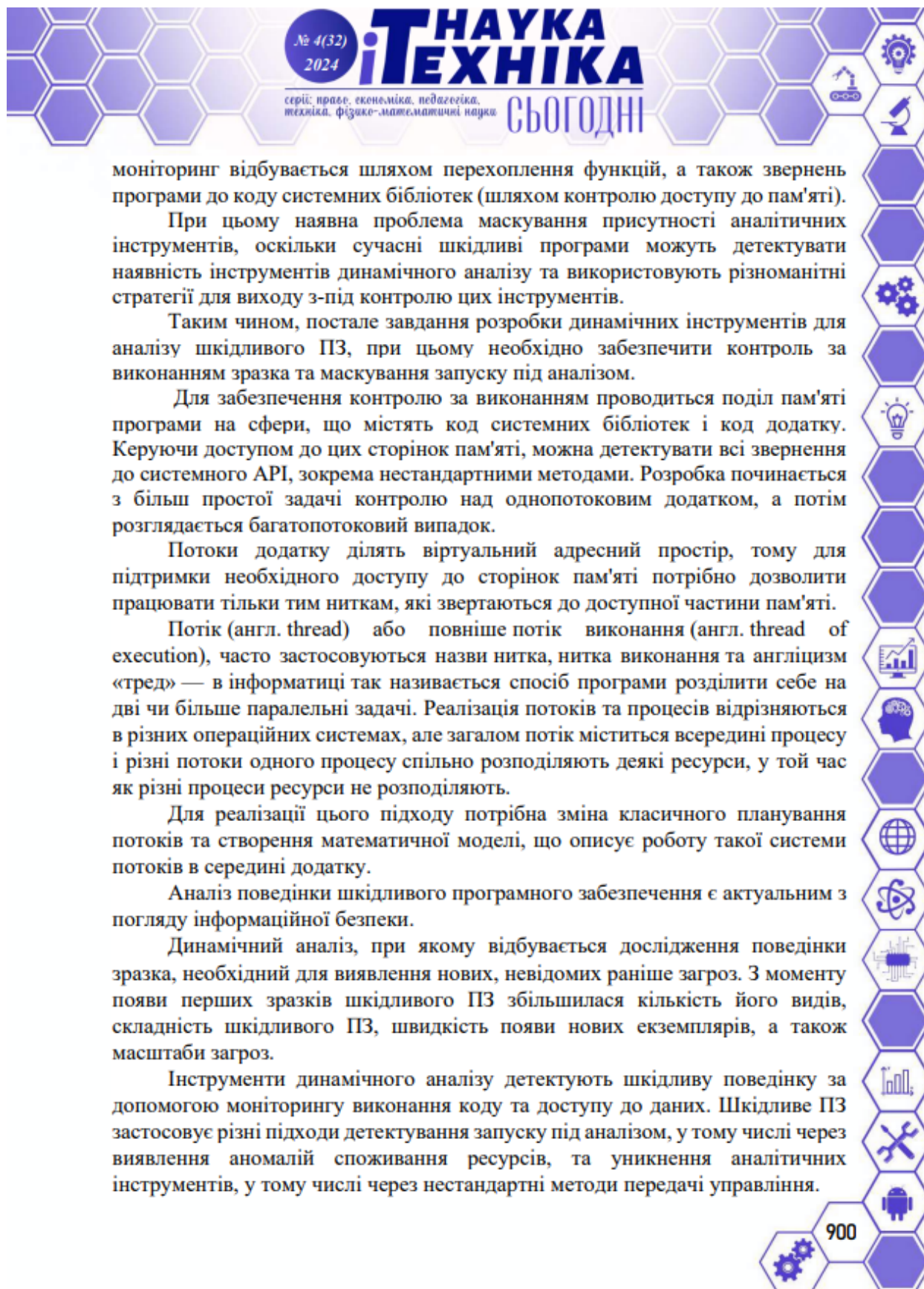
Існує безліч методик виявлення невідомого шкідливого ПЗ. Кожна з них має свої переваги, недоліки та особливості використання. Проте на даний момент не існує методики, яка б повністю вирішувала всі завдання виявлення шкідливих програм з прийнятною ефективністю. Отже актуальним напрямком є дослідження сучасних методів виявлення таких програм. Метою таких досліджень є аналіз і систематизація основних методів виявлення шкідливого ПЗ та дослідження особливостей їх застосування.

Актуальним є динамічний аналіз шкідливого програмного забезпечення, тобто такий аналіз, який відбувається під час виконання програми. Було б доцільним проектування програмно-апаратного комплексу для безпечного запуску досліджуваних зразків на тестових серверах.

Виконання досліджуваних програм здійснюється під контролем інструментів динамічного аналізу, які виконують моніторинг роботи зразка. Щоб вплинути на роботу системи, яка є об'єктом зараження (отримати доступ до файлів, інших процесів тощо), додатку необхідно звертатися до операційної системи.

Аналітичні інструменти відстежують взаємодію зразка з операційною системою через інтерфейс (API), який надає система. Інструменти, що розроблюються названі інвазивними, оскільки код аналізатора впроваджується у цільову програму, застосовуються патчі коду цільової програми, а

899



моніторинг відбувається шляхом перехоплення функцій, а також звернень програми до коду системних бібліотек (шляхом контролю доступу до пам'яті).

При цьому наявна проблема маскування присутності аналітичних інструментів, оскільки сучасні шкідливі програми можуть детектувати наявність інструментів динамічного аналізу та використовують різноманітні стратегії для виходу з-під контролю цих інструментів.

Таким чином, постало завдання розробки динамічних інструментів для аналізу шкідливого ПЗ, при цьому необхідно забезпечити контроль за виконанням зразка та маскування запуску під аналізом.

Для забезпечення контролю за виконанням проводиться поділ пам'яті програми на сфери, що містять код системних бібліотек і код додатку. Керуючи доступом до цих сторінок пам'яті, можна детектувати всі звернення до системного API, зокрема нестандартними методами. Розробка починається з більш простої задачі контролю над однопотоковим додатком, а потім розглядається багатопотоковий випадок.

Потоки додатку ділять віртуальний адресний простір, тому для підтримки необхідного доступу до сторінок пам'яті потрібно дозволити працювати тільки тим ниткам, які звертаються до доступної частини пам'яті.

Потік (англ. thread) або повніше потік виконання (англ. thread of execution), часто застосовуються назви нитка, нитка виконання та англіцизм «тред» — в інформатиці так називається спосіб програми розділити себе на дві чи більше паралельні задачі. Реалізація потоків та процесів відрізняються в різних операційних системах, але загалом потік міститься всередині процесу і різні потоки одного процесу спільно розподіляють деякі ресурси, у той час як різні процеси ресурси не розподіляють.

Для реалізації цього підходу потрібна зміна класичного планування потоків та створення математичної моделі, що описує роботу такої системи потоків в середині додатку.

Аналіз поведінки шкідливого програмного забезпечення є актуальним з погляду інформаційної безпеки.

Динамічний аналіз, при якому відбувається дослідження поведінки зразка, необхідний для виявлення нових, невідомих раніше загроз. З моменту появи перших зразків шкідливого ПЗ збільшилася кількість його видів, складність шкідливого ПЗ, швидкість появи нових екземплярів, а також масштаби загроз.

Інструменти динамічного аналізу детектують шкідливу поведінку за допомогою моніторингу виконання коду та доступу до даних. Шкідливе ПЗ застосовує різні підходи детектування запуску під аналізом, у тому числі через виявлення аномалій споживання ресурсів, та уникнення аналітичних інструментів, у тому числі через нестандартні методи передачі управління.





серед: право, економіка, педагогіка,
техніка, фізико-математичні науки

СЬОГОДНІ

Таким чином, вирішення таких завдань, як забезпечення контролю за виконанням досліджуваної програми та маскування аналітичних інструментів, є актуальним.

Сутність сучасних розробок полягає в пропозиції нового підходу до динамічного аналізу, заснованого на забезпеченні контролю над аналізованим зразком за допомогою поділу виконуваної пам'яті на два класи, математичної моделі планування при поділі потоків на два пула за класом виконуваної пам'яті та алгоритму чесного ієрархічного планувальника для даної моделі, методів маскування аналітичних інструментів, заснованих на перехопленні API та контролю над плином часу для досліджуваного ПЗ.

Для практичного виконання такого завдання виконуються роботи за такими етапами:

1. Розробка інструментів динамічного аналізу ПЗ, при цьому:
 - а. здійснення моніторингу активності додатку (низькорівневих подій процесу, таких як виклики системного API);
 - б. забезпечення контролю за доступом до коду додатку та системного коду.
2. Розробка математичної моделі та алгоритму планування виконання потоків в умовах контролю за доступом до пам'яті та впровадження його в аналітичні інструменти, що розробляються.
3. Розробка механізмів маскування присутності аналітичних інструментів та деградації продуктивності системи через присутність аналітичних інструментів.

Інструменти, про які йдеться, базуються на таких методах, як перехоплення виклику функції та зміна прав доступу до сторінки. Приділяється увага маскуванню аналітичних інструментів. Антивірусне програмне забезпечення намагається виявити шкідливі програми, використовуючи різні методи, включаючи динамічний аналіз.

У свою чергу, кіберзлочинці адаптують шкідливе програмне забезпечення для ухилення від аналізу та проходження антивірусного сканування. Варто також відзначити, що наявність аналітичних інструментів може впливати на продуктивність ОС. Незвичайна зміна часу виконання програми може бути виявлено шкідливим програмним забезпеченням і зазначено як факт виконання під аналізом або в середовищі з обмеженими ресурсами.

Продуктивність також впливає на пропускну здатність аналітичної системи (тобто кількість екземплярів, які можна запустити під контролем аналітичних інструментів за одиницю часу). Зниження продуктивності можна замаскувати, контролюючи протягом часу процесу під час виконання під аналізом.

Історія шкідливого ПЗ та потенційно небажаного ПЗ (potentially unwanted application, PUA), його кількість треба розглядати з точки зору виділення етапів його розвитку: від перших самовідтворюваних програм у

№ 4(32)
2024

І НАУКА ТЕХНІКА

серії: право, економіка, педагогіка,
техніка, фізико-математичні науки

СЬОГОДНІ

1970-х роках до сучасного етапу (починаючи з 2004 р.), на якому шкідливе ПЗ стає засобом кримінального заробітку і з'являються значні сучасні загрози, такі як програми-вимагачі.

Ключовими подіями в історії розвитку шкідливого ПЗ та методів антивірусного захисту є такі, як поява вірусів, що шифрують свій код, поліморфних та метаморфних вірусів, подальший розвиток технологій шкідливого ПЗ включив в себе застосування прийомів анти-налагодження, що перешкоджають виконанню програми під контролем відладчика, та анти-реверсингу, що перешкоджають дизасемблюванню коду програми.

Технології антивірусного захисту включають в себе широке коло засобів від пошуку в базі даних сигнатур (реактивний захист) антивірусні рішення переходять до динамічного аналізу, запуску в контрольованому середовищі, а шкідливе програмне забезпечення починає детектувати такий запуск (наприклад, ознаки емуляції). Існують методи захисту від виявлення антивірусним сканером з боку шкідливого програмного забезпечення та методи їх обходу з боку аналітичних інструментів.

При цьому механізми, які використовуються обома сторонами, є досить схожими, і аналітичні програми змушені самі застосовувати «вірусні» технології. Це призвело до так званої гонки озброєнь у галузі маскування та ухилення від виявлення між експертами з інформаційної безпеки та розробниками шкідливого ПЗ. Шкідливе ПЗ може детектувати віртуальне оточення та припиняти свою роботу, маскуючи шкідливу активність у ситуаціях потенційного дослідження аналітичними інструментами.

Сучасні антивірусні програми використовують евристичні та емулятори та ведуть активний моніторинг того, що відбувається в операційній системі (проактивний захист). З'являється так званий next-gen підхід, при якому застосовуються методи штучного інтелекту (наприклад, машинне навчання). Розвиток та сучасний стан технологій захисту з боку апаратних засобів підтриманий операційною системою Windows (зокрема, такі технології, як DEP, CET, VBS), ключовими компонентами захисту Windows (такі як PatchGuard, HyperGuard, Code integrity guard).

Існуючі підходи до аналізу шкідливого ПЗ (статичний, динамічний та гібридний аналіз) використовують інструменти для здійснення статичного та динамічного аналізу. Питання запуску зразків шкідливого ПЗ, потребує розгляду у тому числі таких аспектів, як автоматизація та безпека. Запуск зразків шкідливого програмного забезпечення під контролем аналітичних інструментів вимагає наявності тестового середовища.

Дослідження потребують вирішення важливих питань автоматизації запуску зразків та отримання даних, продуктивності системи (вона визначає кількість зразків, яка може бути запущена та проаналізована, наприклад, протягом доби), а також безпеки запуску шкідливого ПЗ (щоб не допустити неконтрольованого зараження системи).

902



№ 4(32)
2024

НАУКА і ТЕХНІКА

серії: право, економіка, педагогіка,
техніка, фізико-математичні науки

СЬОГОДНІ

При створенні відповідного інструментарію використані відомості з області операційних систем, внутрішнього пристрою Windows та системного програмування. Описується формат файлів PE, що виконуються, таблиці імпорту та експорту. Також розглядається інжектування коду в адресний простір процесу, патч та перехоплення функцій.

Розглядається обробка виняткових ситуацій, структурний (SEH) та векторний (VEH) механізми. Відбувається планування потоків у Windows. Застосовується чесний підхід до планування та ієрархічний чесний планувальник. Перші алгоритми чесного планування було запроваджено для мереж та завдання формування трафіку (Weighted fair queueing, WFQ, Start-time fair queueing, SFQ). Далі вони були адаптовані для планування виконання CPU (Borrowed-virtual-time, BVT), включаючи підтримку багатопроцесорності (Surplus fair scheduling, SFS).

З'явився перший ієрархічний чесний планувальник CPU, що базується на SFQ. ОС Linux та гіпервізор KVM реалізували CFS (Completely Fair Scheduler), починаючи з версії ядра 2.6. Згадані вище алгоритми мають складність $O(\log N)$, що вважається проблемою.

Алгоритм Distributed Weighted Round Robin (DWRR) був розроблений для створення чесного ієрархічного планувальника $O(1)$ поверх класичного алгоритму Round Robin. При цьому можна розглянути ідеалізовану модель Generalized Processor Sharing (GPS), розрахунки затримок (короткочасних помилок з точки зору чесного планування) для GPS та реалістичного алгоритму DWRR та провести їх порівняння. DWRR працює поверх системного планувальника, який використовує черги готових потоків для кожного CPU (як у сімействі Windows NT, починаючи з Windows Server 2003), є розподіленою версією класу алгоритмів WRR (Weighted Round Robin), найбільш відомим представником якого є алгоритм DRR (Deficit Round Robin). Операційна система та додаток може стежити за плином часу за допомогою апаратних таймерів, представлених в системі, описується підрахунок часу на основі тиків і без використання тиків.

Відбувається розгляд величин, пов'язаних з часом, які використовує Windows (такі як системний час, час роботи Windows, час переривань) та API для їх отримання, лічильники продуктивності Windows та API для їх отримання. Також описуються проблеми віртуалізації часу та підхід гіпервізорів для їх вирішення.

Існує багато методів виявлення шкідливого коду у програмному забезпеченні. На сьогодні для виявлення шкідливих програм переважно використовують підхід на основі сигнатури або підхід, заснований на аномаліях. Методи, що базуються на сигнатурах, протягом десятиліть активно використовувались для антивірусного ПЗ. Сигнатура — це унікальна послідовність байтів, що є у шкідливому двійковому файлі та у файлах, які були пошкоджені цим шкідливим ПЗ. Сигнатура повинна містити тільки

903





унікальні рядки з цього файлу, настільки характерні, щоб гарантувати мінімальну можливість неправильного спрацьовування — це головний пріоритет будь-якої антивірусної компанії. Цей підхід швидкий і має високу точність. Але при всій своїй простоті має наступні значні недоліки.

1. Захист відбувається лише від відомих вірусів. Тут слід зазначити, що сигнатури, зазвичай, створюються так, аби покривати не один, а якомога більшу кількість вірусів — сімейство вірусів. Однак завжди існує така зміна виконавчого файлу, при якому сигнатура перестає виявлятися.

2. Постійне зростання бази даних сигнатур. Зі збільшенням кількості вірусів, їх типів, а також здатність вірусів змінюватися збільшується і швидкість наповнення бази.

3. При появі вірусу і до оновлення бази сигнатур клієнт вразливий для нової шкідливої програми. Тільки визначивши досліджуваний файл як вірус можна отримати його сигнатуру і додати в базу. Більш того, розробники шкідливих програм навчилися успішно обходити пошук сигнатур за допомогою обфускації тіла вірусу. Це змусило антивірусні компанії розробляти альтернативні способи захисту.

При підході виявлення аномалій розробниками антивірусного рішення формуються база даних дій, які вважаються безпечними. Якщо процес виконання програми порушує будь-який із цих заздалегідь визначених правил, він позначається як шкідливий. Хоча за допомогою методу, заснованому на аномаліях, є можливість для виявлення нових зразків шкідливих програм, натомість частота помилкових викликів є дуже висока.

Використовуються у багатьох антивірусних пакетах алгоритми аналізу послідовності команд з метою формування деякої статистики та прийняття рішень про можливість зараження для кожного об'єкта, що перевіряється. Вони отримали назву методів евристичного сканування. Причому, на відміну від сигнатурного методу, евристичний підхід може детектувати як відомі, так і невідомі віруси (тобто ті, що створені після евристичної обробки).

У цьому підході аналітики застосовують методи машинного навчання для класифікації шкідливих програм. Статичні, динамічні, візуальні представлення елементів, або їх комбінації використовуються для навчання класифікатора (classifier) на наборі даних, що складається як із шкідливих, так і з нешкідливих двійкових файлів. Різні техніки машинного навчання, такі як метод опорних векторів (support vector machine, SVM), випадкові ліси (random forest, RF), дерева ухвалення рішень (decision trees, DT), наївний баєсів класифікатор (naïve bayes, NB), k-найближчих сусідів (k-nearest neighbor, kNN) та посилення градієнта пропонуються для класифікації та виявлення зразків шкідливого ПЗ та їх відповідних класів, для фільтрації шкідливого ПЗ, яке вимагає подальшого дослідження аналітиком.

Статичний аналіз (Static Approach) — це процес аналізу бінарного шкідливого ПЗ без фактичного запуску коду. Шабини, виявлені при такому

НАУКА і ТЕХНІКА

серії: право, економіка, педагогіка,
техніка, фізико-математичні науки

СЬОГОДНІ

аналізі, включають рядки сигнатур, розподіл частоти послідовностей байтів або опкодів (opcode — operation code), n-грами на рівні байт або n-грами на рівні опкодів, виклики API (Application Programming Interface), структуру дизасембльованої програми тощо.

Загальним для всіх підходів на основі динамічного аналізу (Dynamic Approach) є виконання шкідливого програмного зразка у контрольованому середовищі для вилучення особливостей поведінки (віртуальна машина, емулятор, пісочниця тощо). Моніторинг поведінки здійснюється за допомогою таких інструментів, як Process Monitor, Process Explorer, Wireshark або Capture BAT.

Окремого статичного або динамічного аналізу недостатньо для точної та ефективної класифікації зразків шкідливих програм. Це відбувається тому, що окреме використання цих методів достатньо просто обійти, використовуючи обфускацію коду або різні техніки зупинення при виконанні. Також динамічним аналізом неможливо дослідити всі шляхи виконання програмного файлу. Контрольоване середовище, в якому здійснюється моніторинг шкідливого ПЗ, відрізняється від реального, програма може поводитися по-різному, тому що деяка поведінка шкідливого ПЗ може запускатися лише за певних умов, наприклад, за допомогою певної команди або на конкретну дату системи і, як наслідок, неможливо виявити у віртуальному середовищі. Тому були створені гібридні підходи (Hybrid Approach), які поєднують статичні та динамічні підходи одночасно для поліпшення виявлення та більшої точності класифікації шкідливих програм.

Ще одним напрямком є підходи до аналізу шкідливих програм, що засновані на візуалізації. Для візуалізації та редагування двійкового файлу було доступно кілька інструментів, які відображають файл у шістнадцятковому та ASCII-форматах, але не передають жодної структурної інформації для аналітика.

Є точка зору, що одним з найрозповсюдженіших та легких методів боротьби з хакерами - своєчасне оновлення програмного забезпечення, вірусних баз, інсталяція та налаштування брандмауера. Все що пов'язано з оновленням програмного забезпечення – це реакція на вже виявлені загрози. Тому оновлення програмного забезпечення не надає захист від щойно виявлених загроз. Єдиним ефективним методом виявлення нових загроз та створення ефективних локальних та мережових сигнатур це аналіз щойно виявленого шкідливого програмного забезпечення. Тому аналіз шкідливого програмного забезпечення є задачею актуальною. Але вирішення вищевказаної задачі численними дослідниками мають різноманітні недоліки:

1. Розроблено метод оцінки зрілості екосистем але не розглянуто оцінку шкідливого програмного забезпечення, яке здатне проникнути в цю екосистему. В результаті заражена вірусною програмою екосистема буде працювати неналежним чином, або на користь зловмисника.
2. Побудована математична модель кіберзахисних дій, що дозволяє оцінити вартість кіберзахисту але не розглянуті методи забезпечення кіберзахисту.

НАУКА і ТЕХНІКА

серії: право, економіка, педагогіка,
техніка, фізико-математичні науки

СЬОГОДНІ

3. Розглянуті технології для поліпшення безпеки польотної зони. Але автори не врахували той факт, що програмні системи керування можуть контролюватися зловмисником. Для ефективного усунення зламу необхідно буде аналізувати код програми, за допомогою якої зламник контролює систему.

Метод виявлення шкідливого коду складається з таких етапів:

1. Аналіз та пошук строк;
2. Аналіз структури файлів;
3. Аналіз дизасембльованого тексту.

Аналіз та пошук строк. Строка в програмі являє собою деяку послідовність символів. Наприклад send. Якщо програма копіює будь-яку інформацію, звертається за url або IP адресою, виводить сповіщення, створює файл - це ознаки того, що програма містить строки.

Здійснюючи пошук строк в програмі можна скласти уявлення про загальний функціонал програми. Припустимо, якщо програма звертається за url або IP адресою, то в програмі можна знайти відповідні строки, що містять url, IP адресу, номер порта. Строки зберігаються в програмі в форматі ASCII, або Unicode та закінчуються нульовим символом, що вказує на кінець строки.

Існує безліч програм, які здатні шукати строки в програмах. Наприклад, Strings. Ця програма дозволяє шукати строки в файлах будь-якого типу ігноруючи при цьому контекст та форматування. Але при цьому може виявити строки, що такими не є.

На рис. 1 показано уривок результату пошуку строк в шкідливій програмі, що була виявлена на комп'ютері.

p@@@	
%\0@	
[Window: %s - at %s]	(1)
1337	(2)
127.0.0.1	(3)
[BACKSPACE]	(4)
[ENTER]	(5)
[SPACE]	(6)
[TAB]	(7)
[SHIFT]	(8)
[CONTROL]	(9)
SetWindowsHookExA	(10)
CallNextHookEx	(11)
GetKeyState	(12)
USER32.dll	(13)
WS2_32.dll	(14)

Рис. 1. Уривок результату пошуку строк в шкідливій програмі.



№ 4(32)
2024

НАУКА і ТЕХНІКА

серії: право, економіка, педагогіка,
техніка, фізико-математичні науки

СЬОГОДНІ

Строка (1) являє собою формат для текстового сповіщення. Строки (2), (3) є портом та IP адресою відповідно. IP адреса була змінена навмисно для безпечного запуску програми. Інформація, що міститься в строках (4)–(9) наводить на думку, що цей файл є кейлоггером, що передає зібрану інформацію за зазначеною IP адресою. Це припущення підтверджується інформацією, що міститься в строках (10)–(14). SetWindowsHookExA, що займає строку (10), встановлює визначену програмою процедуру перехоплення сповіщень в ланцюжок перехоплень. Може використовуватись для моніторингу системи щодо певних типів подій. Ці події пов'язані або з певним потоком, або з усіма потоками на одному робочому столі, з якого був викликаний потік. Буква «A» у кінці API функції означає, що ця функція працює зі строками ASCII. CallNextHookEx, що займає позицію (11) передає інформацію про перехоплення до наступної процедури перехоплення в поточному ланцюжку перехоплень. Процедура перехоплення може викликати цю функцію до або після обробки інформації про перехоплення. GetKeyState, що розташована в позиції (12) отримує статус вказаного віртуального ключа. Статус визначає те, що клавіша натиснута, не натиснута або перемикається (по черзі при кожному натисканні клавіші натискається і відпускається). Бібліотека USER32.dll містить елементи графічного інтерфейсу користувача та WS2_32.dll містить функції роботи з мережею. Під час аналізу структури файлів необхідно вивчити вміст заголовків файлів та секцій. Під час аналізу дизасембльованого тексту за допомогою дизасемблера вивчається вміст ключових фрагментів коду отриманого вихідного тексту.

Висновки. Оскільки на даний момент не існує ефективної методики виявлення невідомого шкідливого програмного забезпечення, тому для проведення ефективного пошуку і знищення шкідливих програм потрібно комбінувати всі сучасні методи, способи і засоби, враховуючи всі особливості їх використання. Складний вірус CaddyWiper може перетворити будь-яку машину, проти якої він розгорнутий, на непотрібний пристрій. Традиційним рішенням безпеки кінцевих точок важко запобігти таким атакам, як CaddyWiper. Завдяки своїй поліморфній природі CaddyWiper приховує свою функціональність від моніторингу під час виконання та зіставлення шаблонів. Реактивні та статичні антивірусні програми (AV) і рішення для виявлення та реагування на кінцеві точки (EDR) потребують вдосконалення, щоб запобігти APT і знизити ризики порушень.

Література:

1. Войтович О.П., Віток В.О., Каплун В.А. Особливості дослідження ознак шкідливого програмного забезпечення без наявності вихідних кодів. Інформаційні технології та комп'ютерна інженерія. 2013. № 3. С. 4-9.
2. Козачок В.А., Рой А.А., Бурячок Л.В. Технології протидії шкідливим програмам та завідом фальшивому програмному забезпеченню. Сучасний захист інформації. 2017. № 2 (30). С. 30-34.

3. Леонов Б.Д., Серьогін В.С. Удосконалення методичного забезпечення експертних досліджень спеціальних програмних засобів у сфері протидії кіберзлочинності. Інформація і право. № 4(31)/2019. С. 98-106.

4. Марущак А.І. Інформаційно-правові аспекти протидії кіберзлочинності Інформація і право. № 1(18)/2018. С. 127-132.

5. Про електронні комунікації: Закон України від 16.12.20 р. № 1089 URL: <https://zakon.rada.gov.ua/laws/show/1089-20#Text>

References:

1. Vojtovich, O.P., Vitjuk, V.O., Kaplun, V.A. (2013). Osoblivosti doslidzhennja oznak shkidlivogo programnogo zabezpechennja bez najavnosti vihidnih kodiv [Peculiarities of studying the signs of malicious software without the presence of source codes]. *Informacijni tehnologii ta komp'juterna inzhenerija - Information technology and computer engineering*, 3, 4-9 [in Ukrainian].

2. Kozachok, V.A., Roj, A.A., Burjachok, L.V. (2017). Tehnologii protidii shkidlivim programam ta zavidom fal'shivomu programnomu zabezpechennju [Anti-malware and anti-counterfeit software technologies]. *Suchasnij zahist informacii - Modern information protection*, 2 (30), 30-34 [in Ukrainian].

3. Leonov, B.D., Ser'ogin, V.S. (2019). Udoskonalennja metodichnogo zabezpechennja ekspertnih doslidzen' special'nih programnih zasobiv u sferi protidii kiberzlochinnosti [Improvement of methodological support for expert research of special software tools in the field of combating cybercrime]. *Informacija i parvo - Information and law*, 4(31)/2019, 98-106 [in Ukrainian].

4. Marushhak, A.I. (2018). Informacijno-pravovi aspekti protidii kiberzlochinnosti [Informational and legal aspects of combating cybercrime]. *Informacija i parvo - Information and law*, 1(18)/2018, 127-132 [in Ukrainian].

5. Zakon Ukraїni "Pro elektronni komunikacii" [The Law of Ukraine "On electronic communications"]. (n.d). *zakon.rada.gov.ua* Retrieved from <https://zakon.rada.gov.ua/laws/show/1089-20#Text> [in Ukrainian].