Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

на тему
Метод і система управління інформаційною безпекою підприємства

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

КРМКБ.220183.22.01.10 ПЗ

Виконав: студент 2 курсу, група КБм-22-1 _____ Душко Д.О.
Підпис

Керівник доц., к.т.н, доцент _____ Орленко В.С.
Підпис

Нормоконтролер старший викладач _____ Мостовий С.В.
Підпис

До захисту допускаю:
Зав. кафедри кібербезпеки, к.т.н., доц _____ Кльоц Ю.П.
Підпис

8 12 2023 р.

Хмельницький, 2023

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Освітній рівень Магістр

Галузь знань 12 Інформаційних технологій

Спеціальність 125 Кібербезпека

Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ

Зав. кафедри Ю.П. Кльоц

"30" 08 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Душку Дмитру Олександровичу

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Метод і система управління інформаційною безпекою підприємства

Керівник роботи Орленко Вікторія Сергіївна

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

кандидат технічних наук, доцент

Затверджена наказом № 30 ректора університету, додаток №25 від 15.08.2023

2. Строк подання студентом проєкту (роботи) на кафедру 01.12.2023

3. Вихідні дані до проекту (роботи) Розробка адаптивних методів управління інформаційної безпекою в сегменті корпоративної мережі, розробка моделей протидії загрозам та розробка системи прийняття рішень щодо оперативного управління

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити) Вступ. Аналіз проблем захисту інформації. Постановка задачі дослідження. Модель порушника. Методи аналізу інформації та оцінки захищеності ІС. Розробка системи прийняття рішень. Висновки.

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень) Тема, мета кваліфікаційної роботи, наукова новизна, практична значимість, публікації. Дослідження предметної області. Модель порушника. Метод оцінювання ризику ІС. Графи зв'язків варіантів реагування і результатів. Структура системи. Висновки.

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали і посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Мостовий С.В. Старший викладач кафедри кібербезпеки		

7. Дата видачі завдання «01» вересня 2023р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Вибір напряму дослідження і узгодження тематики КРМ з керівником	01.06.2023	
2	Ознайомлення з предметною областю; формулювання мети і задач дослідження; визначення об'єкта і предмета дослідження	04.09.2023	
3	Робота над розділом 1 – наявні методи управління захищеністю інформації; моделі захищеності; постановка задачі	18.09.2023	
4	Робота над розділом 2 – розробка моделей і методів для вирішення поставленої задачі	02.10.2023	
5	Робота над розділом 3 – розробка алгоритмів і технологій, їх аналіз	16.10.2023	
6	Робота над розділом 4 – апробація запропонованих рішень	06.11.2023	
7	Робота над науковою публікацією	10.11.2023	
8	Узгодження отриманих результатів, оформлення пояснювальної записки згідно вимог	15.11.2023	
9	Попередній захист роботи	17.11.2023	
10	Захист роботи на засіданні ЕК	06.12.2023	

Студент _____ Д.О. Душко
Підпис Ініціали, прізвище

Керівник проекту (роботи) _____ В.С. Орленко
Підпис Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: Метод і система управління інформаційною безпекою підприємства

Автор роботи: Душко Дмитро Олександрович

Керівник роботи: к.т.н., доц. Орленко Вікторія Сергіївна

Загальний обсяг роботи: 87 сторінок, 13 рисунків, 10 таблиць, 1 додаток, 65 посилань.

Ключові слова: захист інформації, корпоративна мережа, управління захищеністю.

Системи управління інформаційною безпекою діють у ситуаціях невизначеності та обмеженої інформації про стан інформаційного середовища. Тому для ефективного управління потрібен системний аналіз та інтелектуальна підтримка.

В роботі представлено розробку адаптивних методів управління інформаційною безпекою в сегменті корпоративної інформаційної системи з метою забезпечення необхідного рівня інформаційної безпеки в умовах невизначеності та наявності атак. Реалізовано структуру системи інтелектуальної підтримки прийняття рішень при оперативному управлінні захистом інформації.

5.12.2023

ANNOTATION

Theme of qualification work: Method and system of managing information security of the enterprise

Author of the work: Dushko Dmytro Oleksandrovych

Mentor: Ph.D., Assoc. Viktoriya Serhiyivna Orlenko

Total volume of work: 87 pages, 13 figures, 10 tables, 1 appendix, 65 references.

Keywords: information protection, corporate network, security management.

Information security management systems operate in situations of uncertainty and limited information about the state of the information environment. Therefore, effective management requires system analysis and intellectual support.

The work presents the development of adaptive information security management methods in the segment of the corporate information system in order to ensure the necessary level of information security in conditions of uncertainty and the presence of attacks. The structure of the intelligent decision-making support system for the operational management of information protection has been implemented.

5. 12. 2023

ЗМІСТ

ВСТУП

Сучасний етап розвитку обміну інформацією характеризується інтенсивним використанням передових інформаційних технологій та поширенням різних рівнів мереж - локальних, корпоративних та глобальних. Цей розвиток створює значний потенціал для використання обміну інформацією в різних галузях бізнесу. Управління бізнесом та можливості розширення його впливу в різних сферах визначаються корпоративними інформаційними системами), які включають в себе інфраструктуру та різноманітні інформаційні послуги. Інфраструктура охоплює мережі, сервери, робочі станції та відділи, розташовані по всьому світу.

Широке використання інформаційних технологій ставить підвищені вимоги до інформаційної безпеки через наявність загроз для захисту інформації. Сучасні теоретичні та практичні розробки, які спрямовані на забезпечення безпеки інформації, мають свої особливості. Зокрема, вони акцентують увагу на безпеці інформаційних об'єктів, встановлюють високі стандарти для забезпечення інформаційної безпеки, дотримуються міжнародних норм і стандартів щодо гарантій інформаційної безпеки. Проте, враховуючи зростаючу кількість кібератак та загроз, витрати на забезпечення інформаційної безпеки також зростають, оскільки збитки, завдані власникам інформаційних ресурсів внаслідок комп'ютерних атак, зростають.

Сучасні підходи до організації інформаційної безпеки не завжди відповідають вимогам інформаційної безпеки. Основні недоліки існуючих систем забезпечення інформаційної безпеки зазвичай пов'язані із складністю архітектури та застосуванням, в основному, стратегій оборонного характеру проти відомих загроз.

Системи управління інформаційною безпекою є складними організаційно-технічними системами, які діють у ситуаціях невизначеності та обмеженої інформації про стан інформаційного середовища. Тому для ефективного управління потрібен системний аналіз та інтелектуальна підтримка. Проблеми забезпечення інформаційної безпеки широко вивчені вченими, але все ще

недостатньо розроблені методи адаптивного захисту інформації, спрямовані на автоматизацію управління інформаційною безпекою систем, забезпечуючи необхідний рівень захисту протягом усього життєвого циклу системи.

Мета даної роботи полягає в розробці адаптивних методів управління інформаційною безпекою в сегменті КІС з метою забезпечення необхідного рівня інформаційної безпеки в умовах невизначеності та інформаційних атак.

Для досягнення вищезазначеної мети в роботі потрібно розв'язати такі завдання: провести аналіз КІС як об'єкта інформаційного захисту і розробити системну модель для протидії інформаційним загрозам; обґрунтувати необхідність розвитку адаптивних методів досягнення заданого рівня інформаційної безпеки в сегменті КІС на основі аналізу основних підходів до вирішення проблеми забезпечення інформаційної безпеки; запропонувати модель для боротьби з інформаційними загрозами в сегменті КІС, що ґрунтується на виборі оптимальних стратегій реакції на інформаційні загрози, з урахуванням оперативних даних про стан інформаційного середовища; розробити схему побудови системи управління інформаційною безпекою з використанням методів інтелектуальної підтримки при прийнятті рішень.

Методологічною основою дослідження є створення системи управління захистом інформації в сегменті корпоративної інформаційної системи на основі формування керуючої інформації.

Для виконання цієї роботи використано різні методи, включаючи системний аналіз, методи теорії управління, теорії множин, методи нечіткої логіки, теорії ймовірностей, теорії прийняття рішень та теорії захисту інформації.

Практичне значення дослідження полягає в можливості використання розробленої структури системи захисту інформації для створення системи захисту інформації корпоративних систем. Даний підхід може бути корисним для підвищення рівня інформаційної безпеки та забезпечення ефективного управління захистом інформації в організаційному контексті.

1 АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ У СЕГМЕНТІ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

1.1 Сутність проблеми управління захищеністю інформації

Сучасні корпорації мають складну розподілену структуру, обумовлену багатопрофільною діяльністю, розташуванням підрозділів на різних територіях і численними корпоративними зв'язками з партнерами. Термін "корпоративні системи" відноситься зазвичай до систем управління підприємством, які мають розвинуту структуру і окремі органи управління. Ці системи можуть включати організаційні, інформаційні та інші компоненти. Більшість бізнес-процесів та управлінських функцій підприємств і організацій покривають КІС, які є важливим інструментарієм для здійснення діяльності.

Впровадження нових інформаційних технологій завжди супроводжується виникненням нових ризиків для підприємств. Складність структури корпоративних інформаційних систем безпосередньо впливає на рівень ризику, пов'язаний з ними. Цей ризик може включати проникнення ззовні, несанкціонований доступ зсередини підприємства, фінансові махінації, розкриття комерційних таємниць, зміни чи знищення інформації та інші загрози. Такі ризики можуть призвести до серйозних втрат для підприємства. Створення високорівневого та надійного інформаційного середовища стало необхідною умовою розвитку окремих корпорацій, а також важливим чинником для розвитку економіки, суспільства та держави в цілому. Тому питання безпеки інформації в сегменті КІС в даний час набули надзвичайної важливості.

Корпоративні інформаційні системи (КІС) представляють собою поєднання людино-машинних і соціо-технічних систем, які включають в себе інформаційну складову підприємства. Для вивчення таких систем використовуються різні види моделей. Процес функціонування КІС підприємства відбувається в умовах взаємодії підприємства, розглядається як соціо-технічна система з одного боку, і сукупність конкурентів, зловмисників, природних катастроф та інших факторів і

подій з іншого боку.

Зростання складності та розширення сучасних КІС призводять до збільшення кількості мережевих пристроїв та інших засобів захисту інформації, що в свою чергу породжує велику кількість подій у сфері безпеки.

Слід зауважити, що сучасні технологічні процеси випереджають теоретичні осмислення та практичні розробки у сфері інформаційних технологій і нових комунікаційних можливостей. Це свідчить про те, що існуючі теоретичні концепції можуть бути недостатньо адаптовані до потреб сучасного інформаційного захисту, як з практичного, так і з теоретичного погляду.

Серед основних недоліків широко використовуваних систем захисту інформації можна визначити їх обмеженість з огляду на суворі архітектурні принципи та спрямованість на використання в основному захисних або наступальних стратегій захисту від відомих та найбільш небезпечних загроз.

Для вирішення цих проблем та ефективного використання сучасних корпоративних інформаційних систем необхідне адекватне управління не лише мережами, а також системою захисту інформації та всіма заходами, які забезпечують безпеку мережі. Це означає, що потрібні методи, які дозволили б швидко виявляти зміни в операційному середовищі системи та запобігати можливим порушенням інформаційної безпеки, керуючи як мережевим обладнанням, так і обладнанням безпеки.

На сьогоднішній день ефективним підходом до забезпечення інформаційної безпеки в КІС є використання інтелектуальних інструментів для підтримки прийняття рішень у сфері управління інформаційною безпекою.

Наразі активно розробляється інтегрована система управління інформаційною безпекою, яка охоплюватиме всю інфраструктуру організації та дозволить керувати інформаційною інфраструктурою незалежно від масштабу КІС. Структуроване представлення усіх аспектів управління захистом інформації можна побачити на рисунку 1.1.

Рисунок 1.1 - Структурування проблеми управління захистом інформації

У сучасному світі практично неможливо знайти виробників, які б надавали споживачам повний набір апаратних та програмних засобів, необхідних для побудови систем захисту інформації, які б відповідали сучасним вимогам. Більшість систем захисту інформації складаються з компонентів, які виробляються різними виробниками. Для забезпечення надійності захисту інформації в різноманітних корпоративних інформаційних системах потрібна система управління інформаційною безпекою, яка може гарантувати правильну конфігурацію кожного з її компонентів та надавати автоматичну підтримку у процесі ухвалення рішень щодо захисту інформації, постійно відстежуючи зміни, що відбуваються, та контролюючи діяльність користувачів мережі.

Такий комплексний підхід до вирішення цієї проблеми дозволяє створити дійсно безпечне середовище для функціонування корпоративних інформаційних систем підприємства.

Проведений аналіз дає підстави стверджувати, що на рівні сегменту КІС система управління, що відповідає за кілька важливих функцій, має функціонувати незалежно:

– отримувати і оцінювати об'єктивні дані щодо поточного рівня безпеки КІС (аудит);

– керувати подіями, за якими здійснюється протоколювання;

– визначати склад модульних компонентів системи захисту інформації та

точки, де створюються інструменти для забезпечення безпеки інформації в корпоративній комп'ютерній мережі підприємства.

Міжнародний стандарт ISO/IEC 27001 описує моделі, що використовуються для створення, впровадження, експлуатації, постійного моніторингу, аналізу, обслуговування та покращення систем управління інформаційною безпекою (СУІБ).

Особливості проектування та реалізації СУІБ компанії визначаються її потребами, цілями, вимогами до захисту інформації, розміром і структурою організації. Для ефективного функціонування необхідно ідентифікувати різні види діяльності та ефективно керувати ними.

Процесний підхід до управління захистом інформації, передбачений цим стандартом, допомагає виділити наступні аспекти:

– визначення принципів, цілей, процесів і процедур, що стосуються управління ризиками і покращення захисту інформації для досягнення результатів, що відповідають цілям компанії;

– впровадження та функціонування нормативних документів, засобів контролю, процесів і процедур СУІБ;

– оцінка та вимірювання показників процесів, пов'язаних з політикою, цілями і практичним досвідом управління захистом інформації, а також проведення аналізу цих показників;

– здійснення коригувальних та запобіжних заходів на основі результатів внутрішнього аудиту та аналізу з метою постійного покращення управління захистом інформації.

Система управління інформаційною безпекою включає в себе:

– організаційну структуру;

– політику і заходи планування;

– набір процедур, процесів і ресурсів.

Метою системи управління інформаційною безпекою є проектування, впровадження, експлуатація, постійний контроль, аналіз та покращення системи

захисту інформації. Для створення такої системи підприємству необхідно виконати наступні кроки:

– визначити межі системи;

– розробити принципи захисту інформації, враховуючи законодавчі вимоги та встановлені цілі захисту;

– розробити критерії для оцінки значущості ризиків;

– вибрати методологію оцінки ризику, яка відповідає системі управління інформаційною безпекою та відповідає нормативним вимогам, і забезпечити, щоб оцінки ризику надавали конкретні результати;

– визначити прийнятний рівень ризику;

– ідентифікувати ризики, включаючи активи, загрози, негативні впливи, що можуть призвести до втрати конфіденційності, цілісності та доступності активів та критичних вразливостей у системі;

– оцінити значущість ризиків, враховуючи ймовірність порушень інформаційної безпеки у контексті існуючих загроз та вразливостей. Оцінити рівні ризику та визначити, чи ризики є прийнятними, чи вимагають відповідної реакції;

– розглянути можливості управління ризиками, включаючи застосування заходів зменшення чи прийняття ризику;

– вибрати методи управління та обробки ризиків, які враховують критерії для прийняття ризиків;

– здійснити затвердження використання СУІБ з керівництвом та підготувати заяву про ступінь застосування, включаючи мету управління, засіб керування та обґрунтування вибору.

Етап реалізації та експлуатації СУІБ підприємства включає такі дії:

– формулювання плану обробки ризику, який визначає необхідні кроки управління ризиками, потрібні ресурси та відповідальність;

– виконання цього плану, включаючи фінансування;

– впровадження інструментів управління, спрямованих на досягнення цілей управління;

– запровадження процедур та інших засобів управління, які дозволяють виявляти події в системі і реагувати на інциденти в системі;

– швидке виявлення існуючих та минулих порушень і інцидентів у системі;

– виявлення подій у системі і запобігання інцидентам, використовуючи індикатори;

– вимірювання результативності інструментів управління для перевірки виконання вимог;

– оновлення планів захисту інформації для врахування даних, отриманих під час діяльності, пов'язаної як з постійним контролем, так і з аналізом.

Для відповідного планування і реалізації СУІБ критичним є підготовка документації, яка повинна включати в себе опис методики оцінювання ризику, плани зниження ризику та докладні процедури, необхідні для успішного планування та впровадження СУІБ.

Міжнародний стандарт ISO/IEC 17799 встановлює рекомендації, які слід дотримуватися під час розробки СЗІ. В стандарті визначається мета управління та перелік інструментів для управління. Мета політики інформаційної безпеки полягає в забезпеченні визначення напрямків та підтримки керівництвом системи інформаційної безпеки згідно з бізнес-вимогами та вимогами законодавства. Політику інформаційної безпеки слід регулярно оцінювати з визначеною періодичністю, щоб забезпечити її відповідність та адекватність.

З точки зору управління активами, мета полягає в забезпеченні та підтримці необхідних ресурсів для захисту активів організації в умовах робочого середовища, що вимагає чіткої визначеності. Важливо створити та підтримувати реєстри важливих активів, а також активів, які пов'язані з обробкою інформації. Ця інформація повинна бути класифікована за її важливістю та критичністю для компанії.

Важливо, щоб ролі та обов'язки співробітників та користувачів щодо інформації та її захисту були чітко задокументовані у відповідності до політики

інформаційної безпеки в компанії.

Мета управління мережевою безпекою полягає в забезпеченні захисту інформації в мережах і забезпеченні безпеки мережевої інфраструктури. Ефективне керування мережею є необхідним для захисту від ризиків.

Метою постійного моніторингу є виявлення дій, пов'язаних з обробкою інформації. Важливо розробити процедуру для постійного моніторингу використання інструментів, які використовуються для обробки інформації, та регулярно перевіряти результати цього моніторингу.

Метою управління доступом користувачів є гарантування належного доступу для зареєстрованих користувачів і запобігання несанкціонованому доступу до КІС. Призначення та використання дозволів повинні бути контрольовані і обмежені, встановлення паролів має бути підконтрольним формальним процесом, який проводить адміністратор. Важливо створити формальну процедуру реєстрації користувачів.

Метою управління інцидентами в СЗІ є забезпечення того, щоб всі події та вразливості, пов'язані з КІС, були вчасно повідомлені та виправлені шляхом впровадження коригувальних заходів. Для цього необхідно встановити відповідальність керівництва і процедури швидкого, ефективного та регламентованого реагування на всі інциденти в СЗІ. Важливо мати механізм, який дозволяє класифікувати типи і обсяги інцидентів в СЗІ та проводити постійний контроль над ними.

В моделі зрілості процесів управління інформаційною безпекою, де найвищим рівнем є "керований" і "оптимізований". Рівень "керований" характеризується моніторингом на об'єкті захисту та оцінкою процесів управління, з оптимізацією та частковим впровадженням автоматизації. Рівень "оптимізований" характеризує високий рівень опрацьованості процесів управління інформаційною безпекою, здатність до швидкої адаптації в разі змін у бізнес-процесах і комплексне використання заходів захисту, які створюють основу для поліпшення процесів управління.

Основні кроки, які необхідно виконати, включають в себе процес управління

інформаційною безпекою:

– планування - це процес аналізу та оцінки ризиків інформаційної безпеки, визначення політик СУІБ, вибір заходів для захисту і їх оновлення з метою мінімізації ризиків, прийняття рішень щодо впровадження системи управління інформаційною безпекою;

– використання та експлуатація системи управління інформаційною безпекою включає розробку планів з обробки ризиків інформаційної безпеки, реалізацію заходів щодо захисту, управління її функціонуванням, виявлення та реагування на виникаючі інциденти безпеки;

– перевірка (Моніторинг і аналіз) включає аналіз продуктивності, включаючи аналіз рівнів залишкового ризику інформаційної безпеки, а також аналіз внутрішніх аудитів системи управління інформаційною безпекою;

– вдосконалення СУІБ, включає в себе використання тактичних і стратегічних поліпшень у системі, що вимагають прийняття рішень на рівні планування та оцінки досягнення мети.

Аналіз існуючих стандартів управління безпекою дозволив зрозуміти, що вони спрямовані на створення загальних концепцій і моделей управління безпекою, але не включають конкретних підходів до управління інформаційною безпекою в корпоративних інформаційних системах.

1.2 Інфраструктура розподіленої корпоративної інформаційної системи і модель захищеності інформації в ній

КІС в сучасних компаніях є важливим інструментом для керування бізнесом та виробництва. Структура КІС включає два основних компонента:

– інформаційна інфраструктура, що становить матеріальну базу та середовище для операцій інформаційної служби компанії;

– інформаційні послуги, які надаються користувачам на основі інформаційної інфраструктури.

Інфраструктура компанії і сучасного суспільства може бути організована таким чином, що включає в себе просторово розподілені підрозділи компанії, а також її партнерів, клієнтів і постачальників. Основні взаємодії між цими суб'єктами відбуваються в рамках розподіленої КІС, і вони використовують пристрої та комунікаційні канали, надані операторами зв'язку, і користуються різними мережевими програмами та послугами.

Сегментація мережі за територіальною приналежністю є ключовим принципом структури розподіленої КІС. Основною складовою одиницею КІС є розподілений сегмент. Кожен розподілений сегмент може включати складну інформаційну систему, яка працює на регіональному рівні. Кожен сегмент КІС може включати робочі станції, сервери і мережу, яка включає маршрутизатори, комутатори, цифрові модеми, телефонні лінії, оптоволоконні і бездротові зв'язкові канали.

На рисунку 1.2 відображено результат структурного розподілу КІС.

Впровадження Інтернету в корпоративні комунікації привело до суттєвого зростання числа користувачів зовнішніх мереж, розширення різноманітності каналів зв'язку та призводить до використання нових мережевих та інформаційних технологій. Це підвищило вимоги до безпеки у всіх аспектах корпоративних мереж, включаючи сервери, маршрутизатори, сервери віддаленого доступу, мережеві канали, операційні системи, бази даних та додатки. Ризики для кожного компонента системи забезпечення безпеки постійно зростають, і ця тенденція буде продовжуватися і надалі.

Проблема внутрішніх загроз інформаційній безпеці також актуальна, особливо для великих корпорацій, які мають розподілені підрозділи. У таких великих організаціях, де працює багато співробітників та функціонує значна кількість обчислювальної техніки, існує велика ймовірність виникнення серйозних інцидентів, які можуть призвести до витоку конфіденційної інформації або пошкодження корпоративної бази даних, що містить важливу інформацію для конкурентоспроможності компанії.

Чим більша компанія та обсяги її фінансових операцій, тим більше зростає

ймовірність спрямованих і професійних атак, які можуть бути впроваджені інсайдерами. З розвитком і інтеграцією інформаційних технологій у корпоративні бізнес-процеси збільшується небезпека внутрішніх загроз інформаційній безпеці.

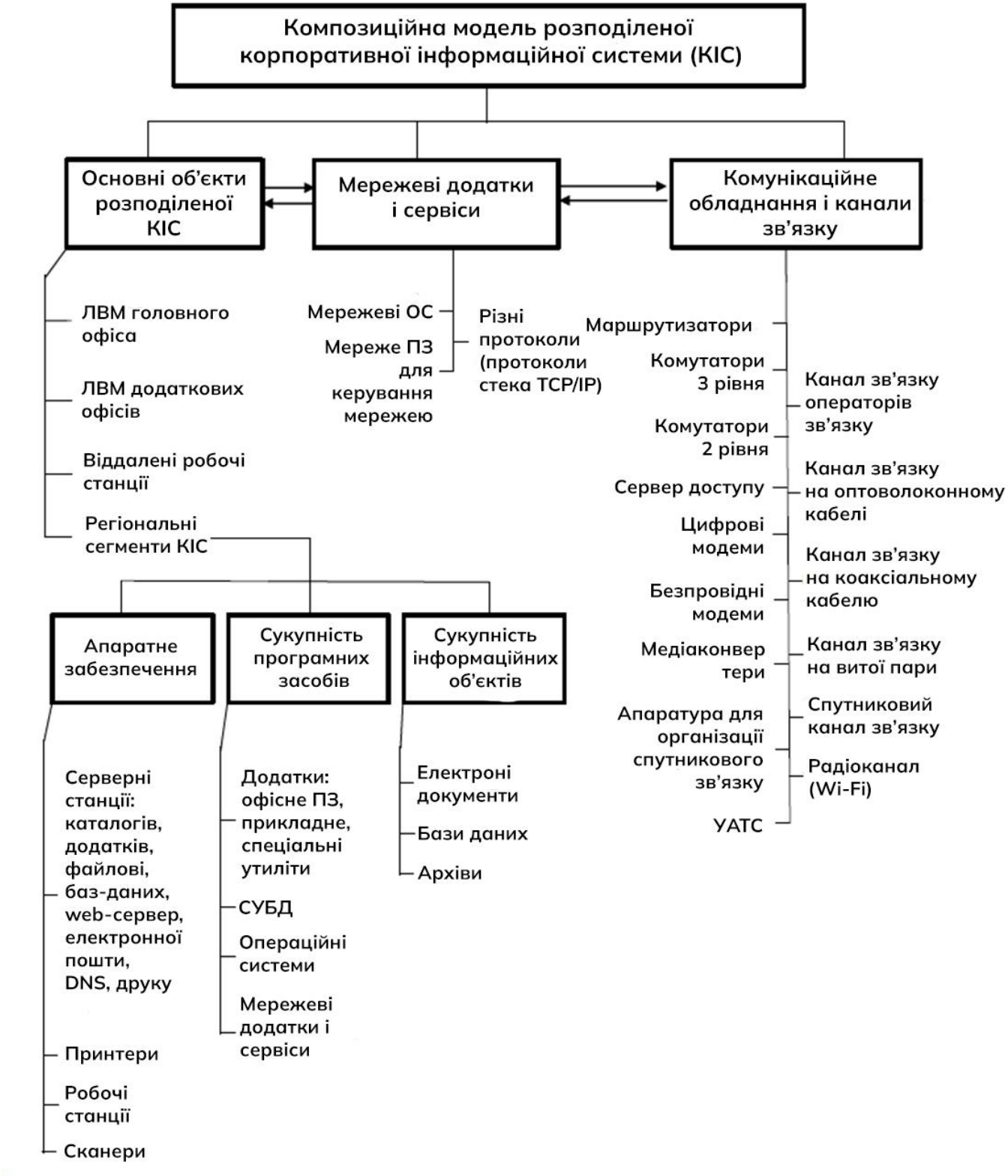

Рисунок 1.2 - Модель розподіленої КІС із деталізацією

Сучасні методи злому комп'ютерних мереж та крадіжки інформації швидко розвиваються, на рівні з іншими високотехнологічними галузями інформаційних технологій. Тому забезпечення інформаційної безпеки КІС стає однією з найважливіших пріоритетів для керівництва компаній. Збереження конфіденційності, цілісності та доступності інформаційних ресурсів компанії значно впливає на якість і швидкість процесу прийняття стратегічних рішень керівництвом компанії.

Вирішити завдання щодо забезпечення інформаційної безпеки КІС можна шляхом створення ефективної СУІБ.

Модель елементів СЗІ для корпоративних інформаційних систем відображено на рисунку 1.3.

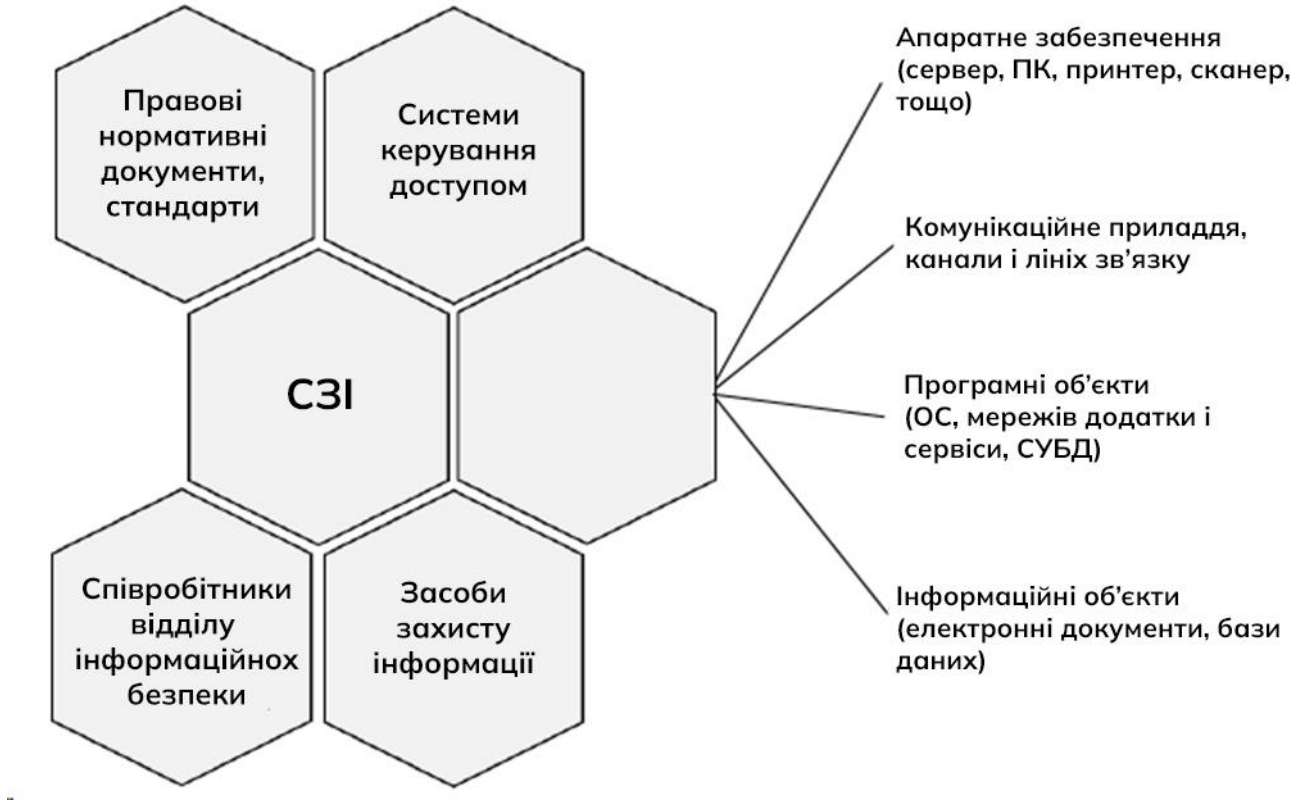

Рисунок 1.3 - Модель елементів СЗІ для КІС

СУІБ повинна відповідати вимогі абсолютної прозорості для вже існуючих додатків в межах КІС, а також вимогі сумісності з використовуваними

корпорацією мережевими технологіями.

Для забезпечення надійного захисту ресурсів КІС, СЗІ мають базуватися на сучасних та перспективних технологіях в галузі інформаційної безпеки.

Отже, для забезпечення успішної діджиталізації в корпорації необхідно гарантувати параметри безпеки інформаційних ресурсів, такі як цілісність, конфіденційність та правдивість ділової інформації, що циркулює в локальних та глобальних інформаційних мережах.

1.3 Сучасні концепції захищеності інформації в корпоративних інформаційних системах

Розробка та вдосконалення шкідливого програмного забезпечення продовжує активно розвиватися, і це відбувається паралельно з постійним вдосконаленням систем захисту. Кіберзлочинці активно використовують нові досягнення в галузі інформаційних технологій, такі як хмарні обчислення, нові алгоритми шифрування та інше. За даними звіту Cisco з кібербезпеки, для того щоб скоротити час виявлення кіберзлочинців, фахівці з кібербезпеки все частіше використовують та закуповують інструменти, які використовують штучний інтелект і машинне навчання. Шифрування, з одного боку, допомагає підвищити безпеку, але, з іншого боку, зростання обсягу як легітимного, так і шкідливого зашифрованого трафіку, створює проблеми для тих, хто відповідає за виявлення потенційних загроз і моніторинг їхньої активності. Протягом останніх 12 місяців експерти з кібербезпеки в Cisco зафіксували більш як триразове зростання обсягу зашифрованого мережевого трафіку від зразків шкідливого програмного забезпечення.

Використання інтелектуальних технологій та машинного навчання демонструє добрі результати в сфері інформаційної безпеки, оскільки з часом ці технології автоматично виявляють нетипові шаблони в зашифрованому веб-трафіку, у хмарних обчисленнях та середовищах Інтернету речей. Поступове вдосконалення технологій машинного навчання та штучного інтелекту з часом

допоможе зменшити кількість "хибних спрацювань" і дозволить точно визначати "нормальну" мережеву активність, відрізняючи її від реальних атак.

Атаки можуть впливати на комп'ютери в масштабах великих мереж, а їхні наслідки можуть тривати місяці або навіть роки. Важливо пам'ятати про потенційні ризики використання програмного і апаратного забезпечення від організацій, які не дотримуються серйозного підходу до проблем інформаційної безпеки.

Для зменшення ризику атак на ланцюжок поставок важливо переглянути процедури стороннього аудиту, щоб оцінити ефективність технологій інформаційної безпеки. Захист інформаційних систем стає складнішим з ростом різноманітності вразливостей.

Організації, щоб захистити себе, використовують складні комбінації програмних та апаратних застосунків різних виробників. Ця збільшена складність при зростаючій різноманітності вразливостей негативно впливає на здатність організацій захищати свою інформацію від атак і призводить, серед іншого, до збільшення фінансових ризиків та можливих втрат.

Згідно звіту Cisco:

– у 2020р. 25% фахівців з інформаційної безпеки повідомили, що використовують продукти від 11-20 вендорів, в 2019р. так відповіли 18%;

– фахівці з інформаційної безпеки повідомили, що 32% вразливостей торкнулися більше половини систем, у 2019 р. так відповіли 15%;

– фахівці з інформаційної безпеки оцінили користь засобів поведінкового аналізу виявлення шкідливих об'єктів: 92% фахівців вважають, що засоби поведінкового аналізу добре справляються з поставленою завданням; 2/3 представників сектора охорони здоров'я і представники індустрії фінансових послуг вважають поведінкову аналітику корисний для виявлення шкідливих об'єктів;

– зростає використання хмарних технологій; зловмисники користуються відсутністю просунутих засобів забезпечення безпеки;

– 27% фахівців з інформаційної безпеки повідомили про використання зовнішніх приватних хмар (показник 2019 р. — 20%); з них 57% розміщують мережу в хмарі заради кращою захисту даних, 48% - заради масштабованості, 46% - заради зручності експлуатації.

Хоча хмара забезпечує підвищену безпеку даних, зловмисники користуються тим, що компанії не дуже добре захищають хмарні конфігурації, що розвиваються і розширюються. Ефективність захисту таких змін підвищується за рахунок використання комбінації передових технологій, таких як машинне навчання та інструменти безпеки світового класу, такі як хмарні платформи інформаційної безпеки.

В останні роки також спостерігається тенденція до зростання шкідливих програм та часу виявлення. Ключовим фактором для Cisco в процесі скорочення часу виявлення і підтримки його на низькому рівні стала технологія інформаційної безпеки. Чим коротший час виявлення, тим швидше атаку буде зупинено.

Щодо описаних тенденцій, додатковими рекомендаціями для підрозділів інформаційної безпеки, є:

– контроль за дотриманням політик і практик компанії щодо оновлення додатків, систем та пристроїв;

– своєчасне отримання точних даних про загрози і наявність процесів використання цих даних для моніторингу безпеки;

– проведення поглибленого аналізу;

– регулярне резервне копіювання даних і перевірка процедур відновлення - критичні дії в контексті швидкого розвитку мережевих здирників та шкідливих програм;

– виконання перевірок безпеки на мікро сервісах, хмарних сервісах та системах адміністрування додатків.

Багато компаній використовують механізми для інтеграції управління засобів захисту інформації у традиційні системи управління мережею. Однак цей тип інтегрованої системи управління є дорогими, а деякі питання управління

інформаційної безпекою не вирішуються такими системами.

Ефективна система управління ІБ мережевої КІС повинна супроводжуватися системою ієрархічного управління, що складається із:

– централізованого управління на рівні глобальної політики щодо інформаційної безпеки, відповідної до бізнес-процесів підприємства і визначати набір правил безпеки для всіх взаємодій об'єктів КІС, а також об'єктів КІС і зовнішніми об'єктами;

– системи протоколювання подій у мережі, моніторингу та аудиту, які можуть працювати автономно в конкретній підсистемі КІС.

Для того щоб забезпечити інформаційну безпеку в сегменті КІС в сучасних умовах компанії почали використовувати усе більше автоматизованих СУІБ на основі систем SIEM.

Найбільш широке поширення на ринку SIEM-систем отримали системи, що використовують сигнатурні методи кореляції подій інформаційної безпеки, що обумовлено насамперед простотою реалізації даних систем, а також гнучкістю при інтеграції в систему і подальшої експлуатації. До таких систем відносяться: HP ArcSight; IBM QRadar; Symantec SIM; RSA Envision та інші. Недоліком є те, що системи, збудовані за цим принципом, не адаптуються до умов швидко змінного складу КІС через заздалегідь вбудовані у систему випадки інформаційної безпеки. До недоліків таких систем також відноситься велика кількість хибних спрацьовувань і відносна складність конфігурації та реалізації.

Покращена аналітика на великих даних BigData відіграє важливу роль у SIEM-системах, використовуваних в сегменті КІС. Великий інтерес представляє технологія UEBA (User and Entity Behavior Analytics - поведінкова аналітика користувачів і сутностей) для інтеграції в SIEM-системи. Один з найбільш корисних варіантів застосування модуля UEBA - це виявлення інсайдерів шляхом детектування статистичних аномалій. Якщо співробітники, що володіють легітимним доступом до інформації, починають нестандартно діяти, робити більше запитів або отримувати інформацію за блоками даних, до яких раніше не отримували, то самонавчені системи безпеки будуть видавати відповідні

сповіщення.

Можна констатувати тенденцію розвитку автоматизованих систем управління захистом інформації для сегменту КІС. Однак існуюча методологія інформаційного ризик-менеджменту не передбачає комплексний підхід до управлінню інформаційним ризиком. Використання економіко-математичних моделей управління захистом інформації не завжди орієнтовано на досягнення кінцевого результату бізнес-процесів, що призводить до зниження ефективності управління ризиками всього підприємства.

1.4 Постановка задачі

Мета кваліфікаційної роботи магістра – розробка методу і системи управління інформаційною безпекою підприємства. Для досягнення поставленої мети слід виконати наступне:

– проаналізувати наявні рішення та розробити оптимальні методи аналізу інформації для ідентифікації атак та оцінки захищеності системи;

– змоделювати аналіз факторів інформаційного ризику на основі лінгвістичного підходу;

– побудувати модель системи захисту;

– розробити модель прийняття рішень в випадку потенційно можливої міжсегментної атаки;

– розробити модель прийняття рішень щодо реагування у разі потенційно можливого зовнішнього вторгнення по радіоканалу;

– розробити модель прийняття рішень щодо реагування у разі потенційно можливого зовнішнього вторгнення через периметр через лінії зв'язку;

– розробити структуру системи інтелектуальної підтримки прийняття рішень задля оперативного управляння захистом інформації.

2 МЕТОДОЛОГІЧНІ ОСНОВИ УПРАВЛІННЯ ЗАХИСТОМ ІНФОРМАЦІЇ У КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

2.1 Основні науково-теоретичні підходи до розробки систем управління захистом інформації

Захист інформації та методи його забезпечення є предметом активного обговорення. Продовжують розробляти нові методи, способи та засоби забезпечення безпеки інформації, створюються нові системи захисту та проводяться науково-дослідні роботи з розробки методики управління захистом інформації.

Аналіз результатів науково-дослідних робіт в галузі захисту інформації показує, що значні досягнення в теорії захисту інформації досягнуті у роботах, присвячених розробці нових засобів захисту інформації різних видів, які забезпечують безпеку інформації на різних рівнях (технічні пристрої, програмно-апаратні комплекси, криптографічні засоби захисту і таке інше), а також інтегровані системи захисту інформації. Результати таких змін та досліджень представлені в роботах багатьох авторів. Ключовим висновком цього роду досліджень є створення основ теорії захисту інформації.

Масове використання інформаційних технологій корпораціями, значне зростання обсягу критично важливої інформації, яка зберігається та передається у цифровому форматі, а також підвищення важливості захисту інформації, є факторами, що підштовхнули активізацію теоретичних досліджень, пов'язаних із забезпеченням безпеки інформації. У роботах [1-3] розглядаються питання та проблеми комп'ютерної безпеки. Також актуальними є питання використання криптографічних методів і засобів у сфері захисту інформації [4-7], а також питання виявлення вторгнень [8-10].

Деякі роботи [11-12] підкреслюють важливість застосування системного підходу при розробці ефективних засобів захисту інформації. Вони відзначають необхідність створення моделей загроз, декомпозицію розроблюваних систем

захисту інформації на функціональні підсистеми для визначення факторів, які можуть впливати на них, та виявлення можливих загроз. Також, система індикаторів, яка характеризує ефективність системи захисту інформації, визнається важливою частиною цього процесу.

Багато авторів, які досліджують питання інформаційної безпеки, вважають, що для успішного вирішення цієї проблеми необхідно встановити методологічну основу для розглянутого питання, вивчити адаптивну організацію систем захисту інформації і також розглянути питання автоматизації систем захисту інформації [13-16].

Основою для розробки систем захисту інформації повинні слугувати плати обробки інформації, які встановлюються на захищуваному об'єкті, і проводити аналіз критичності. Відповідно до результатів аналізу формуються вимоги до системи захисту інформації. На основі сформульованих вимог розробляється набір засобів для забезпечення відповідного рівня захисту. Аргументоване обґрунтування складу системи захисту інформації є важливою частиною управління системою захисту інформації.

Особливості проектування СЗІ розглядаються авторами в [17-18]. Аналіз робіт дозволяє виділити два основні підходи щодо побудови системи ЗІ:

– продуктний підхід;
– проектний підхід.

Підходи до забезпечення інформаційної безпеки можуть бути розділені на продуктний та проектний. В продуктному підході спочатку формується набір засобів захисту інформації, і потім на основі функцій, які ці засоби виконують, розробляється політика безпеки. У випадку проектного підходу спочатку формується політика безпеки, і потім, враховуючи певні вимоги, обираються засоби захисту інформації, необхідні для її реалізації.

Як вказано в [19-21], системи, розроблені з використанням проектного підходу, зазвичай краще оптимізовані та ефективні, що робить їх більш підходящими для використання в гетерогенних мережах. Також важливо зазначити, що рішення, розроблені з використанням проектного підходу, зазвичай

мають більший термін служби.

Основні принципи та методи вибору засобів захисту інформації на основі критерію оптимальності, який враховує мінімізацію витрат при досягненні певного рівня захисту інформації, описані в [22-25]. Ця методика базується на оцінці ефективності виконання різних функцій засобами захисту інформації.

Деякі автори, такі як [26-28], розглядають управління операціями та стратегічне планування використання засобів захисту як ключові процеси макроуправління. Оперативне управління включає динамічне управління інформаційною безпекою при її автоматизованій обробці. В рамках операційного управління важливим є постійне визнання стану системи захисту інформації і прийняття рішень щодо необхідних оперативних втручань для забезпечення безпеки. Для прийняття правильних рішень вибір повинен бути здійснений із попереднього реєстру рішень, що створюється заздалегідь.

Планування захисту інформації означає розробку програм, які протягом певного часового періоду дозволять оптимально використовувати бюджет, щоб забезпечити необхідний рівень захисту. Під оптимальністю розуміється досягнення необхідного рівня захисту при мінімізації витрат.

Багато авторів, які вивчають проблеми інформаційної безпеки, підкреслюють складність завдання прийняття рішень у цій області. Це завдання важке і водночас важливе для автоматизації управління інформаційною безпекою.

У роботах [29-31] відзначено, що обмеженням для задоволення зростаючих вимог щодо інформаційної безпеки є недостатність наявних науково-технічних засобів. Щоб забезпечити потрібний рівень захисту, необхідно, щоб науково-технічне забезпечення відповідало змінам в інформаційному середовищі і стратегіях інформаційного протистояння. На жаль, досліджень в цій області недостатньо, що є ще одним обмежуючим фактором для розвитку теорії управління інформаційною безпекою.

У роботі [32-34] наведено формалізований опис методів синтезу ідеальних стратегій управління інформаційною безпекою в моделях ігор для прийняття рішень. Також розглянуто методи управління квантуванням пакетів інформації

при передачі, відновлення цілісності інформації та оцінки інформаційної безпеки в умовах вірусних програм.

У дослідженні [35-36] управління інформаційною безпекою розглядається як організаційний процес. В рамках цього підходу, завдання забезпечення інформаційної безпеки можуть бути вирішені адміністративними групами, такими як менеджери і адміністратори безпеки, а також оператори. Управління інформаційною безпекою включає в себе контроль розподілу інформації в корпоративній мережі, забезпечення функціональної працездатності засобів захисту інформації, фіксацію подій, пов'язаних із порушеннями інформаційної безпеки, а також регулярне оновлення баз даних інформаційного захисту.

Роботи [37-38] розглядають основні науково-теоретичні питання, пов'язані із створенням адаптивних інформаційних систем забезпечення безпеки і їхнім використанням у комп'ютерних інформаційних системах. В цих дослідженнях особливий акцент робиться на тому, що не можливо гарантувати абсолютну безпеку окремих компонентів системи чи системи в цілому через відсутність часових обмежень. Тому доцільно розглядати лише той рівень захисту, для якого витрати на подолання можливих загроз перевищують користь від отримання інформації. Однак на сьогоднішній день є великою складністю формалізувати кількісну оцінку рівня інформаційної безпеки системи.

Важливо підкреслити, що ступінь ризику залежить від різних факторів, таких як цінність інформаційних ресурсів, ймовірність загроз і вразливість, а також ефективність заходів безпеки. Єдиним контрольованим фактором серед перерахованих є рівень захисту. Тож правильний вибір захисних заходів може знизити ризик до прийнятного рівня. Результати оцінки ризику становлять основу для обґрунтування вибору комплексу заходів для захисту системи.

Ефективність системи інформаційної безпеки залежить не лише від використовуваних продуктів і методів, але також від регулярного аудиту системи для виявлення вразливостей і моніторингу трафіку для виявлення можливих загроз і розробки рекомендацій для їх усунення.

Усі зазначені заходи мають взаємодіяти з персоналом служби безпеки КІС,

але вони можуть створювати складнощі для аналізу і оперативної реакції з боку адміністраторів безпеки. Отже, велика увага приділяється необхідності автоматизації процесу реагування на інформаційні загрози. Тому перед розробниками стоїть завдання створення та формалізації моделей прийняття рішень щодо класифікації інформаційних загроз за активністю та небезпекою для системи та реалізації заходів по їх запобіганню.

У роботах [39-41] розглянута багатокритеріальна модель оцінки безпеки та метод вибору міжмережевих екранів за допомогою методу нечітких множин. Також вивчено синтез підсистем аналізу безпеки та виявлення загроз, а також методи прийняття рішень в умовах інформаційних загроз.

Роботи [42-43] розглядають питання, пов'язані із адаптивним управлінням безпекою інформаційних систем в контексті захисту від несанкціонованого доступу. У цих дослідженнях розглянуто розробки підсистем управління інформаційною безпекою, які впроваджують концепцію адаптивного управління та використовують неявну користувацьку модель об'єкта управління в основному циклі. Крім цього, досліджено метод, який дозволяє визначити оптимальний склад і структуру системи захисту інформації на етапі проектування, використовуючи метод мінімаксу та враховуючи показник досяжності характеристик "еталонної" системи. Досліджується також метод зміни структури та модифікацій системи інформаційної безпеки під час її функціонування, який використовує критерій максимального підвищення рівня безпеки при обмеженні витрат.

Важливо зауважити, що створення "еталонної" системи захисту на різних етапах життєвого циклу інформаційної системи відзначається високою складністю.

2.2 Модель порушника

Модель порушника ІС - це концептуальне уявлення про типові характеристики, методи, мети та способи дії осіб або груп, які намагаються незаконно отримати доступ до інформації, зламати безпеку комп'ютерних систем

чи виконати інші атаки на цифрову інфраструктуру. Модель порушника допомагає аналізувати потенційні загрози для інформаційної безпеки та розуміти, які ризики можуть існувати для конкретних інформаційних систем.

Модель порушника ІС потрібна для систематизації даних про можливості та типи суб'єктів, цілі несанкціонованих впливів та вироблення адекватних організаційних та технічних методів протидії. При розробці моделі порушника ІС слід враховувати:

– категорії осіб, до яких можна віднести порушника;
– цілі, градації за рівнем небезпеки та важливості;
– аналіз його технічної потужності;
– припущення та обмеження про характер дій.

За наявності права разового чи постійного доступу порушники поділяються на два типи: порушники, які використовують зовнішні загрози та порушники, які мають доступ до ІС та використовують внутрішні загрози. У таблиці 2.1 наведено категорії осіб, які можуть використовувати внутрішні або зовнішні загрози.

Таблиця 2.1 – Типи порушників та відповідні категорії осіб

Тип порушника	Категорії осіб
зовнішній	кримінальні структури; відвідувачі; розвідувальні служби держав; особи, які випадково або навмисне порушили пропускний режим; будь-які особи за межами контрольованої території
внутрішній	персонал, що обслуговує технічні засоби (інженери, техніки); співробітники відділів; адміністратори ІС; працівники служби безпеки; керівники різних рівнів

Ще одну модель порушника показано на рисунку 2.1.

На підприємствах з метою зменшення ймовірності несанкціонованого доступу до різних частин підприємства, реалізовано метод створення меж захисту.

Територія підприємства ділиться на кілька зон, які ранжирувані за рівнем секретності та рівня доступу. У результаті має можливість для розмежування доступу до важливих інформаційних ресурсів. Прикладом може бути рисунок 2.2.

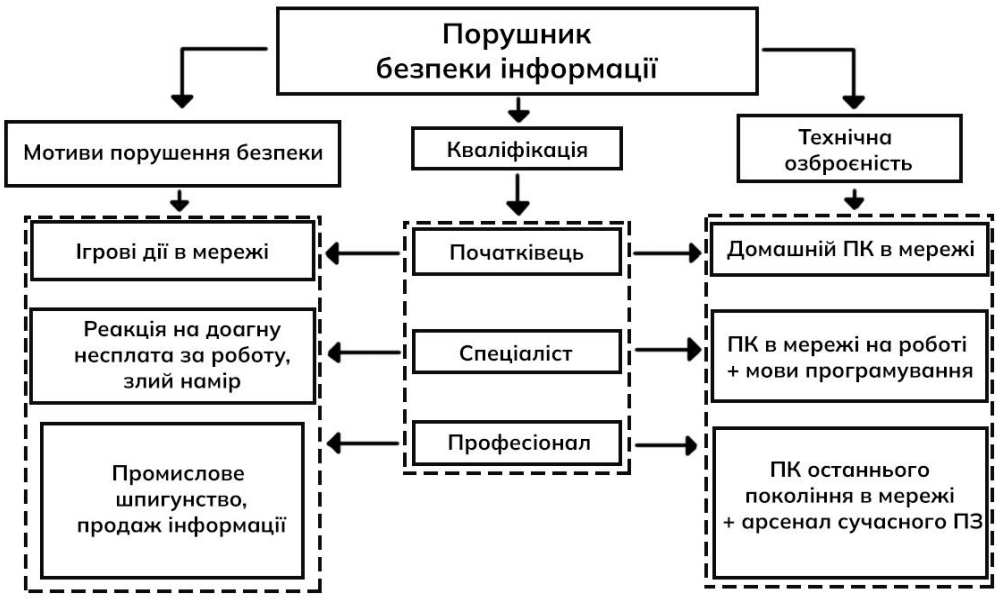

Рисунок 2.1 – Модель порушника

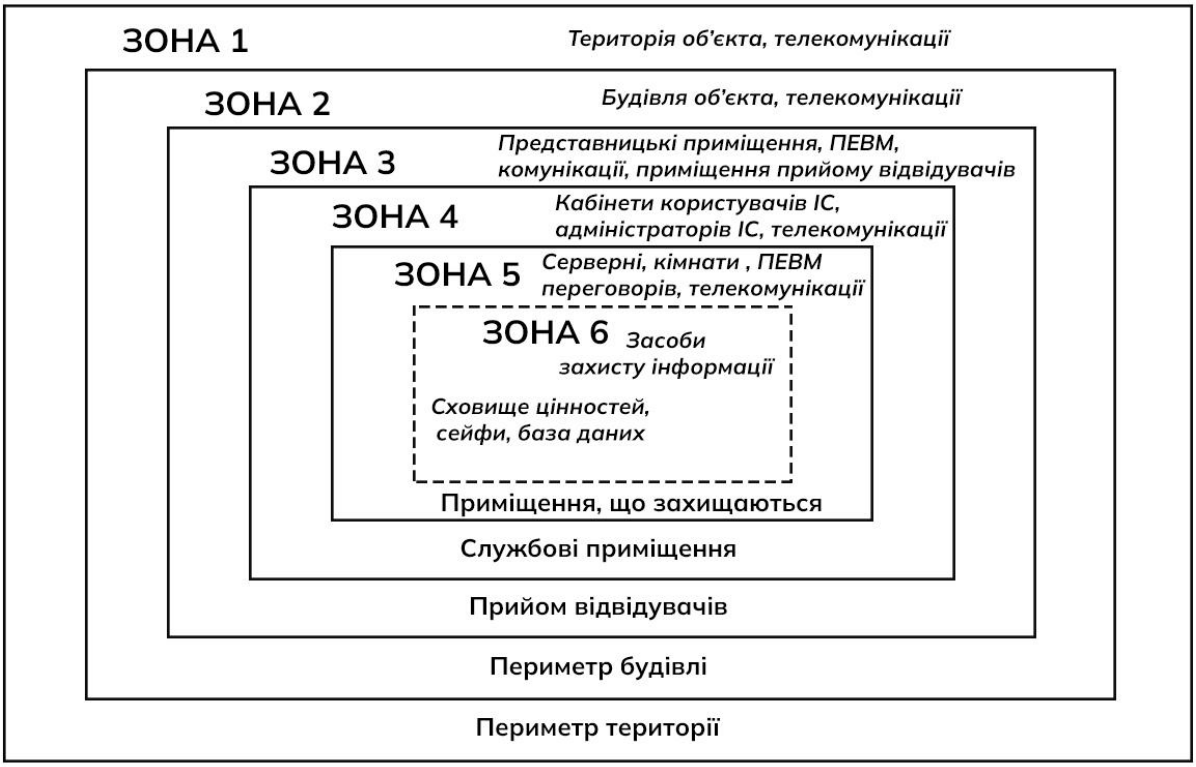

Рисунок 2.2 – Поділ підприємства на зони

У таблиці 2.2 наведено групи внутрішніх порушників щодо меж захисту підприємства та можливості доступу.

Таблиця 2.2 - Групи внутрішніх порушників

Позначення	Межа	Характеристика порушника	Можливості
1	2	3	4
M_1	Територія об'єкта, телекомунікації	Особи які мають санкціонований доступ на територію, але не мають доступу до будівель та приміщень	Дозволяє несанкціонований доступ до каналів зв'язку, які йдуть за межі будівлі. Перехоплення даних по технічних каналах.
M_2	Будинки об'єкта, телекомунікації	Особи мають санкціонований доступ на територію, будівлі, але не мають доступу до службових приміщень	Мати інформацію про розміщення поста охорони, систему відеоспостереження та приміщенні для прийому відвідувачів
M_3	Представницькі приміщення, ПЕОМ, комунікації	Особи що мають доступ до спеціальних приміщень, але не мають доступу до службових приміщень	Перехоплення даних по технічних каналах. Мати інформацію про розміщення поста охорони, систему відеоспостереження та приміщенні для прийому відвідувачів.

Продовження таблиці 2.2 - Групи внутрішніх порушників

1	2	3	4
M_4	Кабінети користувачів ІС, адміністраторів ІС	1. Зареєстровані користувачі ІС, які мають обмежений доступ до ресурсів. 2. Зареєстровані користувачі ІС які мають віддалений доступ до інформаційної системи. 3. Зареєстровані користувачі ІС з правами адміністратора безпеки сегмента. 4. Зареєстровані користувачі з правами системного адміністратора ІС. 5. Зареєстровані. користувачі з правами адміністратора безпеки ІС. 6. Програмісти-розробники ПЗ. 7. Особи, що реалізують обслуговування ІС	1. Мати доступ до шматків конфіденційних даних. Мати шматки даних про топологію ІС. Вносити програмно-апаратні закладки. 2. Має дані про топологію сегмента, має фізичний доступ до сегментів та елементів мережі. 3. Має повну інформації про ІС. 4. Має всю інформацію про ІС, має повний доступ. 5. Має доступ до методів захисту ІС. 6. Має дані про алгоритми та ПЗ для обробки даних в ІС. 7. Має доступ до внесення закладок у технічні засоби ІС.

Кінець таблиці 2.2 - Групи внутрішніх порушників

1	2	3	4
M_5	Серверні кімнати конфіденційних переговорів, ПЕОМ	1. Зареєстровані користувачі з правами адміністратора безпеки. 2. Зареєстровані користувачі з правами системного адміністратора. 3. Працівники які мають право доступу до приміщень конфіденційних переговорів.	1. Має доступ до налаштування сегмента мережі. 2. Має санкціонований доступ до приміщення, має своє ім’я користувачі та доступ до конфігурації ІС. 3. Має доступ до приміщення.
M_6	Методи захисту інформації	Зареєстровані користувачі сервера з правами адміністратора безпеки ІС	Має доступ до всіх приміщень, має доступ до всієї інформації про ІС

2.3 Методи аналізу інформації по ідентифікації атак

Методи аналізу інформації, виявлення атак та процеси прийняття рішень, які використовуються у системах захисту інформації, на останок визначають ефективність таких систем. Основні методи ідентифікації атак, що використовуються в цих системах, включають статистичну систему та експертні системи [44-46], а також методи що основані на нейронних мережах [47].

Статистичний метод базується на створенні статистичного профілю для кожного інформаційного суб'єкта в межах системи. Цей профіль адаптується до поведінки кожного суб'єкта, і потім здійснюється аналіз для виявлення відхилень від стандарту. Якщо такі відхилення виявляються (порівняно з еталоном), це

свідчить про можливу несанкціоновану діяльність. Основною перевагою цього методу є його універсальність та здатність функціонувати без попередніх знань про можливі види атак. Однак важкість полягає в невизначеності параметрів, які слід відстежувати, що ускладнює адекватну ідентифікацію аномальної активності. Ці методи можуть бути неефективними при реагуванні на раніше невідомі атаки.

Експертна система складається з набору правил, які включають в себе знання, надані експертом. Таким чином, всі інформаційні атаки представлені у формі правил, що визначають послідовність дій, які варто вживати в разі виявлення або підозри на інформаційну загрозу. Експертна база даних такої системи повинна містити знання або сценарії щодо більшості відомих інформаційних загроз та видів атак і потребує постійного оновлення. Однією з переваг цього підходу є мінімізація помилкових викликань, однак головним недоліком є неспроможність реагувати на незнану атаку, і, крім того, випадок, коли відома атака здійснюється з невеликими змінами, може призвести до неефективної реакції системи.

Незважаючи на існуючі недоліки, статистичний підхід та аналіз інформаційного простору на основі правил використовуються у більшості сучасних методів виявлення атак. Проте зі зростанням якісної і кількісної складності атак і збільшенням їх видів стає очевидним, що навіть за постійного оновлення бази даних експертної системи, такий підхід не може гарантувати виявлення всього різноманіття атак.

Відмінність нейромережевого підходу від експертних систем полягає в тому, що нейромережі здатні проводити аналітичну роботу та оцінювати відповідність між характеристиками роботи системи та тими, на які нейромережа навчена реагувати. Вони оцінюють наявність чи відсутність потенційних загроз, і таким чином визначають ступінь небезпеки. Нейронні мережі проходять навчання щодо ідентифікації об'єктів у предметній області на попередньо сформованих вибірках. Під час цього навчання мережа налаштовується для досягнення задовільних результатів розпізнавання. Протягом роботи і проведення аналізу, нейромережа набуває досвіду, що робить результати розпізнавання більш коректними. За

допомогою навчання в ході аналізу характеристик, нейромережа здатна ідентифікувати атаки та загрози, навіть ті, які їй раніше не зустрічалися.

Технологія адаптивного профілювання, розроблена на основі вивчення імунної системи людини, застосовується для забезпечення захисту найцінніших інформаційних ресурсів. Ця система демонструє високу точність в розпізнаванні мережевих атак або несанкціонованих дій. Технологія адаптивного профілювання працює подібно до імунної системи людини, спостерігаючи нормальну поведінку програм (спостереження за процесом виконання коду в штатному режимі в нормальних програмах). Потім навчена система аналізує роботу інформаційної системи і виявляє будь-які відхилення в конфігурації, помилки в програмному забезпеченні та інші вразливості. Такі виявлені проблеми ідентифікуються цією технологією, і здійснюється їх блокування (припинення роботи за допомогою системних викликів). Такий підхід виявляється ефективним для захисту серверних додатків.

Продовжуючи процес навчання, система набуває навичок розпізнавання припустимих змін у додатках, що в кінцевому результаті призводить до мінімізації хибних спрацювань. Ця технологія виявляється дієвою для захисту як від відомих раніше, так і від невідомих атак, навіть у випадку зашифрованої інформації.

Як у статистичних, так і у нейромережевих методах є свої переваги та недоліки. Крім того, багато систем захисту інформації та розробок у цій галузі мають закритий код та використовують невідому методологію.

За словами [48], методологічні та технологічні засади створення інтелектуальних засобів запобігання комп'ютерним атакам у КІС все ще перебувають на ранній стадії розробки. На сучасному етапі розвитку інформаційних технологій виникає велика потреба у розробці комплексних рішень для впровадження засобів оцінки та запобігання потенційно небезпечним подіям в інформаційних мережах, а також у керуванні засобами та мережевим обладнанням.

2.4 Методи оцінки захищеності інформаційної системи

Під час створення інформаційної структури (ІС) безсумнівно настає момент, коли потрібно вивчити та правильно оцінити ступінь захищеності цієї системи. Оцінка рівня захищеності важлива, але також складна задача, яка повинна враховувати багато різних аспектів. Серед них важливо враховувати, наскільки ефективно використовуються різні засоби і механізми захисту, а також які ризики та загрози існують для системи. Крім того, потрібно визначити, який рівень захисту є необхідним та достатнім в конкретному середовищі, де працює ІС. Це вимагає сформулювати і визначити критерії для оцінки загальної захищеності інформаційної системи. Ці питання активно вивчаються в багатьох дослідженнях і наукових роботах, таких як ті, які вказані в літературних джерелах [49-50].

Одним із ключових завдань при створенні систем інформаційного захисту є вибір критеріїв (формалізованих методів оцінки) для визначення рівня захисту системи. Під "формалізованими методами" розуміють способи оцінки "сили" конкретної характеристики або використання цифрової шкали для оцінки різних показників системи [51]. Концепція оцінки рівня захищеності шляхом використання різних критеріїв була введена, наприклад, в Помаранчевій книзі для застосування у системах управління базами даних та операційних системах.

Якщо ми маємо сформовану шкалу критеріїв для оцінки рівня захищеності ІС, то порівняти різні системи захисту можна шляхом простого порівняння числових показників, визначених для кожної з систем. Однак у сфері захисту від несанкціонованого доступу на жаль відсутня стандартизована шкала оцінки, що ускладнює процес порівняння різних систем. У ролі критеріїв для оцінки захищеності від несанкціонованого доступу можна розглядати показники, такі як інтенсивність атак на систему та ймовірність їхньої реалізації, розраховані на певний період часу. Проте існує проблема з такими показниками - вони є апостеріорними та можуть бути обмежено корисними на практиці.

Для більш об'єктивної оцінки реальної загрози реалізації атак, необхідно враховувати інші критерії. Ці критерії можуть включати умови використання ІС,

рівень кваліфікації користувачів, використовувані технології обробки та зберігання даних і інші параметри. Складністю є факт, що необхідно враховувати не лише категоризацію цих факторів, але й розробляти повний перелік можливих факторів, які можуть впливати на реалізацію можливих загроз в системі інформаційного захисту.

Найбільш оптимальним способом для практичної оцінки рівня безпеки інформаційної системи є використання апріорних критеріїв, що дозволяють уникнути обмежень, пов'язаних із апостеріорними показниками. Ці критерії можна визначити шляхом порівняння самої системи та її стану з набором еталонних профілів для сервісів інформаційного захисту. Якщо профілі забезпечують необхідний рівень безпеки за певних умов, то вони можуть бути використані як еталонні. Іншими словами, дві системи можуть мати однаковий рівень безпеки, якщо вони впроваджують однаковий набір захисних механізмів, які мають однакову "силу". Отже, система 1 може бути вищим рівнем безпеки, якщо хоча б один із реалізованих захисних механізмів має вищий рівень "сили" в порівнянні з механізмами системи 2. Також, система 1 може вважатися більш безпечною, якщо вона впроваджує механізми захисту, які взагалі відсутні в системі 2.

У дослідженні [52], автор запропонував наступну формулу для обчислення інтегрованого показника безпеки для ІС:

$$Z(T) = \Phi[K, R(T)], \qquad (2.1)$$

де K - показник цілісності обліку можливих стратегій атаки; R - показник ефективності застосування захисних стратегій, конструктивно закладених у СЗІ у тимчасовому інтервалі [0, T].

На прикладі формули 2.1 розглянуті різні варіанти створення функції Ф для різних інформаційних середовищ і ситуацій. Проте важливо зауважити, що дослідження не займається конкретним визначенням значень показників K і R. Відомо, що визначення цих показників є нетривіальною задачею. Частина необхідної інформації може бути отримана шляхом розрахунку вихідних

ймовірностей реалізації для різних загроз.

Останнім часом в підходах до аналізу ризиків рівень безпеки тісно пов'язаний із ризиками, а це означає, що рівень безпеки системи можна визначити на основі аналізу можливих ризиків і навпаки. Відповідно до праць у галузі управління ризиками [53-54], аналіз ризиків рекомендується проводити у таких випадках:

– суттєва зміна в структурі або оновлення інформаційної системи;

– зміна технологічних аспектів, пов'язаних із побудовою корпоративної системи;

– впровадження нових або додаткових підключень в компанії;

– розширення підключення до глобальних мереж, які раніше були недоступними;

– фундаментальні зміни в стратегії та тактиці ведення бізнесу в організації;

– запланована або непередбачена перевірка ефективності СЗІ.

У відповідності до попереднього дослідження, процес управління ризиками включає в себе наступні етапи:

– оцінка потенційних втрат, які можуть виникнути внаслідок реалізації ризиків;

– аналіз ідентифікації потенційних загроз в інформаційному середовищі;

– оцінка вразливостей інформаційної системи;

– вибір необхідних заходів і засобів захисту, які дозволять знизити ризик до прийнятного рівня в межах заданих фінансових обмежень.

Автори статті [55] описують управління ризиками як процес вибору та реалізації комплексу заходів, які мають на меті забезпечити потрібний рівень безпеки системи на основі попереднього аналізу ризиків. Згідно з цим дослідженням, на кожному етапі життєвого циклу інформаційної системи повинні бути впроваджені відповідні контрзаходи, охоплюючи різні аспекти безпеки, такі як:

– розробка та впровадження політики інформаційної безпеки та внесення змін у неї;

– створення та актуалізація регламентів для функціонування, обслуговування системи і посадових інструкцій;

– застосування додаткових програмно-технічних засобів захисту для забезпечення інформаційної безпеки.

Відповідно до роботи [56], процес оцінки ризиків інформаційної системи повинен ураховувати наступні чинники:

– оцінка цінності інформаційних ресурсів, які підлягають захисту;

– визначення значущості потенційних загроз та існуючих вразливостей;

– оцінка ефективності раніше розроблених (існуючих) та запланованих засобів захисту інформації.

Аналіз ризиків виконує важливу роль в контексті подальшої порівняльної оцінки різних можливих варіантів впровадження системи захисту. Це особливо актуально, враховуючи зростаючі вимоги до систем забезпечення інформаційної безпеки.

Міжнародний стандарт ICO/МЕК 15408, відомий як "Загальні критерії оцінки безпеки IT", встановлює чіткі та структуровані вимоги щодо інформаційної безпеки для різних класів інформаційних систем. Однак у цьому стандарті відсутня конкретна методологія для оцінки цих критеріїв. Проведений аналіз різних стандартів, що застосовуються в області управління ризиками інформаційної безпеки, як і зарубіжних, так і вітчизняних, показав, що ці стандарти не містять докладних вказівок щодо методології оцінки ризиків. Для успішного застосування їх на практиці потрібно надавати докладні вказівки. Крім того, для здійснення компетентної оцінки ризиків, важливо розробити додаткові методи, які враховують якісні та кількісні аспекти.

В роботі [57] підкреслюється важливість та актуальність створення науково-методологічної основи проблеми оцінки безпеки інформації.

Процес вирішення завдання щодо забезпечення заданого рівня захищеності

може бути поділений на дві послідовні задачі:

– оцінка в кількісному виразі рівня захищеності інформації в системі;

– аналіз даних та прийняття рішень стосовно необхідних налаштувань параметрів та властивостей системи захисту для підтримки необхідного рівня безпеки.

Очевидно, що для визначення кількісних показників критеріїв рівня безпеки необхідно прийняти рішення щодо коригування складу властивостей системи захисту. Крім того, необхідно враховувати динаміку змін в часі показників рівня безпеки, які базуються на змінах зовнішніх і внутрішніх умов інформаційної системи. Інструменти для оцінки параметрів рівня безпеки та аналізу існуючих ризиків в сфері інформаційної безпеки повинні дозволяти створювати об'єктно-орієнтовані структурні моделі інтелектуальної власності, а також моделі ризиків окремих сегментів комп'ютерно-інформаційної системи. Отже, можна зробити висновок, що створення та розвиток інтелектуальних СЗІ є серйозною науковою проблемою, яка вимагає розробки методів та методології, що є науково обґрунтованими та застосованими в рамках створення теорії інтелектуальної безпеки.

2.5 Висновки до розділу

Як показує проведений аналіз, роботи, спрямовані на вирішення проблем створення нових інформаційних засобів захисту різного характеру, представляють собою значні досягнення в галузі теорії захисту інформації. Вони стали основою для розробки нових методів створення комплексних систем захисту інформації.

Для побудови систем інформаційної безпеки загалом використовуються два основних підходи: продуктний і проектний. В продуктному підході виходять з уже наявних засобів захисту інформації, вибираючи необхідні кошти ЗІ, і на цій основі розробляють політику безпеки. Проектний підхід, навпаки, передбачає формування політики безпеки на першому етапі, і вже відповідно до цієї політики обираються відповідні засоби захисту інформації.

3 МОДЕЛЬ ОЦІНКИ РІВНЯ ІНФОРМАЦІЙНИХ РИЗИКІВ У СЕГМЕНТІ КОРПОРАТИВНИЙ ІНФОРМАЦІЙНОЇ СИСТЕМИ

3.1 Методологічна база дослідження інформаційних ризиків

Наукова література відводить велике місце проблемі управління захистом інформації, особливо у зв'язку з широким застосуванням інформації у сучасній діяльності корпорацій. При аналізі існуючих стандартів у галузі управління інформаційною безпекою [58] можна відзначити, що ці стандарти мають на меті сформулювати загальні концепції та послідовні етапи управління. Проте вони не надають конкретних підходів до процесів управління безпекою систем; вони встановлюють функціональні вимоги до засобів захисту, але не пропонують методів для порівняльного аналізу різних комплексів засобів захисту для вибору оптимального варіанту системи інформаційної безпеки.

Вчені розробили загальні принципи та інструменти для управління економічними ризиками. Математичні методи та інструменти економіко-математичного моделювання були розглянуті в роботах [59] та інших фахівців. Статистичні методи моделювання можуть бути застосовані для дослідження інформаційних ризиків в поєднанні з неформальними методами досліджень [60]. Управління інформаційними ризиками в умовах невизначеності може здійснюватися за допомогою гнучких методів, таких як інтервальний метод, нейронні мережі, генетичні алгоритми, а також застосування нечітких множин і нечіткої логіки.

Найкращим визначенням "інформаційного ризику" є поняття "загрози інформаційній безпеці". Інформаційний ризик можна оцінювати як потенційну подію, яка може вивести інформацію з-під контролю, спотворити її або порушити конфіденційність та доступність [61].

Інша група експертів визнає, що інформаційний ризик полягає в можливості понесення збитків, втрати прибутку і інших негативних наслідків для підприємства. Такий підхід визначається, наприклад, у наступному визначенні.

Інформаційні ризики - це можливість виникнення збитків або негативних наслідків через використання інформаційних технологій компанією. Іншими словами, ці ризики пов'язані з утворенням, передачею, зберіганням та використанням інформації, використовуючи електронні пристрої та інші засоби зв'язку.

Недоліком вищеописаного визначення є його нечітке охоплення об'єктів, збитків або змін у властивостях, які можуть призвести до втрат унаслідок ризикованих подій. Це визначення обмежує врахування інформаційних ризиків, які можуть бути пов'язані з процесом документообігу, впливом кіберзлочинців на інформаційні ресурси через шпигунську або диверсійну діяльність і т.д.

Автори багатьох досліджень запропонували ретельний аналіз джерел ризику та розробили власну модель. Вибір методу моделювання і рівня деталізації об'єктів і процесів залежить від мети дослідження та джерел ризику.

Один із розділів математики, який знаходить широке застосування у моделюванні складних систем, включаючи інформаційні системи, - це теорія множин. Розширення можливостей класичної теорії множин надає теорія нечітких множин [62]. При моделюванні складних систем, особливо при обмеженій кількості інформації та випадковості процесів, використання інструментів нечітких множин стає доцільним. Це особливо актуально при дослідженні інформаційних ризиків, коли необхідно класифікувати ризики та отримувати комплексні оцінки. Методи нечітких множин і нечіткої логіки дозволяють використовувати як кількісні, так і якісні оцінки, що полегшує роботу з експертними оцінками.

У даному дослідженні пропонується розробити механізм отримання оцінок ризику, який замінює старий метод оцінки ризику за допомогою наближених табличних методів сучасними математичними інструментами.

Створення системи математичних моделей та методів для управління інформаційними ризиками базується на наступних ключових концепціях:

– розробка та застосування методів ідентифікації інформаційних ресурсів (активів) корпорації, які можуть стати об'єктами інформаційних ризиків та погроз для цих ресурсів;

– розробка і використання моделей для кількісного аналізу і оцінювання факторів, таких як уразливість, ефективність засобів захисту та інші, а також загального рівня інформаційних ризиків з використанням інструментів нечіткої логіки;

– розробка математичних моделей для обґрунтування економічної доцільності використання механізмів (засобів), які спрямовані на зменшення рівня інформаційних ризиків. Це також включає забезпечення відповідності функціональним критеріям захисту інформації, таким як конфіденційність, цілісність і доступність, а також зниження пов'язаних із цими ризиками втрат та збитків для підприємства.

У методиках аналізу інформаційних ризиків доволі часто застосовують моделі оцінки ризику, які базуються на трьох ключових компонентах: загроза, вразливість та потенційні збитки [63].

Аналіз інформаційних ризиків включає чотири ключових етапи:

– ідентифікація компонентів, включаючи інформаційні ресурси і потенційні загрози;

– оцінка частоти можливих загроз на основі їхньої ймовірності;

– оцінка розміру потенційних збитків, які можуть виникнути;

– результат аналізу інформаційних ризиків в системі інформаційної безпеки оцінюється за загальною шкалою рівня ризиків, де "C" вказує на "критичний", "H" на "високий", "M" на "середній" та "L" на "низький" рівень ризику в корпоративній системі.

Запропоновано використовувати лінгвістичний підхід у моделюванні аналізу факторів інформаційного ризику. Цей підхід дозволяє надавати якісні описи окремих елементів моделі в умовах нечіткої інформації про значення критеріїв оцінки ризикових факторів, їх можливих наслідків при дії загроз, а також альтернативних шляхів для уникнення негативних наслідків інформаційних ризиків. За лінгвістичним підходом, не лише проводиться кількісна оцінка, але і враховується лінгвістичне описання цих параметрів.

Пропонується впроваджувати інтелектуальні методи в системи інтелектуальної підтримки для оперативного управління інформаційною безпекою в КІС. Ці методи включають в себе нечіткий висновок для чисельної оцінки ймовірності інформаційних атак, організовану класифікацію інформації про події в базі знань, моделювання нейтралізації загроз та прийняття рішень щодо вибору оптимальних дій для реагування на події в системі інформаційної безпеки.

Остаточний вибір комплексу захисних засобів для системи інформаційної безпеки може бути здійснений ітеративно, крок за кроком, наближаючи до раціонального складу, який відповідає прийнятному рівню витрат на впровадження цієї системи.

3.2 Постановка завдання оцінювання ризику інформаційної системи

Запропоновано створити механізм для оцінки ризику, який замінить традиційний табличний метод оцінки ризику сучасними математичними інструментами.

Розробка системи математичних моделей та методів управління інформаційними ризиками базується на наступних концептуальних принципах:

– Розробка та використання методів ідентифікації інформаційних ресурсів (активів) підприємства, які можуть бути об'єктами інформаційних ризиків та загроз для цих ресурсів.

– Створення та використання моделей для кількісного аналізу і оцінки факторів (включаючи уразливості, ефективність засобів захисту та інше) та загального рівня інформаційних ризиків з використанням інструментів нечіткої логіки.

– Розробка математичних моделей для економічного обґрунтування ефективності використання механізмів та засобів зниження рівня інформаційних ризиків. Ці механізми спрямовані на забезпечення відповідності функціональним критеріям інформаційної безпеки, таким як конфіденційність, цілісність, доступність та спостережливість, і на зниження пов'язаних із цим втрат і збитків

для підприємства.

Існує чотири основних етапи аналізу інформаційних ризиків [64]:

I. Ідентифікація компонент:

1. Інформаційні ресурси (активи) компанії, які можуть бути об'єктом ризику. Згідно стандарту безпеки ISO/IEC 27001: 2013 інформаційний актив представляє собою матеріальний або нематеріальний об'єкт, котрий представляє собою інформацію або містить інформацію, використовується для зберігання або обробки інформації і є цінним для підприємства чи організації;

2. Можливі загрози (комбінації загроз) активу. Для ефективного контролю над ризиками необхідно визначити потенційні загрози, що можуть вплинути на КІС. Такими можуть бути, наприклад, стихійне лихо, відключення електроживлення, атака зловмисника з різними ступенями складності наслідків.

II. Оцінка частоти подій можливих втрат у результаті дії ризику:

1. Можливий рівень сили (Threatcapability), з якої агенти загрози будуть діяти на актив. Допускається, що деяка частина популяції агентів загрози є більш здатною до впливу на актив, інша - менш здатна. Проводиться експертне оцінювання рівня загроз по набору показників, що характеризують можливість доступу порушника відповідного класу до інформаційним ресурсів по наступною шкалою:

P_VH - "дуже високий";

P_H - "Високий";

P_M - "середній";

TC_L - "низький";

P_VL - "дуже низький".

2. Очікувана дієвість коштів контролю (Controlstrength) на протягом відведеного часового інтервалу. Взявши за основу орієнтацію на середню здібність агентів загрози, приймається базовий рівень ефективності контролю.

Для оцінювання рівня захисту використовується така шкала:

D_VH - "дуже високий";

D_H - "високий";

D_M - "середній";

D_L - "низький";

D_VL - "дуже низький".

Вразливість розглядається як результат впливу факторів можливого рівня сили загрози та дієвості засобів контролю та оцінюється за шкалою:

B_VH - "дуже високий";

B_H - "високий";

B_M - "середній";

B_L - "низький";

B_VL - "дуже низький".

Приклад бази знань для оцінки рівня чутливості наведено в табл. 3 при реалізації факторів ризику (агентів загрози) в межах певного часового інтервалу.

Таблиця 3.1. Оцінка рівня чутливості корпоративної системи

		Чутливість				
Можливий рівень сили погрози	P_VH	B_VH	B_VH	B_VH	B_H	B_M
	P_H	B_VH	B_VH	B_M	B_M	B_ L
	P_M	B_VH	B_H	B_M	B_ L	B_VL
	P_L	B_H	B_M	B_ L	B_VL	B_VL
	P_VL	B_M	B_ L	B_VL	B_VL	B_VL
		D_VL	D_L	D_M	D_H	D_VH
		Дійсність засобів контролю				

Під факторами слід розуміти опис типів зловмисників, які навмисно або випадково, діями або бездіяльністю здатні завдати збитків корпоративній системі.

Оцінка частоти реалізації факторів ризику може проводитися по шкалою: RFR_VH - "дуже висока"; RFR_H - "висока"; RFR_M - "середня"; RFR_L - "низька"; RFR_VL - "дуже низька".

Частота виникнення подій втрат - можлива частота протягом певного

часового інтервалу, з якої агент загрози наносить шкода активу, розглядається як результат впливу факторів частоти виникнення загрози та вразливості.

Використовуються наступні оцінки рівня частоти подій втрат інформаційних активів:

OFR_VH - "дуже високий";

OFR_H - "високий";

OFR_M - "середній";

OFR_L - "низький";

OFR_VL - "дуже низький".

Приклад бази знань для оцінювання рівня частоти виникнення подій втрат наводиться в таблиці 3.2.

Таблиця 3.2. Оцінювання рівня частоти подій втрат внаслідок інформаційних ризиків

		Частота подій втрат				
Частота виникнення погроз	P_VH	B_VH	B_VH	B_VH	B_H	B_M
	P_H	B_VH	B_VH	B_H	B_M	B_ L
	P_M	B_VH	B_H	B_M	B_ L	B_VL
	P_L	B_H	B_M	B_ L	B_VL	B_VL
	P_VL	B_M	B_ L	B_VL	B_VL	B_VL
		D_VL	D_L	D_M	D_H	D_VH
		Дійсність засобів контролю				

III. Оцінювання величини можливих збитків: визначення можливої дії кожного з агентів загрози інформаційному активу; оцінювання величини кожною з можливих форм збитків, які пов'язані з дією певного агента загрози; оцінювання величини всіх можливих форм збитків за шкалою:

PD_VH - "дуже великі";

PD_H - "великі";

PD_Sg - "істотні";

PD_M - "середні";

PD_L - "малі";

PD_VL - "дуже малі" збитки в відповідних грошових одиницях.

Визначення величини можливих збитків може проводитися щодо бюджету корпоративної системи з обліком вартості інформаційних активів, вартості репутації підприємства, і тому подібне.

IV. Результат аналізу інформаційних ризиків корпоративної системи зводиться до оцінки спільного рівня інформаційного ризику в КІС за наведеною нижче шкалою:

С - "критичний";

Н - "високий";

М - "середній";

L - "низький" рівень інформаційних ризиків.

Приклад бази знань, яка може бути використана для оцінювання спільного рівня інформаційного ризику, наводиться в табл. 3.3.

Таблиця 3.3. Оцінювання спільного рівня

		Рівень інформаційних ризиків				
Величини можливих збитків	PD_VH	H	H	C	C	C
	PD_H	M	H	H	C	C
	PD _Sg	M	M	H	H	C
	PD_M	L	M	M	H	H
	PD_L	L	L	M	M	H
	PD _VL	L	L	L	M	M
		OFR_VL	OFR_L	OFR_M	OFR_H	OFR_VH
		Частота подій втрат				

3.3 Моделювання аналізу факторів інформаційного ризику на основі лінгвістичного підходу

Пропонується використовувати лінгвістичний підхід для моделювання аналізу факторів інформаційного ризику. Цей підхід дозволяє надавати кількісні характеристики окремим елементам моделі в умовах невизначеності інформації щодо значення критеріїв оцінки ризику фактору, їх наслідків в контексті дії агента загрози та альтернативних шляхів для уникнення негативного впливу інформаційних ризиків. Відповідно до лінгвістичного підходу, не лише проводиться кількісна оцінка значень критеріїв та характеристик взаємозв'язків між ними, але й надається можливість описувати ці характеристики природньою мовою. На основі розрахованих значень груп показників, які відображають частоту виникнення втрат інформаційних активів та величину можливих збитків внаслідок інформаційних ризиків, проводиться оцінка загального рівня інформаційних ризиків в КІС:

$$\Delta = f(\gamma, P), \tag{3.1}$$

де γ - оцінка рівня частоти подій втрат інформаційних активів; P - попередньо оцінена величина можливих збитків.

Терм-множина вхідний змінної v, що є безліччю ступенів частоти виникнення можливих втрат, має вигляд:

$$OFR = \{OFR\_VH, OFR\_H, OFR\_M, OFR\_L, OFR\_VL\}, \tag{3.2}$$

де OFR_VH - "дуже висока" частота; OFR_H - "висока частота"; OFR_M - "середня частота"; OFR_L - "низька частота"; OFR_VL - "дуже низька".

Терм-множина вхідної змінної P, яка описує величину втрати щодо бюджету КІС, записується в вигляді:

$$LD = \{PD\_VH, PD\_H, PD\_Sg, PD\_M, PD\_L, PD\_VL\}, \quad (3.3)$$

де PD_VH - "дуже велика"; PD_H - "велика"; PD_Sg - "суттєва"; PD_M - "Середня"; PD_L - "мала"; PD_VL - "дуже мала".

Для оцінювання та опрацювання лінгвістичної змінної рекомендовано скористатися шкалою з чотирьох якісних термів:

C - "критичний";

H - "високий";

M - "середній";

L - "низький" рівень ризику.

Терм-множина вихідний змінної B представляється в вигляді:

$$IR=\{C, H, M, L\}, \quad (3.4)$$

Далі в процесі аналізу необхідно створити нечітку систему знань для оцінки кожного з рівнів інформаційних ризиків. Сформовано набір вирішальних правил, які реалізують співвідношення (1). У таблиці 3.4 наведено такий набір.

Таблиця 3.4 - База знань для визначення рівня інформаційних ризиків

Номер вихідної комбінації	Узагальнені значення груп показників		Значимість m ij	Вихідна змінна Δ
	Рівень частоти виникнення можливих втрат	Величина можливих збитків P		
1	2	3	4	5
11	PD_VH	OFR_M	m 11	C
12	PD_VH	OFR_H	m 12	
13	PD_VH	OFR_VH	m 13	
14	PD_H	OFR_H	m 14	
15	PD_H	OFR_VH	m 15	
16	PD _Sg	OFR_VH	m 16	

Кінець таблиці 3.4 - База знань для визначення рівня інформаційних ризиків

1	2	3	4	5
21	PD_VH	OFR_VL	m 21	H
22	PD_VH	OFR_L	m 22	
23	PD_H	OFR_L	m 23	
24	PD_H	OFR_M	m 24	
25	PD _Sg	OFR_M	m 25	
26	PD _Sg	OFR_H	m 26	
27	PD_M	OFR_H	m 27	
28	PD_M	OFR_VH	m 28	
29	PD_L	OFR_VH	m 29	
31	PD_H	OFR_VL	m 31	M
32	PD _Sg	OFR_VL	m 32	
33	PD _Sg	OFR_L	m 33	
34	PD_M	OFR_L	m 34	
35	PD_M	OFR_M	m 35	
36	PD_L	OFR_M	m 36	
37	PD_L	OFR_H	m 37	
38	PD_VL	OFR_H	m 38	
39	PD_VL	OFR_VH	m 39	
41	PD_M	OFR_VL	m 41	L
42	PD_L	OFR_VL	m 42	
43	PD_L	OFR_L	m 43	
44	PD_VL	OFR_VL	m 44	
45	PD_VL	OFR_L	m 45	
46	PD_VL	OFR_M	m 46	

Наступним кроком є визначення математичної форми записи вирішальних правил з допомогою функцій приналежності для визначення рівнів інформаційних

ризиків. Наприклад, вирішальне правило для визначення інформаційних ризиків рівня М може бути записано таким чином:

$$\mu^{M}(x,P) = m_{31}[\mu^{OFR_{VL}}(\gamma) * \mu^{PD_{H}}(P)] \vee m_{32}[\mu^{OFR_{VL}}(\gamma) * \\ * \mu^{PD_{Sg}}(P)] \vee m_{33}[\mu^{OFR_{L}}(\gamma) * \mu^{PD_{Sg}}(P)] \vee m_{34}[\mu^{OFR_{L}}(\gamma) * \\ * \mu^{PD_{M}}(P)] \vee m_{35}[\mu^{OFR_{M}}(\gamma) * \mu^{PD_{M}}(P)] \vee \\ \vee m_{36}[\mu^{OFR_{M}}(\gamma) * \mu^{PD_{L}}(P)] \vee m_{37}[\mu^{OFR_{H}}(\gamma) * \mu^{PD_{L}}(P)] \vee \\ \vee m_{38}[\mu^{OFR_{H}}(\gamma) * \mu^{PD_{VL}}(P)] \vee m_{39}[\mu^{OFR_{VH}}(\gamma) * \mu^{PD_{VL}}(P)], \quad (3.5)$$

де $\mu^{M}(\Upsilon,P)$ - функція приналежності вихідний змінної Λ значенню М з нечіткого терма (3.4); $m_{3k}(k=1,9)$ - ваговий коефіцієнт для відповідної k -й комбінації; $\mu^{ofrj}(\Upsilon)$ - функція приладдя параметра Υ нечіткому терму ofr_j з терм-множини OFR (3.2); $\mu^{ldi}(P)$ - функція приналежності параметра Р до нечіткого терму ld_i з терм-множини LD (3.3).

Таким чином, вся база знань формується з використанням експертних даних і виводиться система нечітких логічних рівнянь.

Результатом представленої концепції та інструментарію оцінювання рівня частоти подій втрат і величини можливих втрат інформаційних активів є лінгвістичний опис загального рівня інформаційних ризиків в КІС.

Було побудовано дзвін-подібні функції приналежності вихідний термів змінної В до множинного числа терма, параметри яких представлені в табл. 3.5:

$$\mu^{T}(x) = \frac{1}{1+\left|\frac{x-c}{a}\right|^{2b}}, \quad (3.6)$$

де Т – довільний нечіткий терм; а - коефіцієнт концентрації; b - коефіцієнт крутості; с - координата максимуму функції, $\mu^{T}(c)=1$.

Таблиця 3.5 - Параметри функцій приналежності термів до терм-множини IR

Назва терма	Функція приналежності	Параметри		
		Коефіцієнт максимуму c	Коефіцієнт концентрації a	Коефіцієнт крутості b
L	$\mu^1(x)$	0	0,1	2
M	$\mu^2(x)$	0,33	0,1	2
H	$\mu^3(x)$	0,67	0,1	2
C	$\mu^4(x)$	1	0,1	2

Графічне представлення функції приналежності вихідної змінної, бази логічного висновку представлені на рисунках 3.1 і 3.2 відповідно.

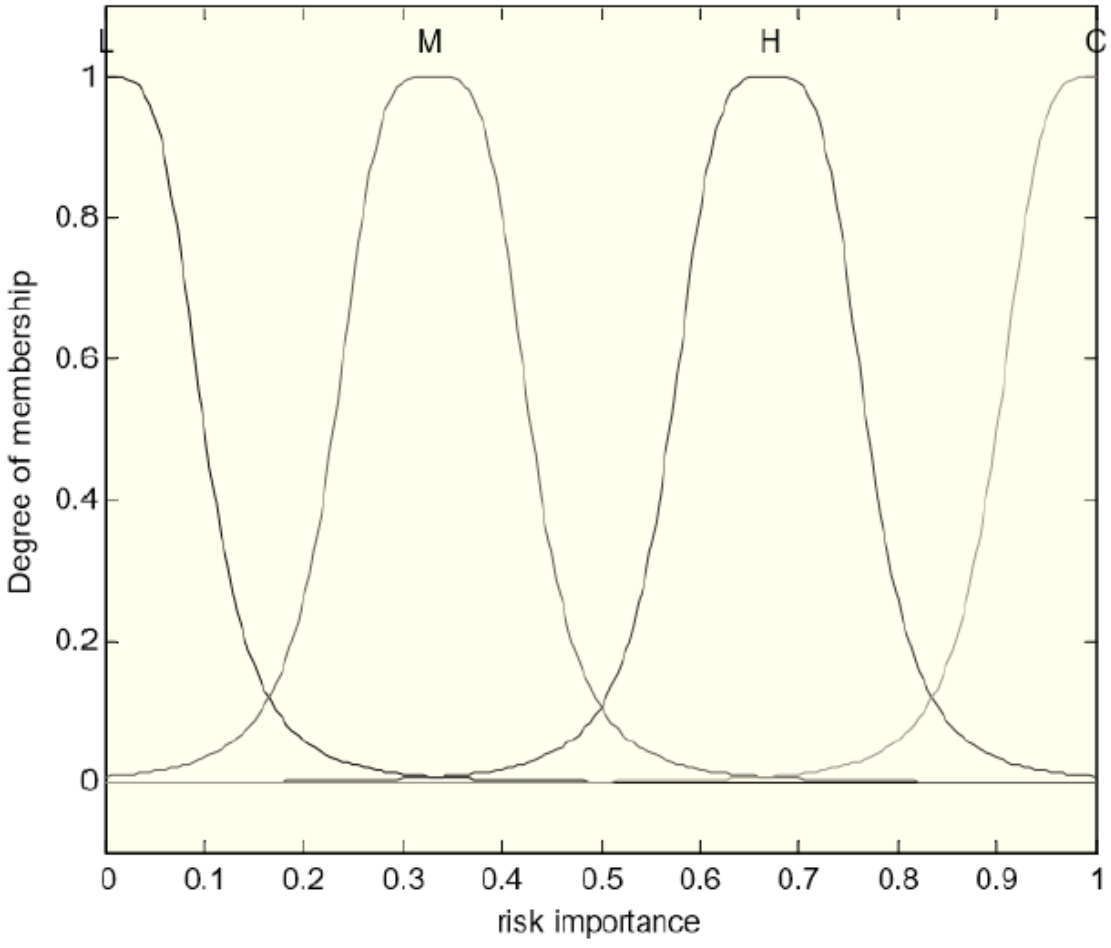

Рисунок 3.1 - Графіки функцій належності показника рівня інформаційних ризиків у КІС

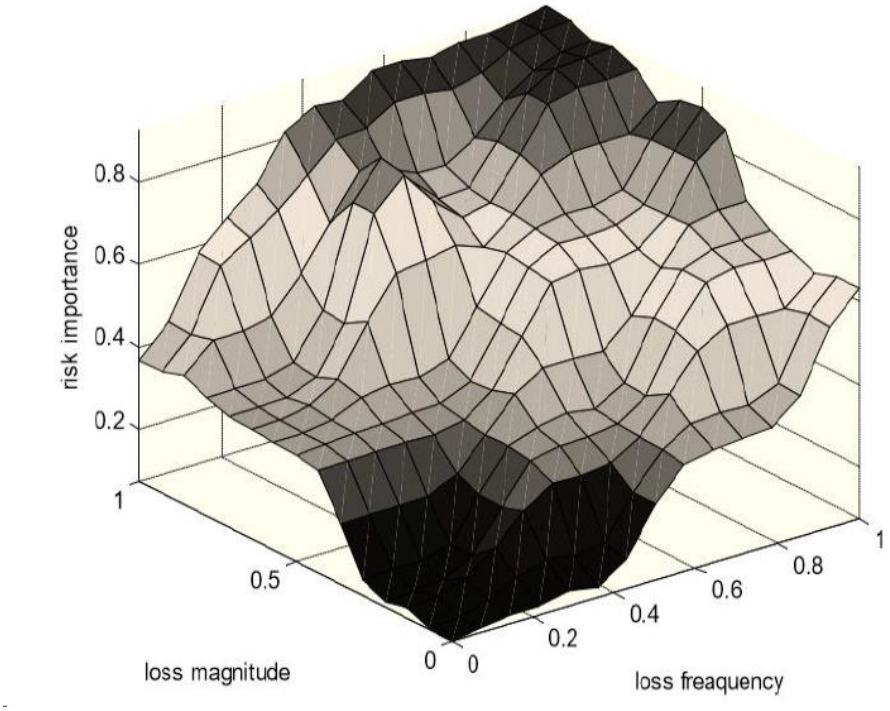

Рисунок 3.2 - Графічне представлення системи нечіткого виведення показника рівня інформаційних ризиків

Результати проведених досліджень щодо оцінювання рівня інформаційних ризиків в КІС представлені в табл. 3.6.

Таблиця 3.6. Оцінка рівня інформаційних ризиків

Назва підприємства	Величина можливих збитків	Рівень частоти можливих втрат	Рівень інформаційних ризиків
Підприємство 1	PD_M 0,4012	OFR_L 0.3545	M 0,3751
Підприємство 2	PD_Sg 0,5971	OFR_M 0.5799	H 0,6348
Підприємство 3	PD_Sg 0,5991	OFR_M 0.4376	H 0,6252
Підприємство 4	PD_P 0,7749	OFR_L 0.1740	H 0,6109

Як видно з табл. 3.6, на Підприємстві 2, Підприємстві 3 і Підприємстві 4 знайдений рівень інформаційних ризиків відповідає оцінки "високий", на Підприємстві 1 - "середній".

За результатам оцінки факторів інформаційних ризиків було прийнято рішення про методи зниження рівня інформаційних ризиків на підприємствах. Наприклад, на Підприємстві 3 необхідно прийняти додаткові заходи щодо підвищення рівня дієвості засобів захисту, оскільки високий рівень уразливості був викликаний саме недоліками роботи цих ресурсів і їх невідповідності високому рівнем погроз інформаційної безпеки підприємства

Можна зробити висновок, що подібна модель оцінки загального рівня ризику гнучка і адаптивна і може бути налаштована в відповідно з отриманої базою знань.

3.4 Висновки до розділу

Категорію "інформаційний ризик" слід розглядати через призму підприємського керівника, який бажає приймати рішення щодо всіх ризиків, пов'язаних із використанням управлінської інформації у бізнесі, оскільки в сучасному бізнес-середовищі інформаційний ризик став невід’ємною частиною управління підприємством. Пропонується враховувати ризики, пов'язані з інформацією, не лише в контексті порушень інформаційної безпеки, але також у зв'язку з втратою якості бізнес-процесів. Важливо враховувати, що інформаційний ризик може виникати не лише зовнішньо через атаки та порушення безпеки, але і внутрішньо через недоліки в управлінні інформацією, помилки персоналу, втрату даних тощо. Аналіз інформаційних ризиків є основою для створення підсистеми управління інформаційною безпекою підприємства, яка включає в себе розробку стратегій, політик та процедур для забезпечення інформаційної безпеки, а також впровадження технічних засобів та навчання персоналу. Підприємство повинно бути готове до виявлення, оцінки та управління ризиками, пов'язаними з інформацією, які можуть виникнути на будь-якому етапі свого функціонування.

Під час аналізу і оцінки рівня інформаційних ризиків слід дотримуватися

таких кроків:

– Визначення ідентифікації інформаційних ресурсів (активів) компанії, які можуть бути об'єктом ризику, потенційних загроз активам і встановлення рівня загроз для інформаційної безпеки корпоративної системи підприємства.

– Оцінка ефективності заходів контролю безпеки корпоративної системи.

– Аналіз вразливості корпоративної системи, яка розглядається як результат впливу можливих загроз і рівня ефективності контрольних заходів.

– Оцінка частоти виникнення подій втрат від інформаційних ризиків як наслідку впливу факторів частоти виникнення загрози та вразливості корпоративної системи.

– Оцінка величини можливих збитків від інформаційних ризиків в КІС.

– Оцінка загального рівня інформаційних ризиків в КІС як результату взаємодії двох факторів: частоти виникнення втрат і розміру можливих збитків від інформаційних ризиків.

Була розроблена модель для оцінки загального рівня інформаційних ризиків у сегменті КІС з використанням лінгвістичного підходу. Цей підхід надає можливість надавати кількісні описи окремих елементів моделі, навіть при обмеженій чіткості інформації щодо значень критеріїв оцінки факторів (чинників) ризику. Це дозволяє виділяти важливі фактори ризику, їх наслідки при впливі агента загрози і, відповідно, визначати можливі альтернативи для зменшення негативного впливу ризику:

– Зміна або модифікація засобів контролю безпеки.

– Використання механізмів захисту відповідно до можливого рівня загроз певних класів порушників інформаційної безпеки.

– Запровадження режиму функціональної ізоляції, що забороняє використання апаратного та програмного забезпечення, яке не має відповідних паспортів безпеки і інших аналогічних заходів.

Результатом використання цієї технології та інструментарію для оцінки рівня

інформаційних ризиків у сегменті КІС є можливість лінгвістичного опису та аналізу факторів інформаційних ризиків, зокрема рівня частоти виникнення загроз і вразливості КІС. Розроблений концептуальний підхід дозволяє створити модель, яка не лише може бути адаптована до конкретної інформаційної системи, але й піддаватися переоцінці ризику в майбутньому. Така модель характеризується гнучкістю та можливістю точного налаштування на основі накопичених знань.

Запропоновану модель оцінки рівня інформаційних ризиків можна використовувати як основу для розвитку підсистеми управління інформаційними ризиками, як на етапі проектування КІС підприємства, так і під час її експлуатації. Ця модель легко адаптується для виконання завдань управління інформаційними ризиками нарівні з іншими завданнями. Важливо відзначити, що для досягнення цієї мети не потрібно робити радикальні зміни в організаційній структурі корпорації, адже достатньо просто адаптувати її до розв'язання завдань управління захистом інформації в КІС.

Незважаючи на важливі досягнення, існують невирішені завдання, включаючи:

– Розвиток математичних моделей та відповідного інструментарію для зменшення впливу факторів вразливості або підвищення впливу факторів ефективності заходів безпеки на загальний рівень інформаційних ризиків.

– Розробка положень щодо впровадження механізмів управління окремими факторами інформаційних ризиків.

Необхідно активно працювати над вирішенням цих проблем для подальшого розвитку і вдосконалення системи управління інформаційними ризиками.

4 МОДЕЛЮВАННЯ РАЦІОНАЛЬНОГО МОДЕЛЬНОГО СКЛАДУ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

4.1 Побудова моделі системи захисту інформації

КІС складається з апаратних засобів, таких як сервери, серверне обладнання, робочі станції, канали зв'язку, а також програмного забезпечення. З урахуванням сучасних підходів до створення СЗІ, можна зробити висновок, що при розробці ефективної системи захисту інформації важливо дотримуватися ряду ключових принципів:

– Система захисту інформації повинна бути складною і добре згорнутою. Це означає, що при її розробці необхідно використовувати різноманітні інструменти та методи захисту, але при цьому важливо забезпечувати цілісність системи та уникати "слабких місць" у взаємодії окремих її компонентів.

– Потрібно розробляти рівні захисту, враховуючи важливість та критичність інформації, а також ймовірність потенційних загроз (оцінки можливих атак). Це означає, що заходи захисту повинні бути адаптовані до конкретних потреб та умов.

– Для оцінки ефективності системи захисту інформації потрібно враховувати витрати на створення та підтримку системи та можливий збиток, який може виникнути в разі порушення безпеки.

Після аналізу можливих загроз, пов'язаних з несанкціонованим доступом до інформаційного середовища, і враховуючи зазначені раніше принципи структурування системи інформаційної безпеки, запропоновано модель СЗІ, яку розроблено у вигляді трьох рівнів захисту:

– Периметр об'єкта захисту, який включає набір функціональних підсистем, спрямованих на захист інформаційної системи від зовнішніх загроз і шкідливих дій зловмисників.

– Периметр сегмента мережі, який включає набір функціональних

підсистем, призначених для захисту від віддалених і міжсегментних атак.

– Внутрішній периметр, який включає набір функціональних підсистем, чия головна мета - захист інформаційного середовища окремих персональних комп'ютерів та серверів.

З урахуванням поширення інформаційних атак та використання гібридних методів, ефективний захист інформаційного середовища вимагає застосування багаторівневої, сходової системи захисту інформації. Схему цієї пропонованої трьохрівневої системи можна побачити на рисунку 4.1.

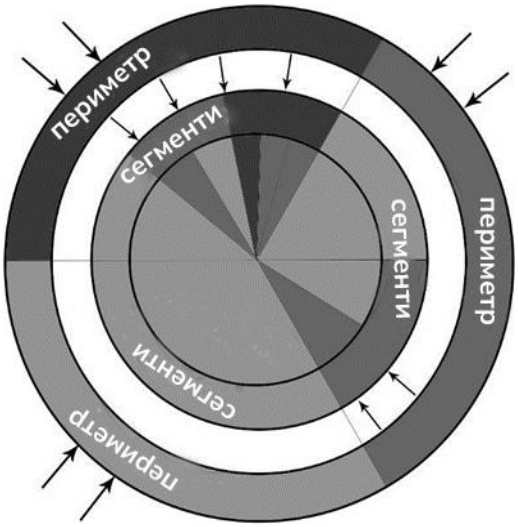

Рисунок 4.1 - Трирівнева модель СЗІ (стрілки вказують на зовнішні та внутрішні загрози)

Отже, розроблена модель СЗІ буде включати у себе три ключових компоненти:

– модель захисту периметра об'єкта,

– модель забезпечення безпеки мережевого сегмента,

– модель захисту внутрішнього сегмента (особистих комп'ютерів та серверів).

Для кожної з розглянутих меж, враховуючи ступінь важливості оброблюваної в них інформації та необхідність її захисту, модель буде включати в себе N різних морфологічних матриць (модель рівня N).

Завданням цієї упорядкованої та системної організації інформації є зменшення рівня невизначеності при прийнятті рішень щодо структури системи захисту інформації. Це досягається на підставі інформації про можливі потенційні загрози в конкретному контурі та інформаційному середовищі, а також необхідних бар'єрів для захисту від відповідних загроз.

Отже, при наявності структурованої інформації щодо можливих загроз та доступних методів захисту інформації, на основі певних процедур проводиться багатокритеріальне порівняння альтернативних варіантів реалізації засобів захисту. Цей процес допомагає визначити найкращі (самі ефективні та відповідні обмеженням ресурсів) варіанти захисту інформаційних об'єктів.

4.2 Розробка моделей протидії погроз інформаційної безпеки в умовах невизначеності

Для більш ретельного аналізу процесу прийняття рішень у справі протидії загрозам, розглянемо декілька типових інформаційних атак, включаючи:

– Міжсегментні атаки, які спрямовані на порушення безпеки мережевих сегментів та передачу даних між ними.

– Зовнішні атаки через точки бездротового доступу, які включають в себе атаки, спрямовані на вразливості в бездротових мережах та точках доступу.

– Зовнішні атаки через периметр через високошвидкісний канал доступу, що охоплюють атаки на системи, які користуються високошвидкісними каналами зв'язку для впровадження шкідливого впливу.

Цей аналіз допоможе краще зрозуміти та оцінити заходи забезпечення безпеки, які слід вживати для захисту від різних видів інформаційних атак.

4.2.1 Прийняття рішень у випадку потенційно можливої міжсегментної атаки

Представимо модель протидії у вигляді зв'язного графа (рис. 4.2), де Un - це варіанти реагування, а Vn - варіанти результатів при реалізації протидії загрозам. Функція реалізації, відповідна даної матриці, представлена в таблиці 4.1.

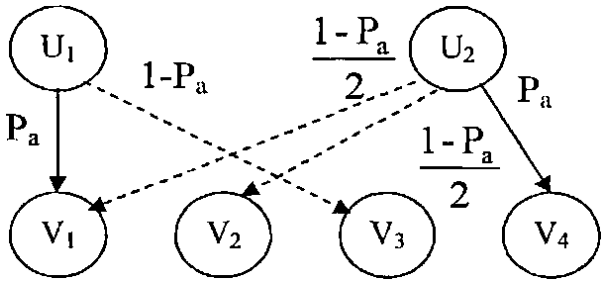

Рисунок 4.2 - Граф зв'язку варіантів реагування і результатів

Таблиця 4.1 - Функція реалізації

U	Z					
	$P(z_1)$	$P(z_2)$	$P(z_3)$	$P(z_4)$	$P(z_5)$	$P(z_6)$
U_1	$C(V_1)$	$C(V_2)$	$C(V_3)$	$C(V_4)$	$C(V_5)$	$C(V_6)$
U_2	$C(V_1)$	$C(V_2)$	$C(V_3)$	$C(V_4)$	$C(V_5)$	$C(V_6)$

Наступні варіанти відповіді наведено в таблиці нижче:

U_1 – завершення сеансу з атакуючим вузлом;

U_2 – надсилання попередження користувачеві або зменшення пріоритету користувача.

Оцінка можливих результатів проводиться в відповідність з сумою можливих збитків в результаті реалізації функцій захисту:

$C(V_1)$ - немає пошкоджень;

$C(V_2)$ - незначні збитки (збитки користувачеві);

$C(V_3)$ - середня шкода (шкода системі);

$C(V_4)$ - максимальний шкода, що нанесена системі в результаті здійснення атаки.

При виборі варіанта реагування U_1 з ймовірністю (1–Pa) буде отримано середню шкоду, оскільки в якості атаки прийнято при стандартному режимі роботи мережі ненавмисний шкідливий вплив від користувача або помилкове розпізнавання як атаки сигналів з сенсорів.

Реалізація варіанта реагування (керуючого впливу) U_2, може мати три різні варіанти результату. Якщо події, розпізнані як аномальні і дійсно є атакою, то з

ймовірністю P_a буде реалізований максимальний збиток при відсутності блокування атакуючої дії. У випадку, якщо розпізнана аномальна подія була причиною помилкових дій користувача, то шкоди не буде (вона буде дорівнює нулю). Якщо керуючий вплив буде реалізовано внаслідок помилкового розпізнавання сигналів як атаки і користувачеві буде відправлено попередження і знижений його пріоритет - буде завдано незначну шкоду користувачеві. У останніх двох варіантах ймовірності результатів складуть одну і ту ж величину $(1-P_a)/2$.

Після чисельних розрахунків отримано:

– при $P_a=0,238$ мінімальне значення цільової функції досягається при виборі альтернативи U_2:$J(U_1,z)=0,381$, $J(U_2,z)=0,276$;

– при $P_a=0,57$ мінімальне значення цільової функції досягається при виборі альтернативи U_1:$J(U_1,z)=0,215$, $J(U_2,z)=0,5915$.

Для чисельних розрахунків були прийняті значення $C(V_1)=0$, $C(V_2)=0,1$, $C(V_3)=0,5$, $C(V_4)=1$.

4.2.2 Прийняття рішень щодо реагування у разі потенційно можливого зовнішнього вторгнення по радіоканалу

Для виконання зовнішнього вторгнення в даному сценарії атаки, зловмиснику необхідно мати доступ до бездротового адаптера та перебувати в радіусі дії бездротової мережі. У порівнянні з атакою за допомогою кабельного з'єднання, в цьому випадку ризик і можливість завдати максимальної шкоди вищі.

В обраному об'єкті атаки, а саме точці доступу, використовуються системи WIDS (системи виявлення бездротових атак). Вони базуються на сигнатурному аналізі та кореляції поведінки. Події щодо безпеки (наприклад, спроби впливу на інформаційну систему) генеруються, коли виявляються відхилення параметрів точки доступу від заданих значень.

Створюється передбачуваний (еталонний) мережевий профіль, який включає в себе наступні параметри, що постійно контролюються:

– Допустима кількість підключень до точки доступу.

– Якість сигналу.

– Кількість переданих та прийнятих широкомовних пакетів.

– Частота та кількість повторних передач пакетів.

– Відсоткове співвідношення цілісних та фрагментованих фреймів.

– Параметри передачі даних, такі як швидкість та її зміни.

– Виникнення та частота помилок контрольної суми при передачі пакетів.

– Використані MAC-адреси для автентифікації повідомлень.

– Використовувані технології автентифікації та шифрування при передачі даних.

Для забезпечення ефективного захисту інформації, процедури реагування повинні бути налаштовані таким чином, щоб мінімізувати можливий збиток від можливого вторгнення або збою взаємодії через точку доступу.

Модель захисту і відповідні функції реалізації цієї моделі подані у графічному вигляді на рисунку 4.3, а також наведені в таблиці 4.2.

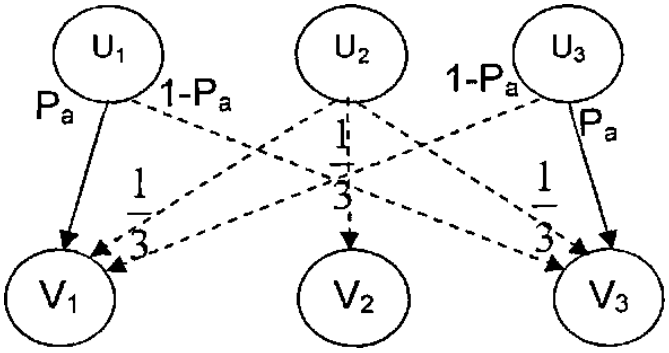

Рисунок 4.3 - Граф зв'язку варіантів реагування і результатів

Таблиця 4.2 - Функція реалізації

U	Z											
	$P_{(z1)}$	$P_{(z2)}$	$P_{(z3)}$	$P_{(z4)}$	$P_{(z5)}$	$P_{(z6)}$	$P_{(z7)}$	$P_{(z8)}$	$P_{(z9)}$	$P_{(z10)}$	$P_{(z11)}$	$P_{(z12)}$
U_1	$C(V_1)$	$C(V_3)$	$C(V_1)$	$C(V_3)$	$C(V_1)$	$C(V_3)$	$C(V_1)$	$C(V_3)$	$C(V_1)$	$C(V_3)$	$C(V_1)$	$C(V_3)$
U_2	$C(V_1)$	$C(V_1)$	$C(V_2)$	$C(V_2)$	$C(V_3)$	$C(V_3)$	$C(V_1)$	$C(V_1)$	$C(V_2)$	$C(V_2)$	$C(V_3)$	$C(V_3)$
U_3	$C(V_1)$	$C(V_1)$	$C(V_1)$	$C(V_1)$	$C(V_1)$	$C(V_1)$	$C(V_3)$	$C(V_3)$	$C(V_3)$	$C(V_3)$	$C(V_3)$	$C(V_3)$

Отримано наступні варіанти керуючих впливів (реагування системи):

U_1 – блокування точки доступу;

U_2 - здійснення DOS-атаки на станцію, що реалізує атаку;

U_3 - відсутність реагування.

Розподілимо по величині можливого шкоди ймовірні результати керуючий впливів:

$C(V_1)$ – нульовий збиток;

$C(V_2)$ - середній збитки;

$C(V_3)$ - максимальні збитки.

Якщо система реалізує вплив U_1, то з ймовірністю шкоди P_a шкоди системі не буде (канал повністю перекритий і дії зловмисника припинено). Ймовірність P_a в даному випадку дорівнює ймовірність атаки. Якщо за реалізацію атаки були помилково розпізнані сигнали сенсорів або відбулася помилка в діях користувача, то шкода при виборі керуючого впливу U_1 буде максимальною (блокування точки доступу відбулося безпідставно, стався збій у нормальною роботі системи). Ймовірність $(1-P_a)$ такого результату відповідає ймовірності помилковою інтерпретації сигналів системою або помилки користувача.

Якщо вибрано варіант реагування U_3, то у разі реалізації атаки максимальні збитки будуть отримані з ймовірністю P_a (ймовірність атаки) – атаку зловмисника не відстежено системою. Якщо даний варіант реагування обраний в ситуації помилкового розпізнавання сигналів сенсорів як атаки, то шкода буде нульовою - система захисту не втручається в роботу і продовжується робота в штатному режимі (ймовірність складе $(1-P_a)$ для цього результату).

Якщо системою обраний варіант реагування U_2 (здійснення у відповідь DOS-атаки), то можливі три варіанти результату (нульовий - запобігли дії зловмисника, середній - заблоковано користувач за помилкові дії, або максимальний - порушено працездатність мережі, збитки), ймовірності яких рівні 1/3.

4.2.3 Прийняття рішень щодо реагування у разі потенційно можливого зовнішнього вторгнення через периметр через лінії зв'язку

Для цього варіанта загрози модель протидії проілюстрована на рис.4.4.

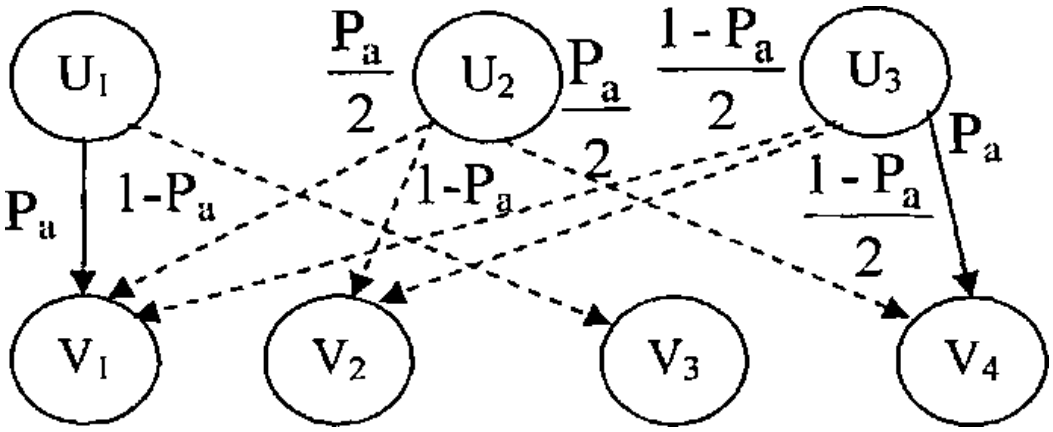

Рисунок 4.4 - Граф підключення варіантів відповіді і результатів

Ця опція атаки генерує наступні варіанти відповіді (керуючі дії):

U_1 - блокування доступу користувачів до відповідної послуги в мережі;

U_2 – реконфігурація служб безпеки для блокування взаємодії за конкретною IP-адресою;

U_3 – відправка сповіщення відповідному користувачеві за його IP-адресою, відправка інформації адміністратору про збільшенні активності цього користувача.

Як і в попередніх варіантах, ранжуємо ймовірні результати щодо можливому шкоди:

$C(V_1)$ - нульові збитки;

$C(V_2)$ – незначна шкода (шкода, завдана тільки віддаленому користувача);

$C(V_3)$ - середній шкода (пошкодження системи);

C(V 4) - максимальна шкода (атака реалізована і система пошкоджена).

Якщо система вибирає варіант реагування U_1 то з ймовірністю P_a, яка дорівнює ймовірності реалізації атаки, збитки інформаційній системі дорівнюють нулю (тобто, відсутні), оскільки система захисту припинила атаку.

Якщо ж здійснено керуючий вплив (U_1), але відбулося хибне спрацювання сенсорів або була зроблена помилка користувачем, то збитки будуть середніми (безпідставно заблоковані системою безпеки пакети, приходять по даному протоколу). Ймовірність даного результату складе $(1-P_a)$.

Реалізація рішення U_2 може призвести або до шкоди для віддаленого

користувача (якщо аномальні події не були викликані реалізацією атаки) з ймовірністю (1-P_a), або (якщо була реалізована атака) можливі два рівноймовірних (P_a/2) за принципом Бернуллі результату.

Коли контрольна дія U_3 та атака здійснені, результатом буде максимальна шкода (реалізована атака не була пригнічена системою захисту з ймовірністю P_a, рівною ймовірності атаки. У випадку хибного спрацювання датчиків або помилка користувача, з рівною ймовірністю (1-P_a)/2 кінцевому користувачеві буде завдано незначної шкоди, інакше не буде ніякого шкоди як системі, так і користувачеві.

4.3 Розробка структури системи інтелектуальної підтримки прийняття рішень по оперативному управлінню захистом інформації

Управління включає процес перетворення інформації про стан об'єкта управління на командну інформацію [65]. Цей процес включає в себе різноманітні функції перетворення інформації, які взаємопов'язані між собою, і реалізація однієї з них зазвичай передбачає реалізацію інших.

Однією з ключових функцій в рамках забезпечення безпеки інформації є оперативне управління, виконання якого сприяє ефективному функціонуванню системи захисту інформації. Оперативне управління забезпечує сталу працездатність системи, швидко реагуючи на зміни в оточуючому середовищі функціонування інформаційної системи, включаючи зовнішні та внутрішні загрози.

Одним з ключових завдань теорії управління є синтез структури системи захисту інформації та параметрів системи управління для захисту певних обсягів інформації. Структурна схема системи оперативного управління може різнитися в залежності від наявної інформації про об'єкт управління, даних про середовище функціонування системи та ступеня невизначеності цієї інформації. Невизначеність, яка існує в системі, пов'язана з невідомими діями потенційних зловмисників.

Умови інформаційної невизначеності, яка включає недостатність даних про

стан об'єкта чи можливі загрози, що призводить до великої невизначеності при ухваленні керуючих рішень, можуть бути краще керовані за допомогою ієрархічного підходу в структурі системи управління.

У системах управління захистом інформації важливою стає роль процесів контролю та аналізу, оскільки такі системи виходять за межі простого регулювання. Розподіл функціонального навантаження може бути організованим наступним чином: регулювання виконується керуючими модулями, тоді як система для прийняття рішень відповідає за аналіз, контроль, планування та ухвалення рішень. Іншими словами, ця система включає в себе функції, які не просто обмежуються регулюванням управління захистом інформації.

Необхідність ієрархічної структури управління оперативною системою обумовлена декількома чинниками:

– Параметри, які підлягають контролю керуючою системою, можуть мати як якісну, так і кількісну природу.

– Зв'язки між параметрами інформаційної системи, що контролюються керуючою системою, та впливами, які генеруються керуючою системою, можуть бути менш формалізованими.

– Інформація, яка надходить від сенсорів чи інших систем щодо стану контрольованого об'єкта, може недостатньо точно відображати справжній стан об'єкта управління у реальному часі.

Усе це обумовлює необхідність розробки багаторівневої системи управління з метою зниження невизначеності при ухваленні рішень та підвищення надійності системи.

Щоб побудувати ієрархічну структуру, слід обрати наступні елементи управління:

– засоби управління - засіб і заходи безпеки;

– модулі управління, вбудовані в захисне обладнання або мережеве обладнання;

– система підтримки прийняття рішень по оперативному управлінню ЗІ

(СППР ОУ).

Введемо позначення інформаційних потоків, що діють в системі:

$U_{зовн}$ - зовнішні загрози,

$U'^{зовн}$ - інформація про стан навколишнього середовища, що доступна в СППР ОУ,

U - інформація про команду на виході СППР ОУ,

$U_{кд}$ - контрольна дія,

X - інформація про стан ОУ - контрольовані параметри,

X' – інформація про контрольовані параметри доступна в СППР ОУ.

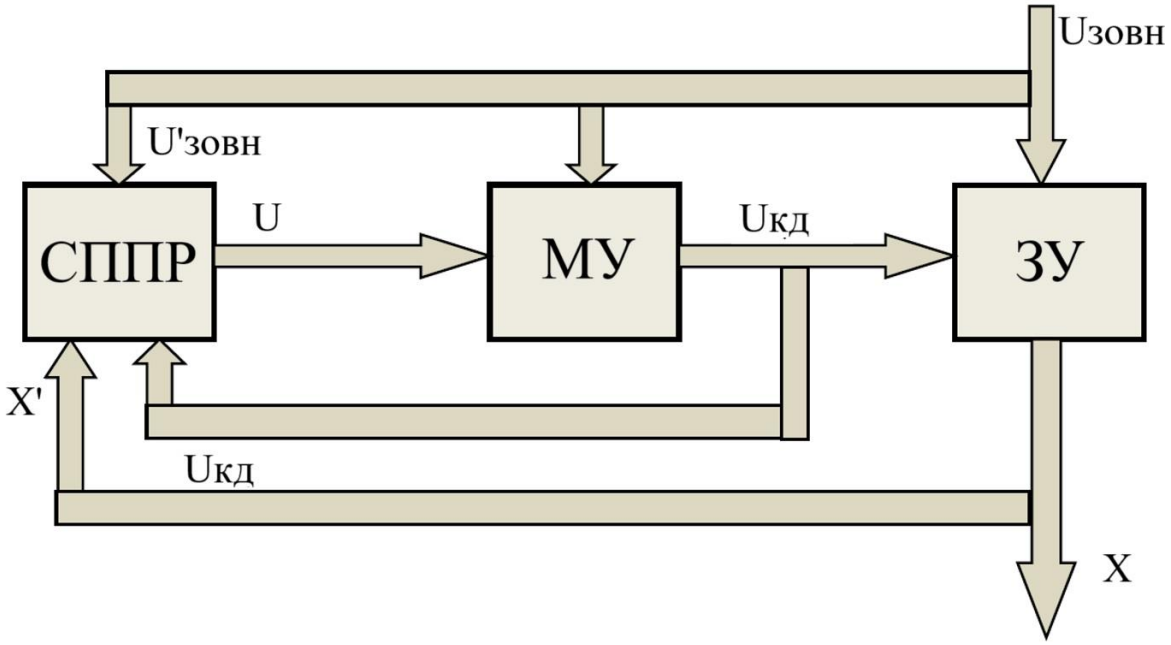

Рисунок 4.5 - Ієрархічна структура керуючої системи

Зниження рівня інформаційної невизначеності є критичним фактором для підвищення якості рішень, які приймаються в системах підтримки процесів управління об'єктами управління. Процес прийняття рішень в таких системах представляє собою складний багатокроковий процес, який залучає керуючі модулі. В ході цього процесу, на підставі наявних даних щодо результатів контролю рішень, обирається варіант реакції на одну або кілька аномальних подій. У цьому контексті вхідні дані, які впливають на вибір реакції, називаються змінними

вибору, оскільки вони впливають на вибір керуючої системи, посилюючи позитивні реакції і послаблюючи негативні.

У випадках, коли завдання не піддається формалізації і прийняття рішення на основі набору даних та наявних реакцій не можливе, потрібна участь людського інтелекту. Автоматизовані системи (у відміну від автоматичних) призначені для часткового виконання завдань такого типу людиною, як наприклад, експертна оцінка.

Крім безпосереднього управління, система управління захистом інформації забезпечує збір та аналіз інформації про процеси управління і результати виконання різних рішень. Це сприяє зниженню рівня невизначеності при прийнятті рішень і підвищенню їх ефективності, оскільки керуюча система накопичує дані, які дозволяють точніше прогнозувати результати виконання різних рішень.

Створення архітектурного рішення для системи підтримки процесів управління об'єктами управління, відповідно до вищезазначеного, передбачає використання інтелектуальних інформаційних технологій, включаючи:

– оцінку ймовірності того, що аномальна подія є атакою, яка реалізується з використанням механізму нечіткого висновку;

– упорядкування інформації та даних про систему, а також даних про події безпеки, які накопичуються системою під час роботи, в спеціальній базі знань керуючої системи;

– реалізацію інтелектуальних алгоритмів для вибору рішень стосовно застосування керуючого впливу при виникненні аномальних подій в системі.

На рисунку 4.6 представлено запропоновану архітектурну будову системи інтелектуальної підтримки прийняття рішень в рамках оперативного управління.

Головним завданням системи підтримки процесів управління об'єктами управління (СППР ОУ) є розробка оптимального керуючого рішення, яке забезпечить захист інформаційної системи від зовнішніх атак на об'єкт захисту і, при цьому, мінімізуватиме вплив цього рішення на нормальну роботу інформаційної системи.

СППР ОУ діє в динамічному режимі, проводячи постійний моніторинг та

аналіз даних, що надходять із датчиків, у режимі реального часу. Система контролю інформаційної безпеки відстежує й аналізує навколишнє середовище функціонування для виявлення потенційно небезпечних подій.

Необхідність визначення максимально можливої кількості атак передбачає використання підсистем виявлення аномалій, які діють на різних рівнях комп'ютерно-інформаційної системи в системі управління. Підмножина контрольованих параметрів може включати параметри, що описують стан мережі, процеси та стани ресурсів користувачів, а також стан системних ресурсів. Отримані дані, зареєстровані в відповідних журналах, піддаються оперативному аналізу.

Для отримання даних використовуються датчики, розташовані в різних сегментах мережі, включаючи точки виходу в глобальну мережу, окремі сегменти локальної мережі інформаційної системи, комутатори, маршрутизатори та інші компоненти. Кожен датчик збирає інформацію про події безпеки, які відбуваються в відповідному вузлі, і передає цю інформацію для протоколювання в відповідних журналах. Також інформацію від датчиків може передаватися через додаткові програмні компоненти.

Аналізуючи вхідні дані від датчиків, механізм виявлення аномалій та оперативний аналіз даних визначають, чи події, які відбуваються, є нормою, чи їх можна визнати аномальними, виявляючи в послідовності подій відхилення від стандартних шаблонів дій.

Це дозволяє системі захисту інформації виявляти не лише відомі атаки, які були раніше відомі, але і ті, які системі невідомі, як зовнішні, так і внутрішні (наприклад, порушення дозволів користувачів для доступу до інформації).

Важливо відзначити, що не кожен випадок аномальних подій пов'язаний із спробою здійснення атаки. Такі події можуть бути спричинені, наприклад, помилками користувачів, неправильною роботою датчиків тощо. В результаті формування керуючого впливу, відповідного атаки, систему може бути виведено зі стандартного режиму роботи при відсутності загрози безпеки (тобто спричинено помилкове спрацювання).

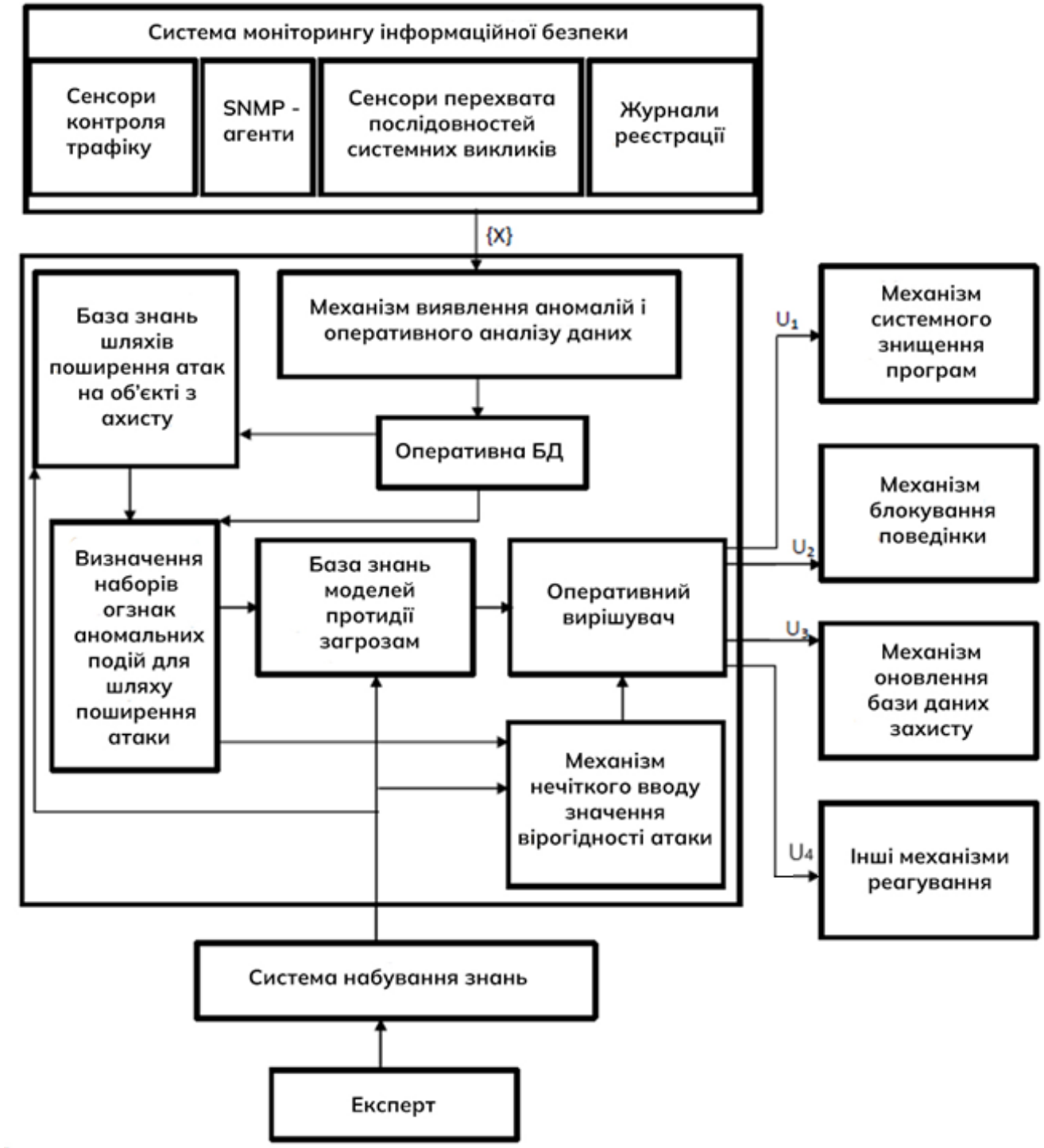

Рисунок 4.6 – Структура системи інтелектуальної підтримки прийняття рішень в рамках оперативного управління ЗІ

Для вирішення цієї проблеми в запропонованій СППР ОУ керуючі рішення приймаються на підставі розрахунку ймовірності того, що розглянута подія є атакою. Для проведення цього розрахунку застосовується механізм нечіткого логічного висновку, оскільки параметри, що дозволяють однозначно віднести

аномалії до класу атак, не завжди мають кількісні показники і не завжди можуть бути однозначно описані.

Модуль "Механізм нечіткого висновку ймовірності атаки" впроваджується в запропонованій архітектурі СППР ОУ. Завдяки цьому підходу механізм прийняття рішень дозволяє оптимально використовувати накопичений експертний досвід та подолати інформаційні проблеми, такі як неповнота та суперечливість інформації щодо її стану, що в свою чергу допомагає зменшити невизначеність при процесі прийняття рішень.

У системі може бути використана різна кількість датчиків, сенсорів та підсистем виявлення, і для обчислення числового значення "Коефіцієнта впевненості" необхідно узагальнювати дані, отримані від них. Для зручності узагальнення даних можна використовувати стандартизований формат даних.

Аналізатор повинен передавати модуль вектора, що має вигляд:

$$S = (I_o, I_p, T), \tag{4.1}$$

де I_0 - системний ідентифікатор виявника, I_p - ідентифікатор шляху атаки, T - системний час.

Ефективність використаного алгоритму для вибору керуючого рішення має вирішальне значення для продуктивності всієї системи захисту інформації. У запропонованому варіанті СППР ОУ, варіант реагування формується в оперативному приймачі на основі обчисленого "коефіцієнта впевненості", де значення ймовірностей результатів розраховуються як функція цього коефіцієнта. Ефективним методом організації тематичної інформації є її модельне представлення. Таблична форма бази даних моделей захисту від загроз зберігає функції реалізації для кожного типу атаки та шляхи її поширення, які були визначені експертами.

У процесі процеси накопичення знань автоматизованою системою СППР ОУ можна виділити кілька ключових етапів.

На етапі концептуалізації реалізуються наступні процеси:

– вибір і формалізація наборів змінних, які описують (характеризують) події безпеки, що відбуваються в системі;

– експертне завдання функцій приналежності, визначення характеристик подій безпеки, які можуть бути віднесені до класу атак;

– формування експертом правил, які задають реакцію системи в відповідь на виявлення потенційно небезпечні події;

– формування бази даних про можливі джерела і шляхи;

– поширення атак;

– формування структури інформаційних джерел про можливі загрози і атаки;

– аналіз варіантів реагування, альтернатив дій системи (U_i) і зіставлення цих варіантів з ймовірними наслідками (V_j) і потенційною шкодою від даних результатів (C_j).

Всі знання задаються на основі знань у єдиній формалізованій формі уявлення.

Для реалізації описаного вище методу прийняття рішення модель протидії загрозам кожної ситуації на основі знань моделей може бути задана в табличній формі функцією реалізації, причому кожен варіант відповіді відповідає результату та його оцінка залежить від стану середовища z_j.

Інженер на основі знань генерує опис рішення проблеми на формальну мовою для операційного вирішувача. У робочому рішенні ймовірності $p(z_j)$, і функція $J(U,z)$ розраховуються для кожної альтернативи на основі функції реалізації, визначеної для ситуації з бази моделі. Далі вибирається найкращий варіант відповіді U^*, щоб забезпечити мінімальне пошкодження системи.

Інформація в базі знань повинна доповнюватись та актуалізуватися по мірі оновлення і доповнення даних про поточний стан інформаційної системи та середовища її роботи.

У модулі «Визначення наборів аномальних подій для шляху поширення атаки» генеруються блоки знань, узагальнюється інформація, що постачається

датчиками і сигнальними системами про реалізовані атаки і далі ця інформація використовується для актуалізації бази знань і подальшого застосування при обчисленні «коефіцієнта впевненості» та вибору функції реалізації реакції системи з наявної в наявності бази знань моделей протидії загроз. У ході такої актуалізації всі сигнали, що надходять від аналізаторів, прив'язуються до єдиної тимчасової осі і формується шлях поширення атаки. Таким чином, кожна послідовність подій безпеки, які можуть бути кваліфіковані як атака, має послідовність повідомлень від сигналізаторів, впорядкований за часом. Відповідно, кожен шлях поширення атак обробляється індивідуально і вироблення керуючого впливу виготовляється в залежності від цього шляху.

Точне і детальне налаштування механізму нечіткою логіки і формування адекватної бази знань є критично важливим, оскільки зростанням ймовірності виявлення потенційної атаки, зростає і ймовірність виникнення помилкового спрацювання, якщо механізм прийняття рішень при високій чутливості аналізаторів не адекватно оцінює значимість подій безпеки.

Серед можливих варіантів реагування системи безпеки можуть бути запрограмовані як некритичні дії (такі як тимчасове блокування користувача або процесу, зниження його пріоритету), так і більш серйозний вплив (повне блокування потенційно небезпечних процесів, портів, переривання процесів, знищення програмною системи).

Використання цією моделі управління інформаційної безпекою дозволяє контролювати трафік і необхідні вузли, а також своєчасно реагувати на зміни в операційної середовищі найбільш ефективним чином.

4.4 Висновки до розділу

Математична модель інформаційної системи, розроблена на основі теоретичного підходу до наборів, представляє собою систему зі складовими елементами, які розподілені за трьома рівнями конфіденційності і взаємодіють певними співвідношеннями. Такий підхід дозволяє ідентифікувати численні

джерела загроз для елементів кожного сегмента та можливі шляхи атак. Для кожного сегмента проводиться оцінка кількості можливих шляхів атаки у кількісному виразі. Для прийняття обґрунтованих управлінських рішень може бути впроваджена система функціональних показників, які відображають реалізацію атак на кожному шляху.

Вводиться поняття "коефіцієнта впевненості", яке дозволяє визначити подію як атаку або ймовірність атаки на основі механізму нечіткого логічного виведення. Використовуючи зібраний досвід від кваліфікованих експертів, який узагальнено в формі бази правил і сформульовано на основі лінгвістичних змінних, пов'язаних з аномальними подіями, можна оцінити ймовірність атаки за допомогою числового значення.

У запропонованому методі прийняття рішень раціональний варіант полягає в тому, що ймовірність результату не визначається на основі статистичних даних, а обчислюється з використанням ймовірності атаки з застосуванням механізму нечіткого висновку. Це підвищує надійність прийняття рішення стосовно наявності атаки та зменшує ризик ухвалення нераціональних рішень.

Розроблена структура системи підтримки прийняття рішень для оперативного управління включає модулі на основі інтелектуальних технологій, які ефективно вирішують завдання вибору раціональних реакцій на події в галузі безпеки.

ВИСНОВКИ

У магістерській роботі розглянуто методологічні основи управління інформаційною безпекою в сегменті комп'ютерної інформаційної системи, використовуючи принципи системного аналізу та загальні принципи створення систем управління, що представляє новий підхід до структури системи управління інформаційною безпекою з використанням інтелектуальних технологій.

Модель протидії загрозам, представлена в роботі, базується на оцінці ймовірності атаки, яка реалізована з використанням механізму нечіткої логіки. Цей механізм обирає раціональне рішення на основі оперативних даних про події безпеки, які надходять з різних джерел інформації. Ця модель допомагає зменшити можливі збитки від атак на інформаційну систему та сприяє реакції системи захисту інформації.

На основі трьохрівневої моделі захисту інформації були проведені розрахунки, які дали можливість кількісно оцінити кількість можливих шляхів поширення атак до вузлів в сегментах. Було впроваджено показник "коефіцієнт впевненості", який дозволяє класифікувати аномальні події інформаційної системи як атаку за допомогою механізму нечіткої логічної інтерпретації.

Ієрархічна структура системи інтелектуальної підтримки прийняття рішень для оперативного управління інформаційною безпекою, а також структура системи інтелектуальної підтримки прийняття рішень при оперативному управлінні захистом інформації було розроблено. Запропонована структура рішень, прийнятих системою, стосується вибору раціональних варіантів реагування на події безпеки за допомогою застосування інтелектуальних технологій для вирішення слабо формалізованих завдань класифікації подій безпеки в системі та вибору шляхів реагування на них.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. M. T. Arefin, M. R. Uddin, N. A. Evan, M. R. Alam. Enterprise Network: Security Enhancement and Policy Management Using Next-Generation Firewall (NGFW). *Computer Networks, Big Data and IoT. Lecture Notes on Data Engineering and Communications Technologies*. 2021. Vol. 66. DOI: https://doi.org/10.1007/978-981-16-0965-7_59

2. T. Musa et al. Analysis of Complex Networks for Security Issues using Attack Graph. *International Conference on Computer Communication and Informatics (ICCCI)*. 2019. PP. 1-6. DOI: 10.1109/ICCCI.2019.8822179.

3. X. Lyu, Y. Ding, S.-H. Yang. Safety and security risk assessment in cyber-physical systems. *IET Cyber-Physical Systems: Theory & Applications*. 2019. Vol. 4, No. 3. PP. 221-232. DOI: https://doi.org/10.1049/iet-cps.2018.5068

4. B. Vaishnavi, D. Savant, D. Rupali, A. Kasar. A Review on Network Security and Cryptography. *Research Journal of Engineering and Technology*. 2021. Vol. 12, No. 4. DOI: 10.52711/2321-581X.2021.00019

5. F. Alkhudhayr, S. Alfarraj, B. Aljameeli, S. Elkhdiri. Information Security: A Review of Information Security Issues and Techniques. *2nd International Conference on Computer Applications & Information Security (ICCAIS)*. 2019. PP. 1-6. DOI: 10.1109/CAIS.2019.8769504.

6. O. C. Abikoye, A. D. Haruna, A. Abubakar, N. O. Akande, E. O. Asani. Modified Advanced Encryption Standard Algorithm for Information Security. *Symmetry*. 2019. Vol. 11. DOI: https://doi.org/10.3390/sym11121484

7. AM Qadir and N. Varol, "A Review Paper on Cryptography", *2019 7th International Symposium on Digital Forensics and Security (ISDFS)* , Barcelos, Portugal, 2019, pp. 1-6, doi: 10.1109/ISDFS.2019.8757514.

8. Amarudin, R. Ferdiana, Widyawan. A Systematic Literature Review of Intrusion Detection System for Network Security: Research Trends, Datasets and Methods. *4th International Conference on Informatics and Computational Sciences (ICICoS)*. 2020. PP. 1-6. DOI: 10.1109/ICICoS51170.2020.9299068.

9. Ilhan Firat Kilincer, Fatih Ertam, Abdulkadir Sengur. Machine learning methods for cyber security intrusion detection: Datasets and comparative study. *Computer Networks*. 2021. Vol. 188. DOI: https://doi.org/10.1016/j.comnet.2021.107840.

10. I. A. Khan, D. Pi, N. Khan. A privacy-conserving framework based intrusion detection method for detecting and recognizing malicious behaviours in cyber-physical power networks. *Appl Intell*. 2021. Vol. 51. PP. 7306–7321. DOI: https://doi.org/10.1007/s10489-021-02222-8

11. Arwa Aldweesh, Abdelouahid Derhab, Ahmed Z. Emam. Deep learning approaches for anomaly-based intrusion detection systems: *A survey, taxonomy, and open issues. Knowledge-Based Systems*. 2020. Vol. 189. DOI: https://doi.org/10.1016/j.knosys.2019.105124.

12. D. Liu, B. Lang. Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey. *Appl. Sci.* 2019. Vol. 9. DOI: https://doi.org/10.3390/app9204396

13. M. Poongodi, V. Vijayakumar, F. Al-Turjman, M. Hamdi, M. Ma. Intrusion Prevention System for DDoS Attack on VANET With reCAPTCHA Controller Using Information Based Metrics. *IEEE Access*. 2019. Vol. 7. PP. 158481-158491. DOI: 10.1109/ACCESS.2019.2945682.

14. K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, M. Xu. A Survey on Machine Learning Techniques for Cyber Security in the Last Decade. *IEEE Access*. 2020. Vol. 8. PP. 222310-222354. DOI: 10.1109/ACCESS.2020.3041951.

15. I. H. Sarker, M. H. Furhad, R. Nowrozy. AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. *SN COMPUT. SCI.* 2021. Vol. 2. P. 173. DOI: https://doi.org/10.1007/s42979-021-00557-0

16. W. Wang, J. Song, G. Xu, Y. Li, H. Wang, C. Su. ContractWard: Automated Vulnerability Detection Models for Ethereum Smart Contracts. *IEEE Transactions on Network Science and Engineering*. 2021. Vol. 8, No. 2. PP. 1133-1144. DOI: 10.1109/TNSE.2020.2968505.

17. Sara Mohammadi, Hamid Mirvaziri, Mostafa Ghazizadeh-Ahsaee, Hadis Karimipour. Cyber intrusion detection by combined feature selection algorithm. *Journal of Information Security and pplications*. 2019. Vol. 44. PP. 80-88. DOI: https://doi.org/10.1016/j.jisa.2018.11.007.

18. W. Dimitrov, B. Jekov, E. Kovatcheva, L. Petkova. AN ANALYSIS OF THE NEW CHALLENGES FACING CYBER SECURITY EXPERTISE. *12th International Conference on Education and New Learning*. 2020. PP. 2978-2986. DOI: 10.21125/edulearn.2020.0890

19. Juan Camilo Correa Chica, Jenny Cuatindioy Imbachi, Juan Felipe Botero Vega. Security in SDN: A comprehensive survey. *Journal of Network and Computer Applications*. 2020. Vol. 159. DOI: https://doi.org/10.1016/j.jnca.2020.102595.

20. A. Yazdinejad, R. M. Parizi, A. Dehghantanha, K.-K. R. Choo. Blockchain-Enabled Authentication Handover With Efficient Privacy Protection in SDN-Based 5G Networks. *IEEE Transactions on Network Science and Engineering*. Vol. 8, No. 2. PP. 1120-1132. DOI: 10.1109/TNSE.2019.2937481.

21. P. I. Radoglou-Grammatikis, P. G. Sarigiannidis. Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems. *IEEE Access*. 2019. Vol. 7. PP. 46595-46620. DOI: 10.1109/ACCESS.2019.2909807.

22. Ikuobase Emovon, Okpako Stephen Oghenenyerovwho. Application of MCDM method in material selection for optimal design: A review. *Results in Materials*. 2020. Vol. 7. DOI: https://doi.org/10.1016/j.rinma.2020.100115.

23. Anjum Nazir, Rizwan Ahmed Khan. A novel combinatorial optimization based feature selection method for network intrusion detection. *Computers & Security*. 2021. Vol. 102. DOI: https://doi.org/10.1016/j.cose.2020.102164.

24. Gang Kou, Pei Yang, Yi Peng, Feng Xiao, Yang Chen, Fawaz E. Alsaadi. Evaluation of feature selection methods for text classification with small datasets using multiple criteria decision-making methods. *Applied Soft Computing*. 2020. Vol. 86. DOI: https://doi.org/10.1016/j.asoc.2019.105836.

25. M. Injadat, A. Moubayed, A. B. Nassif, A. Shami. Multi-Stage Optimized Machine Learning Framework for Network Intrusion Detection. *IEEE Transactions on*

Network and Service Management. 2021. Vol. 18, No. 2. PP. 1803-1816. DOI: 10.1109/TNSM.2020.3014929.

26. Atif Ahmad, Jeb Webb, Kevin C. Desouza, James Boorman. Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. *Computers & Security*. 2019. Vol. 86. PP. 402-418. DOI: https://doi.org/10.1016/j.cose.2019.07.001.

27. S. Pandey, R. K. Singh, A. Gunasekaran, A. Kaushik. Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing*. 2020. Vol. 13, No. 1. PP. 103-128. DOI: https://doi.org/10.1108/JGOSS-05-2019-0042

28. Muhammed Zekeriya Gunduz, Resul Das. Cyber-security on smart grid: Threats and potential solutions. *Computer Networks*. 2020. Vol. 169. DOI: https://doi.org/10.1016/j.comnet.2019.107094.

29. Malyun Hilowle, William Yeoh, Marthie Grobler, Graeme Pye & Frank Jiang. (2023) Users' Adoption of National Digital Identity Systems: Human-Centric Cybersecurity Review. *Journal of Computer Information Systems* 63:5, pages 1264-1279.

30. C. Peng, H. Sun, M. Yang, Y.-L. Wang. A Survey on Security Communication and Control for Smart Grids Under Malicious Cyber Attacks. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*. 2019. Vol. 49, No. 8. PP. 1554-1569. DOI: 10.1109/TSMC.2018.2884952.

31. M. Alazab, S. P. RM, P. M, P. K. R. Maddikunta, T. R. Gadekallu, Q.-V. Pham. Federated Learning for Cybersecurity: Concepts, Challenges, and Future Directions. *IEEE Transactions on Industrial Informatics*. 2022. Vol. 18, No. 5. PP. 3501-3509. DOI: 10.1109/TII.2021.3119038.

32. Zhang, Yuhang, Ming Ni. Security-Oriented Cyber-Physical Risk Assessment for Cyberattacks on Distribution System. *Applied Sciences*. 2023. Vol. 13, No. 20. DOI: https://doi.org/10.3390/app132011569

33. S. J. Pinto, P. Siano, M. Parente. Review of Cybersecurity Analysis in Smart Distribution Systems and Future Directions for Using Unsupervised Learning Methods for Cyber Detection. *Energies*. 2023. Vol. 16. DOI: https://doi.org/10.3390/en16041651

34. S. Shamshad, F. Riaz, R. Riaz, S. S. Rizvi, S. Abdulla. An Enhanced Architecture to Resolve Public-Key Cryptographic Issues in the Internet of Things (IoT), Employing Quantum Computing Supremacy. *Sensors*. 2022. Vol. 22. DOI: https://doi.org/10.3390/s22218151

35. H. Aldawood, G. Skinner. Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. *Future Internet*. 2019. Vol. 11. DOI: https://doi.org/10.3390/fi11030073

36. Marijn Janssen, Paul Brous, Elsa Estevez, Luis S. Barbosa, Tomasz Janowski. Data governance: Organizing data for trustworthy Artificial Intelligence. *Government Information Quarterly*. 2020. Vol. 37, No. 3. DOI: https://doi.org/10.1016/j.giq.2020.101493

37. Hind Benbya, Ning Nan, Huseyin Tanriverdi, Youngjin Yoo. Complexity and Information Systems Research in the Emerging Digital World. *MIS Quarterly*. 2020. Vol. 44, No. 1. PP. 1-17.

38. Ting (Carol) Li, Yolande E. Chan. Dynamic information technology capability: Concept definition and framework development. *The Journal of Strategic Information Systems*. 2019. Vol. 28, No. 4. DOI: https://doi.org/10.1016/j.jsis.2019.101575.

39. C. Cubukcu, C. Cantekin. Using a combined fuzzy-AHP and topsis decision model for selecting the best firewall alternative. *Journal of Fuzzy Extension and Applications*. 2022. Vol. 3, No. 3. PP. 192-200. DOI: 10.22105/jfea.2021.313606.1167

40. N. Bhatt, J. Kaur, A. Anand, O. H. Alhazmi. Selecting best software vulnerability scanner using intuitionistic fuzzy set topsis. *Computers, Materials & Continua*. 2022. Vol. 72, No. 2. PP. 3613–3629. DOI: 10.32604/cmc.2022.026554

41. C. Cubukcu, C. Cantekin. Using a Fuzzy-AHP Decision Model for Selecting the Best Firewall Alternative. *Intelligent and Fuzzy Techniques for Emerging Conditions and Digital Transformation. INFUS 2021. Lecture Notes in Networks and Systems*. 2021.

Vol 307. DOI: https://doi.org/10.1007/978-3-030-85626-7_50

42. Jiaming Pei, Kaiyang Zhong, Mian Ahmad Jan, Jinhai Li. RETRACTED: Personalized federated learning framework for network traffic anomaly detection. *Computer Networks*. 2022. Vol. 209. DOI: https://doi.org/10.1016/j.comnet.2022.108906.

43. J. H. Addae, X. Sun, D. Towey. Exploring user behavioral data for adaptive cybersecurity. *User Model User-Adap Inter* . 2019. Vol. 29. PP. 701–750. DOI: https://doi.org/10.1007/s11257-019-09236-5

44. Meenal Jain, Gagandeep Kaur, Vikas Saxena. A K-Means clustering and SVM based hybrid concept drift detection technique for network anomaly detection. *Expert Systems with Applications*. 2022. Vol. 193. DOI: https://doi.org/10.1016/j.eswa.2022.116510.

45. Zhengbing Hu, Roman Odarchenko, Sergiy Gnatyuk, Maksym Zaliskyi, Anastasia Chaplits, Sergiy Bondar, Vadim Borovik. Statistical Techniques for Detecting Cyberattacks on Computer Networks Based on an Analysis of Abnormal Traffic Behavior. *International Journal of Computer Network and Information Security(IJCNIS)*. 2020. Vol. 12, No. 6. PP. 1-13. DOI: 10.5815/ijcnis.2020.06.01

46. A. Banitalebi Dehkordi, M. Soltanaghaei, F. Z. Boroujeni. The DDoS attacks detection through machine learning and statistical methods in SDN. *J Supercomput*. 2021. Vol. 77. PP. 2383–2415. DOI: https://doi.org/10.1007/s11227-020-03323-w

47. S. Mahdavifar, A. Ghorbani. DeNNeS: deep embedded neural network expert system for detecting cyber attacks. *Neural Comput & Applic*. 2020. Vol. 32. PP. 14753–14780. DOI: https://doi.org/10.1007/s00521-020-04830-w

48. M. I. Malik, A. Ibrahim, P. Hannay, L. F. Sikos. Developing Resilient Cyber-Physical Systems: A Review of State-of-the-Art Malware Detection Approaches, Gaps, and Future Directions. *Computers*. 2023. Vol. 12. DOI: https://doi.org/10.3390/computers12040079

49. D. Ding, Q. -L. Han, X. Ge, J. Wang. Secure State Estimation and Control of Cyber-Physical Systems: A Survey. *IEEE Transactions on Systems, Man, and*

Cybernetics: Systems. 2021. Vol. 51, No. 1. PP. 176-190. DOI: 10.1109/TSMC.2020.3041121.

50. С.В. Батечко, О.Ю. Лебедєва, В.В. Зоріло. Методика оцінки захищеності інформаційних систем. Інформатика та математичні методи в моделюванні. *Informatics and Mathematical Methods in Simulation*. 2021. Vol. 11, No. 3. PP. 173-180. DOI: 10.15276/imms.v11.no3.173

51. О. В. Потій, Ю.І. Горбенко, О.А. Замула, К.В. Ісірова. Аналіз методів оцінки і управління ризиками кібер- і інформаційної безпеки. *Моделі, методи та засоби захисту інформації в інформаційно-комунікаційних системах*. *Радіотехніка.* 2021. Вип. 206. DOI:10.30837/rt.2021.3.206.01

52. A. Yeboah-Ofori, S. Islam. Cyber Security Threat Modeling for Supply Chain Organizational Environments. *Future Internet.* 2019. Vol. 11, No. 63. DOI: https://doi.org/10.3390/fi11030063

53. Гур'єв В.І. Інформаційна безпека держави: навч. посіб. Ніжин: ФОП Лук'янченко В.В. ТПК «Орхідея», 2018. – 166 с.

54. V. Tsurkan, O. Shapoval. Analysis of computer network security risk assessment methods. *Collection "Information Technology and Security"*. 2022. Vol. 10, No. 2. PP. 204–215. DOI: https://doi.org/10.20535/2411-1031.2022.10.2.270437

55. L. Kozubtsova, I. Rudomino-Dusyatska, V. Snovida. Calculation of performance indicators of the information protection and cybersecurity system. *Computer-Integrated Technologies: Education, Science, Production*. 2021. Vol. 45. PP. 19-25. DOI: https://doi.org/10.36910/6775-2524-0560-2021-45-03

56. David Rios Insua, Aitor Couce-Vieira, A. An Adversarial Risk Analysis Framework for Cybersecurity. *Risk Analysis*. 2021. Vol. 41, No. 1. PP. 16-36. DOI: https://doi.org/10.1111/risa.13331

57. Adéle da Veiga, Liudmila V. Astakhova, Adéle Botha, Marlien Herselman. Defining organisational information security culture — Perspectives from academia and industry. *Computers & Security*. 2020. Vol. 92. DOI: https://doi.org/10.1016/j.cose.2020.101713.

58. Вступ до кібербезпеки: навч. посіб / Смірнов О.А. та ін.

Кропивницький: ЦНТУ, 2022. – 967 с.

59. Л. Ф. Дзюба, О. Ю. Чмир. Оцінювання ризиків інформаційної безпеки з використанням методів математичної статистики. *Вісник ЛДУБЖД*. 2022. № 26. ст. 47-54. DOI: 10.32447/20784643.26.2022.06

60. A. Aljuhani. Machine Learning Approaches for Combating Distributed Denial of Service Attacks in Modern Networking Environments. *IEEE Access*. 2021. Vol. 9. PP. 42236-42264. DOI: 10.1109/ACCESS.2021.3062909.

61. Олена Данченко, Євген Ланських, Олександр Семко. Інформаційні ризики цифрового формату. *Вісник Черкаського державного технологічного університету*. 2020. ст. 58-66. DOI: 10.24025/2306-4412.3.2020.200792.

62. Ю. Руденко. Методи навчання теорії нечітких множин студентів. *European Science.* 2023. Vol. 2. PP. 53–64. DOI: https://doi.org/10.30890/2709-2313.2023-17-02-028

63. V. Lakhno, A. Blozva, M. Misiura, D. Kasatkin, B. Gusev. Модель показника поточного ризику реалізації загроз інформаційно-комунікаційним системам. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2020. Vol. 2, No. 10. PP. 113–122. DOI: https://doi.org/10.28925/2663-4023.2020.10.113122

64. S. Honchar, A. Onyskova, A. Relevance of the subjective component in cybersecurity risk assessment. *Збірник наукових праць ΛΌГОΣ*. 2020. PP. 22-23. DOI: https://doi.org/10.36074/24.07.2020.v2.07

65. S. Zheng, S. Shu, F. Lin. Modeling and Control of Discrete Event Systems Under Joint Sensor-Actuator Cyber Attacks. *IEEE Transactions on Control of Network Systems.* DOI: 10.1109/TCNS.2023.3312249.

ДОДАТОК А ПЕРЕЛІК НАУКОВИХ ПРАЦЬ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
НАУКОВА АСОЦІАЦІЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

УДК 004.4

Тези доповідей

**VII Міжнародної науково-практичної конференції
до 30-ти річчя кафедри кібербезпеки та програмного забезпечення**

"Інформаційна безпека та комп'ютерні технології"

1 листопада 2023 року

Кропивницький 2023

УДК 004.4

Матеріали VII Міжнародної науково-практичної конференції "Інформаційна безпека та комп'ютерні технології" до 30-ти річчя кафедри кібербезпеки та програмного забезпечення: тези доповідей, 1 листопада 2023 р. – Кропивницький: ЦНТУ, 2023. – 135 с.

Наведені тези пленарних та секційних доповідей за теоретичними та практичними результатами наукових досліджень і розробок. Представлені результати теоретичних досліджень в галузях проектування інформаційних систем, технологій захисту інформації, використання сучасних інформаційних технологій в управлінні системами за різними галузями народного господарства.

Матеріали публікуються в авторській редакції.

За достовірність викладених фактів, цитат та інших відомостей відповідальність несуть автори.

ЗМІСТ

СЕКЦІЯ 1. ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ, СУСПІЛЬСТВА ТА ОСОБИСТОСТІ

УДК 004.056

Д.О. Душко[1], Н.С.Петляк[1]
ddushko@khmnu.edu.ua, npetlyak@khmnu.edu.ua
[1]Хмельницький національний університет, м. Хмельницький

МЕТОД ТА СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

Корпоративна інформаційна система - це комплекс апаратних засобів (сервера та серверне обладнання, робочі станції, канали зв'язку та ін.), каналів зв'язку та програмного забезпечення даної системи [1].

Задля створення ефективної системи захисту інформації важливо під час розробки дотримуватися низки ключових принципів, а саме:

– комплексність та узгодженість – побудова системи захисту інформації передбачає застосування досить широкого спектру інструментів та методів захисту, при цьому важливо підтримувати цілісність системи та уникати вразливостей у взаємодії окремих компонентів системи;

– диференціація – кожен рівень захисту має розроблятися з урахуванням рівня важливості та критичності інформації, оцінки потенційних атак;

– достатність механізмів захисту - передбачає оцінку співвідношення витрат на створення та підтримку системи захисту інформації та можливої шкоди.

Проаналізувавши можливі шляхи здійснення несанкціонованого доступу до інформаційного середовища [2] та ґрунтуючись на вищезазначених принципах організації системи інформаційної безпеки, запропоновано модель системи захисту інформації (СЗІ), що буде складатися із трьох основних компонентів: захист від зовнішніх загроз та руйнівних дій зловмисників, захист від віддалених та міжсегментних атак, захист інформаційного середовища від окремих ПК та серверів у мережі. Таким чином, розроблена модель СЗІ включатиме три компоненти: модель захисту від зовнішніх загроз, модель захисту від віддалених та міжсегментних атак та модель захисту у внутрішньому сегменті мережі.

З метою аналізу процесу прийняття рішень щодо протидії загрозам, представимо кілька типів атак: міжсегментну атаку, зовнішню атаку через точку бездротового доступу, зовнішню атаку через інтернет.

Пропонуємо модель протидії у формі зв'язного графа (рис.1а), де U_n – це варіанти реагування, а V_n – варіанти результатів під час реалізації протидії загроз.

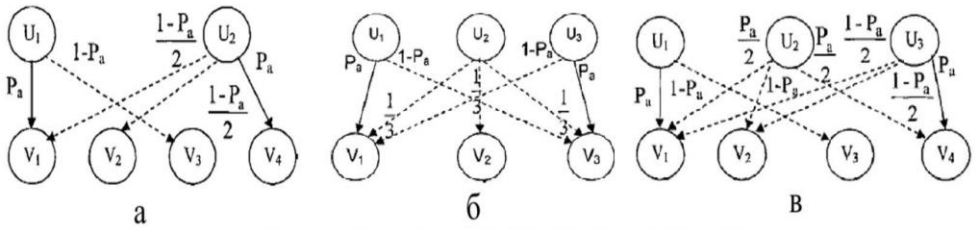

Рис. 1. Граф зв'язків варіантів реагування та результатів:
а) при прийнятті рішень при міжсегментній атаці, б) рішень при зовнішній атаці через Wi-Fi мережу, в) при зовнішній атаці через провайдера

При виборі варіанту реагування U_1 з ймовірністю $1\text{-}P_a$ буде отримано середні втрати, оскільки в якості атаки прийнято при стандартному режимі роботи мережі ненавмисні шкідливі впливи від користувача або помилкове розпізнавання як атаки сигналів із сенсорів.

Реалізація варіанту реагування U_2, може мати три різні варіанти результату. Якщо події, розпізнані як аномальні, дійсно є атакою, то з ймовірністю P_a буде реалізовано максимальні збитки за відсутності блокування атакуючого впливу. У разі якщо розпізнана аномальна дія була причиною помилкових дій користувача, то шкоди не буде (тобто дорівнює нулю). Якщо керуючий вплив буде реалізовано внаслідок помилкового розпізнавання сигналів як атаки, то користувачеві буде відправлено попередження та знижено його пріоритет – буде нанесено незначні збитки користувачеві. У останніх двох варіантах ймовірності результатів складати одну й ту саму величину $(1\text{-}P_a)/2$.

Для реалізації зовнішнього вторгнення зловмиснику потрібен доступ до бездротового адаптера і необхідно, щоб він знаходився в радіусі дії бездротової мережі. На відміну від атаки за допомогою провідної лінії, маємо більш високу ступінь погрози та можливість нанесення максимальної шкоди. Об'єктом атаки в даному випадку є точка доступу.

Для забезпечення захисту використовуються системи виявлення бездротових атак, основою роботи яких є сигнатурний аналіз та аналіз поведінки. Події безпеки генеруються при виявленні відхилення параметрів точки доступу від заданих. Для реалізації захисту інформації процедури реагування повинні бути сформовані

таким чином, щоб були максимально знижені можливі збитки як від реалізації вторгнення, так і від можливого збою взаємодії через точку доступу. Модель протидії у графічному вигляді представлена на рис.1б.

Якщо система реалізує вплив U_1, то з ймовірністю P шкоди системі не буде завдано. Ймовірність P_a, у разі рівна ймовірності атаки. Якщо за реалізацію атаки були помилково розпізнані сигнали сенсорів чи відбулася помилка в діях користувача, то шкода при виборі варіанта реагування впливу U_1 буде. Імовірність $1–P_a$ такого результату відповідає ймовірності помилкової інтерпретації сигналів системою чи помилки користувача. Якщо обраний варіант реагування U_3, то в разі реалізації атаки максимальну шкоду буде отримано з ймовірністю P_a – атаку не відстежено системою. Якщо даний варіант реагування обраний у ситуації помилкового розпізнавання сигналів сенсорів як атаки, то шкода буде нульовою – система захисту не втручається у роботу та продовжується робота в штатному режимі (ймовірність складе $1-P_a$ для даного результату). Якщо системою обраний варіант реагування U_2 (здійснення DOS -атаки), то можливі три варіанти результату (нульовий - запобігання дії зловмисника, середній – заблокований користувач за помилкові дії або максимальний – порушено працездатність мережі, завдано збитки), ймовірності яких дорівнюють 1/3.

Для прийняття рішень з реагування в разі можливого зовнішнього вторгнення через провайдера запропоновано модель протидії, що зображено на рис.1в.

Якщо система вибирає варіант реагування U_1, то з ймовірністю P_a, яка дорівнює ймовірності реалізації атаки, збитки інформаційної системи дорівнює нулю, оскільки система захисту нейтралізувала атаку. Якщо здійснено U_1, але відбулося хибне спрацювання сенсорів або було зроблено помилку користувачем, то шкода буде середнього значення. Ймовірність даного результату становитиме $1-P_a$. Реалізація рішення U_2 може призвести або для завдання шкоди віддаленому користувачеві з ймовірністю $1-P_a$, або у разі реалізованої атаки можливі два рівноймовірні $P_a/2$ результати. Коли U_3 атака здійснена, то результатом буде максимальний збиток (реалізована атака не буде зупинена системою захисту з ймовірністю P_a, що дорівнює ймовірність атаки. У разі помилкового спрацьовування датчиків або помилки користувача, з рівною ймовірністю $(1-P_a)/2$ кінцевому користувачеві буде завдано незначної шкоди, інакше не буде ніякої шкоди як системі, так і користувачеві.

Для реалізації системи управління інформаційною безпекою підприємства, що зображена на рис.2, використано наступні елементи: засоби управління (ЗУ); модулі управління (МУ); система підтримки прийняття рішень керування захистом інформації (СППР); зовнішні загрози (Uзовн); доступна в СППР інформація про стан навколишнього середовища (U'зовн); інформація про команду на виході СППР (U); контрольна дія (Uкд); інформація про стан оперативного керування (X); інформація про контрольовані параметри, що доступні в системі підтримки прийняття рішень керування захистом (X').

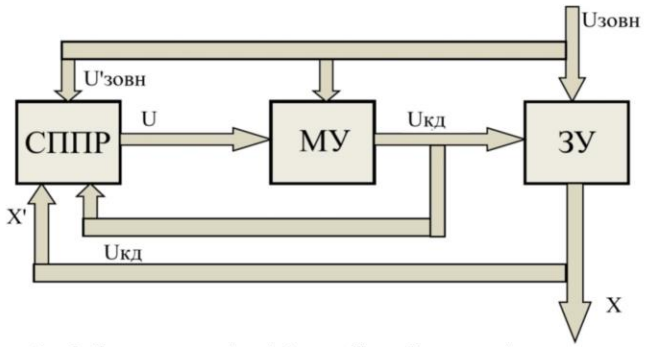

Рис.2. Система управління інформаційною безпекою підприємства

Список літератури

1. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 80/94. Дата оновлення: 01.07.2022. URL: https://zakon.rada.gov.ua/laws/show/80 /94-вр (дата звернення: 28.09.2023)

2. Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Балюнов О.О. Захист інформації в комп'ютерних системах: підручник. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. – 236с.

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Душка Дмитра Олександровича
ПІБ здобувача вищої освіти

студента ФІТ, 2 курсу, групи КБм-22-1

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений (а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

5.12.2023
дата

підпис

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 0.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 3%**

ID: 121615 Назва: Метод і система управління інформаційною безпекою підприємства Додано в БД: 2023-12-03 Автора: Душко Д.О. Керівники: Орленко В.С. Консультанти: Опоненти:	Документ		Сумарний збіг по Базі Даних	
	Символи	Лексеми	Символи	Лексеми
	104394	748	200 (0%)	2 (0%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

UNICHECK
by Turnitin

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1015963701

Дата перевірки:
03.12.2023 19:09:12 EET

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
03.12.2023 19:10:10 EET

ID користувача:
100008300

Назва документа: **Записка Душко_плагіат**

Кількість сторінок: **75** **Кількість слів:** **14608** **Кількість символів:** **117250** **Розмір файлу:** **1.86 MB** **ID файлу:** **1015641973**

4.07%
Схожість

Найбільша схожість: **1.99%** з Інтернет-джерелом (https://www.researchgate.net/publication/283739154_MODEL_OF_INFO.

4.04% Джерела з Інтернету	91	Сторінка 77
0.25% Джерела з Бібліотеки	54	Сторінка 77

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

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

Замінені символи	106

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:
Назва: Метод і система управління інформаційною безпеко підприємства

Автор: Душко Дмитро Олександрович
Спеціальність: 125 – Кібербезпека
Освітня програма: освітньо-професійна
Науковий керівник: Орленко Вікторія Сергіївна, к.т.н, доцент
Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою Unichek складає 4,07%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 0%.

Згідно з правилами чинного Положення «Про систему забезпечення академічної доброчесності у хмельницькому національному університеті» від 31.08.2023, авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 90-100 %, визнається роботою з високою унікальністю тексту і допускається до захисту.

Виявлені системою Unichek модифікації стосуються математичних формул і не є порушенням академічної доброчесності.

Керівник роботи _____ В.С. Орленко

Гарант ОП _____ В.Ю. Тітова

Завідувач кафедри кібербезпеки _____ Ю.П. Кльоц

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «магістр»

Студент Душко Дмитро Олександрович

Тема Метод і система управління інформаційною безпекою підприємства

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «магістр»:

кількість листів креслень - ; кількість сторінок записки 82

1. Короткий зміст роботи та прийнятих В рамках роботи проведено дослідження проблем захисту інформації у сегменті корпоративних інформаційних систем та розроблено систему захисту інформації. В роботі поставлено та вирішено наступні задачі: аналіз наявних рішень управління інформаційною безпекою; розробити метод аналізу інформації для ідентифікації атак та оцінки захищеності системи; змоделювати аналіз факторів інформаційних ризиків на основі лінгвістичного підходу; розробити модель системи захисту; розробити моделі прийняття рішень щодо реагування у разі міжсегментної атаки, зовнішнього вторгнення по радіоканалу, зовнішнього вторгнення через лінії зв'язку; розробити структуру системи інтелектуальної підтримки прийняття рішень задля оперативного управління захистом інформації.

2. Висновок про відповідність кваліфікаційної роботи завданню Кваліфікаційна робота відповідає поставленому завданню як в теоретичній, так і в практичній частині

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: : У вступі обґрунтовується актуальність теми дослідження; її зв'язок із науковими програмами, планами, темами та сформульовано мету та основні завдання дослідження. У першому розділі було досліджено сучасні підходи до захисту інформації та проведено аналіз наявних проблем управління захищеністю інформації, сформовано типову модель розподіленої інформаційної системи підприємства. У другому розділі описано актуальні підходи до розробки системи управління захистом інформації та модель порушника, визначено методику для оцінювання захищеності інформаційної системи. У третьому розділі розроблено модель для оцінки рівня інформаційних ризиків у сегменті корпоративної мережі. уточнено метод оцінювання ризиків безпеки інформаційної системи із застосуванням системи штучного інтелекту. У четвертому розділі представлено розроблену модель систем захисту інформації, розроблено моделі протидії загрозам інформаційної безпеки, запропоновано систему прийняття рішень.

4. Позитивні сторони роботи проекту полягають в підвищенні рівня інформаційної безпеки задля забезпечення ефективного управління захистом інформації завдяки запропонованому методу.

5. Негативні сторони роботи У роботі недостатньо приділено увагу формулюванню визначень понятійного апарату дослідницької роботи. У роботі недостатньо описано особливості впровадження системи управління.

6. Оцінка графічного оформлення та пояснювальної записки роботи Оформлення всіх матеріалів кваліфікаційної роботи є якісним, здійснене з дотриманням актуальних стандартів та інституційних положень ХНУ. Пояснювальна записка відповідає нормам щодо її оформлення як за структурою, так і за представленням і форматуванням матеріалу.

7. Відгук про роботу в цілому Кваліфікаційна робота заслуговує позитивної оцінки.

8. Інші зауваження

9. Оцінка кваліфікаційної роботи Розглянувши позитивні та негативні сторони представленої дипломної роботи, можна зробити висновок, що дипломна робота заслуговує оцінки «добре».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) Завідувач кафедри автоматизації, комп'ютерно-інтегрованих технологій та робототехніки, доктор технічних наук, професор Мартинюк Валерій Володимирович.

« 8 » грудня 2023 року _____ (підпис)