МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Інженерний навчально-науковий інститут ім. Ю.М. Потебні
Кафедра інформаційної економіки, підприємництва та фінансів

КВАЛІФІКАЦІЙНА РОБОТА

НА ТЕМУ: «УПРАВЛІННЯ ЗАХИЩЕНІСТЮ ІНФОРМАЦІЇ ПРОМИСЛОВОГО ПІДПРИЄМСТВА НА ОСНОВІ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ»

другий (магістерський)
(рівень вищої освіти)

Виконав: студент 2 курсу, групи 8.0512-ie
спеціальності 051 Економіка
(шифр і назва спеціальності)
освітньої програми Інформаційна економіка
(назва освітньої програми)
О.В. Тарасенко
(ініціали та прізвище)
Керівник професор кафедри інформаційної економіки, підприємництва та фінансів, доцент, д-р екон. наук Клопов І.О.
(посада, вчене звання, науковий ступінь, прізвище та ініціали)
Рецензент доцент кафедри інформаційної економіки, підприємництва та фінансів, доцент, канд. екон. наук Сіліна І.В.
(посада, вчене звання, науковий ступінь, прізвище та ініціали)

Запоріжжя – 2023

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІНЖЕНЕРНИЙ НАВЧАЛЬНО-НАУКОВИЙ
ІНСТИТУТ ім. Ю.М. ПОТЕБНІ

Кафедра інформаційної економіки, підприємництва та фінансів

Рівень вищої освіти другий (магістерський)

Спеціальність 051 Економіка
(шифр і назва)

Освітня програма Інформаційна економіка

ЗАТВЕРДЖУЮ

Завідувач кафедри інформаційної економіки, підприємництва та фінансів, д-р екон. наук, проф.

_____ Шапуров О.О..
(підпис)

“ ____ ” _____ 202_ р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТОВІ

Тарасенку Олексію Володимировичу
(прізвище, ім’я та по-батькові)

1. Тема роботи Управління захищеністю інформації промислового підприємства на основі інтелектуальних технологій

керівник роботи Клопов Іван Олександрович, д-р екон. наук, доцент
(прізвище, ім’я та по-батькові, науковий ступінь, вчене звання)

затверджені наказом ЗНУ від « 01 » травня 2023 року № 642-с

2. Строк подання студентом роботи 27.11.2023

3. Вихідні дані до роботи 1. Постановка задачі.
2. Перелік літератури.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Методологічні основи управління захистом інформації в корпоративних інформаційних системах.
2. Модель оцінки рівня інформаційних ризиків у сегменті корпоративної інформаційної системи.
3. Моделювання системи захисту інформації промислового підприємства.

5. Перелік графічного матеріалу (з точним зазначенням обов’язкових креслень)
презентація

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв

7. Дата видачі завдання 12.05.2023

К А Л Е Н Д А Р Н И Й П Л А Н

№	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Розробка плану роботи.	23.06.2023	
2.	Збір вихідних даних.	04.08.2023	
3.	Обробка методичних та теоретичних	01.09.2023	
	джерел.		
4.	Розробка першого та другого розділу.	03.11.2023	
5.	Розробка третього розділу.	17.11.2023	
6.	Оформлення та нормоконтроль	24.11.2023	
	кваліфікаційної роботи магістра.		
7.	Захист кваліфікаційної роботи.	15.12.2023	

Студент _____ О.В. Тарасенко
(підпис) (ініціали та прізвище)

Керівник роботи _____ І.О. Клопов
(підпис) (ініціали та прізвище)

Нормоконтроль пройдено

Нормоконтролер _____ О.О. Шапуров
(підпис) (ініціали та прізвище)

РЕФЕРАТ

Кваліфікаційна робота магістра «Управління захищеністю інформації промислового підприємства на основі інтелектуальних технологій»: 69 с., 9 рис., 7 табл., 40 джерел, 1 додаток.

ЗАГРОЗА, ЗАХИСТ, ІНФОРМАЦІЙНА БЕЗПЕКА, КОРПОРАТИВНІ ІНФОРМАЦІЙНІ СИСТЕМИ, РИЗИК.

Магістерська робота присвячена розробці адаптивних методів управління захистом інформації у сегменті корпоративних інформаційних технологій. В роботі проведено аналіз корпоративних інформаційних систем як об'єкта інформаційного захисту; розроблено системну протидію інформаційним загрозам; обґрунтовано необхідність розвитку адаптивних методів досягнення заданого рівня захищеності інформації з використання інтелектуальних технологій; розроблено етапи побудови системи управління інформаційною безпекою із застосуванням методів інтелектуальної підтримки прийняття рішень. Уточнено модель протидії загрозам інформаційної безпеки в умовах невизначеності. Дістала подальшого розвитку система інтелектуальної підтримки прийняття рішень щодо оперативного управління захистом інформації на основі інтелектуальних технологій.

ABSTRACT

Master's qualifying paper «Information Security Management for Industrial Enterprises Based on Intelligent Technologies»: 69 pages, 9 figures, 7 tables, 40 references, 1 supplement.

THREAT, PROTECTION, INFORMATION SECURITY, CORPORATE INFORMATION SYSTEMS, RISK.

The master's thesis is devoted to the development of adaptive methods for managing information security in the corporate information technology segment. The work analyses corporate information systems as an object of information protection; develops a systematic counteraction to information threats; substantiates the need to develop adaptive methods for achieving a given level of information security using intellectual technologies; develops stages of building an information security management system using intellectual decision support methods. The model of counteracting information security threats under conditions of uncertainty has been refined. The system of intellectual decision support for the operational management of information security based on intellectual technologies has been further developed.

ЗМІСТ

ВСТУП

Актуальність роботи. Поточний етап розвитку в області обміну інформацією представляє собою інтенсивне використання сучасних інформаційних технологій, масовим поширенням мереж різного рівня охоплення – локального, корпоративного, глобального, створює величезний потенціал застосування інформаційного обміну у різноманітних сферах бізнесу. Технології управління бізнесом, можливості його масштабу у різних сферах діяльності визначаються корпоративними інформаційними системами (КІС), що об'єднують в собі інфраструктуру та різноманітні інформаційні послуги. Інфраструктура КІС включає мережі, сервери, робочі станції, охоплюючи підрозділи, які можуть бути розгорнуті по всьому світі. Сегмент (СГ КІС) є структурною одиницею КІС.

Масове використання ІТ-технології в КІС змушує серйозно ставитись до інформаційної безпеки через наявність загроз захисту інформації.

Сучасні теоретичні і практичні розробки, гарантуючі захист інформації (ЗІ) мають деякі протиріччя: загостреною увагою до безпеки інформаційних об'єктів, значно підвищеними вимогами, що пред'являються до ЗІ, використанням прийнятих міжнародних стандартів по гарантіям інформаційної безпеки (ІБ), зростаючими витратами для забезпечення ЗІ, з однієї сторони, а з іншої сторони збитки, які наносяться власникам інформаційних ресурсів комп'ютерними атаками.

Результативне використання інформаційних технологій у діяльності корпорацій вимагає ефективно керованих систем ЗІ, оскільки система, що реалізує процеси управління подіями ІБ, планування модульної структури системи ЗІ та аудит інформаційної безпеки, повинна проводитися автономно на рівні сегменту КІС.

Способом вирішення зазначеної вище проблеми може бути інтелектуальна підтримка в управлінні ЗІ у сегменті КІС, яка включає моделі, методи, алгоритми

і програмне забезпечення.

Об'єкт дослідження: процеси забезпечення інформаційної захищеності підприємства.

Предмет дослідження: методи управління захищеністю інформації на основі інтелектуальних технологій.

Метою дослідження є розробка адаптивних методів управління захистом інформації у сегменті корпоративних інформаційних технологій.

Для досягнення мети були поставлені та вирішені такі *завдання*:

– проведено аналіз корпоративних інформаційних систем як об'єкта інформаційного захисту;

– розроблено системну протидію інформаційним загрозам;

– обґрунтовано необхідність розвитку адаптивних методів досягнення заданого рівня захищеності інформації з використання інтелектуальних технологій;

– розроблено етапи побудови системи управління інформаційною безпекою із застосуванням методів інтелектуальної підтримки прийняття рішень.

Наукова новизна одержаних результатів полягає у наступному:

уточнено:

– модель протидії загрозам інформаційної безпеки в умовах невизначеності;

дістала подальшого розвитку:

– система інтелектуальної підтримки прийняття рішень щодо оперативного управління захистом інформації на основі інтелектуальних технологій.

Результати наукового дослідження пройшли апробацію на XVI університетській науково-практичній конференції студентів, аспірантів, докторантів і молодих учених «МОЛОДА НАУКА-2023»

РОЗДІЛ 1
МЕТОДОЛОГІЧНІ ОСНОВИ УПРАВЛІННЯ ЗАХИСТОМ ІНФОРМАЦІЇ В КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

1.1 Сутність проблеми управління захищеністю інформації

Сучасні корпорації мають складну розподілену структуру, яка зумовлена багатопрофільною діяльністю, територіальним розміщенням підрозділів, численними корпоративними зв'язками з партнерами. Корпоративними, зазвичай, називають системи управління підприємством, які мають розвинуту структуру і окремі органи управління. Серед корпоративних систем виділяють організаційні, інформаційні і т.п. Більшість бізнес-функцій і управлінських процесів підприємств і організацій охоплюють корпоративні інформаційні системи (КІС), будучи важливим інструментальним засобом ведення бізнесу.

Впровадження нових інформаційних технологій для підприємств завжди пов'язано з виникненням нових ризиків. Чим складніше є структура корпоративної інформаційної системи, тим вищий рівень ризику загроз для неї: проникнення ззовні або несанкціонований доступ зсередини підприємства, зокрема з метою фінансового шахрайства або розкриття комерційної таємниці, зміна або знищення інформації та т.п. [15]. Такі ризики можуть нанести підприємству значної шкоди. Створення розвиненого і захищеного інформаційного середовища є неодмінною умовою розвитку як окремих корпорацій, так і економіки, суспільства та держави в цілому. Тому питання забезпечення захищеності інформації в сегменті КІС стали в даний час дуже злободенними.

КІС є складною людино-машинної або соціо-технічної системою, яка включає інформаційну систему підприємства. Для дослідження таких систем використовуються різні типи моделей. Процес функціонування КІС підприємства здійснюється в умовах протиборства підприємства, як соціо-

технічної системи з однієї сторони, і конкурентів, зловмисників, негативних явищ природи та інших об'єктів і явищ, з іншого боку.

Ускладнення та розширення сучасних КІС призводить до збільшення кількості мережевих пристроїв і різних засобів захисту інформації (СЗІ), що веде до великої кількості небезпечних подій.

Слід зазначити, що сучасні технологічні процеси значно обганяють теоретичні осмислення практичних розробок та застосувань у галузі інформаційних технологій, а також в області нових комунікаційних можливостей.

Основними недоліками СЗІ, які широко використовуються, є їх риси, пов'язані зі строгими архітектурними принципами [9] і використанням в здебільшого оборонних або наступальних стратегіях захисту від найбільш відомих та небезпечних загроз.

Рішення позначених проблем і ефективне використання сучасних КІС вимагає коштів і методів рівного і надійного управління не тільки мережами, а також і системою ЗІ, усіма заходами, що забезпечують безпеку мережі [10]. Потрібні методи, які дозволили б швидко відслідковувати зміни в операційному середовищі системи і запобігати порушенню інформаційної безпеки, керуючи як мережевим обладнанням, так і обладнанням безпеки.

Сучасним підходом забезпечення ефективної захищеності інформації в КІС є використання інтелектуальних інструментів підтримки прийняття рішень (ППР *)* для управління інформаційною безпекою.

В даний час розробляється інтегрована система управління ЗІ, яка буде охоплювати всю інфраструктуру організації і дозволяла б керувати інформаційною інфраструктурою, незалежно від масштабу КІС.

Структуроване подання всього різноманіття аспектів управління захистом інформації наведено наочно на рис. 1.1.

Рисунок 1.1 – Структурування проблеми управління ЗІ

На сьогодні практично не можливо знайти виробників, які б пропонували споживачеві повний спектр засобів, як апаратних, і програмних, необхідних для побудови систем ЗІ, задовольняючи сучасні вимог. Більшість систем ЗІ будується на основі програмно-апаратних засобів, випущених різними виробниками. Для гарантування гетерогенної КІС надійності ЗІ необхідна система управління інформаційної безпекою (СУІБ), яка може забезпечити правильну конфігурацію кожного з її компонентів і забезпечити автоматичну підтримку прийняття рішень щодо ЗІ, постійно відстежуючи зміни, що відбуваються, контролюючи роботу користувачів мережі.

Такий комплексний підхід вирішення проблеми дозволяє створювати справді безпечне середовище функціонування КІС підприємства.

Проведений аналіз дозволяє стверджувати, що на рівні сегменту КІС система управління, яка реалізує ряд функцій управління, повинна функціонувати автономно:

– отримувати і оцінювати об'єктивні дані про поточні стани безпеки КІС *(аудит);*

– керувати подіями, за якими ведеться протоколювання;

– визначати модульний склад системи ЗІ та точки створення засобів захисту інформації в комп'ютерній мережі підприємства.

Міжнародний стандарт ISO/IEC 27001 описує моделі, які використовуються для створення, впровадження, експлуатації, постійного моніторингу і аналізу, обслуговування і покращення систем управління

інформаційної безпекою (СУІБ).

Особливості проєктування і реалізації СУІБ компанії визначаються її потребами та цілями, вимогами захисту, розмірами і структурою організації. Для ефективного функціонування необхідно ідентифікувати різні види діяльності та керувати ними.

Процесний підхід до управлінню ЗІ в цьому стандарті допомагає виділити наступні моменти:

– визначення принципів, цілей, процесів і процедур, які мають відношення до управління ризиками і вдосконалення ЗІ для досягнення результатів, відповідних цілей компанії;

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

– оцінка та вимірювання показників процесів, що відносяться до політики, цілі і практичного досвіду менеджменту захисту інформації, а також проведення їх аналізу;

– виконання коригувальних і попереджуючих процедур, які засновані на результатах проведення внутрішнього аудиту та аналізу з метою постійного покращення управління ЗІ.

Склад СУІБ включає:

– організаційну структуру;

– політику, заходи планування;

– набір процедур, процесів, ресурсів.

Метою СУІБ є проєктування СЗІ, впровадження, експлуатація, постійний контроль, аналіз, покращення ЗІ.

Для створення СУІБ підприємству необхідно виконання наступних дій:

– визначення кордонів системи;

– виробити принцип дії щодо захисту інформації з урахуванням законодавчих норм і встановлених цілей захисту;

– виробити критерії оцінки значимості ризиків;

– вибрати методологію оцінки ризику, яка відповідає системі управління

ЗІ;

– визначити прийнятний рівень ризику;

– виконувати ідентифікацію ризиків (активи, загрози і негативні впливи, які сприяють втраті конфіденційності, цілісності та доступності активів і критичних вразливостей системи визначення місцезнаходження);

– оцінити значимість ризиків (оцінити ймовірність порушень інформаційної безпеки у світлі існуючих загроз та вразливостей, оцінити рівні ризику, визначити, чи є ризики прийнятними або вимагають відповіді);

– знайти можливість управління ризиками (застосування прийнятних засобів зниження чи прийняття ризику);

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

– узгодити з керівництвом використання системи ЗІ і виконати підготовку заяви про ступінь застосування (включаючи мету управління, засіб керування, обґрунтування вибору).

Етап реалізація і експлуатація СУІБ підприємства включає наступні дії:

– формулювання плану обробки ризику, що визначає відповідні дії з менеджменту, необхідні ресурси, відповідальність;

– реалізація цього плану, включаючи фінансування;

– реалізація засобу управління, що має на меті досягнення мети управління;

– впровадження процедур та інших засобів управління, які здатні швидко виявити події в системі ЗІ та реакції на інцидент в системі ЗІ;

– швидке виявлення порушень та інцидентів;

– виявлення подій у системі ЗІ та запобігання інцидентам з допомогою використання індикаторів;

– вимірювання результативності засобів управління для перевірки того, що вимоги було виконано;

– оновлення планів захисту інформації з метою обліку даних, отриманих в процесі діяльності, пов'язаної як з постійним контролем, так і з аналізом.

Документацію СУІБ необхідно підготувати таким чином, щоб вона включала описи методик оцінювання ризику, плани обробки ризику, опис процедур, необхідних підприємству для гарантії результативного планування.

Стандарт ISO/IEC 17799 дає керівні вказівки, які рекомендується використовувати в процесі проєктування системи захисту. У стандарті наводяться мета управління і список засобів управління. Метою політик захисту є забезпечення напрямів і підтримки керівництвом ЗІ відповідно до бізнес-вимог, законодавчих норм. Політику в області ЗІ необхідно аналізуватися з запланованою періодичністю, щоб гарантувати її адекватну придатність та адекватність.

У відношенні управління активами мета складається в тому, щоб забезпечити і підтримувати необхідні засоби захисту активів організації в умовах праці, які вимагають чіткої визначеності. Необхідно скласти та підтримувати реєстри важливих активів, а також активів, які яким-небудь чином пов'язані зі засобами обробки інформації. Інформація має бути класифікована за значимістю та критичністю для компанії.

Роль і відповідальність співробітників, користувачів по відношенню до інформації та її захисту мають бути задокументовані відповідно до політики ЗІ в компанії.

Метою управління мережевою безпекою є захист інформації в мережах та захист мережної інфраструктури. Адекватне керування мережею потрібне для захисту від ризиків. Метою постійного моніторингу є виявлення дій, пов'язаних з обробкою інформації. Необхідно створити процедуру для постійного моніторингу використання інструментів для обробки інформації. Результати повинні регулярно перевірятись.

Метою керування доступом користувачів є гарантований доступ для зареєстрованих користувачів і запобігання несанкціонованого доступу в КІС. Призначення і використання дозволів повинні контролюватися і повинні бути обмежені, встановлення паролів повинно контролюватися формальним процесом адміністратора. Необхідно встановити формальну процедуру

реєстрації користувачів.

Мета менеджменту інцидентів у СЗІ полягає у гарантуванні того, що про події в системі ЗІ, які пов'язані з КІС, повідомляється способом, який дозволяє проводити своєчасні коригувальні процеси. Необхідно встановлення відповідальності керівництва і процедур швидкого, результатного і регламентованого реагування на всі інциденти у системі ЗІ. Необхідно передбачити механізм, який надає можливості визначення кількості типів, обсягів інцидентів в системі ЗІ і виконувати їх постійний контроль.

У [34] наведено модель зрілості процесів управління інформаційною безпекою, в якій найбільш високим рівнем є «керований» і «оптимізований». Керований рівень характеризується моніторингом на об'єкті захисту і оцінкою процесу управління, виконується їх оптимізація, часткове використання засобів автоматизації. Оптимізаційний рівень характеризує опрацьованість процесу управління інформаційної безпекою, здібності до виконання швидкої адаптації в випадку виникнення змін в бізнес-процесах, комплексне використання заходів захисту, які забезпечують основу для поліпшення процесів управління.

Основні кроки, які потрібно виконати, включають процес управління інформаційною безпекою [15]:

– планування – аналіз і оцінка ризику інформаційної безпеки, визначення політик систем управління ЗІ, вибір заходів захисту і їх оновлення для мінімізації ризиків, прийняття рішень про впровадження системи управління ЗІ;

– використання і експлуатація системи управління ЗІ, включаючи розробку планів по обробці ризиків інформаційної безпеки, реалізацію заходів по її захисту, управління роботою, виявлення і реагування на виникаючі інциденти безпеки;

– перевірка (моніторинг і аналіз), в том числі аналіз продуктивності, в том числі аналіз рівнів залишкового ризику інформаційної безпеки, аналіз внутрішніх аудитів системи управління ЗІ;

– вдосконалення системи управління ЗІ, в тому числі використання тактичних та стратегічних поліпшень у системі, що вимагають прийняття

рішення на рівні планування, оцінки досягнення мети.

Стандарт ICO/МЕК 15408-2002 містить етапи управління безпекою; це керівництво по управлінню безпекою інформаційно-комунікаційної системи [4]. Стандарт розкриває загальні проблеми управління, які важливі для ефективного планування, впровадження та підтримки безпеки системи.

Аналіз існуючих стандартів управління безпекою дозволив зробити висновок, що вони прагнуть створити загальні концепції і загальні моделі управління безпекою; однак, ці стандарти не включають конкретні підходи по управлінню інформаційною безпекою в СГ КІС.

КІС сучасної компанії є важливим інструментом управління бізнесом та значним засобом виробництва. Структура КІС складається з двох великих блоків:

– інформаційна *інфраструктура;*

– інформаційні *послуги.*

Блок інформаційної інфраструктури представляє собою матеріальну базу і середовище для функціонування інформаційної служби.

Інфраструктура сучасної компанії і сучасного товариства може бути представлена таким чином, щоб вона складалася з просторово-розподілених підрозділів цього товариства і його партнерів, клієнтів і постачальників. Основні взаємодії між об'єктами компанії здійснюються в рамках розподіленою КІС з використанням пристроїв зв'язку та каналів зв'язку, що призначаються оператором зв'язку з використанням різних мережевих програм і послуг.

Основним принципом структури розподіленої КІС є сегментація мережі за територіальною виробничою приналежністю. Структурними одиницями КІС є розподілений сегмент КІС. Сегмент КІС, в свою чергу, може бути складною інформаційною системою, яка поширюється на регіональному рівні.

Сегмент КІС є мережею, що складається з сегментів мережі другого рівня ієрархії У кожному сегменті є робочі станції, сервери, мережа, маршрутизатори, набір комутаторів, цифрові модеми, телефонні лінії, оптоволоконні канали *FastEthernet*, *E1* і бездротові канали зв'язку.

На рисунку 1.2 показано результат структурного розкладання КІС [20].

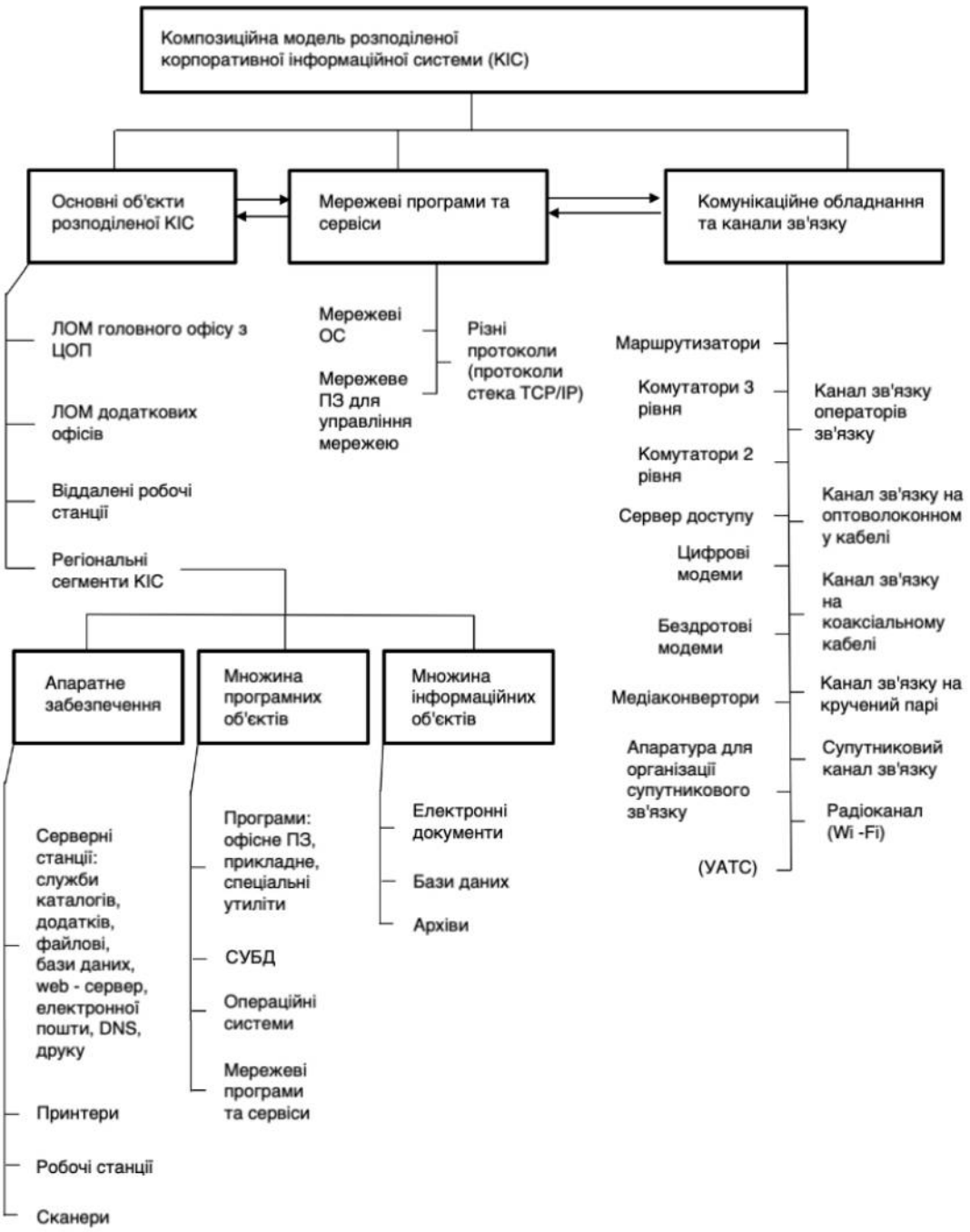

Рисунок 1.2 – Модель розподіленої КІС з деталізацією СГ КІС

Впровадження Інтернету в технології корпоративних комунікацій привело до різкого збільшення числа користувачів зовнішніх мереж, збільшення різноманітності типів каналів зв'язку і використанню нових мережевих і

інформаційних технологій. Це підвищило вимоги безпеки для транзакцій електронних мереж: серверів, маршрутизаторів, серверів віддаленого доступу, каналів зв'язку, операційних систем, баз даних і додатків. Небезпеки в кожному елементі системи захисту швидко ростуть, і ця тенденція збережеться і в майбутньому [18].

Гострою є також проблема можливості внутрішніх загроз захищеності інформації, особливо це стосується великих корпорацій, які мають територіально розподілені підрозділи. Чим більше співробітників та одиниць обчислювальної техніки в корпорації, тим більша ймовірність вчинення серйозних інцидентів, результатом яких може стати викрадення конфіденційної інформації, корпоративної бази даних, що містить важливу для конкурентоспроможності корпорації інформацію.

Чим більша компанія, тим більший об`єм коштів, яким вона керує, тим більше агресивними і професійними можуть бути атаки за участю внутрішніх зловмисників. На думку експертів, розвиток та інтеграція інформаційних технологій у корпоративні бізнес-процеси збільшує небезпеку внутрішніх загроз інформаційної безпеки [30].

Сучасні засоби злому комп'ютерних мереж і крадіжки інформації зазнають швидкий розвиток, поряд з іншими високо технологічними інформаційними галузями. Тому забезпечення інформаційної безпеки КІС стає однією з першочергових завдань менеджменту компаній. Збереження конфіденційності, цілісності та доступності інформаційних ресурсів компанії багато в чому визначає якість і швидкість прийняття стратегічних рішень керівництвом компанії.

Завдання забезпечення інформаційної безпеки в КІС можна вирішити шляхом побудови ефективної *системи ЗІ.*

На рис. 1.3 наочно продемонстровано модель складу системи захисту інформації СГ КІС [18].

До системи ЗІ висувається вимога абсолютної прозорості для вже існуючих у рамках КІС додатків та, крім того, вимога сумісності з використовуваними

корпорацією мережевими технологіями.

Тому, з метою забезпечення надійною захищеності ресурсів КІС, системи ЗІ повинні реалізовуватися на базі найбільш прогресивних і найбільш перспективних технологій в області інформаційного захисту.

Рисунок 1.3 – Модель складу системи захисту інформації СГ КІС

Тому, щоб забезпечити ефективність комп'ютеризації в корпорації, необхідно забезпечити такі параметри безпеки інформаційних ресурсів, як цілісність, конфіденційність, справжність відповідної ділової інформації, яка циркулює в локальних та глобальних інформаційних мережах.

1.2 Сучасні концепції захищеності інформації в корпоративних інформаційних системах

Розвиток та вдосконалення шкідливого ПЗ не стоїть на місці, як і розвиток систем захисту. Зловмисники використовують сучасні досягнення інформаційних технологій (хмарні технології, нові алгоритми шифрування і т.д.). Згідно одинадцятому звіту *Cisco* по кібербезпеці, «щоб скоротити час виявлення зловмисників, фахівці по кібербезпеці починають все більше

застосовувати (і закуповувати) засоби, що використовують штучний інтелект (ШІ) і машинне навчання (МН)» [30]. З одного боку, шифрування допомагає посилити захист, а з іншого – зростання як легітимного, так і шкідливого зашифрованого трафіку примножує проблеми тих, хто захищається у процесі виявлення потенційних загроз та моніторингу їх дій. «За минулі 12 місяців фахівці *Cisco* з інформаційної безпеки зафіксували більш ніж триразове зростання шифрованого мережевого трафіку від інспектованих зразків шкідливого ПЗ» [30].

Використання інтелектуальних технологій та машинного навчання показує хороші результати в галузі інформаційної безпеки, що з часом дозволить автоматично виявляти нестандартні шаблони в зашифрованому веб-трафіку, у хмарних середовищах та середовищах *IoT*. «Деякі з 3600 директорів з інформаційної безпеки, опитаних в ході підготовки звіту *Cisco* 2018 *Security Capabilities Benchmark Study*, заявили, що довіряють таким інструментів, як МН і ШІ, і хотіли б їх використовувати, але вони розчаровані великою кількістю хибних спрацьовувань» [30]. Поступове вдосконалення технологій МН та ІШ з часом дозволить знизити кількість «хибних тривог», і коректно визначати «нормальну» активність мереж, вирізняючи її від реальних атак.

Як вказують сучасні експерти, «еволюція шкідливого програмного забезпечення за минулий рік показала, що зловмисники з більшою винахідливістю стали використовувати незахищені проломи в системах безпеки, – відзначив Джон Стюарт (*John Stewart*), старший віце-президент *Cisco*, директор з інформаційної безпеки. «Для відображення нападів та зменшення схильності до наростаючих ризиків як ніколи раніше важливо стратегічно удосконалювати захист, інвестувати в технології та впроваджувати передові методики» [30]

Деякі результати звіту *Cisco Annual Cybersecurity Report* показують, що:

– фінансова шкода від атак стає все більш реальною;

– більше половини всіх атак нанесли фінансову шкоду на суму понад 500 млн. доларів, включаючи втрачену вигоду, втрату клієнтів та прямі витрати;

– атаки на ланцюжки поставок стають все більше складними і набирають

швидкість.

Такі атаки можуть вплинути на комп'ютери у великих масштабах, та їх наслідки можуть тривати місяцями чи навіть роками. Необхідно пам'ятати про потенційні ризики використання програмного і апаратного забезпечення від організацій, які не сприймають проблеми інформаційної безпеки всерйоз.

Щоб знизити ризик атаки на ланцюжок поставок, необхідно переглянути сторонні процедури для перевірки ефективності технологій інформаційної безпеки. У то же час захист інформаційних систем стає все важчим, вразливості стають все більше різноманітнішими.

Щоб захистити себе, організації використовують складні комбінації продуктів різних виробників. Це ускладнення з зростаючою різноманітністю вразливостей негативно впливає на здатність організацій відбивати атаки і призводить, серед іншого, до збільшення фінансових ризиків та втрат.

Згідно звіту *Cisco*:

– 25% фахівців з інформаційної безпеки повідомили, що використовують продукти від 11-20 вендорів, в 2016 р. так відповіли 18%;

– фахівці з інформаційної безпеки повідомили, що 32% вразливостей торкнулися більше половини систем, у 2016 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 поставленими завданням; 2/3 представників сектора охорони здоров'я і представники індустрії фінансових послуг вважають поведінкову аналітику корисною для виявлення шкідливих об'єктів;

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

– цього року 27% фахівців з інформаційної безпеки повідомили про використання зовнішніх приватних хмар (показник 2016 р. – 20%); з них 57% розміщують мережу в хмарі заради кращого 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, які розвиваються і розширюються. Ефективність захисту таких змін підвищується за рахунок використання комбінації передових технологій, таких як передові технології безпеки, такі як машинне навчання, і інструментів безпеки світового класу, таких як хмарні платформи інформаційної безпеки.

В останні роки також спостерігається тенденція до зростання шкідливих програм та часу виявлення. «Продемонстрована *Cisco* медіана часу виявлення (*timetodetection, TTD*) за період з листопаду 2021 по жовтень 2022 р. склала близько 4,6 години. У листопаді 2020 р. цей показник склав 39 годин, а по даними звіту *Cisco* по кібербезпеці за 2022 р., медіанний час виявлення за період з листопада 2020 року по жовтень 2021 року склав 14 годин».

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 атака буде відображена.

Щодо описаних тенденцій, додаткові рекомендації для підрозділів інформаційної безпеки, такі:

– контроль за дотриманням політик і практик компанії по оновленню 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 шахраїв та шкідливих програм;

– виконувати перевірки безпеки на мікро сервісів, хмарних сервісів та системи адміністрування додатків.

Галицький А. В. зазначає існування «різних підходів до формування архітектури управління інформаційною безпекою КІС:

– використання технології управління усіма пристроями безпеки КІС з

центрального вузла нереалізовано, тому що первинних пристроїв велика кількість, і контроль за ними може викликати занадто велике завантаження центрального вузла управління; важке отримання деталізованої інформації, яка необхідна для управління; локальні методи управління в ряді випадків є технічно необхідними;

З досвіду ведучих виробників засобів забезпечення мережевої безпеки відомо, що організація може успішно реалізовувати свою *політику безпеки* в розподілених КІС при централізованому управлінні безпекою» [10] .

Багато компанії (*CiscoSystems*, *ComputerAssociates*, *PLATINUM*) використовують механізми для інтеграції управління СЗІ у традиційні системи управління мережею [8]. Однак цей тип інтегрованої системи управління є дорогим, 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, яка відповідає бізнес-процесам підприємства і визначає набір правил безпеки для всіх взаємодій об'єктів КІС, а також об'єктів КІС із зовнішніми об'єктами;

– системи протоколювання подій у мережі, моніторингу та аудиту, які не завжди мають вертикальну структуру, а часто працюють автономно в конкретній підсистемі КІС.

Для того щоб забезпечити інформаційну безпеку в сегменті КІС в сучасних умовах компанії почали використовувати все більше автоматизованих систем управління інформаційною безпекою на основі систем *SIEM*.

Астахова Л. В. зазначає, що на сьогодні «найбільш широке поширення на ринку SIEM-систем отримали системи, які використовують сигнатурні методи кореляції подій інформаційної безпеки, що обумовлено, насамперед, простотою реалізацією даних систем, а також гнучкістю при будівництві і подальшій експлуатації» [6]. До таких систем *SIEM* (*Security information and event*

management – управління інформацією і подіями безпеки) відносяться: *HP ArcSight; IBM* QRadar; Symantec *SIM*; *RSA* Envision та інші. Недоліком є те, що системи, збудовані на цьому принципі, не адаптуються до умов швидко мінливого складу КІС. До недоліків таких систем також відноситься велика кількість хибних спрацьовувань і відносна складність конфігурації та реалізації.

Аналіз ринку *SIEM*-систем [28] показує, що в сучасних умовах ринок *SIEM* розвивається повільніше, ніж за кордоном. Не всі закордонні виробники представлені в нашій країні. Але в той же час спостерігається розвиток вітчизняних *SIEM*-систем. *SIEM*-системи реагують на нові досягнення в області обробки даних.Покращена аналітика великих даних *BigData* відіграє важливу роль у *SIEM*-системах, які використовуються в сегменті КІС. Великий інтерес представляє нова технологія *UEBA* (*User and Entity Behavior Analytics* – поведінкова аналітика користувачів і сутностей) для інтеграції в *SIEM*-системи [13]. 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 по тим блоках даних, по яким раніше не отримували, то самонавчені системи безпеки подають про це сигнал. За прогнозам *Gartner*, до 2025 року модулі *UEBA* будуть в кожній четвертій *SIEM*-системі .

Можливо констатувати тенденцію розвитку автоматизованих систем управління захистом інформації для сегменту КІС. Однак існуюча методологія інформаційного ризик-менеджменту не передбачає комплексний підхід до управлінняя 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.

Захист інформації, методи та методики захисту вже близько тридцяти років є предметом активного обговорення як за кордоном, так і вУкраїні. Постійно розробляються нові методи, способи і засоби захисту інформації, випускаються

нові захисні системи, ведуться науково-дослідні роботи по розробці методик управління захистом інформації.

Аналіз результатів науково-дослідних робіт в області ЗІ показує, що значним досягненням у теорії захисту інформації стали роботи, присвячені проблемам створення нових засобів захисту інформації різного характеру, які здійснюють захист інформації на різних рівнях (технічні засоби, програмні і апаратні комплекси, криптографічні засоби захисту і т.д.), а також інтегровані системи захисту інформації [11]. Аналіз результатів таких змін та досліджень був представлений у роботах українських та зарубіжних авторів. Ключовим підсумком такого роду робіт є формування основ теорії захисту інформації.

Масове використання інформаційних технологій комерційними корпораціями, колосальне зростання обсягу критично важливої інформації, що зберігається і переданої в цифровому вигляді, підвищення значимості захисту інформації – фактори, що вплинули на активізацію теоретичних досліджень, пов'язаних з захистом інформації.

У роботах [10, 18, 33] розглядаються питання і проблеми комп'ютерної безпеки. Актуальними є також питання застосування криптографічних методів і засобів в сфері захисту інформації [22], а також питання виявлення небажаних вторгнень [24].

У ряді робіт [19, 20] особливий акцент зроблено на необхідність застосування системного підходу для розробки ефективних засобів ЗІ, розробки моделей загроз, декомпозиції розроблюваних СЗІ (систем захисту інформації), розбиття їх на функціональні підсистеми для визначення факторів, які впливають на них і виявлення можливих загроз, а також для розробки системи індикаторів, які характеризують ефективність СЗІ.

На думку багатьох авторів, які розробляють проблеми ЗІ, для ефективного рішення даної проблеми обов'язковими умовами є формування методологічного базису розглянутого питання, дослідження адаптивної організації систем ЗІ, а також розгляд питань автоматизації ЗІ [12].

На думку [11] базою для формування СЗІ повинні служити плати обробки

інформації, які встановлюються на об'єкт захисту, і завдяки яким проводиться аналіз критичності, відповідно з цим далі проводиться обґрунтування вимог до СЗІ. На підставі сформульованих вимог формується набір засобів захисту інформації, застосування яких дасть можливість забезпечення необхідного рівня захисту. Аргументоване обґрунтування складу (набору засобів) ЗІ – це загальне завдання всього механізму управління ЗІ.

Особливості проєктування систем ЗІ розглядаються авторами в [12]. Аналіз робіт дозволяє виділити два основні підходи щодо побудови системи ЗІ:

– продуктний підхід;

– проєктний підхід.

Продуктний підхід має на увазі, що первинним є формування набору засобів ЗІ, а далі, на основі функцій, що виконуються цими засобами, формується політика безпеки. Відповідно, проєктний підхід передбачає, в першу чергу, формування політики безпеки, після чого на підставі певних вимог вибираються необхідні для її реалізації засоби ЗІ.

Як зазначається в [9], системи на основі проєктного підходу краще оптимізовано і є більше ефективними, що робить їх більш підходящими для використання в гетерогенних мережах. Крім того, слід зазначити, що рішення, спроєктовані за допомогою проєктного підходу, є більше довготривалими.

Загальні принципи та методика вибору засобів захисту інформації на основі критерію оптимальності (має на увазі мінімізацію витрат при забезпеченні заданого рівня захищеності інформації), наведено в [14]. Основою даної методики є оцінка ефективності виконання різних функцій за допомогою засобів ЗІ.

На думку деяких авторів, наприклад [34], управління операціями і стратегічне *планування* використання захисного обладнання розглядаються як найважливіші процеси макроуправління. В цьому контексті оперативне управління має на увазі динамічне управління інформаційною безпекою при її автоматизованій обробці. В рамках оперативного управління повинно бути постійне визнання стану системи захисту інформації, а також прийняття і

реалізація рішень щодо необхідності оперативних втручань у роботу системи задля забезпечення ЗІ. Для прийняття рішень правильне рішення повинно бути обрано з регістра рішень, яки створюється заздалегідь [36].

Планування ЗІ відноситься до процесу, що забезпечує оптимальне використання засобів ЗІ. Оптимальність має на увазі забезпечення необхідного рівня захисту запланованої суми витрат або за мінімізації цієї суми.

Багато з вищевказаних авторів відзначають при цьому, що завдання прийняття рішень є однією з найскладніших у той же час найбільш важливих завдань в області автоматизації управління захистом інформації.

Особливості і основні поняття організаційного управління інформаційною безпекою враховано у роботі [40]. Автор зазначає, що обмеження для забезпечення зростаючих вимог на рівень інформаційної безпеки є недостатність наявного науково-технічного забезпечення (НТЗ). Для забезпечення необхідного рівня захищеності, НТЗ повинно відповідати як динаміці інформаційного середовища, так і динаміці управління стратегіями інформаційного протистояння У цій роботі зазначається, що багато із запропонованих на сьогоднішній день концептуальних підходів до ЗІ носять не конкретний, загальний характер, відповідно, для забезпечення можливості їх застосування у складних розподілених КІС вони мають бути уточнені та вказані з урахуванням процесів, що відбуваються в реальному середовищі інформаційного протистояння. Автор вказує на відсутність систематичних науково-методичних досліджень в цій області в якості ще одного обмежуючого фактор.

У роботі [40] наведено формалізований опис методів синтезу ідеальних стратегій організації управління інформаційною безпекою в моделях ігор для прийняття рішень та, крім того, спосіб управління квантуванням пакетів при передачі інформації, управління відновлення цілісності інформації (алгоритм вибору ідеальною стратегії резервного копіювання) і метод оцінки інформаційної безпеки в умов вірусних програм.

Дослідження [9] управління інформаційною безпекою розглядає здебільшого як організаційний процес. У зв'язку з цим, на думку автора,

завдання управління захистом інформації можуть бути вирішені адміністративною групою (менеджери і адміністратори безпеки, а також оператори). Автор розглядає управління захистом інформації, як здійснення контролю за розподілом інформації в корпоративній мережі, забезпечення функціональної працездатності засобів ЗІ, фіксацію подій, пов'язаних з порушеннями ЗІ та реалізованих при цьому функцій, а також періодичне оновлення інформаційної БД захисту.

Роботи [17, 39] присвячені аналізу основних науково-теоретичних проблем синтезу адаптованих систем із забезпечення інформаційної безпеки, а також питанням застосування цих систем у КІС. У даних роботах особливо підкреслюється неможливість забезпечення абсолютної безпеки як окремих компонентів системи, так і її в цілому, оскільки будь-який захист може бути подолан при відсутності обмеження в часі. Доцільно розглядати лише деякий достатній рівень захищеності, в стані якого вартість його подолання перевищує вартість одержуваної при цьому інформації. До теперішнього часу через велику складність і важку формалізованість не вдається сформувати показники кількісної оцінки рівня захищеності інформаційної системи.

У то же час ступінь ризику залежить від показників цінності інформаційних ресурсів, ймовірності загроз і простоти вразливості, а також від ефективності застосовуваних заходів захисту. Єдиним контрольованим фактором серед вище перелічених є міра захисту. В результаті, оптимальний вибір захисного спорядження може знизити ризик до прийнятного рівня. Результати оцінки ризику служать основою для обґрунтування вибору набору заходів захисту системи.

Ефективність системи ЗІ залежить не тільки від продуктів та методів, що застосовуються, обов'язковою її умовою є також регулярний аудит системи на наявність вразливостей та моніторинг трафіку з метою виявлення потенційних загроз та формування рекомендацій для їх усунення.

Перелічені засоби повинні функціонувати, взаємодіючи з персоналом служби безпеки КІС, але вони створюють значні проблеми для проведення

аналізу та оперативного реагування на різні позаштатні ситуації зі сторони адміністратора безпеки. Відповідно, можливо з впевненістю говорити про необхідність автоматизації процесу реагування на виникаючі інформаційні загрози. Тому перед розробниками стоїть завдання розробки та формалізації моделей прийняття рішень про класифікацію інформаційних загроз за ступенем їхньої активності і небезпеки для системи і про реалізацію протидії цим погроз.

У роботі [16] розглядаються багатокритеріальна модель оцінки безпеки і *метод вибору міжмережевих екранів* з використанням методу нечітких множин, синтез підсистем аналізу безпеки і виявлення загроз, а також метод рішення ігри для боротьби з інформаційними загрозами.

Роботи [18, 39] присвячені проблемам адаптивного управління безпекою в області захисту від несанкціонованого доступу. В цих роботах розглянуто розробки підсистем управління ЗІ, які реалізують парадигму адаптивного управління і використовують неявну *користувальницьку модель* об'єкта управління в головному циклі. Також розглянуто метод, що дозволяє на етапі проєктування визначити раціональний склад та структуру системи захисту інформації, який заснований на методі мінімаксу, з застосуванням показника досяжності характеристик «еталонної» системи. Також розглядається спосіб зміни структур і модифікацій системи ЗІ в часі роботи, в якому використовується критерій максимального збільшення показника безпеки при обмежені по вартості.

Слід відзначити високу складність формування «еталонної» системи захисту на різних етапах життєвого циклу СЗІ.

1.3 Методологічна база оцінювання інформаційних ризиків

Наукова література, національні і міжнародні стандарти приділяють значну увагу проблемі управління захистом інформації, що пов'язано з широким використанням інформації в діяльності сучасних корпорацій.

Аналіз існуючих стандартів в області менеджменту інформаційної безпеки [18] показує, що метою стандартів є формулювання загальних концепцій, а також етапів управління. Однак стандарти не визначають конкретні підходи до процесів управління безпекою систем; вони встановлюють функціональні вимоги до засобів захисту, але не представляють методи порівняльного аналізу різних комплексів засобів захисту для вибору раціонального варіанта системи ЗІ.

Вчені Бернстайн П., Бланк І. А., Вітлінський В. В., Луман Н.,Марковіц Р., Найт Ф. Х., Самуельсон П. і інші розробили загальні принципи і інструментарій управління економічними ризиками. Математичні методи і інструментарій економіко-математичного моделювання представлені в роботах Клейнера Г.Б., Кульбі В. В., Матвійчука О. В., Сігала А. В. та інших спеціалістів. Статистичні методи моделювання можуть використовуватися для вивчення інформаційних ризиків в поєднанні з неформальними методами досліджень [24]. Управління інформаційними ризиками за умов невизначеності може здійснюватися з використанням гнучких методів, таких як інтервальний метод, нейронні мережі, генетичні алгоритми, а також нечіткі множини та нечітка логіка.

Найбільш відповідним суті поняттям «інформаційного ризику» є поняття «загроза безпеки інформації». Липаєв В. В. вкладає у поняття «інформаційний ризик» наступного змісту: це потенційна подія, яка руйнує несанкціоновану інформацію, спотворює інформацію, порушує її конфіденційність або доступність.

Проблеми оцінювання якості інформації, а також надійності апаратних і програмних засобів інформаційних систем розглядали у своїх роботах Байхельт Ф., Зегжда П. Д., Стенг Д. І., Франкен П. та ін. які додатково обмежують поняття інформаційного ризику та враховують тільки загрози інформаційної безпеки в комп'ютерних системах. Прихильники такого підходу до визначення «інформаційний ризик», як правило, є експертами в області ЗІ.

Інша група фахівців під інформаційним ризиком розуміє можливості отримання збитків, недоотримання прибутку і інші негативні наслідки для підприємства. Прикладом такого підходу є наступне визначення М. Мура:

«Інформаційні ризики – це небезпека виникнення збитків або шкоди в результаті застосування компанією інформаційних технологій. Іншими словами, інформаційні ризики пов'язані зі створенням, передачею, зберіганням та використанням інформації за допомогою електронних носіїв і інших засобів зв'язку» [23].

Недоліком вищенаведеного визначення є розмитий контур об'єктів, пошкодження або зміна властивостей, які призведуть до втрат внаслідок ризикованої події. Наведене вище визначення виключає з розгляду інформаційні ризики, які можуть бути пов'язані з оформленням документів, впливом кіберзлочинців на інформаційні ресурси в результаті шпигунської або диверсійної діяльності та т.д. п.

Автори багатьох робіт, зокрема М. Мур та Дж. Джонс, після докладного аналізу джерел ризику пропонують створення своєї моделі. Залежно від мети дослідження та джерел ризику вибирається метод моделювання і рівень деталізації об'єктів і процесів.

Одним з розділів математики, який знайшов широке застосування в моделюванні складних систем, якими є КІС, це теорія множин. Розширити можливості класичної теорії множин дозволяє теорія нечітких множин [34]. При моделюванні складних систем доцільно використовувати апарат нечітких множин для розподілу об'єктів на підмножини в умовах недостатності інформації і випадковості процесів. При дослідженні інформаційних ризиків таке завдання стоїть, наприклад, під час вирішення завдання віднесення довільного ризику до множини значних ризиків у конкретній корпоративній системі. Методи нечітких множин і нечіткої логіки дозволяють використовувати як кількісні, так і якісні оцінки, отримувати інтегральні показники.

У роботі пропонується розробити механізм отримання оцінок ризику, який замінив би метод приблизної табличної оцінки ризику сучасними математичними інструменти.

Формування системи математичних моделей та методів управління інформаційними ризиками ґрунтується на наступних концептуальних

положеннях:

– розробка та застосування методів ідентифікації інформаційних ресурсів (активів) корпорації, які можуть стати об'єктами інформаційних ризиків та загроз цим ресурсам;

– розробка і застосування моделей кількісного аналізу і оцінювання факторів (уразливість, дієвість засобів захисту тощо) та спільного рівня інформаційних ризиків з застосуванням інструментарію нечіткої логіки;

– розробка математичних моделей щодо економічного обґрунтування ефективності використання механізмів (засобів) зниження ступеня інформаційних ризиків, забезпечення відповідності функціональним критеріям захищеності інформації(конфіденційності, цілісності, доступності) та зниження пов'язаних з цих втрат (збитків, шкоди) підприємству.

В іноземних методиках аналізу інформаційних ризиків часто використовують моделі оцінки ризику, які засновані на трьох факторів: загроза, вразливість, можливі збитки [38].

Виділяють чотири основні етапи аналізу інформаційних ризиків:

– ідентифікація компонент: інформаційних ресурсів і можливих загроз;

– оцінка частоти подій можливих загроз через схильність ризику;

– оцінка величини можливих збитків;

– результат аналізу інформаційних ризиків КІС зводиться до оцінки загального рівня інформаційних ризиків у корпоративній системі за шкалою: С – «критичний», Н – «високий», М – «середній», L – «низький».

Пропонується застосувати лінгвістичний підхід до моделювання аналізу факторів інформаційного ризику. Такий підхід забезпечує кількісні описи окремих елементів моделі при умові нечіткої інформації про значення критеріїв оцінки факторів ризику, їх наслідків в умовах дії агента загрози, альтернативних шляхів для уникнення негативного впливу інформаційних ризиків. Відповідно до лінгвістичного підходу, як значення критеріїв та характеристики відносин між ними допускається не лише кількісне оцінювання, але й лінгвістичне.

Пропонується використовувати інтелектуальні методи в системах

інтелектуальної підтримки для оперативного управління інформаційною безпекою в КІС: нечіткий висновок чисельної оцінки ймовірності інформаційних атак; організувати класифікацію інформації про події в базі знань; модель нейтралізації загроз; прийняти рішення про вибір оптимального варіанта реагування на події у системі інформаційної безпеки.

РОЗДІЛ 2
МОДЕЛЬ ОЦІНКИ РІВНЯ ІНФОРМАЦІЙНИХ РИЗИКІВ У СЕГМЕНТІ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

2.1 Методи аналізу та оцінювання захищеності інформації

Методи аналізу інформації, ідентифікації атак і прийняття рішень, що використовуються в системі захисту інформації, зрештою визначають ефективність системи ЗІ.

Основними методами ідентифікації атак, що використовуються в таких системах, є статистична система експертних оцінок [24] та метод нейронної мережі [17].

Статистичний метод заснований на статистичному пристрої, який адаптується до поведінки відповідної особи. Для кожного інформаційного суб'єкта формується його профіль в рамках інформаційної системи, далі проводиться аналіз наявності відхилень (шляхом порівняння з еталонним) і при виявленні таких фіксується наявність несанкціонованої інформаційної діяльності. Перевагою даного методу є універсальність статистичних методів і відсутність необхідності знань про можливі атаки для проведення аналізу. При цьому складністю є невизначеність при визначені граничних характеристик параметрів, які відстежуються, що створює труднощі для адекватної ідентифікації здійсненої діяльності як аномальної. Такі методи виявляються непридатними для реагування на невідомі раніше атаки.

Набір правил, які охоплюють знання експерта, складають експертну систему. Таким чином, всі знання про інформаційні атаки подаються як правила, які, в свою чергу, записуються в вигляді порядку (послідовності) дій, що застосовуються за наявності або реалізації інформаційної загрози. Експертна база даних такої системи повинна утримувати знання (сценарії) всіх або більшою частини відомих інформаційних загроз та видів атак, крім того,

необхідне постійне оновлення. Перевагою даного методу є дуже мала кількість хибних тривог, а його ключовим недоліком – нездатність реагувати на появу невідомої атаки, крім того, відома атака, реалізована з невеликими змінами, може призвести до неефективного спрацьовування системи.

Незважаючи на наявні недоліки, статистичний підхід і аналіз інформаційного простору на основі правил використовується в більшості сучасних методів виявлення атак. Однак, зростаюче кількісно та якісно число атак та їх видів призводить до того, що навіть за постійного оновлення бази даних експертної системи, така система не гарантує покриття всього діапазону атак.

Нейромережевий підхід, на відміну від експертних систем, дозволяє проводити аналітичну роботу і визначити відповідність наявних характеристик роботи системи та тих, які мережа навчена розпізнавати, оцінивши наявність чи відсутність потенційної небезпеки. Нейронні мережі проходять навчання ідентифікації об'єктів предметної області на попередньо сформованій вибірці, в процесі якого відбувається налаштування нейромережі для досягнення задовільних результатів розпізнавання. В міру проведення аналізу, нейромережа набирає досвіду, що робить результат розпізнавання коректнішим. При цьому нейромережа здатна по результатам вивчення характеристик ідентифікувати атаки і загрози, відмінні від тих, що їй зустрічалися раніше.

Технологія адаптивного профілювання, розроблена на основі досліджень імунної системи людини, використовується для вирішення проблеми захисту найважливіших інформаційних ресурсів. Така система показує високі результати в точності визначення мережевих атак або несанкціонованих дій [37]. Технологія адаптивного профілювання працює подібно до імунної системі людини, попередньо вивчаючи нормальну поведінку додатків (спостерігаючи процес виконання коду в штатному режимі в нормально працюючих програмах). Далі навчена система аналізує працюючу ІС і будь-які відхилення в конфігурації, помилки ПЗ і інші вразливості ідентифікуються даної технологією, і відбувається їх блокування (припинення їх роботи за допомогою блокування

системних викликів). Така технологія виявляється ефективною для захисту серверних додатків.

Продовжуючи процес навчання, система навчається розпізнавати допустимі зміни додатків, що в кінцевому результаті призводить до мінімізації хибних спрацьовувань. Дана технологія виявляється ефективною для захисту як від відомих раніше, так і від невідомих атак, та навіть у разі зашифрованої інформації.

Як статистичний, так і нейромережевий методи мають як переваги, так і недоліки. Крім того, багато систем захисту інформації та розробки в даній галузі є запатентованими продуктами іноземних компаній, із закритим кодом та невідомими методами, застосовуваними в даних системах.

Зі слів автора [20], методологічні і технологічні основи створення інтелектуальних засобів запобігання комп'ютерних атак в КІС все ще знаходяться на ранній стадії розробки. На сучасному етапі інформаційного розвитку стоїть гостра необхідність у розробці комплексних рішень щодо реалізації засобів оцінки і протидії потенційно небезпечним подіям, що відбуваються в інформаційній мережі, а також по управлінню засобами та мережевим обладнанням.

Питання адекватної оцінки ступеня захищеності ІС неминуче при створенні інформаційної структури ІС. Оцінка ступеня захищеності повинна також враховувати такі параметри, як: відповідність використаних засобів і механізмів захисту і рівня існуючих ризиків і загроз; визначення необхідного і достатнього рівня захищеності в залежно від середовища функціонування ІС, склад критеріїв для оцінки захищеності інформаційної системи. Дані питання розглядаються в великій кількості робіт, зокрема [17, 21, 33].

Одним із концептуальних завдань створення систем ЗІ є вибір критеріїв (формалізованих заходів оцінки) для визначення рівня захищеності системи. Зазвичай під формалізованими заходами мають на увазі спосіб оцінки «сили» певної характеристики, або засновані на застосуванні цифрової шкали оцінки реальних показників системи [33]. Ідея оцінки рівня захищеності за допомогою

ряду критеріїв була вперше запропоновано в Помаранчевій книзі для застосування до СУБД та операційних систем.

Якщо шкала критеріїв оцінки ступеня захищеності ІС сформована, то порівняння різних систем захисту здійснюється шляхом простого порівняння відповідних числових показників для кожної з систем. Такі шкали критеріїв сформовані для оцінки криптографічних механізмів і для систем радіоелектронного захисту, однак, у сфері захисту від несанкціонованого доступу така шкала відсутня.

Як критерії оцінки захищеності від несанкціонованого доступу можна, було б використовувати показники інтенсивності атак на систему і ймовірності їх реалізації, розрахованої в певний проміжок часу, але проблемою таких показників є їх апостеріорність, що знижує їх практичну цінність. Для оцінки реальної загрози реалізації атак необхідно застосовувати інші критерії, які враховують такі параметри, як умови використання ІС, кваліфікація користувачів, застосовувані технології обробки і зберігання даних та ін. Складним питанням є фактично, не тільки категоризація, а й повний перелік можливих факторів, що можуть бути причетні до реалізації можливих загроз в системі ЗІ.

Найбільш ефективним для практичної оцінки рівня безпеки системи ЗІ є використання критеріїв не апостеріорних, а апріорних критеріїв. Ці критерії можуть бути надані шляхом порівняння системи та її стану з набором еталонних профілів для службзахисту. Профілі, які забезпечують певний рівень безпеки, необхідний при певних умовах, використовуються в якості еталонних профілів. Таким чином, можемо сказати, що дві системи мають однаковий рівень безпеки, якщо вони реалізують один і той самий набір захисних механізмів, які мають однакову «силу». Отже, система 1 має більш високий рівень безпеки, якщо «сила» хоча б одного з реалізованих механізмів захисту вища, ніж у механізмів системи 2, або якщо система 1 реалізувала механізми захисту, відсутні в системі 2 [33].

У роботі [11] автором була запропоновано наступна формула, за

допомогою якої може бути визначено інтегрований показник безпеки для ІС:

$$Z(T) = F[K, R(T)], \tag{2.1}$$

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

У вище вказаній роботі на підставі формули 2.1 розглянуті різні варіанти формування функції F для різних інформаційних середовищ і ситуацій. Однак, слід відзначити, що в роботі не розглядається питання реального визначення значення показників K і R. При цьому очевидно, що визначення цих показників є нетривіальнім завданням. Частина необхідної інформації, очевидно, може бути визначена з приватних ймовірностей реалізації, розрахованих для різних загроз.

Таким чином, можна констатувати, що в роботі, що розглядається не розкрито питання методики та критеріїв визначення рівня захищеності ІС. Фактично, робота не розкриває питання, а лише формулює загальну постановку завдання, яке вимагає рішення.

Відповідно до фундаментальних робіт в сфері управління ризиками [14, 23], аналіз ризиків рекомендовано проводити в наступних випадках:

- суттєва зміна в структурі інформаційної системи або її оновлення;
- зміна технологій побудови корпоративної системи;
- реалізація нових/додаткових підключень в компанії;
- фундаментальні зміни в стратегії і тактиці ведення бізнесу в компанії;
- планова або позапланова перевірка ефективності СЗІ.

Відповідно до вищевказаної роботи управління ризиками складається з наступних етапів:

- оцінка можливих втрат при реалізації ризиків;
- аналіз можливих (потенційних) загроз в даному інформаційному

середовищі;

– аналіз вразливостей інформаційної системи;

– добір заходів та засобів захисту, що забезпечують скорочення ризику до прийнятного рівня при заданих цінових обмеженнях.

Автор роботи [14] «управління ризиками» розцінює як процес вибору та реалізації комплексу контрзаходів, здатних забезпечити необхідний рівень захищеності системи відповідно попередньо проведеного аналізу ризиків. Відповідно до даної роботи, на кожній стадії життєвого циклу ІС повинні бути реалізовані відповідні контрзаходи по різним аспектам безпеки, а саме:

– формування політики ІБ та внесення в неї змін;

– формування і коригування регламентів робіт, обслуговування систем в посадових інструкціях;

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

Згідно роботі [23], при проведенні оцінки ризиків інформаційної системи повинні бути враховані такі фактори, як:

– цінність інформаційних ресурсів, які захищаються;

– оцінка величини значимості потенційних загроз і наявних вразливостей;

– ефективність розроблених раніше (існуючих) і запланованих засобів захисту інформації .

Аналіз ризиків важливий для подальшої порівняльної оцінки різних можливих варіантів реалізації системи захисту, що особливо важливо в зв'язку з підвищеними вимогами до СЗІ.

У міжнародному стандарті *ICO/MEK 15408* «Загальні критерії оцінки безпеки ІТ» чітко структуровані і сформульовані вимоги по інформаційної безпеки для різних класів інформаційних систем. Однак, водночас, цей документ не містить методологію оцінки цих критеріїв.

Аналіз різних стандартів, прийнятих в області управління ризиками інформаційної безпеки (як іноземних, так і вітчизняних), показує, що ці

стандарти не містять деякі важливі деталі методології оцінки ризиків; для їх успішного застосування на практиці їх необхідно вказати; потрібні також додаткові методи оцінки, що враховують суттєві якісні та кількісні показники.

Важливість і актуальність формування науково-методологічної основи проблеми оцінки захищеності інформації підкреслюється в роботі [7].

Процес рішення проблеми забезпечення заданого рівня захищеності можна розбити на дві задачі, які мають бути вирішені послідовно:

– оцінка в кількісному виразі рівня захищеності інформації в системі;

– аналіз даних і прийняття рішень про необхідність налаштування параметрів і властивостей системи захисту для підтримки необхідного рівня безпеки.

Очевидно, що для визначення кількісних показників критеріїв рівня безпеки необхідно прийняти рішення про необхідність коригування складу властивостей СЗІ, крім того, необхідно стежити за динамікою змін в часі індикаторів рівня безпеки, які засновані на змінах зовнішніх і внутрішніх умов ІС.

Інструменти для оцінки параметрів рівня безпеки, а також оцінки існуючих ризиків порушення ІБ, повинні дозволяти будувати об'єктно-орієнтовані структурні моделі інтелектуальної власності, а також моделі ризиків окремих сегментів КІС.

Таким чином, можна, сказати, що створення і розвиток інтелектуальних систем захисту інформації є серйозною науковою проблемою, яка вимагає розробки ряду методів і методологій, науково обґрунтованих та застосованих в рамках створення теорії інтелектуальної безпеки.

2.2 Оцінювання рівня ризику інформаційної системи

Система корпорації є складною людино-машинної або технічною соціо-системою, яка включає в свій склад інформаційну систему підприємства. Для

дослідження таких систем використовуються різні типи моделей. Процес функціонування КІС підприємства здійснюється в умовах протиборства підприємства як технічної і соціосистеми, з однієї сторони, і конкурентів, зловмисників, негативних впливів природи і інших об'єктів і явищ, з іншого боку.

Одним з розділів математики, які знайшли широке застосування в моделюванні складних систем, є теорія множин. Розширити можливості класичною теорії множин дозволяє теорія нечітких множин [14].

При моделюванні складних систем доцільно використовувати апарат нечітких множин для розподілу об'єктів за підмножинамив умовах недостатньої інформації і випадковості процесів. При дослідженні інформаційних ризиків таке завдання стоїть, наприклад, при рішенні завдання віднесення довільного ризику до множини значимих ризиків у конкретній корпоративній системі. Методи нечітких множин і нечіткої логіки дозволяють використовувати як кількісні, так і якісні оцінки, отримувати інтегральні показники. Вони найбільше підходять для роботи з експертними оцінками.

Пропонується розробити механізм отримання оцінок ризику, який замінив би табличний метод приблизної оцінки ризику сучасними математичними інструментами.

Формування системи математичних моделей та методів управління інформаційними ризиками ґрунтується на наступних концептуальних положеннях:

– розробка та застосування методів ідентифікації інформаційних ресурсів (активів) підприємства, які можуть стати об'єктами інформаційних ризиків та загроз цим ресурсам;

– розробка та застосування моделей кількісного аналізу та оцінки факторів (уразливості, дієвості засобів захисту тощо) та загального рівня інформаційних ризиків з застосуванням інструментарію нечіткої логіки;

– розробка математичних моделей економічного обґрунтування ефективності використання механізмів способів зниження інформаційних ризиків, забезпечення відповідності функціональним критеріям захищеності

інформації (конфіденційності, цілісності, доступності) та зниження пов'язаних з цих втрат (збитків, шкоди) підприємству.

У іноземних методиках аналізу інформаційних ризиків використовується модель оцінювання ризику за трьома факторами: загроза, вразливість, величина можливих збитків.

Виділяють чотири основних кроки аналізу інформаційних ризиків [14]

Ідентифікація компонент:

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, який представляє собою інформацію або містить інформацію, використовується для зберігання або обробки інформації і є цінним для підприємства (організації);

Можливі загрози (комбінації загроз) активу. Для управління ризиками необхідно ідентифікувати можливі небезпеки, які загрожують КІС. Такими можуть бути, наприклад, стихійне лихо, відключення електроживлення, атака зловмисника з різними ступенями складності наслідків.

Оцінка частоти подій можливих втрат у результаті дії ризику:

Можливий рівень сили (*Threat capability*), з якою агенти загрози будуть діяти на актив. Допускається, що деяка частина популяції агентів загрози є більш здатною до впливу на актив, інша – менш здатна [40]. Проводиться експертне оцінювання рівня загроз по набору показників, які характеризують можливість доступу порушника відповідного класу до інформаційних ресурсів за наступною шкалою:

TC_VH – «дуже високий»;

TC_H – «високий»;

TC_M – «середній»;

TC_L – «низький»;

TC_VL – «дуже низький».

Очікувана дієвість засобів контролю (*Control strength*) протягом відведеного часового інтервалу. Взявши за основу орієнтацію на середню

здібність агентів зарози, приймається базовий рівень ефективності контролю [34].

Для оцінювання рівня захисту використовується така шкала:

CS_VH – «дуже високий»;

CS_H – «високий»;

CS_M – «середній»;

CS_L – «низький»;

CS_VL – «дуже низький».

Вразливість розглядається як результат впливу факторів можливого рівня сили загрози та дієвості засобів контролю [34] та оцінюється по шкалою:

V_VH – «дуже високий»;

V_H – «високий»;

V_M – «середній»;

V_L – «низький»;

V_VL – «дуже низький».

Приклад бази знань для оцінки рівня чутливості наведено в табл. 2.1.

Реалізації факторів ризику (агентів загрози) в межах певного часового інтервалу.

Таблиця 2.1 – Оцінка рівня чутливості корпоративної системи

		Чутливість				
Можливий рівень сили загрози	*TC_VH*	*V_VH*	*V_VH*	*V_VH*	*V_H*	*V_M*
	TC_H	*V_VH*	*V_VH*	*V_M*	*V_M*	*V_L*
	TC_M	*V_VH*	*V_H*	*V_M*	*V_L*	*V_VL*
	TC_L	*V_H*	*V_M*	*V_L*	*V_VL*	*V_VL*
	TC_VL	*V_M*	*V_L*	*V_VL*	*V_VL*	*V_VL*
		CS_VL	*CS_L*	*CS_M*	*CS_H*	*CS_VH*
		Дієвість засобів контролю				

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

системі [16].

Оцінка частоти реалізації факторів ризику може проводитися за шкалою:

TEF_VH – «дуже висока»;

TEF_H – «висока»;

TEF_M – «середня»;

TEF_L – «низька»;

TEF_VL – «дуже низька».

Частота виникнення подій втрат – можлива частота протягом певного інтервалу, з якою агент загрози наносить шкоду активу, розглядається як результат впливу факторів частоти виникнення загрози та вразливості [16].

Використовуються наступні оцінки рівня частоти подій втрат інформаційних активів:

LEF_VH – «дуже високий»;

LEF_H – «високий»;

LEF_M – «середній»;

LEF_L – «низький»;

LEF_VL – «дуже низький».

Приклад бази знань для оцінювання рівня частоти виникнення подій втрат наводиться в табл. 2.2.

Таблиця 2.2 – Оцінювання рівня частоти подій втрат внаслідок інформаційних ризиків

		Частота подій втрат				
Частота виникнення загроз	TC_VH	V_VH	V_VH	V_VH	V_H	V_M
	TC_H	V_VH	V_VH	V_H	V_M	V_ L
	TC_M	V_VH	V_H	V_M	V_ L	V_VL
	TC_L	V_H	V_M	V_ L	V_VL	V_VL
	TC_VL	V_M	V_ L	V_VL	V_VL	V_VL
		CS_VL	CS_L	CS_M	CS_H	CS_VH
		Дієвість засобів контролю				

3. Оцінювання величини можливих збитків:

– визначення можливої дії кожного з агентів загрози інформаційному активу;

– оцінювання величини кожної з можливих форм збитків, які пов'язані з дією певного агента загрози;

– оцінювання величини всіх можливих форм збитків за шкалою:

PL_VH – «дуже великі»; PL_H – «великі»; PL_Sg – «істотні»; PL_M – «середні»; PL_L – «малі»; PL_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.

Результат аналізу інформаційних ризиків корпоративної системи зводиться до оцінки спільного рівня інформаційного ризику в КІС за наведеною нижче шкалою: *C* – «критичний»; *H* – «високий»; *M* – «середній»; *L* – «низький» рівень інформаційних ризиків.

Приклад бази знань, яка може бути використана для оцінювання спільного рівня інформаційного ризику, наводиться в табл. 2.3.

Таблиця 2.3 – Оцінювання спільного рівня інформаційного ризику

		Рівень інформаційних ризиків				
Величини можливих збитків	*PL_VH*	*H*	*H*	*З*	*З*	*З*
	PL_H	*M*	*H*	*H*	*З*	*З*
	PL _Sg	*M*	*M*	*H*	*H*	*З*
	PL _M	*L*	*M*	*M*	*H*	*H*
	PL_L	*L*	*L*	*M*	*M*	*H*
	PL _VL	*L*	*L*	*L*	*M*	*M*
		LEF_VL	*LEF_L*	*LEF_M*	*LEF_H*	*LEF_VH*
		Частота подій втрат				

2.3 Моделювання впливу факторів інформаційного ризику на основі лінгвістичного підходу

Пропонується застосувати лінгвістичний підхід до моделювання аналізу факторів інформаційного ризику[34]. Такий підхід забезпечує кількісні описи окремих елементів моделі при умові нечіткої інформації про значення критерію оцінки фактора ризику, їх наслідків в умовах дії агента загрози, альтернативні шляхи для уникнення негативного впливу інформаційних ризиків.

Відповідно до лінгвістичного підходу, як значення критеріїв та характеристики відносин між ними допускається не лише кількісне оцінювання, але і пропозиція на природній мові. На підставі розрахованих значень груп показників рівня частоти подій втрат інформаційних активів і величини можливих збитків в результаті інформаційних ризиків проводиться оцінювання спільного рівня інформаційних ризиків в КІС:

$$\Delta = f(\gamma, P) \tag{2.1}$$

де γ – оцінка рівня частоти подій втрат інформаційних активів;

P – попередньо оцінена величина можливі збитки.

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

$$LEF = \{LEF\_VH, LEF\_H, LEF\_M, LEF\_L, LEF\_VL\} \tag{2.2}$$

де *LEF_VH* – «дуже висока» частота;

LEF_H – «висока частота»;

LEF_M – «середня частота»;

LEF_L – «низька частота»;

LEF_VL – «дуже низька».

Терм-множина вхідної змінної P, яка описує величину втрати щодо

бюджету КІС, записується у вигляді:

$$P = \{PL\_VH, PL\_H, PL\_Sg, PL\_M, PL\_L, PL\_VL\}, \quad (2.3)$$

де *PL_VH* – «дуже велика»;

PL_H – «велика»;

PL_Sg – «суттєва»;

PL_M – «середня»;

PL_L – «мала»;

PL_VL – «дуже мала».

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

C – «критичний»;

H – «високий»;

M – «середній»;

L – «низький» рівень ризику.

Терм-множина вихідний змінної Δ представляється в вигляді:

$$\Delta = \{C, H, M, L\}. \quad (2.4)$$

Наступним етапом аналізу є формування системи нечітких знань для визначення кожного з рівнів інформаційних ризиків.

Використовуючи [40], сформовано набір вирішальних правил, які реалізують співвідношення (2.1). У табл. 2.4 наведено такий набір.

Наступним кроком є визначення математичної форми запису вирішальних правил за допомогою функцій приналежності для визначення рівнів інформаційних ризиків. Наприклад, вирішальне правило для визначення інформаційних ризиків рівня *M* може бути записано таким чином:

Таблиця 2.4 – База знань для визначення рівня інформаційнихризиків

Номер вихідної комбінації	Узагальнені значення груп показників		Значимість m_{ij}	Вихідна змінна Δ
	Рівень частоти виникнення можливих втрат	Величина можливих збитків P		
11	*PL_VH*	*LEF_M*	m_{11}	*C*
12	*PL_VH*	*LEF_H*	m_{12}	
13	*PL_VH*	*LEF_VH*	m_{13}	
14	*PL_H*	*LEF_H*	m_{14}	
15	*PL_H*	*LEF_VH*	m_{15}	
16	*PL _Sg*	*LEF_VH*	m_{16}	
21	*PL_VH*	*LEF_VL*	m_{21}	H
22	*PL_VH*	*LEF_L*	m_{22}	
23	*PL_H*	*LEF_L*	m_{23}	
24	*PL_H*	*LEF_M*	m_{24}	
25	*PL _Sg*	*LEF_M*	m_{25}	
26	*PL _Sg*	*LEF_H*	m_{26}	
27	*PL_M*	*LEF_H*	m_{27}	
28	*PL_M*	*LEF_VH*	m_{28}	
29	*PL_L*	*LEF_VH*	m_{29}	
31	*PL_H*	*LEF_VL*	m_{31}	M
32	PL _Sg	LEF_VL	m_{32}	
33	PL _Sg	LEF_L	m_{33}	
34	PL_M	LEF_L	m_{34}	
35	PL_M	LEF_M	m_{35}	
36	PL_L	LEF_M	m_{36}	
37	PL_L	LEF_H	m_{37}	
38	PL_VL	LEF_H	m_{38}	
39	PL_VL	LEF_VH	m_{39}	
41	PL_M	LEF_VL	m_{41}	L
42	PL_L	LEF_VL	m_{42}	
43	PL_L	LEF_L	m_{43}	
44	PL_VL	LEF_VL	m_{44}	
45	PL_VL	LEF_L	m_{45}	
46	PL_VL	LEF_M	m_{46}	

$$\mu^M(\gamma,P) = m_{31}[\mu^{LEF\_VL}(\gamma) * \mu^{PL\_H}(P)] \vee m_{32}[\mu^{LEF\_VL}(\gamma) * \mu^{PL\_Sg}(p)] \vee \quad (2.5)$$

$$m_{33}[\mu^{LEF\_L}(\gamma) * \mu^{PL\_Sg}(P)] \vee m_{34}[\mu^{LEF\_L}(\gamma) * \mu^{PL\_M}(p)] \vee$$

$$m_{35}[\mu^{LEF\_M}(\gamma) * \mu^{PL\_M}(P)] \vee m_{36}[\mu^{LEF\_M}(\gamma) * \mu^{PL\_L}(p)] \vee$$

$$m_{37}[\mu^{LEF\_H}(\gamma) * \mu^{PL\_L}(P)] \vee m_{38}[\mu^{LEF\_H}(\gamma) * \mu^{PL\_VL}(p)] \vee$$

$$\vee m_{39}[\mu^{LEF_{VH}}(\gamma) * \mu^{PL_{VL}}(p)],$$

де $\mu^M(\gamma,P)$ – функція приналежності вихідний змінної μ значенням M з

нечіткого терма (2.4);

$m_{3k}(k = 1,9)$ – ваговий коефіцієнт для відповідної k -ї комбінації;

$\mu^{LEFj}(\gamma)$ – функція приналежності параметра γ нечіткому терму lef_i терм-множини LEF (2.2);

$\mu^{PLi}(p)$ – функція приналежності параметра p нечіткому терму pl_i з терм-множини PL (2.3).

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.

Були збудовані «дзвоно» подібні функції приналежності термів вихідної змінної Δ до множинного числа (2.4) терма, параметри яких представлені в табл. 2.5:

$$\mu^T = \frac{1}{1 + \left|\frac{x - c}{a}\right|^{2b}}, \tag{2.6}$$

де T – довільний нечіткий терм; a – коефіцієнт концентрації; b – коефіцієнт крутості; c – координата максимуму функції, $\mu^T(c) = 1$.

Таблиця 2.5 – Параметри функцій приналежності термів до терм-множини Δ

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 подання функції приналежності вихідної змінної, бази логічного висновку представлені на рис. 2.1 і 2.2 відповідно.

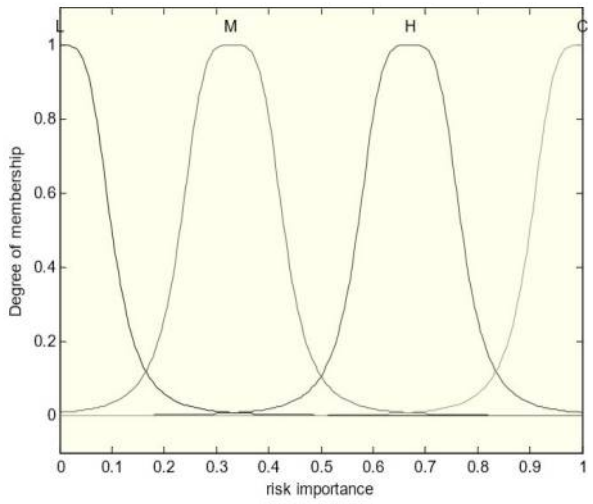

Рисунок 2.1 – Графіки функцій приналежності показника рівня інформаційних ризиків в КІС

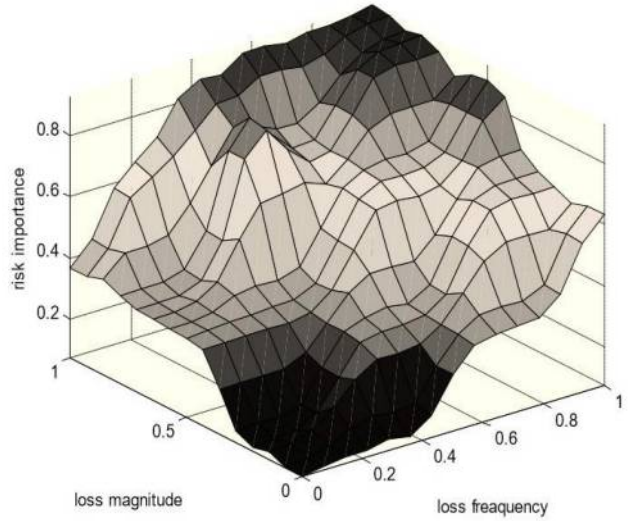

Рисунок 2.2 – Графічне уявлення системи нечіткого висновку показника рівня інформаційних ризиків

Як приклад результати проведених досліджень для трьох промислових підприємств, щодо оцінювання рівня інформаційних ризиків в КІС представлені в табл. 2.6.

Таблиця 2.6 – Оцінка рівня інформаційних ризиків

Назва підприємства	Величина можливих збитків	Рівень частоти можливих втрат	Рівень інформаційних ризиків
Підприємство 1	PL_M 0,4012	LEF_L 0.3545	M 0,3751
Підприємство 2	PL_Sg 0,5971	LEF_M 0.5799	H 0,6348
Підприємство 3	PL_Sg 0,5991	LEF_M 0.4376	H 0,6252
Підприємство 4	PL_P 0,7749	LEF_L 0.1740	H 0,6109

Як видно з табл. 2.6, для Підприємства 2, Підприємства 3 і Підприємства 4 знайдений рівень інформаційних ризиків відповідає оцінці «високий», для Підприємства 1 – «середній».

За результатам оцінки факторів інформаційних ризиків може бути 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 вразливості був викликаний саме недоліками роботи цих ресурсів і їх невідповідності високому рівню загроз інформаційній безпеці підприємства.

Можна зробити висновок, що подібна модель оцінки загального рівня ризику гнучка і адаптивна і може бути налаштована у відповідності до отриманої бази знань.

РОЗДІЛ 3
МОДЕЛЮВАННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ПРОМИСЛОВОГО ПІДПРИЄМСТВА

3.1 Побудова моделі системи захисту інформації

Під моделлю захисту інформації мається на увазі опис (представлений в формалізованому або неформалізованому вигляді) використовуваного в СЗІ комплексу апаратних та програмних засобів та заходів захисту організаційного характеру [21]. Модель захисту інформації є фундаментом для розробки безпосередньо СЗІ.

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. Узагальнюючи напрацювання, зроблені в сучасних концепціях побудови СЗІ [39], можна зробити висновок, що для створення ефективної системи захисту інформації важливо при розробці дотримуватися ряду ключових принципів, а саме:

– комплексність та узгодженість – побудова системи захисту інформації припускає застосування достатньо широкого спектру інструментів та методів захисту, при цьому важливо підтримувати цілісність системи і уникати «слабких місць» у взаємодії окремих компонентів системи;

– диференціація – кожен рівень захисту має розроблятися з обліком рівня важливості і критичності інформації і ймовірності потенційних загроз (оцінки потенційних атак);

– достатність механізмів захисту – має на увазі оцінку співвідношення витрат на створення і підтримку системи захисту інформації та можливої шкоди.

Проаналізувавши можливі шляхи реалізації загроз (здійснення несанкціонованого доступу до інформаційного середовища) та ґрунтуючись на

вищезгаданих принципах організації системи інформаційної безпеки, запропонована модель СЗІ, яка розроблена у вигляді тристоронньої схеми:

– кордон: периметр об'єкта захисту : набір функціональних підсистем, до складу яких входить захист ІС від зовнішніх загроз і руйнівних дій зловмисників;

– кордон: периметр сегменту мережі: набір функціональних підсистем, що забезпечують захист від віддалених та міжсегментних атак;

– кордон: внутрішній периметр : набір функціональних підсистем, завданням яких є захист інформаційного середовища окремих ПК та серверів.

Автор роботи [33] зазначає, що в умовах розвитку засобів інформаційних нападів і застосування гібридних атак, для ефективного захисту інформаційного середовища необхідне застосування багаторівневої, ешелонованої системи захисту інформації.

Схема запропонованого тристоронього захисту наведено на рис. 3.1.

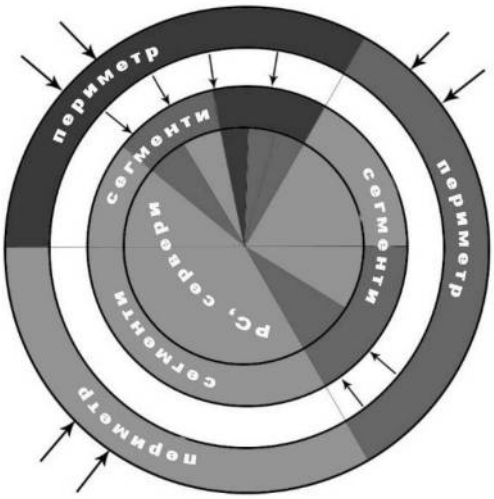

Рисунок 3.1 – Трикордонна модель СЗІ (стрілки вказують на зовнішні та внутрішні загрози)

Таким чином, розроблена модель СЗІ буде включати трикомпонента:

– модель охорони периметра об'єкта захисту;

– модель безпеки мережевого сегменту;

– модель захисту внутрішнього сегмента (ПК і робочий сервер).

Для кожної з розглянутих меж, залежно від ступеня критичності

оброблюваної в ній інформації, яка підлягає захисту, модель буде включати в себе *N* морфологічних матриць (модель рівня *N*).

Завданням упорядкування і системної організації інформації є зменшення невизначеності в процесі прийняття рішень про склад системи захисту інформації, яка ґрунтується на інформації про можливі потенційні загрози в даному контурі і даному інформаційному середовищі та відповідних цим загрозам необхідних бар'єрів.

Таким чином, маючи впорядковану інформацію про потенційні загрози і доступні засоби реалізації захисту, ґрунтуючись на певних процедурах, виробляється багатокритеріальне порівняння альтернативних реалізацій засобів захисту. Результатом такого порівняння є виявлення серед наявної підмножини найкращого (найбільш ефективного і відповідного обмеженням по ресурсах) варіанту реалізації захисту інформаційного об'єкта.

3.2 Реалізація моделей протидії загрозам інформаційній безпеці в умовах невизначеності

Щоб проаналізувати процес прийняття рішень по протидії загрозам, розглянемо кілька типових видів інформаційних атак: міжсегментна атака, зовнішня атака через точку бездротового доступу, зовнішня атака через периметр через високошвидкісний канал доступу.

Прийняття рішень у випадку потенційно можливої міжсегментної атаки.

Представимо модель протидії як зв'язаний граф (рис. 3.2),

де U_n – це варіанти реагування, V_n – варіанти результатів при реалізації протидії загрозам. Функція реалізації, яка відповідає даній матриці, представлена в табл. 3.1.

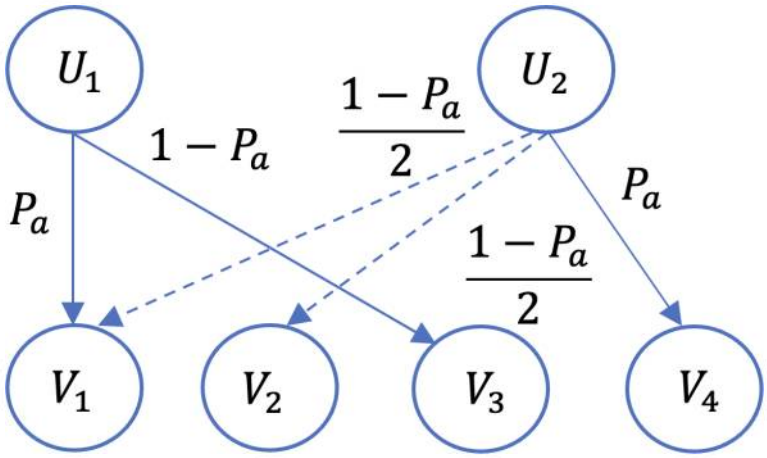

Рисунок 3.2 – Граф зв'язку варіантів реагування і результатів

Таблиця 3.1 – Функція реалізації

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

Наступні варіанти відповіді наведено в таблиці нижче:

U_1 – завершує сеанс з атакуючим вузлом;

U_2 – надсилання попередження користувачеві або зменшення пріоритету користувача.

Оцінка можливих результатів проводиться відповідно до суми можливих збитків в результаті реалізації функцій захисту:

$C(V_1)$ – без ушкоджень;

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

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

$C(V_4)$ – максимальна шкода, нанесена системі в результаті здійснення атаки.

При виборі варіанта реагування U_1 із ймовірністю $(1-P_a)$ буде отримано середню шкоду, оскільки в якості атаки прийнято при стандартному режимі роботи мережі ненавмисні шкідливі впливи 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, дійсно є атакою, то з ймовірністю P_a буде реалізована максимальна шкода при відсутності блокування атакуючої дії. У випадку, якщо розпізнана аномальна подія мала причиною помилкові дії користувача, то шкоди не буде (вона буде дорівнювати нулю). Якщо керуючий вплив буде реалізовано внаслідок помилкового розпізнавання сигналів як атаки і користувачеві буде відправлено попередження і знижений його пріоритет – буде завдано незначної шкоди користувачеві. В останніх двох варіантах ймовірності результатів складуть одну і ту ж величину $(1 - P_a)/2$.

Після чисельних розрахунків отримуємо:

– 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 $C(V_1) = 0,\ C(V_2) = 0{,}1,\ C(V_3) = 0{,}5,\ C(V_4) = 1$.

Прийняття рішень щодо реагування у разі потенційно можливого зовнішнього вторгнення по радіоканалу (*Wi-Fi*, *Wi-MAX* з'єднання).

Для реалізації зовнішнього вторгнення в даному варіанті атаки, зловмиснику необхідний доступ до бездротового адаптеру і необхідно, щоб він знаходився в радіусі дії бездротової мережі. На відмінну від атаки за допомогою провідної лінії, маємо більш високій ступінь загрози і можливість нанесення максимальної шкоди.

Об'єктом, схильним до атаки, в даному випадку, є точка доступу. Для забезпечення захисту використовують системи *WIDS* (системи виявлення бездротових атак), основою роботи яких є сигнатурний аналіз і кореляція поведінки. Події безпеки (вироблення керуючого впливу на інформаційну систему) генеруються при виявленні відхилення параметрів точки доступу, що діагностується від заданих.

Формується заздалегідь визначений (еталонний) мережевий профіль,який включає підтримувані стандарти, застосовувані мережею протоколи, використовувану політику трафіку і стан фізичних і канальних рівнів передачі даних, які постійно відстежують:

– допустиму кількість підключень до точки доступу;
– якість сигналу;
– кількість переданих та прийнятих широкомовних пакетів;
– частоту і кількість повторних передач пакетів;
– відсоткове співвідношення цілісних і фрагментованих фреймів;
– параметри передачі даних (швидкість і її зміни);
– виникнення і частота помилок контрольної суми при передачі пакетів;
– використовувані для повідомлень автентифікації *MAC*-адреси;
– застосовувані при передачі даних технології автентифікації і шифрування.

Для реалізації захисту інформації процедури реагування повинні бути сформовані таким чином, щоб була максимально знижена можлива шкода як від реалізації вторгнення, так і від можливого збою взаємодії через точку доступу.

Модель протидії в графічному вигляді представлена на рис. 3.3, а відповідні даній моделі функції реалізації – в таблиці 3.2.

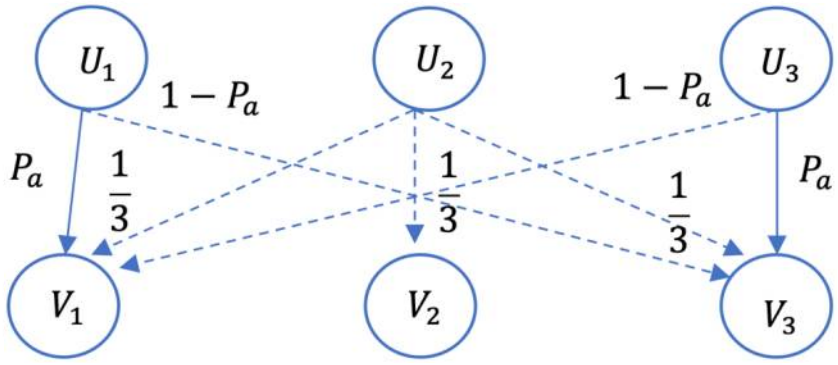

Рисунок 3.3 – Граф зв'язку варіантів реагування і результати

Таблиця 3.2 – Функція реалізації

U	Z											
	$P(z_1)$	$P(z_2)$	$P(z_3)$	$P(z_4)$	$P(z_5)$	$P(z_6)$	$P(z_7)$	$P(z_8)$	$P(z_9)$	$P(z_{10})$	$P(z_{11})$	$P(z_{12})$
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	$C(V_1)$	$C(V_1)$	$C(V_2)$	$C(V_2)$	$C(V_3)$	$C(V_3)$	$C(V_1)$	$C(V_1)$	$C(V_2)$	$C(V_2)$	$C(V_2)$	$C(V_3)$
U_3	$C(V_1)$	$C(V_1)$	$C(V_1)$	$C(V_1)$	$C(V_1)$	$C(V_1)$	$C(V_3)$	$C(V_3)$	$C(V_3)$	$C(V_3)$	$C(V_3)$	$C(V_3)$

Маємо 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 можливої шкоди ймовірні результати керуючих впливів:

$C(V_1)$ – нульовий збиток;

$C(V_2)$ – середні збитки;

$C(V_3)$ – максимальні збитки.

Якщо система реалізує реакцію (вплив) U_1, то з ймовірністю збиту 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 управителя впливу U_1 буде максимальною (блокування точки доступу відбулося безпідставно, стався збій у нормальній роботі системи). Ймовірність $(1 - P_a,)$ такого результату відповідає ймовірності помилкової інтерпретації сигналів системою або помилки користувача.

Якщо обрано варіант реагування U_3, то у разі реалізації атаки максимальні збитки будуть отримані з ймовірністю P_a, (ймовірність атаки) – атака зловмисника не відстежена системою. Якщо даний варіант реагування обраний в ситуації помилкового розпізнавання сигналів сенсорів як атаки, то шкода буде нульовою – система захисту невтручається 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.

Після виконання чисельних розрахунків бачимо, що мінімальне значення цільової функції досягається шляхом вибору наступних альтернатив:

– при $P_a = 0{,}3$ мінімальне значення цільової функції досягається при виборі альтернативи $U_3 : J(U_1, z) = 0{,}699, J(U_2, z) = 0{,}36; J(U_3, z) = 0{,}3;$

– при $P_a = 0{,}4$ мінімальне значення цільової функції досягається при виборі альтернативи $U_1 : J(U_1, z) = 0{,}6, J(U_2, z) = 0{,}3663; J(U_3, z) = 0{,}399;$

– при $P_a = 0{,}678$ мінімальне значення цільової функції досягається при виборі альтернативи $U_1 : J(U_1, z) = 0{,}322, J(U_2, z) = 0{,}366; J(U_3, z) = 0{,}6774.$

Розрахунки проводилися для числових значень $C(V_1) = 0,\ \ C(V_2) = 0{,}1,$ $C(V_3) = 0{,}5,\ C(V_4) = 1.$

Прийняття рішень щодо реагування у разі потенційно можливого зовнішнього вторгнення через периметр по лініях зв'язку.

Для цього варіанту загроз модель протидії проілюстрована на рис.3.4 функції реалізації, що відповідають цій моделі, наведені в додатку А.

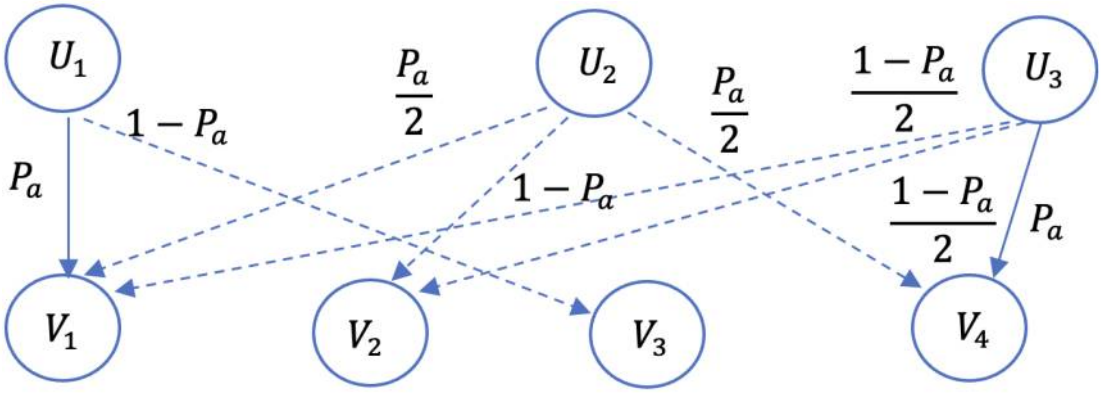

Рисунок 3.4 – Граф підключення варіантів відповіді і результатів

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

U_1 – блокування доступу користувачів до відповідної послуги в мережі;

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

U_3 – відправка оповіщення (попередження) відповідному користувачеві по його IP-адресу, відправка інформації адміністратору про збільшенні активності цього користувача.

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

$C(V_1)$ – нульові збитки;

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

$C(V_3)$ – середня шкода (пошкодження системи);

$C(V_4)$ – максимальна шкода (атака реалізована і систему пошкоджено).

Якщо система вибирає варіант реагування U_1 *mo* 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 зроблено 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 результати.

Коли контрольна дія U_3та атака здійснені, результатом буде максимальна шкода (реалізована атака не буде знищена системою захисту з ймовірністю P_a, рівною ймовірності атаки. У випадку хибного спрацювання 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.

За результатами чисельних розрахунків, можна сказати, що мінімальне

значення цільовий функції досягається при виборі:

– при $P_a = 0{,}05$ мінімальне значення цільової функції досягається при виборі альтернативи $U_3 : J(U_1, z) = 0{,}4948, J(U_2, z) = 0{,}107; J(U_3, z) = 0{,}05948;$

– при $P_a = 0{,}238$ мінімальне значення цільової функції досягається при виборі альтернативи $U_2 : J(U_1, z) = 0{,}380, J(U_2, z) = 0{,}195; J(U_3, z) = 0{,}276;$

– при $P_a = 0{,}742$ мінімальне значення цільової функції досягається при виборі альтернативи $U_1 : J(U_1, z) = 0{,}129, J(U_2, z) = 0{,}3968; J(U_3, z) = 0{,}7549.$

Розрахунки проводилися для числових значень $C(V_1) = 0,\ \ C(V_2) = 0{,}1,$ $C(V_3) = 0{,}5,\ \ C(V_4) = 1.$

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

Управління полягає у перетворенні інформації про стан об'єкта управління в командну інформацію [19]. Процес управління включає велику кількість різних функцій перетворення інформації. Ці функції перетворення взаємопов'язані, реалізація однієї з функцій зазвичай включає в себе реалізацію інших функцій.

Оперативне управління є однієї з ключових функцій в рамках забезпечення захисту інформації, реалізація якої може забезпечити ефективне функціонування СЗІ.

Оперативне управління забезпечує стабільне функціонування системи за рахунок гнучкого реагування на зміни середовища функціонування інформаційної системи (вплив зовнішніх та внутрішніх загроз).

Синтез структури СЗІ і параметрів системи управління для забезпечення захисту певних масивів інформації є однією з ключових завдань теорії управління. В залежності від наявної в розпорядженні інформації про об'єкти управління, даних про середовище, в якому функціонує система, а також про ступінь невизначеності даної інформації, структурна схема системи оперативного управління може відрізнятися. Існуюча в системі невизначеність пов'язана з невідомими діями потенційних зловмисників.

Оперативне управління в умовах інформаційної невизначеності (недостатність даних про стан об'єкта або можливі загрози, тягне за собою

високу невизначеність при прийнятті керуючих рішень) може бути ефективно організовано при реалізації ієрархічного принципу в структурі керуючої системи.

Важливу значимість в системах управління захистом інформації набувають процеси контролю і аналізу, так як така система не обмежується регулювальною функцією. Розподіл функціонального навантаження відбувається наступним чином: процес регулювання покладається на керуючі модулі, а система підтримки прийняття рішень реалізує такі функції як аналіз, контроль, планування і прийняття рішень (тобто усі ті функції, які не відносяться безпосередньо до процесу регулювання управління ЗІ).

Необхідність ієрархічної структури побудови керуючої оперативної системи обумовлена такими факторами:

– параметри, що контролюються керуючою системою можуть мати як кількісний, так і якісний характер;

– зв'язок між параметрами інформаційної системи, контрольованими керуючою системою і вироблюваними керуючими впливами слабо формалізована;

– наявна інформація (що надходить від сенсорів або іншихсистем) про стан контрольованого об'єкта в зв'язку зі змінами середовища в реальному часі може не повною мірою відображати стан об'єкта управління.

Все це зумовлює необхідність створення багаторівневої системи управління для зменшення ступеня невизначеності при прийнятті рішень та підвищення надійності системи.

Щоб побудувати ієрархічну структуру, необхідно обрати наступні елементи управління:

– засоби управління;

– засіб і заходи безпеки;

– модулі управління (розум), які вбудовані в захисне обладнання або мережеве обладнання;

– система підтримки прийняття рішень по оперативному управлінню

ЗІ.

У разі наявності завдання, де формалізація завдань та вироблення рішення на основі набору даних з набору наявних реакцій неможлива, потрібне використання інтелекту людини. Автоматизовані системи (на відміну від автоматичних) розраховані на часткове виконання завдань такого класу людиною (прикладом такого завдання може бути експертна оцінка).

Крім безпосереднього управління, в СУЗІ забезпечується накопичення і аналіз інформації про процеси управління і результати реалізації різних рішень. Таким чином, знижується невизначеність при прийнятті рішень, підвищується їх ефективність,так як керуюча система накопичує дані, що дозволяють точніше передбачити результат застосування того або іншого управителя дії.

Розробка архітектурного рішення СППР відповідно з вищесказаним, припускає використання інтелектуальних інформаційних технологій, а саме:

– реалізація чисельної оцінки ймовірності того, що аномальна подія є атакою, виконується з використанням механізму нечіткого висновку;

– інформація і дані про системи, а також дані про події безпеки, що накопичуються системою в процесі роботи, упорядковуються в базі знань керуючої системи;

– система реалізує інтелектуальні алгоритми вибору рішень про реалізований керуючий вплив при виникненні аномальних подій в системі.

На рис. 3.4 представлено запропоновану архітектурну побудову СППР.

Завданням СППР є вироблення оптимального керуючого рішення яке має захистити інформаційну систему від впливу зовнішніх атак на об'єкт захисту та, при цьому, мінімізувати наслідки впливу такого рішення на нормальну роботу інформаційної системи.

СППР працює в динамічному режимі, відстежуючи і аналізую дані про об'єкт захисту, що надходять із датчиків, у режимі реального часу. Безперервне спостереження і аналіз середовища функціонування виявлення потенційно небезпечних подій реалізує *система контролю інформаційної безпеки.*

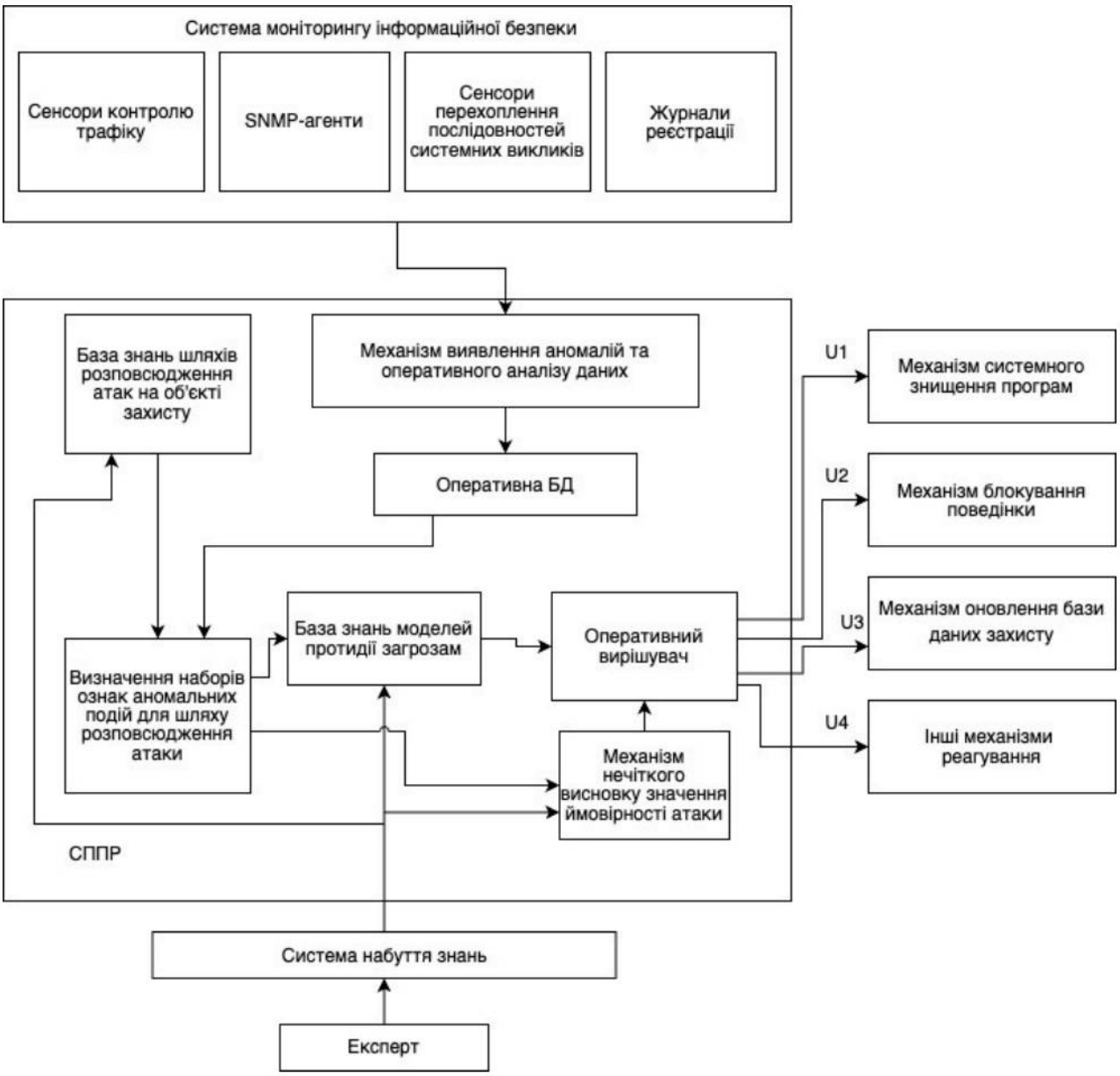

Рисунок 3.4 – Структура системи інтелектуальної підтримки прийняття рішень в контурі оперативного управління ЗІ

Необхідність визначення максимально можливої кількості атак вимагає використання підсистем виявлення аномалій, які працюють на різних рівнях КІС в системі управління. Підмножина контрольованих параметрів може включати в себе параметри, які описують рівень мережі, процеси та стани користувальницьких ресурсів, стан системних ресурсів отримані дані, що зареєстровані в відповідних журналах, і які піддаються оперативному аналізу.

Для отримання даних застосовуються датчики, розташовані в різних сегментах мережі (точки виходу в глобальну мережа, окремі сегменти локальної

мережі інформаційної системи, комутатори, маршрутизатори та ін). Кожен датчик збирає інформацію про ті події безпеки, які відбуваються в відповідному вузлі, і передає їх для протоколювання в відповідних журналах. Також інформація від датчиків може передаватися не безпосередньо, а через додаткові програмні компоненти.

Аналізуючи вхідні відомості від датчиків, *механізм виявлення аномалій і оперативного аналізу* даних визначає, чи є події, що відбуваються нормою або їх можна класифікувати як аномальні, виявляючи в послідовності подій відхилення від стандартних наборів дій.

Завдяки цьому система захисту інформації може виявляти не тільки відомі, раніше зареєстровані атаки, але ті, які системі не відомі, як зовнішні, так і внутрішні (наприклад, порушення користувачами допусків на доступ до інформації).

Однак, слід відзначити, що не кожен випадок аномальних подій пов'язаний із спробою реалізації атаки. Такі події можуть бути пов'язані, наприклад, з помилками користувачів, хибними спрацьовування датчиків і т.д. У результаті формування управителя впливу, який відповідає атаці, може вивести систему з штатного режиму роботи при відсутності загрози безпеки (помилкова тривога).

Для вирішення цієї проблеми у запропонованій СППР керуючі рішення приймаються на підставі розрахунку ймовірності того, що розглянута подія є атакою. Для проведення розрахунку цього «коефіцієнта впевненості» застосовується механізм нечіткого логічного висновку, що пов'язано з неможливістю однозначного та повного опису параметрів, що дозволяють однозначно віднести аномальні події до класу атак, а також з тим, що не всі показники мають кількісне вираження.

Реалізацію цього механізму у запропонованій архітектурі СППР здійснює модуль «Механізм нечіткого висновку ймовірності атаки». Реалізований з допомогою такого підходу механізм прийняття рішень дозволяє максимально ефективно використовувати досвід і напрацювання експертних знань та подолати властиві інформаційному середовищу проблеми неповноти та

суперечливості інформації про його стан, тим самим скоротивши невизначеність при прийнятті рішень.

В системі може бути використана різна кількість датчиків, сенсорів, підсистем виявлення і для визначення чисельного значення «коефіцієнта впевненості» необхідно узагальнювати дані, отримані від них. Для узагальнення даних зручно використовувати стандартизований формат даних.

Аналізатор повинен передавати модуль вектора, що має вигляд:

$$S = I_0, I_p, T, \tag{3.1}$$

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

Ефективність застосовуваного алгоритму при виборі управителя рішення має критичне значення для ефективності роботи всієї системи захисту інформації. У запропонованому варіанті СППР варіантреагування формується в *оперативному вирішувачі* на підставі розрахованого «коефіцієнта впевненості», в якому значення ймовірності результатів розраховуються як функція цього коефіцієнта. Ефективним засобом організації тематичної інформації є її модельне уявлення. База даних моделей захисту від загроз в табличній формі зберігає функції реалізації для кожного типу шляху поширення атаки, зазначеного експертом.

Розглянемо процеси накопичення знань автоматизованою системою СППР. У даному процесі 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 у відповідь на виявлення потенційно небезпечних подій;

– 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 в базі знань у єдиній формалізованій формі уявлення.

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

Інженер по знанням генерує опис рішення проблеми на формальній мові для операційного вирішувача. У робочому рішенні ймовірності $p(z_i)$, 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, які поступають 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, впорядкованих за часом. Відповідно, кожен шлях поширення атак обробляється індивідуально і вироблення управителя впливу відбувається в залежності від цього шляху.

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

Серед можливих варіантів реагування (керівників впливів) системи безпеки можуть бути запрограмовані як некритичні дії (такі як тимчасове блокування користувача або процесу, зниження його пріоритету і ін), так і більше серйозні впливи (повне блокування потенційно небезпечних процесів, портів, переривання процесів, знищення програмної системи).

Використання цієї моделі управління інформаційною безпекою дозволяє контролювати трафік і необхідні вузли, а також своєчасно реагувати на зміни в операційному середовищі найбільш ефективним чином.

ВИСНОВОК

У магістерської роботі розглянуті методологічні основи управління інформаційною безпекою в сегменті КІС з використанням принципів системного аналізу та загальних прав створення систем управління, що є новим у побудові архітектури системи управління інформаційною безпекою з використанням інтелектуальних технологій.

Модель протидії загрозам, що представлена в роботі, базується на оцінці ймовірності атаки, реалізованої з використанням механізму нечіткої логіки, який обирає раціональне рішення на основі оперативних даних про події безпеки з різних джерел інформації. Ця модель дозволяє мінімізувати збитки від можливого здійснення атак на інформаційну систему і реагування самої системи захисту інформації.

На основі трикордонної моделі захисту інформації проведено розрахунки, що дозволяють отримати у кількісному вираженні оцінку числа шляхів поширення атак до вузлів в сегментах. Введено показник «коефіцієнт впевненості», що дозволяє віднести сукупність аномальних подій інформаційної системи до атаки з використанням механізму нечіткого логічного виведення.

Розроблена ієрархічна структура системи інтелектуальної підтримки прийняття рішень для оперативного управління інформаційною безпекою, а також структура системи інтелектуальної підтримки прийняття рішень в оперативному управлінні захистом інформації. Запропонована структура рішень, прийнятих системою, про вибір раціонального варіанту реагування на події безпеки за рахунок застосування інтелектуальних технологій для рішення слабо формалізованих завдань класифікації подій безпеки в системі і вибору шляхів реагування на них.

Таким чином, поставлені перед магістерської роботою завдання повністю виконані.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Архипов О. Інформаційні ризики: методи та способи дослідження, моделі ризиків і методи їх ідентифікації. *Захист інформації.* 2013. Т. 15, № 4. С. 366–375.

2. Берко А. Ю. Методи та засоби оцінювання ризиків безпеки інформації в системах електронної комерції. *Вісник Національного університету «Львівська політехніка».* 2018. № 610. С. 20–33.

3. Бінько І. Ф. Національна безпека України в умовах глобальної інформатизації. Київ : Національний ін–т стратегічних досліджень, 1996. Вип.61. 54 с.

4. Бойченко О. В. Політика інформаційної безпеки в системі інформаційного забезпечення органів внутрішніх справ. *Форум права.* 2009. № 1. С. 50–55.

5. Бодрук О. Структури воєнної безпеки : національний та міжнародний аспекти : монографія. Київ : НІПМБ, 2001. 300 с.

6. Домарёв В. В. Безопасность информационных технологий. Системный подход. Київ : ООО «ТИД «ДС», 2004. 992 с.

7. Дубов Д. Підходи до формування тезаурусу у сфері кібербезпеки. *Політичний менеджмент.* 2010. № 5. С. 19–30.

8. Дудоров О. М. Можливі варіанти побудови інтелектуальної системи виявлення несанкціонованою роботи програмного забезпечення. *Математичні структури та моделювання* 2005. № 15. С.116-124.

9. Золотар О. О. Класифікація загроз інформаційній безпеці. *Інформація і право*. 2013. №3(9). С. 105–112.

10. Зубок М. Інформаційна безпека в підприємницькій діяльності. Підручник. Київ : 2015. 216 с.

11. Керівництво з управління ризиками для систем інформаційних

технологій. Рекомендації Національного інституту Стандартів і технологій. Gaithersburg: National Institute of Standards and Technology, 2002. 95 с.

12. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України: Монографія. Одеса : Юридична література, 2013. 472 с.

13. Литвиненко О. Проблема інформаційної безпеки в контексті міграційних процесів. URL: //www.nbuv.gov.ua/portal/soc_gum/Ukralm/2012_ 7/lytvynenko.pdf (дата звернення: 10.09.2023).

14. Марущак А. І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки. *Державна безпека України.* 2011. № 21. С. 92–95.

15. Марущак А. І. Пріоритети розвитку інформаційного права України. *Інформація і право.* 2011. № 1. С. 20–24.

16. Міжнародний стандарт ISO/IEC 27001 «Інформаційні технології. Технології безпеки. Система керування інформаційною безпекою. Вимоги» URL: http://www.ni.din.de/sc27.html. (дата звернення: 10.09.2023).

17. Матвійчук О. В.Моделювання економічних процесів із застосуванням методів нечіткої логіки. К. : КНЕУ, 2007. 264 с.

18. Машкіна Д. С, Васильєв С. І. Підхід до розробці інтелектуальної системи захисту інформації. *Інформаційні технології.* 2007. № 6 . С. 2-6.

19. Машкіна Д. С, Гузаїрів М. Б. Інтелектуальна підтримка прийняття рішень по управлінню захистом інформації в критично важливих сегментах інформаційних систем. *Інформаційні технології.* 2009. №7. С. 25-32.

20. Машкіна Д. С, Рахімов Є. А. Система підтримки прийняття рішень по управлінню захистом інформації. *Безпека інформаційних технологій.* 2006. №2. С. 62-67.

21. Мельник Р. Модель оцінювання рівня інформаційних ризиків в корпоративних системах. Вісник Київського національного університету ім. Т.Г. Шевченка, 2015. № 6 (171). С. 54-60.

22. Мур М. Управління інформаційними ризиками. *Фінансовий директор*. 2003. С.64-69.

23. Пилипчук В. Г. Системні проблеми розвитку правової науки в

інформаційній сфері. *Вісник Академії правових наук Україн*и. 2011. № 3. С. 16–27.

24. Погребняк А. В. Технології комп'ютерної безпеки : монографія. Рівне : МЕГУ, 2011. 117 с.

25. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : Постанова Кабінету Міністрів України від 29.03.06 р. № 373 // *Офіційний вісник України.* 2006. № 13. С. 20–22.

26. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 − 2015 роки : Закон України : від 09.01.07 р. № 537-V. *Відомості Верховної Ради України.* 2007. № 12. С. 102–103.

27. Про основи національної безпеки України : Закон України : від 19.06.03 р. № 964-IV. *Відомості Верховної Ради України.* 2003. № 39. С. 11–23.

28. Нестеренко В. А. Статистичні методи виявлення порушень безпеки в мережі. *Інформаційні процеси*. 2006. Вип. 3. С. 208-217.

29. Сороківська О. А. Інформаційна безпека підприємства: нові загрози та перспективи. URL: http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf (дата звернення: 10.09.2023).

30. Сорокін О. Л. Інформаційна безпека та її складові: проблеми визначення концепту. *Держава та право.* 2014. №8. С. 18–22.

31. Стенг Д. І. Секрети безпеки мереж. К. : Діалектика, 1996. 544 с.

32. Цвілій О. Безпека інформаційних технологій: сучасний стан стандартів ISO27k системи управління інформаційною безпекою. *Телекомунікаційні та інформаційні технології.* 2014. № 2. С. 73–79.

33. Цимбалюк В. С. Окремі питання щодо визначення категорії «інформаційна безпека» у нормативно-правовому аспекті. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.* 2004. №8. С. 30–33.

34. Фурашев В. М. Питання законодавчого визначення понятійно-категорійного апарату у сфері інформаційної безпеки. Інформація і право:

науковий журнал. 2012. № 1(4). С.46–56.

35. Шубіна О. В. Державна інформаційна безпека: проблеми визначення концепту. Держава та права. 2014. №3. С. 26–31.

36. Miller DR Security Information and Event Management (SIEM) implementation. *DR Information Technology. Information Security. Information Обслуговування*. URL: http://www.isaca.org. (дата звернення: 10.09.2023).

37. Jones J. An Introduction to FAIR. Trustees of Norwich University, 2005. 67 p.

38. Zadeh L. Fuzzy sets. *Information and* Control, 2005. №8. P. 338-353.

39. Zadeh L. On optimal control and linear programming. *IRE Trans. Automaticcontrol*, Ac-7, 2002. P. 45-46.

40. Zimmermann H.-J. Fuzzy Sets, Decision Making and Expert Systems. Kluwer:Dordrecht, 2007. 335 p.

ДОДАТКИ

Додаток А

Таблиця А.1 – Функція реалізації

U	Z																	
	$P(z_1)$	$P(z_2)$	$P(z_3)$	$P(z_4)$	$P(z_5)$	$P(z_6)$	$P(z_7)$	$P(z_8)$	$P(z_9)$	$P(z_{10})$	$P(z_{11})$	$P(z_{12})$	$P(z_{13})$	$P(z_{14})$	$P(z_{15})$	$P(z_{16})$	$P(z_{17})$	$P(z_{18})$
U_1	$C(V_1)$	$C(V_1)$	$C(V_3)$	$C(V_1)$	$C(V_3)$	$C(V_1)$	$C(V_3)$	$C(V_3)$	$C(V_1)$	$C(V_3)$	$C(V_1)$	$C(V_3)$	$C(V_1)$	$C(V_3)$	$C(V_1)$	$C(V_3)$	$C(V_1)$	$C(V_3)$
U_2	$C(V_1)$	$C(V_1)$	$C(V_1)$	$C(V_2)$	$C(V_2)$	$C(V_4)$	$C(V_4)$	$C(V_1)$	$C(V_2)$	$C(V_2)$	$C(V_4)$	$C(V_4)$	$C(V_1)$	$C(V_1)$	$C(V_2)$	$C(V_2)$	$C(V_4)$	$C(V_4)$
U_3	$C(V_1)$	$C(V_4)$	$C(V_4)$	$C(V_4)$	$C(V_4)$	$C(V_4)$	$C(V_4)$	$C(V_2)$	$C(V_2)$	$C(V_2)$	$C(V_2)$	$C(V_2)$	$C(V_4)$	$C(V_4)$	$C(V_4)$	$C(V_4)$	$C(V_4)$	$C(V_4)$