

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЗАПОРІЗЬКА ПОЛІТЕХНІКА»

Інститут інформатики та радіоелектроніки
Факультет комп'ютерних наук та технологій
Кафедра комп'ютерних систем та мереж

Пояснювальна записка

до дипломного проекту (роботи)

магістра

(ступінь вищої освіти (освітній ступінь))

на тему **КОМП'ЮТЕРНА СИСТЕМА З ПІДВИЩЕНИМ РІВНЕМ БЕЗПЕКИ
НА ОСНОВІ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ**

Виконав: студент 2 курсу, групи КНТ-511м
спеціальності _____

123 «Комп'ютерна інженерія»

(код і назва спеціальності)

Поліщук Владислав Олександрович

(прізвище та ініціали)

Керівник Ільяшенко М.Б.

(прізвище та ініціали)

Рецензент Самойлик С. С.

(прізвище та ініціали)

м. Запоріжжя
2022 рік

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»
 (повне найменування вищого навчального закладу)

Інститут, факультет інформатики та радіоелектроніки, комп'ютерних наук і технологій
 Кафедра «Комп'ютерні системи та мережі»
 Ступінь вищої освіти (освітній ступінь) магістерський
 Спеціальність 123 Комп'ютерна інженерія
 (код і назва)
 Освітня програма (спеціалізація) Комп'ютерні системи та мережі
 (назва)

ЗАТВЕРДЖУЮ

Зав. кафедри Кудерметов Р.К.

“ ” 2022 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Поліщук Владислав Олександрович

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) Комп'ютерна система з підвищеним рівнем безпеки на основі інтелектуальних технологій

керівник проекту (роботи) Ілляшенко Матвій Борисович, к. т. н., доцент

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від “07” листопада 2022 року № 367

2. Строк подання студентом проекту (роботи) 10 грудня 2022 року

3. Вихідні дані до проекту (роботи) безпека системи, модель протидії загрозам, розрахунки безпеки системи

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1) Аналіз проблеми захисту інформації у сегменті корпоративних інформаційних систем;

2) Методологічні основи управління захистом інформації у корпоративних інформаційних системах;

3) Модель оцінки рівня інформаційних ризиків у сегменті корпоративної інформаційної системи.

4) Моделювання раціонального модельного складу системи захисту інформації

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

Плакат 1 – Модель складу системи захисту інформації СГ КІС;

Плакат 2 – Графіки функцій належності показника рівня інформаційних ризиків у КІС;

Плакат 3 – Графічне представлення системи нечіткого висновку показника рівня інформаційних ризиків;

Плакат 4 – Структура системи.

6. Консультанти розділів проекту (роботи)		Підпис, дата	
Розділ	Прізвище, ініціали та посада консультанта	завдання видав	прийняв виконане завдання
1-4	Ільяшенко М.Б., к. т. н., доцент		
Нормоконтроль	Щербак Н.В., ст. викл.		

7. Дата видачі завдання 10.10.2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Аналіз технічного завдання	10.10.2022 р.	
2	Постановка задачі.	15.10.2022 р.	
3	Огляд методологій бази дослідження інформаційних ризиків	20.10.2022 р.	
4	Моделювання аналізу факторів інформаційного ризику на основі лінгвістичного підходу	01.10.2022 р.	
5	Побудова моделі системи захисту інформації	25.11.2022 р.	
6	Розробка моделей протидії загрозам інформації безпеки в умовах невизначеності.	01.12.2022 р.	
7	Захист роботи	16.12.2022 р.	

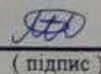
Студент


(підпис)

В.О. Поліщук

(ініціали та прізвище)

Керівник проекту (роботи)


(підпис)

М.Б. Ільяшенко

(ініціали та прізвище)

РЕФЕРАТ

ПЗ: 81 с., 10 рис., 13 табл., 39 джерел.

КІС, СУІБ, ІНФОРМАЦІЙНА СИСТЕМА, СИСТЕМА БЕЗПЕКИ

Мета роботи полягає у розробці адаптивних методів управління захистом інформації в сегменті КІС для забезпечення необхідної захищеності інформації в умовах невизначеності інформаційних атак на основі інтелектуальних технологій.

– найбільш раціональним підходом до ефективної ЗІ у сегменті КІС є використання інтелектуальних засобів для підтримки прийняття рішень під час управління ЗІ

– малодослідженими для вирішення завдання оцінки невідомих атак залишаються такі перспективні методи, як метод нейронних мереж, метод нечіткої логіки та генетичні алгоритми;

– перспективними на сьогодні є технології, які дозволяють у реальному часі оцінити ризик порушення ІБ з малим залученням експертів на базі інформації, що характеризує інформаційну цінність ресурсів, що потребують захисту, технічних характеристик засобів захисту, та врахування особливостей реальних загроз для конкретного об'єкта захисту.

Об'єктом Дослідження у роботі є забезпечення необхідного рівня ЗІ.

Предмет магістерської – гнучкі методи управління ЗІ у сегменті КІС на основі використання інтелектуальних технологій.

ПЕРЕЛІК СКОРОЧЕНЬ

КІС - корпоративна інформаційна система;

СУІБ - систем управління інформаційною безпекою;

ЗЗІ - засобів захисту інформації;

МС - машинне самонавчання;

СППР ОУ - система підтримки прийняття рішень щодо оперативного управління;

ЗМІСТ

1	Аналіз проблеми захисту інформації у сегменті корпоративних інформаційних систем	10
1.1	Сутність проблеми керування захищеністю інформації	10
1.2	Інфраструктура розподіленої корпоративної інформаційної системи та модель захищеності інформації в ній.....	17
1.3	Сучасні концепції захищеності інформації у корпоративних інформаційних системах.....	21
2	Методологічні основи управління захистом інформації у корпоративних інформаційних системах.....	28
2.1	Основні науково-теоретичні підходи щодо розробки систем управління захистом інформації	28
2.2	Методи аналізу інформації щодо ідентифікації атак.....	33
2.3	Метод оцінки захищеності інформаційної системи	36
3	Модель оцінки рівня інформаційних ризиків у сегменті корпоративної інформаційної системи	41
3.1	Огляд методологічної бази дослідження інформаційних ризиків	41
3.2	Постановка задач оцінювання ризику інформаційної системи	44
3.3	Моделювання аналізу факторів інформаційного ризику на основі лінгвістичного підходу.....	48
4	Моделювання раціонального модельного складу системи захисту інформації	56
4.1	Побудова моделі системи захисту інформації.....	56
4.2	Розробка моделей протидії загрозам інформації безпеки в умовах невизначеності	59
4.3	Розробка структури системи інтелектуальної підтримки прийняття рішень щодо оперативного управління захистом інформації.....	66
	Висновки	77

Перелік джерел посилання	78
--------------------------------	----

Перелік графічного матеріалу:

Пл1 – Модель складу системи захисту інформації СГ КІС;

Пл2 – Графіки функцій належності показника рівня інформаційних ризиків у КІС;

Пл3 – Графічне представлення системи нечіткого висновку показника рівня інформаційних ризиків;

Пл4 – Структура системи;

ВСТУП

У магістерській роботі розглядаються питання щодо побудови комплексної системи захисту інформації корпоративної інформаційної системи на основі інтелектуальних технологій. Безпека інформаційних систем - одна з найбільших проблем, що стоять перед технологічним віком суспільства. Високий рівень автоматизації процесів у суспільстві ставить їх у залежність від рівня безпеки застосовуваних інформаційних технологій.

Актуальність роботи. Поточний етап розвитку в галузі обміну інформацією є інтенсивним впровадженням сучасних інформаційних технологій, масовим поширенням мереж різного рівня охоплення – локального, корпоративного, глобального, що створює величезний потенціал застосування інформаційного обміну в різноманітних сферах бізнесу. Технології управління бізнесом, можливості його масштабу у різних сферах діяльності визначаються корпоративними інформаційними системами (KIC), що охоплюють інфраструктуру та різні інформаційні сервіси. Інфраструктура KIC включає мережі, сервери, робочі станції, охоплюючи підрозділи, які можуть бути розгорнуті по всьому світу. Сегмент (СГ KIC) є структурною одиницею KIC.

Масове використання ІТ-технології в KIC змушує серйозно ставитися до інформаційної безпеки через загрози захисту інформації.

Сучасні теоретичні та практичні розробки, що гарантують захист інформації (ЗІ) володіють деякими протиріччями: загостреною увагою до безпеки інформаційних об'єктів, значно підвищеними вимогами, які пред'являються до ЗІ, впровадженням прийнятих міжнародних стандартів з гарантій інформаційної безпеки (ІБ), дедалі зростаючими витратами забезпечення ЗІ, а з іншого боку збитки, які завдають власникам інформаційних ресурсів комп'ютерними атаками, збільшується.

Сучасні підходи до організації інформаційної безпеки не забезпечують належної відповідності вимогам ІБ. Основні недоліки використовуваних систем

(СЗІ) зазвичай обумовлені складними технологіями побудови архітектури СЗІ та використанням стратегій від відомих загроз, як правило, оборонного характеру.

Тому результативне використання інформаційних технологій у діяльності корпорацій потребує ефективно керованих систем ЗІ, оскільки система, яка реалізує процеси управління подіями ІБ, плануванням модульної структури системи ЗІ та аудит інформаційної безпеки, повинні проводитися автономно на рівні сегмента КІС.

1 АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ У СЕГМЕНТІ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

1.1 Сутність проблеми керування захищеністю інформації

Сучасні корпорації мають складну розподілену структуру, зумовлену багатoproфільною діяльністю, територіальним розміщенням підрозділів, численними корпоративними зв'язками з партнерами. Корпоративними, як правило, називають системи управління підприємством, що має розвинену структуру та окремі органи управління. Серед корпоративних систем виділяють організаційні, інформаційні та ін. Більшість бізнес-функцій та управлінських процесів підприємств та організацій охоплюють корпоративні інформаційні системи (KIC), будучи важливим інструментальним засобом ведення бізнесу.

Впровадження нових інформаційних технологій для підприємств завжди пов'язане із виникненням нових ризиків. Чим складнішою 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, зміни або знищення інформації тощо. [15] Такі ризики можуть завдати підприємству значної шкоди. Створення розвиненого та захищеного інформаційного середовища є неодмінною умовою розвитку як окремих корпорацій, так і економіки, суспільства та держави в цілому. Тому питання забезпечення захищеності інформації у сегменті KIC стали нині дуже злободенними.

KIC є складною людино-машинною чи соціо-технічною системою, яка включає до свого складу інформаційну систему підприємства. Для дослідження таких систем використовуються різні типи моделей. Процес функціонування KIC підприємства здійснюється в умовах протидії підприємства як соціо-технічної системи з одного боку, і конкурентів, зловмисників, негативних явищ

природи та інших об'єктів та явищ, з іншого боку.

Ускладнення та розширення сучасних КІС призводить до збільшення кількості мережевих пристроїв та різних засобів захисту інформації, що призводить до великої кількості подій безпеки.

Необхідно відзначити, що сучасні технологічні процеси значно обганяють теоретичні осмислення практичних розробок та застосувань у галузі інформаційних технологій, а також у галузі нових комунікаційних можливостей. Тому є підстави припускати неповну адекватність існуючим теоретичним досягнень завданням захисту інформації, що стоять, як у практичному, так і в теоретичному ключі [37].

Основними недоліками ЗЗІ, що широко використовуються, є їх риси, пов'язані зі суворими архітектурними принципами [9] і використанням в основному оборонних або наступальних стратегій захисту від найбільш відомих і небезпечних загроз.

Вирішення зазначених проблем та ефективне використання сучасних КІС потребує засобів та методів рівного та надійного управління не тільки мережами, а також і системою ЗІ, усіма заходами, що забезпечують безпеку мережі [10]. Нам потрібні методи, які дозволили б нам швидко відслідковувати зміни в операційному середовищі системи та запобігати своєчасним порушенням інформаційної безпеки, керуючи як мережевим обладнанням, так і обладнанням безпеки.

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

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

Структуроване уявлення всієї різноманітності аспектів управління захистом інформації наведено наочно на рисунку. 1.1.



Рисунок 1.1 - Структурування проблеми управління ЗІ

В даний час практично не можна знайти виробників, які б представляли споживачеві повний спектр засобів як апаратних, так і програмних, необхідних для побудови систем ЗІ, що задовольняє сучасним вимогам. Більшість систем ЗІ будується з урахуванням програмно-апаратних засобів, випущених різними виробниками. Для гарантування гетерогенної КІС надійності ЗІ необхідна система управління інформаційною безпекою (СКІБ), яка може забезпечити правильну конфігурацію кожного з її компонентів та 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.

Виконаний нами аналіз дозволяє стверджувати, що на рівні сегмента КІС система управління, яка реалізує низку функцій управління, має функціонувати автономно:

- отримувати та оцінювати об'єктивні дані про поточний стан безпеки КІС(аудит);
- управляти подіями, якими ведуться протоколювання;
- визначати модульний склад системи ЗІ та точки створення засобів

захисту інформації у комп'ютерній мережі підприємства.

Міжнародний стандарт ISO/IEC 27001 [2] описує моделі, що використовуються для створення, впровадження, експлуатації, постійного моніторингу та аналізу, обслуговування та покращення систем управління інформаційною безпекою (СУІБ).

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

Процесний підхід до управління ЗІ у цьому стандарті допомагає виділити такі моменти:

- визначення принципів, цілей, процесів та процедур, які мають відношення до управління ризиками та вдосконалення ЗІ для досягнення результатів, що відповідають цілям компанії;

- впровадження та функціонування правил, засобів контролю, процесів та процедур СУІБ;

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

- виконання коригувальних та попереджувальних процедур, що ґрунтуються на результатах проведення внутрішнього аудиту та аналізу з метою постійного поліпшення управління ЗІ.

Склад СУІБ включає:

- організаційну структуру;
- політику; заходи планування;
- набір процедур, процесів, ресурсів.

Метою СУІБ є проектування СЗІ, використання, експлуатація, постійний контроль, аналіз, поліпшення ЗІ.

Для створення СУІБ підприємству потрібне виконання наступного:

- визначення меж системи;

- виробити принцип дії щодо захисту інформації з урахуванням законодавчих норм та встановлених цілей захисту;
- виробити критерії оцінки важливості ризиків;
- вибрати методологію оцінки ризику, що відповідає системі управління ЗІ та відповідає нормативним вимогам; та здатні забезпечити, щоб оцінки ризику давали конкретні результати;
- визначити прийнятний рівень ризику;
- виконувати ідентифікацію ризиків (активи, загрози та негативні впливи, які сприяють втраті конфіденційності, цілісності та доступності активів та критичних уразливостей системи позиціонування);
- оцінити значущість ризиків (оцінити ймовірність порушень інформаційної безпеки у світлі існуючих загроз та вразливостей, оцінити рівні ризику, визначити, чи є ризики прийнятними чи вимагають відповіді);
- знайти можливість управління ризиками (застосування прийятних засобів зниження чи прийняття ризику);
- вибрати методи управління та обробки ризиків, які б враховували критерії для прийняття ризиків;
- узгодити з керівництвом впровадження системи ЗІ та виконати підготовку заяви про ступінь застосовності (включаючи мету управління, засіб управління, обґрунтування вибору).

Етап реалізація та експлуатація СУІБ підприємства включає такі 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 забезпечити швидко виявити події у системі ЗІ та реакції на інцидент у системі ЗІ;

- швидке виявлення вживаних і відбулися порушень ЗІ та інцидентів;
- виявлення подій у системі ЗІ та запобігання інцидентам за допомогою використання індикаторів;
- вимірювання результативності засобів керування для перевірки того, що вимоги були виконані;
- оновлення планів захисту інформації з метою обліку даних, отриманих у процесі діяльності, пов'язаної як із постійним контролем, так і аналізом.

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

Стандарт ISO/IEC 17799 дає керівні вказівки, які рекомендується використовувати у процесі проектування системи захисту. У стандарті наводяться мета управління та перелік засобів управління. Метою політик захисту є забезпечення напрямів та підтримки керівництвом ЗІ відповідно до бізнесових вимог, законодавчих норм. Політику в галузі ЗІ необхідно аналізувати із запланованою періодичністю, щоб гарантувати її адекватну придатність та адекватність.

Щодо управління активами мета полягає в тому, щоб забезпечити та підтримувати необхідні засоби захисту активів організації в умовах праці, які потребують чіткої визначеності. Необхідно скласти та підтримувати реєстри важливих активів, а також активів, які будь-яким чином пов'язані із засобами обробки інформації. Інформація має бути класифікована за значимістю та критичністю для компанії.

Роль та відповідальність співробітників, користувачів щодо інформації та їх захисту мають бути задокументовані відповідно до політики ЗІ в компанії.

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

результати повинні регулярно перевірятись.

Метою управління доступом користувачів є гарантований доступ для зареєстрованих користувачів та запобігання несанкціонованому доступу до КІС. Призначення та використання дозволів повинні контролюватись та повинні бути обмежені, встановлення паролів має контролюватись формальним процесом адміністратора. Необхідно встановити формальну процедуру реєстрації користувачів.

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

У [34] наведено модель зрілості процесів управління інформаційною безпекою, у якій найвищим рівнем є «керований» та «оптимізований». Керований рівень характеризується моніторингом на об'єкті захисту та оцінкою процесу управління, виконується їх оптимізація, часткове використання засобів автоматизації. Оптимізаційний рівень характеризує опрацьованість процесу управління інформаційною безпекою, здатність до виконання швидкої адаптації у разі виникнення змін у бізнес-процесі, комплексне використання заходів захисту, які забезпечують основу для покращення процесів управління.

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

- планування - аналіз та оцінка ризику інформаційної безпеки, визначення політик систем управління ЗІ, вибір заходів захисту та їх оновлення для мінімізації ризиків, прийняття рішень про впровадження системи управління ЗІ;
- впровадження та експлуатація системи управління ЗІ, включаючи розробку планів з обробки ризиків інформаційної безпеки, реалізацію заходів щодо її захисту, управління роботою, виявлення та реагування на інциденти

безпеки, що виникають;

- перевірка (моніторинг та аналіз), у тому числі аналіз продуктивності, у тому числі аналіз рівнів залишкового ризику
- інформаційної безпеки; аналіз внутрішніх аудитів системи управління ЗІ;
- вдосконалення системи управління ЗІ, у т. ч. запровадження тактичних та стратегічних покращень у системі, що вимагають прийняття рішення на рівні планування, оцінки досягнення мети.

Стандарт ISO/МЕК 15408-2002 містить етапи управління безпекою; це посібник з управління безпекою в інформаційно-комунікаційній системі [4]. Стандарт розкриває загальні проблеми управління, які є важливими для ефективного планування, впровадження та підтримки безпеки системи.

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

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

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

- інформаційна інфраструктура;
- інформаційні послуги.

Блок інформаційної інфраструктури є матеріальну базу та середовище для функціонування інформаційної служби.

Інфраструктура сучасної компанії та сучасного суспільства може бути представлена таким чином, щоб вона складалася з просторово-розподілених підрозділів цього товариства та його партнерів, клієнтів та постачальників.

Основні взаємодії між об'єктами компанії здійснюються в рамках розподіленої КІС з використанням пристроїв зв'язку та каналів зв'язку, що призначаються оператором зв'язку з використанням різних мережевих програм та сервісів.

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

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

На рисунку 1.2 показує результат структурного розкладання КІС [21].

Впровадження Інтернету в технології корпоративних комунікацій призвело до різкого збільшення кількості користувачів зовнішніх мереж, збільшення різноманітності типів каналів зв'язку та використання нових мережевих та інформаційних технологій. Це підвищило вимоги безпеки для транзакцій електронних мереж: серверів, маршрутизаторів, серверів віддаленого доступу, каналів зв'язку, операційних систем, баз даних та додатків. Небезпеки у кожному елементі системи захисту швидко зростають, і це тенденція збережеться й у майбутньому [18].

Гостра також проблема можливості внутрішніх загроз захищеності інформації, особливо це стосується великих корпорацій, що 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.

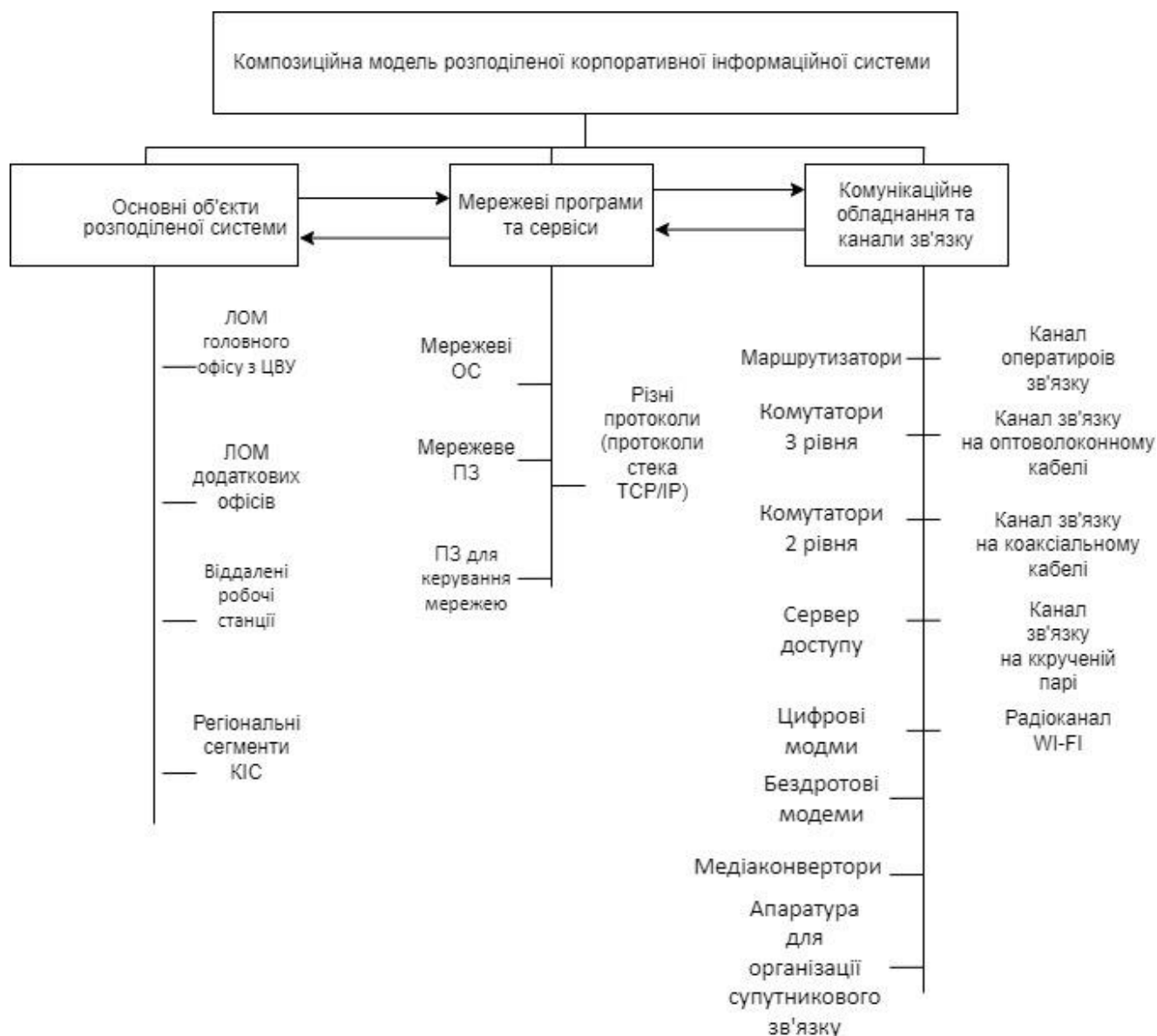


Рисунок 1.2 - Модель распределенной КИС с детализацией СГ КИС

Чим більша компанія, тим більше обсяг коштів, якими вона керує, тим більше агресивними та професійними можуть бути атаки за участю внутрішніх зловмисників. На думку експертів, розвиток та інтеграція інформаційних технологій у корпоративні бізнес-процеси збільшує небезпеку внутрішніх загроз інформаційній безпеці [30].

Сучасні засоби злому комп'ютерних мереж та крадіжки інформації зазнають швидкого розвитку, поряд з іншими високотехнологічними інформаційними галузями. Тому забезпечення інформаційної безпеки КІС стає одним із першочергових завдань менеджменту компаній. Збереження

конфіденційності, цілісності та доступності інформаційних ресурсів компанії багато в чому визначає якість та швидкість прийняття стратегічних рішень керівництвом компанії.

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

На рисунку 1.3 наочно продемонстровано модель складу системи захисту інформації СГ КІС [19].

До системи ЗІ висувається вимога абсолютної прозорості для вже існуючих у рамках КІС додатків і, крім того, вимога сумісності з мережевими технологіями, що використовуються корпорацією.

Тому, з метою забезпечення надійної захищеності ресурсів КІС, системи ЗІ повинні реалізовуватися на базі найпрогресивніших та найперспективніших технологій у галузі інформаційного захисту.

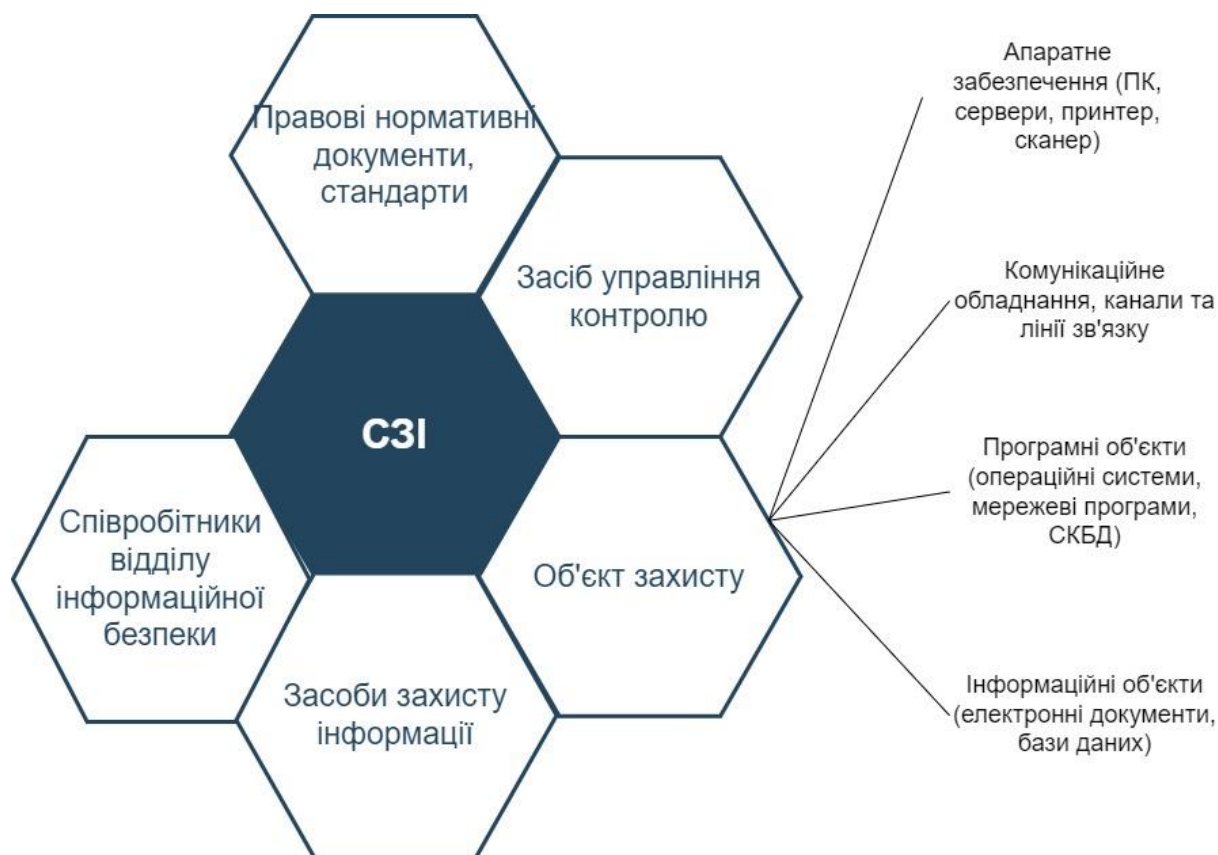


Рисунок 1.3 – Модель складу системи захисту інформації СГ КІС

Тому, щоб забезпечити ефективність комп'ютеризації у корпорації,

необхідно забезпечити такі параметри безпеки інформаційних ресурсів, як цілісність, конфіденційність, справжність відповідної ділової інформації, що циркулює у локальних та глобальних інформаційних мережах.

1.3 Сучасні концепції захищеності інформації у 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 тощо). Згідно з одинадцятим звітом Cisco кібербезпеки, «щоб скоротити час виявлення зловмисників, фахівці з кібербезпеки починають все більше застосовувати (і закуповувати) засоби, що використовують штучний інтелект (ІІ) та машинне самонавчання (МС)» [45]. З одного боку, шифрування допомагає посилити захист, а з іншого - зростання як легітимного, так і шкідливого зашифрованого трафіку (50% з жовтня 2017 року) збільшує проблеми тих, хто захищається у процесі виявлення потенційних загроз та моніторингу їхніх дій. «За минулі 12 місяців фахівці Cisco з інформаційної безпеки зафіксували більш ніж триразове зростання зашифрованого мережевого трафіку від зразків шкідливого ПЗ, що інспектуються» [45].

Використання інтелектуальних технологій та машинного навчання показує хороші результати в галузі інформаційної безпеки, і згодом автоматично виявить нестандартні шаблони у зашифрованому веб-трафіку, у хмарних середовищах та середовищах IoT. «Деякі з 3600 директорів з інформаційної безпеки, опитаних під час підготовки звіту Cisco 2018 Security Capabilities Benchmark Study, заявили, що довіряють таким інструментам, як МС та ІІ, і хотіли б їх використовувати, але вони розчаровані великою кількістю помилкових спрацьовувань»[45]. Поступове вдосконалення технологій МС та ІІ з часом дозволить знизити кількість «хибних

тривог» і коректно визначати «нормальну» активність мереж, відрізняючи 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, - зазначив Джон Стюарт (JohnStewart), старший віце-президент Cisco, директор з інформаційної безпеки. — Для відображення нападів та зменшення схильності до наростаючих ризиків як ніколи раніше важливо стратегічно вдосконалювати захист, інвестувати в технології та впроваджувати передові методики» [45]

Деякі результати звіту Cisco 2018 Annual Cybersecurity Report показують, що:

- фінансові збитки від атак стає дедалі реальнішими;
- більше половини всіх атак завдали фінансових збитків на суму понад 500 млн. доларів, включаючи втрачену вигоду, залишення клієнтів, втрачену вигоду та прямі витрати;
- атаки на ланцюжки поставок стають дедалі складнішими і набирають швидкість. [45]

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

Щоб знизити ризик атаки на ланцюжок постачання, необхідно переглянути сторонні процедури для перевірки ефективності технологій інформаційної безпеки. У той же час захист інформаційних систем стає все важчим, уразливості стають все більш різноманітними.

Щоб захистити себе, організації використовують складні комбінації продуктів різних виробників. Це ускладнення зі зростаючим розмаїттям уразливостей негативно впливає на здатність організацій відбивати атаки і призводить до збільшення ризиків фінансових втрат.

Згідно зі звітом Cisco:

– «У 2017 р. 25% фахівців з інформаційної безпеки повідомили, що використовують продукти від 11—20 вендорів, у 2016 р. так відповіли 18%;

– Фахівці з інформаційної безпеки повідомили, що 32% уразливостей торкнулися більш як половини систем, у 2016 р. так відповіли 15%;

– Фахівці з інформаційної безпеки оцінили користь засобів поведінкового аналізу для виявлення шкідливих об'єктів: 92% фахівців вважають, що засоби поведінкового аналізу добре справляються із поставленим завданням; 2/3 представників сектору охорони здоров'я та представники індустрії фінансових послуг вважають поведінкову аналітику корисною 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 для кращого захисту даних, 48%

– Заради масштабованості, 46% - задля зручності експлуатації»[45].

Хоча хмара забезпечує підвищену безпеку даних, зловмисники користуються тим, що компанії не дуже добре захищають хмарні конфігурації, що розвиваються і розширюються. Ефективність захисту таких конфігурацій підвищується завдяки використанню комбінації передових технологій, таких як передові технології безпеки, такі як машинне навчання, та інструментів безпеки світового класу, таких як хмарні платформи інформаційної безпеки.

В останні роки також спостерігається тенденція до зростання шкідливих програм та часу виявлення. «Продемонстрований Cisco медіаний час виявлення (timetodetection, TTD) за період з листопада 2016 по жовтень 2017 р. становив близько 4,6 години. У листопаді 2015 р. цей показник склав

39 годин, а за даними Звіту Cisco з кібербезпеки за 2017 р., медіанний час виявлення за період з листопада 2015 по жовтень 2016 р. становив 14 годин» [45].

Ключовим фактором для Cisco у процесі скорочення часу виявлення та 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 є:

- контроль за дотриманням політик та практик компанії з оновлення додатків, систем та пристроїв;
- своєчасне отримання точних даних про загрози та наявність процесів використання цих даних для моніторингу безпеки;
- проведення поглибленого та поглибленого аналізу;
- регулярне резервне копіювання даних та перевірка процедур відновлення
- критичні дії в контексті швидкого розвитку мережевих здирників та шкідливих програм;
- виконувати перевірки безпеки на мікро сервісах, хмарних сервісах та системах адміністрування додатків.

Галицький О.В. зазначає існування «різних підходів до формування архітектур управління інформаційною безпекою КІС:

- використання технології управління всіма пристроями безпеки КІС з центрального вузла нереалізовано, так як первинних пристроїв велика кількість, і контроль за ними може викликати велике завантаження центрального вузла управління; важко отримання деталізованої інформації, яка необхідна для управління; локальні методи управління часом є технічно необхідними;
- з досвіду провідних виробників засобів забезпечення мережевої безпеки відомо, що організація може успішно реалізовувати свою безпекову політику в розподілених КІС при централізованому управлінні безпекою »[10, с.286].

Багато компаній (CiscoSystems, ComputerAssociates, PLATINUM) використовують механізми для інтеграції управління СРЗІ до традиційних систем управління мережею [8]. Однак цей тип інтегрованої системи управління є дорогими, а деякі питання управління інформаційною безпекою не вирішуються такими системами.

Ефективна система управління ІБ мережевий КІС має супроводжуватися системою ієрархічного управління, що складається з:

- централізованогоуправління на рівні глобальної політики з

інформаційної безпеки, що відповідає бізнес-процесам підприємства та визначає набір правил безпеки для всіх взаємодій об'єктів КІС, а також об'єктів КІС та зовнішніми об'єктами;

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

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

Астахова Л.В. зазначає, що в даний час «найширше поширення на ринку SIEM-систем отримали системи, що використовують сигнатурні методи кореляції подій інформаційної безпеки, що зумовлено, першу чергу, простотою реалізації даних систем, а також гнучкістю при налаштуванні та подальшій експлуатації» [6, с. 165]. До таких систем SIEM (Security information and event management – управління інформацією та подіями безпеки) відносяться: HP ArcSight; IBM QRadar; Symantec SIM; RSA Envision та інші. Недоліком є те, що системи, побудовані за цим принципом, не адаптуються до умов складу КІС, що швидко змінюється, через заздалегідь визначені випадки інформаційної безпеки, вбудовані в систему. До недоліків таких систем також відноситься велика кількість помилкових спрацьовувань та відносна складність конфігурації та реалізації.

Аналіз ринку SIEM-систем [24] показує, що у сучасних умовах ринок SIEM розвивається повільніше, ніж там. Не всі закордонні виробники представлені нашій країні. Але водночас спостерігається розвиток вітчизняних SIEM-систем. SIEM-системи чуйно реагують на нові досягнення в галузі обробки даних. Покращена аналітика великих даних BigData відіграє важливу роль у SIEM-системах, що використовуються в сегменті КІС. Великий інтерес представляє нова технологія UEBA (User and Entity Behavior Analytics – поведінкова аналітика користувачів та сутностей) для інтеграції до SIEM-систем [13]. Один із найкорисніших варіантів застосування модуля UEBA – це виявлення інсайдерів шляхом детектування статистичних аномалій. Якщо співробітники, які мають

легітимний доступ до інформації, починають нестандартно діяти,

За прогнозами Gartner посилення, до 2020 року модулі UEBA будуть у кожній четвертій SIEM-системі.

Можна констатувати тенденцію розвитку автоматизованих систем управління захистом інформації сегменту KIS. Однак існуюча методологія інформаційного ризик-менеджменту не передбачає комплексного підходу до управління інформаційним ризиком. Використання економіко-математичних моделей управління захистом інформації не завжди орієнтоване на досягнення кінцевого результатів бізнес-процесів, що призводить до зниження ефективності управління ризиками всього підприємства.

Успішне використання сучасних інформаційних технологій неможливе без ефективного управління як комп'ютерної мережею, а й процесом ЗІ. Поліпшення управління інформаційною безпекою можливе за рахунок підвищення якості ефекту управління як за рахунок використання нових методів вирішення проблеми управління, так і за рахунок скорочення тривалості циклів контролю. Отже, обґрунтованим підходом до покращення ефективності заходів захисту інформації можуть стати розробки інтелектуальних засобів прийняття рішень щодо питань управління ЗІ.

Хоча в даний час проводяться активні дослідження з розробки методів і систем ЗІ, залишається досить неопрацьованих питань щодо створення методів створення інтелектуальних засобів ПНР щодо управління ЗІ, що вказує на необхідність комплексних рішень сукупності наукових завдань, спрямованих на вироблення не тільки науково обґрунтованих, а й практично застосовних моделей та методів інтелектуального забезпечення управління процесами ЗІ.

Реалізація запобіжних стратегій захисту інформації потребує складних рішень, які включають розробку методу оцінки підозрілої активності та різних мережевих подій, підготовку інформації для прийняття рішень про управління службами безпеки та мережевими пристроями та реагування в режимі реального часу на зміни умов операційного середовища. Проблема вибору раціональної відповіді на напад не була вирішена на практиці через ймовірність дій у відповідь,

які могли б вплинути на нормальну роботу захищеної КІС. Недостатньо досліджено для вирішення завдань оцінки невідомих втручань залишаються методи нейронних мереж, генетичний алгоритм та методи нечіткої логіки.

Сутність управління захистом інформації полягає у ухваленні рішень щодо вироблення стратегій захисту інформації для всіх етапів життєвого циклу системи ЗІ. Зростаючі вимоги до розробок та заходів впровадження технологій управління захистом інформації не відповідають станам нормативної бази, що існують на даний момент, яка не дозволяє адекватно вирішити проблему вибору раціональної модульної структури СЗІ. Існуючі керівні документи та стандарти задають ряд функціональних вимог до засобів захисту інформації та не дають жодної методики проведення порівняльного аналізу різних наборів засобів ЗІ, які сертифіковані за одним і тим самим класом, маючи на меті виявити більш раціональний цілісний варіант системи захисту інформації.

Дослідження та розробки технологій, методів та інструментів, що дозволяють у реальному часі оцінити ризик порушення ІБ, є багатообіцяючими, а також спрямовані на прогнозування рівня інформаційної безпеки у процесі проектування систем інформаційної безпеки. Слід зазначити, що показники рівня інформаційної безпеки повинні формуватися з мінімальним залученням експертів на основі інформації, що характеризує інформаційну цінність ресурсів, що потребують захисту, даних про технічні характеристики, заходи безпеки, що застосовуються або плануються, з урахуванням врахування великої кількості реальних загроз специфічного функціонування конкретних об'єктів захисту.

Аналізуючи закордонні та національні публікації, пов'язані з цією проблемою, можна виявити зростаючу тенденцію популярності інструментів оцінки ризиків, а також програмних інструментів для їх аналізу та управління ризиками.

Аналіз представлених на сучасному ринку програмних додатків, для автоматизації управління ризиками порушень ІБ, показав, що основними недоліками таких систем є:

- наявність висококваліфікованих спеціалістів;

- проблеми, що виникають при адаптації методів до потреб конкретної організації;
- неможливість оцінки ефективності конкретного комплексу захисту інформації, що використовується в компанії;
- необхідність мати достовірну статистику щодо корпоративних інцидентів інформаційної безпеки.

Однією з основних проблем зі створення систем управління ЗІ є проблема забезпечення автоматизованою підтримкою прийняття рішень щодо управління ЗІ протягом усього періоду роботи КІС та в умовах умов інформаційного середовища, що змінюються. Для цього потрібне інфраструктурне програмне забезпечення, яке підтримує математичні моделі та методи прийняття наукових рішень. Створення інструментальних програмних комплексів, що використовують усі можливості комп'ютера, дозволить приймати науково обґрунтовані рішення, оскільки процес прийняття рішень буде заснований на аналізі та прогнозі, виконаному із застосуванням математичних методів.

2 МЕТОДОЛОГІЧНІ ОСНОВИ УПРАВЛІННЯ ЗАХИСТОМ ІНФОРМАЦІЇ У КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

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

Захист інформації, методи та методики захисту вже близько тридцяти років є предметом активного обговорення як за кордоном, так і в Україні. Постійно розробляються нові методи, засоби та засоби захисту інформації, випускаються нові захисні системи, ведуться науково-дослідні роботи з розробки методик управління захистом інформації.

Аналіз результатів науково-дослідних робіт у галузі ЗІ показує, що значним досягненням у теорії захисту інформації стали роботи, присвячені проблемам

створення нових засобів захисту різного характеру, що здійснюють захист інформації на різних рівнях (технічні засоби, програмні та апаратні комплекси, криптографічні засоби захисту та і т.д.), а також інтегровані системи захисту інформації [11]. Аналіз результатів таких змін та досліджень був представлений у роботах [7, 8, 11, 14, 23, 33] та зарубіжних авторів [23, 37, 44-51]. Ключовим результатом таких робіт є формування основ теорії захисту інформації.

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

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

У ряді робіт [19, 20, 41] особливий акцент зроблений на необхідність застосування системного підходу для розробки ефективних засобів ЗІ, розробки моделей загроз, декомпозиції СЗІ (систем захисту інформації), що розробляються, розбиття їх на функціональні підсистеми для визначення факторів, що впливають на них, і виявлення можливих загроз, а також розробки системи індикаторів, що характеризують ефективність СЗІ.

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

На думку В.А.Герасименко [11] базою для формування СЗІ повинні служити плати обробки інформації, які встановлюються на об'єкт, що захищається, і завдяки якій проводиться аналіз критичності, відповідно до чого далі проводиться обґрунтування вимог до СЗІ. З сформульованих вимог формується набір засобів захисту інформації, застосування яких дасть можливість

забезпечення необхідного рівня захисту. Аргументоване обґрунтування складу (набору коштів) ЗІ – це загальне завдання всього механізму управління ЗІ.

Особливості проектування систем ЗІ розглядаються авторами у [42]. Аналіз робіт дозволяє виділити два основні підходи щодо побудови системи ЗІ:

- продуктний підхід;
- проектний підхід.

Продуктний підхід передбачає, що первинним є формування набору ЗІ, а далі, на основі функцій, що виконуються цими засобами, формулюється політика безпеки. Відповідно, проектний підхід передбачає насамперед формування політики безпеки, після чого на підставі певних вимог обираються необхідні для її реалізації засоби ЗІ.

Як зазначається в [9], системи на основі проектного підходу краще оптимізовані та є більш ефективними, що робить їх більш підходящими для використання у гетерогенних мережах. Крім того, слід зазначити, що рішення, спроектовані за допомогою проектного підходу, є довготривалішими.

Загальні принципи та методика вибору засобів захисту інформації на основі критерію оптимальності (що передбачає мінімізацію витрат при забезпеченні заданого рівня захищеності інформації), наведена у [14]. Основою цієї методики є оцінка ефективності виконання різних функцій за допомогою засобів ЗІ.

На думку деяких авторів, наприклад [34], управління операціями та стратегічне планування використання захисного обладнання розглядаються як найважливіші процеси макроуправління. У цьому контексті оперативне управління має на увазі динамічне управління інформаційною безпекою під час її автоматизованої обробки. У рамках оперативного управління має бути постійне визнання стану системи захисту інформації, а також прийняття та реалізація рішень щодо необхідності оперативних втручань у роботу системи для забезпечення ЗІ. Для прийняття рішень правильне рішення має бути вибрано з реєстру рішень, що створюється заздалегідь [44].

Планування ЗІ відноситься до процесу формування протягом

запланованого періоду програм, що забезпечують оптимальне використання засобів ЗІ. Оптимальність передбачає забезпечення необхідного рівня захисту запланованої суми витрат або за мінімізації цієї суми.

Багато хто з вищевказаних авторів зазначають при цьому, що завдання прийняття рішень є одним із найскладніших і водночас найважливіших завдань у галузі автоматизації управління захистом інформації.

Особливості та основні поняття організаційного управління інформаційною безпекою враховані у роботі [40]. Автор зазначає, що обмеження для забезпечення зростаючих вимог до рівня інформаційної безпеки є недостатністю наявного науково-технічного забезпечення (НТЗ). Для забезпечення необхідного рівня захищеності НТЗ має відповідати як динаміці інформаційного середовища, так і динаміці управління стратегіями інформаційного протистояння. У цій роботі наголошується, що багато з запропонованих на сьогоднішній день концептуальних підходів до ЗІ носять не конкретний, загальний характер, відповідно, для забезпечення можливості їх застосування у складних розподілених КІС вони повинні бути уточнені та вказані з урахуванням процесів, що відбуваються в реальному середовищі інформаційного протистояння.

У роботі [46] 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 категоризованої інформації, управління відновленням цілісності інформації (алгоритм вибору ідеальної стратегії резервного копіювання) та метод оцінки інформаційної безпеки за умов вірусних програм.

Дослідження [9] управління інформаційною безпекою розглядається переважно як організаційний процес. У зв'язку з цим, на думку автора, завдання управління захистом інформації можуть бути вирішені адміністративною групою (менеджери та адміністратори безпеки, а також оператори). Автор розглядає управління захистом інформації, як здійснення контролю за розподілом інформації в корпоративній мережі, забезпечення функціональної працездатності засобів ЗІ, фіксація подій, пов'язаних з порушеннями ЗІ та функцій, що при цьому

реалізуються, а також періодичне оновлення БД інформаційного захисту.

Роботи [17, 49] присвячені аналізу основних науково-теоретичних проблем синтезу адаптованих систем із забезпечення інформаційної безпеки, а також питанням застосування цих систем у КІС. У цих роботах особливо підкреслюється неможливість забезпечення абсолютної безпеки як окремих компонентів системи, і її загалом, оскільки будь-яка захист то, можливо подолана за відсутності обмеження у часі. Доцільно розглядати лише деякий достатній рівень захищеності, у стані якого вартість її подолання перевищує вартість отриманої при цьому інформації. Дотепер через велику складність і важку формалізованість не вдається сформувати показники кількісної оцінки рівня захищеності інформаційної системи.

У той самий час ступінь ризику залежить від показників цінності інформаційних ресурсів, ймовірності загроз і простоти вразливості, і навіть від ефективності заходів захисту. Єдиним контрольованим фактором серед перерахованих вище є міра захисту. В результаті оптимальний вибір захисного спорядження може знизити ризик до прийняттого рівня. Результати оцінки ризику є підставою для обґрунтування вибору набору заходів захисту системи.

Ефективність системи ЗІ залежить не тільки застосовуваними продуктами та методами, обов'язковою її умовою є також регулярний аудит системи на наявність уразливостей та моніторинг трафіку з метою виявлення потенційних загроз та формування рекомендацій для їх усунення.

Перелічені кошти повинні функціонувати, взаємодіючи з персоналом служби безпеки КІС, але створюють значні проблеми щодо аналізу та оперативного реагування на різні позаштатні ситуації з боку адміністратора безпеки. Відповідно, можна з упевненістю говорити про необхідність автоматизації процесу реагування на інформаційні загрози, що виникають. Тому перед розробниками стоїть завдання розробки та формалізації моделей прийняття рішень про класифікацію інформаційних загроз за рівнем їхньої активності та небезпеки для системи та про реалізацію протидії цим загрозам.

У роботі [16] розглядаються багатокритеріальна модель оцінки безпеки та

метод вибору міжмережевих екранів з використанням методу нечітких множин, синтез підсистем аналізу безпеки та виявлення загроз, а також метод вирішення гри для боротьби з інформаційними загрозами.

Робота [18, 39] присвячена проблемам адаптивного управління ЗІ безпекою у сфері захисту від несанкціонованого доступу. У цих роботах розглянуті розробки підсистем управління ЗІ, які реалізують парадигму адаптивного управління та використовують неявну користувальницьку модель об'єкта управління в головному циклі. Також розглянуто метод, що дозволяє на етапі проектування визначити раціональний склад та структуру системи захисту інформації, що ґрунтується на методі мінімаксу, із застосуванням показника досяжності характеристик «еталонної» системи. Також розглядається спосіб зміни структур та модифікацій системи ЗІ під час роботи, в якому використовується критерій максимального збільшення показника безпеки при обмеженнях вартості.

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

2.2 Методи аналізу інформації щодо ідентифікації атак

Методи аналізу інформації, ідентифікації атак та 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 систем [24] та метод нейронної мережі [17].

Статистичний метод заснований на статистичному устрої, який адаптується до поведінки відповідної особи. До кожного інформаційного суб'єкта формується його профіль у межах інформаційної системи, далі проводиться аналіз наявності відхилень (шляхом порівняння з еталонним) і за виявленні таких фіксується

наявність несанкціонованої інформаційної діяльності. Перевагою даного методу є універсальність статистичних методів та відсутність необхідності знання про можливі атаки для проведення аналізу. При цьому складністю є невизначеність при заданні граничних характеристик параметрів, що відстежуються, що викликає труднощі для адекватної ідентифікації діяльності, що виробляється як аномальної. Такі методи виявляються непридатними реагування на невідомі раніше атаки.

Набір правил, що охоплюють знання експерта, є експертною системою. Таким чином, всі знання про інформаційні атаки подаються у вигляді правил, які, у свою чергу, записуються у вигляді порядку (послідовності) дій, які застосовуються за наявності або реалізації інформаційної загрози. Експертна база даних така Система повинна містити знання (сценарії) всіх або більшої частини відомих інформаційних загроз та видів атак, крім того, необхідне постійне її оновлення. Перевагою даного методу є дуже мала кількість помилкових 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 недоліки, статистичний підхід та аналіз інформаційного простору на основі правил використовується в більшості сучасних методів виявлення атак. Однак, кількість кількісно і якісно числа атак і їх видів призводить до того, що навіть при постійному оновленні бази даних експертної системи, така система не гарантує покриття всього діапазону атак.

Нейросетевой підхід, на відміну експертних систем, дозволяє проводити аналітичну роботу й визначити відповідність існуючих показників роботи системи та тих, що мережа навчена розпізнавати, оцінивши наявність чи відсутність потенційної небезпеки. Нейронні мережі проходять навчання ідентифікації об'єктів предметної області на попередньо сформованій вибірці, у процесі якого відбувається налаштування нейромережі задля досягнення задовільних результатів розпізнавання. У міру роботи проведення аналізу, нейромережа набирає досвіду, що робить результат розпізнавання коректнішим. При цьому нейромережа здатна

за результатами вивчення характеристик ідентифікувати атаки та загрози, відмінні від тих, що зустрічалися раніше.

Технологія адаптивного профілювання, розроблена з урахуванням досліджень імунної системи людини, використовується на вирішення проблеми захисту найважливіших інформаційних ресурсів. Така система показує високі результати точно визначення мережових атак чи несанкціонованих дій [37]. Технологія адаптивного профілювання працює подібно до імунної системи людини, попередньо вивчаючи нормальну поведінку додатків (спостерігаючи процес виконання коду в штатному режимі в програмах, що нормально працюють). Далі навчена система аналізує працюючу ІС та будь-які відхилення в конфігурації, помилки ПЗ та інші вразливості ідентифікуються даною технологією, і відбувається їхнє блокування (припинення їх роботи за допомогою блокування системних викликів). Така технологія виявляється ефективною для захисту серверних програм.

Продовжуючи процес навчання, система вчиться розпізнавати допустимі зміни додатків, що зрештою призводить до мінімізації хибних спрацьовувань. Ця технологія виявляється таким чином ефективною для захисту як від відомих раніше, так і від невідомих атак, і навіть у разі зашифрованої інформації.

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

За словами автора [20], методологічні та технологічні основи створення інтелектуальних засобів запобігання комп'ютерним атакам у КІС все ще знаходяться на ранній стадії розробки. На сучасному етапі інформаційного розвитку стоїть гостра необхідність у розробці комплексних рішень щодо реалізації засобів оцінки та протидії потенційно небезпечних подій, що відбуваються в інформаційній мережі, а також з управління засобами та мережевим обладнанням.

2.3 Метод оцінки захищеності інформаційної системи

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

Однією з концептуальних завдань створення систем ЗІ є вибір критеріїв (формалізованих заходів оцінки) визначення рівня захищеності системи. Зазвичай під формалізованими заходами мають на увазі спосіб оцінки "сили" певної характеристики, або засновані на застосуванні цифрової шкали оцінки реальних характеристик системи [33]. Ідея оцінки рівня захищеності за допомогою низки критеріїв була вперше запропонована в Помаранчевій книзі для застосування до СКБД та операційних систем.

Якщо шкала критеріїв оцінки ступеня захищеності ІС сформована, порівняння різних систем захисту здійснюється шляхом простого порівняння відповідних числових показників для кожної із систем. Такі шкали критеріїв сформовані для оцінки криптографічних механізмів та 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 та 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, що враховують такі параметри, як умови використання ІС, кваліфікація користувачів, технології обробки та зберігання даних, що застосовуються, та ін. Складним питанням є

фактично, не тільки категоризація, а й повний перелік можливих факторів, які можуть бути причетні до реалізації можливих загроз у системі ЗІ.

Найбільш ефективним для практичної оцінки рівня безпеки системи ЗІ є використання критеріїв не апостериорних, а апіорних критеріїв. Ці критерії можуть бути надані шляхом порівняння системи та її стану із набором еталонних профілів для служб захисту. Профілі, які забезпечують певний рівень безпеки, необхідний за певних умов, використовуються як еталонні профілі. Таким чином ми можемо сказати, що дві системи мають однаковий рівень безпеки, якщо вони реалізують один і той же набір захисних механізмів, які мають однакову «силу». Отже, система 1 має вищий рівень безпеки, якщо «сила» хоча одного з реалізованих механізмів захисту вище, ніж у механізмів системи 2, або якщо система 1 реалізувала механізми захисту, відсутні в системі 2 [33].

У роботі [11] автором було запропоновано наступну формулу, за допомогою якої може бути визначений інтегрований показник безпеки для ІС:

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

де K – показник цілісності обліку можливих стратегій атаки;

R - Показник ефективності застосування оборонних стратегій, конструктивно закладених у СЗІ в тимчасовому інтервалі $[0, T]$.

У вищезазначеній роботі на підставі формули 2.1 розглянуто різні варіанти формування функції Φ для різних інформаційних середовищ та ситуацій. Проте, слід зазначити, що у роботі не розглядається питання реального визначення значення показників K і R . При цьому очевидно, що визначення цих показників є нетривіальним завданням. Частина необхідної інформації, очевидно, може бути визначена з окремих ймовірностей реалізації, розрахованих для різних загроз.

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

Останнім часом підходи до аналізу ризиків, де ризики органічно пов'язані з безпекою, тобто. потім рівень безпеки системи можна визначити, виходячи з аналізу можливих ризиків і навпаки.

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

- суттєва зміна у структурі інформаційної системи або її оновлення;
- зміна технологій побудови корпоративної системи;
- реалізація нових/додаткових підключень у компанії;
- реалізація підключення до глобальних мереж, яке раніше не було доступним;
- фундаментальні зміни у стратегії та тактиці ведення бізнесу в компанії;
- планова чи позапланова перевірка ефективності СЗІ.

Відповідно до вищевказаної роботи управління ризиками складається з наступних етапів.

У цих роботах пропонуються наступні етапи управління ризиками:

- оцінка можливих втрат під час реалізації ризиків;
- аналіз можливих (потенційних загроз) у даній інформаційній середовищі;
- аналіз уразливостей інформаційної системи;
- добір заходів та засобів захисту, що забезпечують скорочення ризику до прийняттого рівня за заданих цінових обмежень.

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

- формування політики ІБ та внесення до неї змін;
- формування та коригування регламентів роботи, обслуговування систем та у посадових інструкціях;

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

Відповідно до роботи [23], при проведенні оцінки ризиків інформаційної системи мають бути враховані такі фактори, як:

- цінність інформаційних ресурсів, що захищаються;
- оцінка величини значимості потенційних загроз та наявних уразливостей;
- ефективність розроблених раніше (існуючих) та запланованих засобів захисту інформації.

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

У міжнародному стандарті ISO/МЕК 15408 [4] «Загальні критерії оцінки безпеки ІТ» чітко структуровані та сформульовані вимоги щодо інформаційної безпеки для різних класів інформаційних систем. Однак цей документ не містить методології оцінки цих критеріїв.

Аналіз різних стандартів, прийнятих у сфері управління ризиками інформаційної безпеки (як іноземних, і вітчизняних), показує, що ці стандарти не містять деяких важливих деталей методології оцінки ризиків; для їхнього успішного застосування на практиці їх необхідно вказати; потрібні також додаткові методи оцінки, що враховують суттєві якісні та кількісні показники.

Важливість та актуальність формування науково-методологічної основи проблеми оцінки захищеності інформації наголошується у роботі [7]

Процес вирішення проблеми забезпечення заданого рівня захищеності можна розбити на два завдання, які мають бути вирішені послідовно:

- оцінка у кількісному вираженні рівня захищеності інформації у системі;
- аналіз даних та прийняття рішень щодо необхідності налаштування параметрів та властивостей системи захисту для підтримки необхідного рівня безпеки.

Очевидно, що для визначення кількісних показників критеріїв рівня безпеки необхідно ухвалити рішення про необхідність коригування складу властивостей СЗІ, крім того, необхідно стежити за динамікою змін у часі індикатори рівня безпеки, що ґрунтуються на змінах зовнішніх та внутрішніх умов ІВ.

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

Таким чином, можна сказати, що створення та розвиток інтелектуальних систем захисту є серйозною науковою проблемою, що вимагає розробки низки методів і методологій, науково обґрунтованих і застосовних у рамках створення теорії інтелектуальна безпека.

Як показує проведений аналіз, роботи з проблем створення нових засобів захисту різного характеру, стали значним досягненням у теорії захисту і є базисом розробки нових способів створення комплексних систем захисту.

Для побудови систем інформаційної безпеки застосовуються переважно два підходи: продуктний і проектний. Продуктний підхід відштовхується від вибору коштів Зі і вже на підставі реалізованих цим набором функцій виробляється політика безпеки. Проектний підхід передбачає спочатку формування безпекової політики, а вже на підставі неї – вибір відповідних засобів ЗІ.

3 МОДЕЛЬ ОЦІНКИ РІВНЯ ІНФОРМАЦІЙНИХ РИЗИКІВ У СЕГМЕНТІ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

3.1 Огляд методологійної бази дослідження інформаційних ризиків

Наукова література, національні та міжнародні стандарти приділяють значну увагу проблемі управління захистом інформації, що пов'язано із широким використанням інформації у діяльності сучасних корпорацій.

Аналіз існуючих стандартів у сфері управління інформаційної безпеки [18] показує, що метою стандартів є формулювання загальних концепцій, і навіть етапів управління. Проте стандарти не визначають конкретних підходів до процесів управління безпекою систем; вони встановлюють функціональні вимоги до захисних засобів, але не представляють методи порівняльного аналізу різних комплексів захисних засобів для вибору оптимального варіанта системи ЗІ.

Вчені Бернстайн П., Бланк І.А., Вітлінський В.В., Луман Н., Марковіц Г., Найт Ф.Х., Самуельсон П. та інші розробили загальні принципи та інструментарій управління економічними ризиками. Математичні методи та інструментарій економіко-математичного моделювання представлені у роботах Клейнера Г.Б., Кульбі В.В., Матвійчука О.В. [44], Сігала А.В. та інших спеціалістів. Статистичні методи моделювання можуть використовуватись для вивчення інформаційних ризиків у поєднанні з неформальними методами досліджень [24]. Управління інформаційними ризиками в умовах 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". Липасев В.В. вкладає в поняття "інформаційний ризик" наступного змісту: це потенційна подія, яка руйнує несанкціоновану інформацію, спотворює інформацію, конфіденційність чи доступність [18].

Проблеми оцінювання якості інформації, а також надійності апаратних та програмних засобів інформаційних систем розглядали у своїх роботах Байхельт

Ф., Зегжда П.Д., Стенг Д.І., Франкен П. та ін. Стенг Д.І. додатково обмежує поняття інформаційного ризику [37] та враховує лише загрози інформаційної безпеки у комп'ютерних системах. Прихильники такого підходу до визначення «інформаційний ризик» зазвичай є експертами в галузі ЗІ.

Інша група фахівців під інформаційним ризиком розуміє можливості отримання збитків, недоотримання прибутку та інші негативні наслідки для компанії. Прикладом такого підходу є таке визначення М. Мура: "Інформаційні ризики – це небезпека виникнення збитків чи шкоди внаслідок застосування компанією інформаційних технологій. Іншими словами, інформаційні ризики пов'язані зі створенням, передачею, зберіганням та використанням інформації за допомогою електронних носіїв та 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 внаслідок шпигунської або диверсійної діяльності тощо.

Автори багатьох робіт, зокрема М. Мур [23] та Дж. Джонс [47], для докладного аналізу джерел ризику вперше пропонують створення своєї моделі. Залежно від мети дослідження та джерел ризику вибирається метод моделювання та рівень деталізації об'єктів та процесів.

Одним із розділів математики, що знайшов широке застосування в моделюванні складних систем, якою є КІС, є 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 за підмножинами за умов недостатності інформації та випадковості процесів. При дослідженні інформаційних ризиків таке завдання стоїть, наприклад, під час вирішення завдання віднесення довільного ризику до багатьох значимих ризиків у конкретній корпоративній системі. Методи нечітких множин та нечіткої логіки дозволяють використовувати як кількісні, так і якісні

оцінки, отримувати інтегральні показники. Вони найбільше підходять до роботи з експертними оцінками.

У роботі пропонується розробити механізм отримання оцінок ризику, який би замінив метод приблизної табличної 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) корпорації, які можуть стати об'єктами інформаційних ризиків та загроз цим ресурсам;

- розробка та застосування моделей кількісного аналізу та оцінювання факторів (уразливість, дієвість засобів захисту тощо) та загального рівня інформаційних ризиків із 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, що ґрунтуються на трьох факторах: загроза, вразливість, можливі збитки [48].

Виділяють чотири основні етапи аналізу інформаційних ризиків:

- Ідентифікація компонентів: інформаційних ресурсів та можливих загроз;
- Оцінка частоти подій можливих загроз через схильність до 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 за умови 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 і характеристики відносин між ними допускається не тільки кількісне оцінювання, а й лінгвістичне.

Пропонується використовувати інтелектуальні методи в системах інтелектуальної підтримки для оперативного управління інформаційною безпекою у КІС: нечітке виведення чисельної оцінки ймовірності інформаційних атак; організовано класифікацію інформації про події в базі знань; модель нейтралізації загроз; ухвалити рішення про вибір оптимального варіанта реагування на події у системі інформаційної безпеки.

Остаточний вибір складу комплексу засобів захисту системи ЗІ може бути зроблено ітеративно, крок за кроком наближаючись до раціонального складу, який відповідав би вимогам прийнятного рівня витрат на реалізацію системи.

3.2 Постановка задач оцінювання ризику інформаційної системи

I. Ідентифікація компонентів:

- Інформаційні ресурси (активи) компанії, які можуть бути
- Можливі небезпеки (комбінації небезпек) активу. Для управління ризиками необхідно ідентифікувати можливі небезпеки, які загрожують КІС. Такими можуть бути, наприклад, стихійне лихо, відключення електроживлення, атака злоумисника з різними ступенями складності наслідків.

II. Оцінка частоти подій можливих втрат внаслідок дії ризику:

- Можливий рівень сили (Threatcapability), з якою агенти загрози діятимуть актив. Допускається, що частина популяції агентів загрози є більш

здатною до впливу актив, інша - менш здатної [44]. Проводиться експертне оцінювання рівня загроз за набором показників, що 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 (Controlstrength) протягом відведеного часового інтервалу. Взявши за основу орієнтацію на середню здатність агентів загрози, приймається базовий рівень ефективності контролю [44].

Для оцінювання рівня захисту використовується наступна 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 [44] та оцінюється за шкалою:

V_VH - "дуже високий"; V_H - "високий";

V_M - "середній"; V_L - "низький";

V_VL - "дуже низький".

Приклад бази знань з оцінки рівня чутливості наведено у табл. 3.1.

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

Таблиця 3.1 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 чи випадково, діями чи бездіяльністю здатні завдати збитків корпоративній системі [16].

Оцінка частоти реалізації факторів ризику може проводитись 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 годинного інтервалу, з якою агент загрози завдає шкоди активу, розглядається як результат впливу факторів частоти виникнення загрози та вразливості [16].

Використовуються такі 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 основи знань для оцінювання рівня частоти виникнення подій втрат наводиться у табл. 3.2.

Таблиця 3.2 Оцінювання рівня частоти подій втрат внаслідок інформаційних ризиків

		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				

Оцінювання величини можливих збитків:

– визначення можливої дії кожного агента погрози інформаційного активу;

– оцінювання величини кожної з можливих форм збитків, пов'язаних із 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 у відповідних грошових одиницях.

Визначення величини можливих збитків може проводитись щодо бюджету корпоративної системи з урахуванням вартості інформаційних активів, вартості репутації підприємства тощо.

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

C - "критичний"; H - "високий";

M – "середній";

L – "низький" рівень інформаційних ризиків.

Приклад бази знань, яка можна використовуватиме оцінювання загального рівня інформаційного ризику, наводиться у табл. 3.3.

Таблиця 3.3 Оцінювання загального рівня

		Рівень інформаційних ризиків				
Величини можливих збитків	PL_VH	H	H	3	3	3
	PL_H	M	H	H	3	3
	PL_Sg	M	M	H	H	3
	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
		Дієвість засобів контролю				

3.3 Моделювання аналізу факторів інформаційного ризику на основі лінгвістичного підходу

Пропонується застосувати лінгвістичний підхід до моделювання аналізу факторів інформаційного ризику [44]. Такий підхід забезпечує кількісні описи окремих елементів моделі за умови нечіткої інформації про значення критерію оцінки фактора ризику, їх наслідків в умовах дії агента загрози, альтернативні шляхи уникнення негативного впливу інформаційних ризиків. Відповідно до лінгвістичного підходу, як значення критеріїв і характеристики відносин між ними допускається не тільки кількісне оцінювання, а й пропозиція природною мовою. На підставі розрахованих значень груп показників рівня частоти подій втрат інформаційних активів та величини можливих збитків внаслідок інформаційних ризиків проводиться оцінювання загального рівня інформаційних ризиків у KIC:

$$\Delta = f(\gamma, P) \quad (3.1)$$

де γ - оцінка рівня частоти подій втрат інформаційних активів;

P – попередньо оцінена величина можливих збитків.

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

$$LEF = \{LEF_VH, LEF_H, LEF_M, LEF_L, LEF_VL\} \quad (3.2)$$

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 KIC, записується у вигляді:

$$LD = \{PL_VH, PL_H, PL_Sg, PL_M, PL_L, PL_VL\} \quad (3.3)$$

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 V рекомендовано скористатися шкалою з чотирьох якісних термів: C – "критичний";

H - "високий";

M – "середній";

L – "низький" рівень ризику.

Терм-множина вихідної змінної V представляється у вигляді:

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

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

Використовуючи [40,42], сформований набір вирішальних правил, які реалізують співвідношення (1). У табл. 3.4 наведено такий набір.

Таблиця 3.4 База знань для визначення рівня інформаційних ризиків

Номер вихідної комбінації	Узагальнені значення груп показників		Значимість m_{ij}	Вихідна змінна Δ
	Рівень частоти виникнення можливих втрат	Величина можливих збитків Р		
11	PL_VH	LEF_M	m_{11}	С
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}	Н
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}	
32	PL_Sg	LEF_VL	m_{32}	
33	PL_Sg	LEF_L	m_{33}	
34	PL_M	LEF_L	m_{34}	М
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}	

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

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

$$\begin{aligned} \mu M(, P) = & m31[\mu LEF_VL(\gamma) * \mu PL_H(P)]Vm32[\mu LEF_VL(\gamma) * \mu PL_Sg(P)]V \\ & Vm33[\mu LEF_L(\gamma) * \mu PL_Sg(P)]Vm34[\mu LEF_L(\gamma) * \mu PL_M(P)]V \\ & Vm35[\mu LEF_M(\gamma) * \mu PL_M(P)]Vm36[\mu LEF_M(\gamma) * \mu PL_L(P)]V \\ & Vm37[\mu LEF_H(\gamma) * \mu PL_L(P)]Vm38[\mu LEF_H(\gamma) * \mu PL_VL(P)]V \\ & Vm39[\mu LEF_VH(\gamma) * \mu PL_VL(P)] \end{aligned} \quad (3.5)$$

де $\mu^M(\gamma, P)$ – функція належності вихідний змінної Λ значення М з нечіткого терму (3.4);

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

$\mu^{lefj}(\gamma)$ – функція приналежності параметра γ нечіткому терму $lefj$ із термножини LEF (3.2);

$\mu^{ldi}(P)$ – функція приналежності параметра P до нечіткого терму ldi з термножини LD (3.3).

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

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

Було побудовано дзвін подібні функції належності термів вихідної змінної В до множини (4) терму, параметри яких представлені в табл. 3.5:

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

де T – довільний нечіткий терм; a – коефіцієнт концентрації; b – коефіцієнт крутості;

c – координата максимуму функції, $\mu^T(c) = 1$.

Таблиця 3.5 Параметри функцій приналежності термів до терм-множини IR

Назва терма	Функція приладдя	Параметри		
		Коефіцієнт максимуму з	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 уявлення функції власності вихідний змінної, основи логічного висновку представлені на рис. 3.1 та 3.2 відповідно

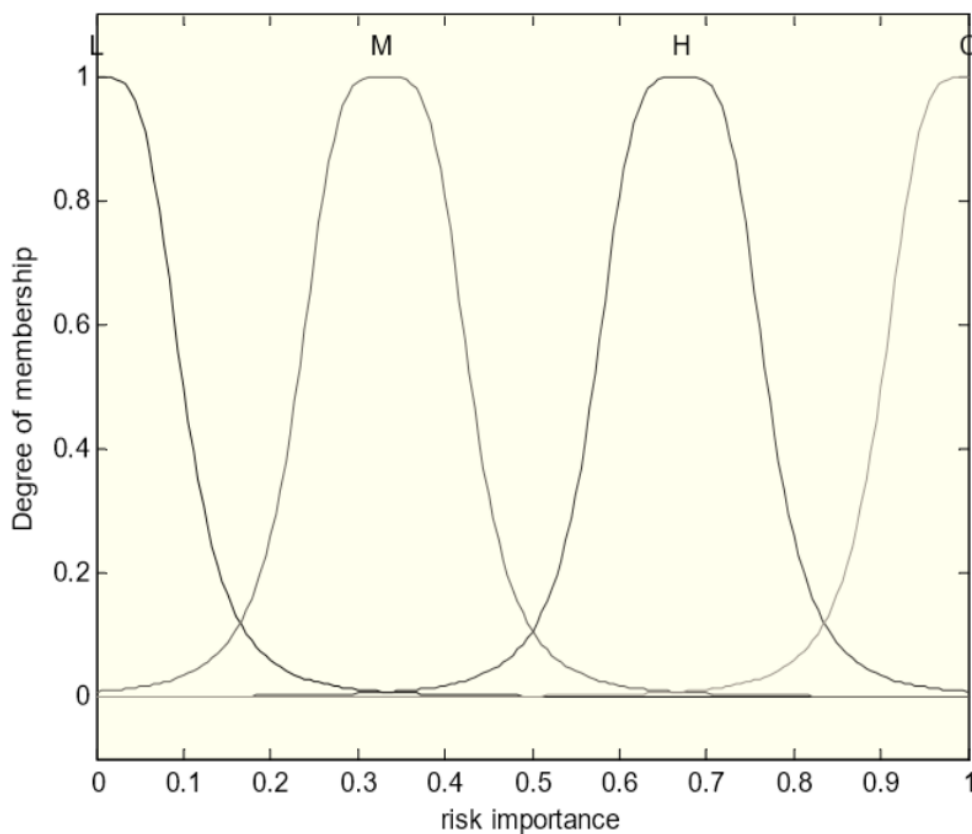


Рисунок 3.1 - Графіки функцій належності показника рівня інформаційних ризиків у КІС

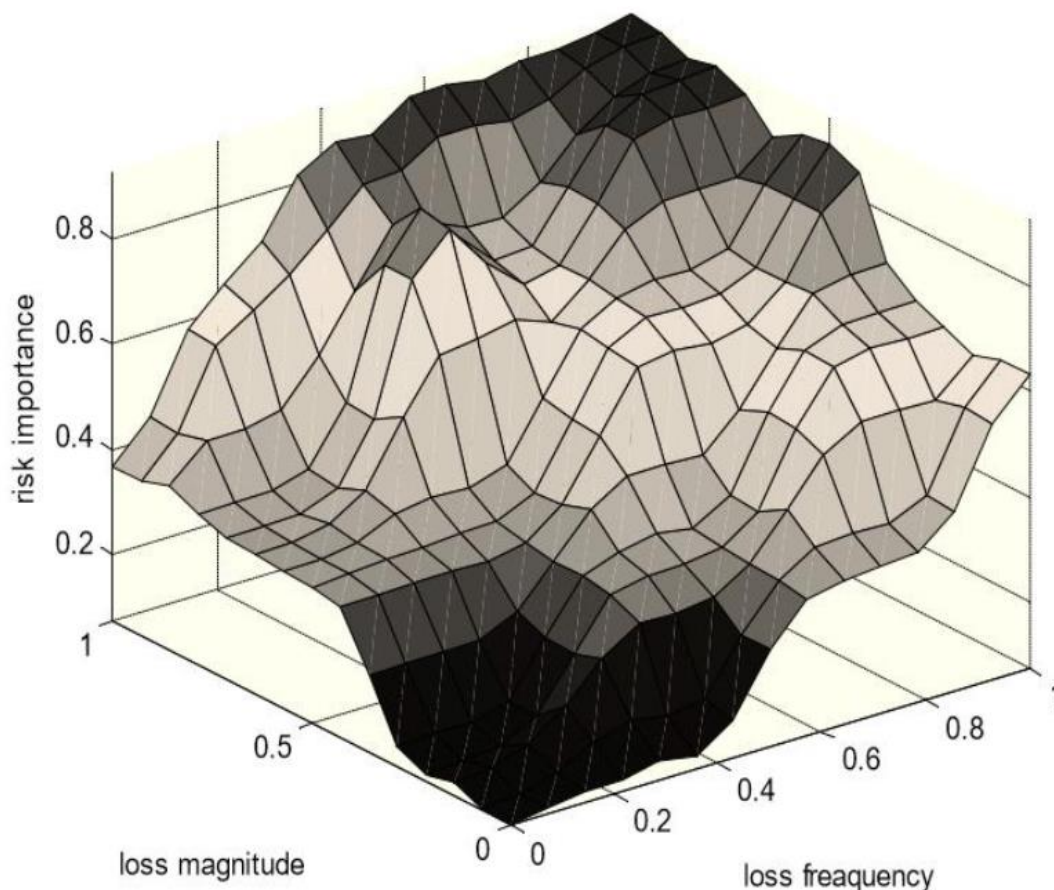


Рисунок 3.2 - Графічне представлення системи нечіткого висновку показника рівня інформаційних ризиків

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

Як очевидно з табл. 3.6, на Підприємстві 2, Підприємстві 3 та Підприємстві 4, знайдений рівень інформаційних ризиків відповідає оцінці "високий", на Підприємстві 1 - "середній".

За результатами оцінки факторів інформаційних ризиків було прийнято рішення щодо методів зниження рівня інформаційних ризиків на підприємствах. Наприклад, на Підприємстві 3 необхідно вжити додаткових заходів щодо підвищення рівня дієвості засобів захисту, оскільки високий рівень уразливості був викликаний саме недоліками роботи цих ресурсів та їх невідповідності до високого рівня загроз інформаційній безпеці підприємства.

Таблиця 3.6 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

Можна дійти висновку, що подібна модель оцінки загального рівня ризику є гнучкою та адаптивною і може бути налаштована відповідно до отриманої бази знань.

Категорія "інформаційний ризик" має розглядатися з позицій керівника підприємства, який бажає керувати всіма ризиками, пов'язаними з використанням управлінської інформації у бізнесі. Пропонується пов'язати ризики, пов'язані з інформацією, не лише з порушеннями інформаційної безпеки, але й із втратою якості бізнес-процесів. Аналіз інформаційних ризиків є основою побудови підсистеми управління інформаційної безпекою підприємства.

Під час аналізу та оцінки рівня інформаційних ризиків слід дотримуватись наступних кроків:

- ідентифікація інформаційних ресурсів (активів) компанії, які можуть бути об'єктом ризику, можливих загроз активу та визначення рівня загроз безпеці КІС підприємства;
- оцінювання рівня дієвості засобів контролю безпеки корпоративної системи;
- оцінювання вразливості корпоративної системи, що розглядається як результат впливу факторів можливого рівня сили загрози та рівня дієвості засобів контролю;

- оцінювання частоти подій втрат від інформаційних ризиків як результату впливу факторів частоти виникнення загрози та вразливості корпоративної системи;
- оцінювання величини можливих збитків від інформаційних ризиків у КІС;
- оцінювання рівня інформаційних ризиків у КІС як результуючої двох факторів: частоти подій втрат та величини можливих втрат від інформаційних ризиків.

Побудовано модель оцінки загального рівня інформаційних ризиків у сегменті КІС із застосуванням лінгвістичного підходу, що забезпечує кількісні описи окремих елементів моделі за умов нечіткої інформації про значення критеріїв оцінки факторів (факторів) ризику. Це дає можливість виділити значущі фактори ризику, їх наслідки в умовах дії агента загрози, і тим самим визначити альтернативні шляхи для уникнення негативного впливу ризику:

- заміна чи модифікація засобів контролю безпеки;
- запровадження механізмів захисту відповідно до можливого рівня загроз певних класів порушників інформаційної безпеки;
- реалізація режиму функціональної замкнутості, який виключав би використання апаратного та програмного забезпечення, не має відповідного паспорта безпеки тощо.

Результатом представленої технології та інструментарію оцінки рівня інформаційних ризиків у сегменті КІС є лінгвістичний опис та можливість аналізу та оцінки факторів інформаційних ризиків, а саме, рівня частоти подій загроз та вразливості КІС. Розроблений концептуальний підхід дозволяє нам створити модель не лише з можливістю адаптації її до конкретної інформаційної системи, а й з урахуванням переоцінки ризику надалі. Подібна модель має властивості гнучкості та адаптивності, тонкого налаштування відповідно до отриманої бази знань.

Запропонована модель оцінки рівня інформаційних ризиків може бути покладена в основу розвитку підсистеми управління інформаційними ризиками як

на стадії проектування КІС підприємства, так і під час її експлуатації. Модель легко адаптується до виконання завдань управління інформаційними ризиками лише з іншими завданнями. При цьому не потрібно кардинально змінювати організаційну структуру корпорації, потрібно лише реорганізовувати її, максимально пристосовуючи вирішення завдань управління захистом інформації в КІС.

Незважаючи на вагомість здійснених напрацювань, залишається низка невирішених проблем, а саме:

- розвиток математичних моделей та відповідного інструментарію для зниження (факторів уразливості) або підвищення (факторів дієвості засобів захисту) впливу факторів на загальний рівень інформаційних ризиків;
- розробка положень щодо застосування механізмів керування окремими факторами інформаційних ризиків.

4 МОДЕЛЮВАННЯ РАЦІОНАЛЬНОГО МОДЕЛЬНОГО СКЛАДУ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

4.1 Побудова моделі системи захисту інформації

Під моделлю захисту інформації мається на увазі опис (представлений у формалізованому чи неформалізованому вигляді) використовуваного у ЗЗІ комплексу апаратних і програмних засобів і заходів захисту організаційного характеру [21]. Модель захисту є фундаментом розробки безпосередньо ЗЗІ.

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 у сучасних концепціях побудови СЗІ [39], можна дійти невтішного висновку, що з створення ефективної системи захисту інформації важливо під час розробки дотримуватися низки ключових принципів, а именно:

– комплексність та узгодженість – побудова системи захисту інформації передбачає застосування досить широкий спектр інструментів та методів захисту, при цьому важливо підтримувати цілісність системи та уникати "слабких місць" у взаємодії окремих компонентів системи;

– диференціація – кожен рівень захисту повинен розроблятися з урахуванням рівня важливості та критичності інформації та ймовірності потенційних загроз (оцінки потенційних атак);

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

Проаналізувавши можливі шляхи реалізації загроз (здійснення несанкціонованого доступу до інформаційного середовища) та ґрунтуючись на вищезазначених принципах організації системи інформаційної безпеки, запропоновано модель СЗІ, розроблену у вигляді тристоронньої схеми:

– межа: периметр об'єкта захисту: набір функціональних підсистем, до складу яких входить захист ІВ від зовнішніх загроз та руйнівних дій злоумисників;

– межа: периметр сегмента 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 та застосування гібридних атак, для ефективного захисту інформаційного середовища необхідне застосування багаторівневої, ешелонованої системи захисту інформації.

Схема запропонованого тристороннього захисту наведена на рис. 4.1.

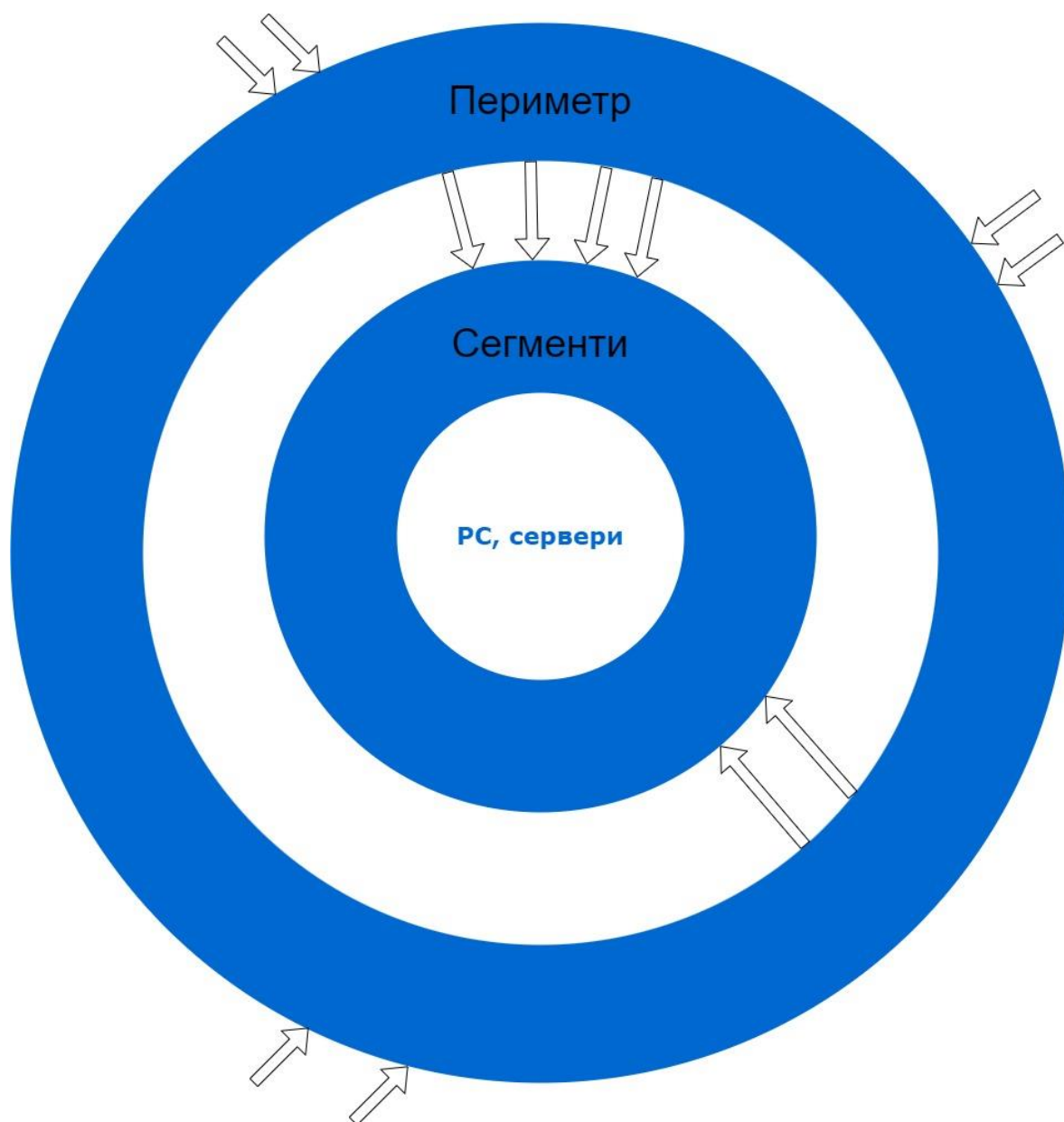


Рисунок 4.1 - Трикордонна модель СЗІ (стрілки вказують на зовнішні та внутрішні загрози)

Таким чином, розроблена модель СЗІ включатиме три компоненти:

- модель охорони периметра об'єкта захисту,
- модель безпеки мережевого сегмента
- модель захисту внутрішнього сегмента (ПК та робочий сервер).

Для кожного з розглянутих меж, залежно від ступеня критичності інформації, що обробляється в ньому, і підлягає захисту, модель буде включати в себе N морфологічних матриць (модель рівня N).

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

Таким чином, маючи впорядковану інформацію про потенційні загрози та доступні засоби реалізації захисту, ґрунтуючись на певних процедурах, проводиться багатокритеріальне порівняння альтернативних реалізацій засобів захисту. Результатом такого порівняння є виявлення серед наявного підмножини найкращого варіанта реалізації захисту інформаційного об'єкта.

4.2 Розробка моделей протидії загрозам інформації безпеки в умовах невизначеності

Щоб проаналізувати процес прийняття рішень щодо протидії загрозам, ми розглянемо кілька типових типів інформаційних атак: міжсегментну атаку, зовнішню атаку через точку бездротового доступу, зовнішню атаку через периметр через високошвидкісний канал доступу.

Модель протидії як зв'язкового графа (рис. 4.2), де U_n – це варіанти реагування, а V_n – варіанти результатів під час реалізації протидії загрозам. Функція реалізації, що відповідає даній матриці, представлена в табл. 4.1.

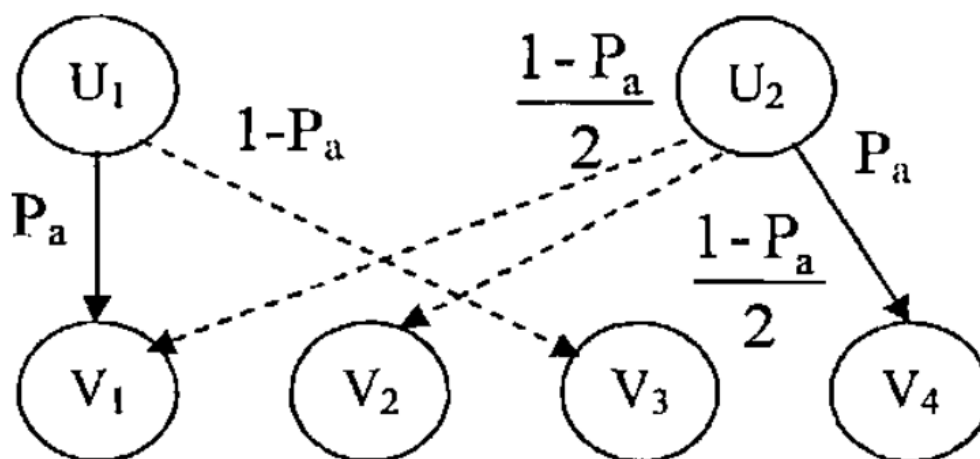


Рисунок 4.2 – Граф зв'язку варіантів реагування та наслідків

Таблиця 4.1 - Функція реалізації

U	Z					
	P(z ₁)	P(z ₁)	P(z ₁)	P(z ₁)	P(z ₁)	P(z ₁)
U ₁	C(V ₁)	З(V ₃)	C(V ₁)	З(V ₃)	C(V ₁)	З(V ₃)
U ₂	C(V ₁)	C(V ₁)	C(V ₂)	C(V ₂)	З(V ₄)	З(V ₄)

Наступні варіанти відповіді показані в таблиці нижче: U₁ завершує сеанс з атакуючим вузлом;

U₂ - відправка попередження користувачеві зменшення пріоритету користувача.

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

З (V₁) – немає пошкоджень;

З (V₂) - незначні збитки (збитки користувачеві); С (V₃) – середня шкода (збиток системі);

С (V₄) – максимальна шкода, нанесена системі в результаті здійснення атаки.

При виборі варіанта реагування U₁ з ймовірністю (1-P_a) буде отримано середні збитки, оскільки в якості атаки прийняті при стандартному режимі роботи

мережі ненавмисні шкідливі впливи від користувача або помилкове розпізнавання як атаки сигналів із сенсорів.

Реалізація варіанта реагування (керуючого впливу) U_2 може мати три різних варіанти результату. Якщо події, розпізнані як аномальні, дійсно є атакою, то з ймовірністю P_a буде реалізовано максимальну шкоду за відсутності блокування атакуючого впливу. У разі, якщо розпізнана аномальна подія спричинила помилкові дії користувача, то шкоди не буде (він дорівнює нулю). Якщо керуючий вплив буде реалізовано внаслідок помилкового розпізнавання сигналів як атаки і користувачеві буде відправлено попередження та знижено його пріоритет – буде завдано незначної шкоди користувачеві. В останніх двох варіантах ймовірності наслідків 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 було прийнято значення $3(V_1)=0$, $3(V_2)=0,1$, $(V_3)=0,5$, $(V_4)=1$.

Для реалізації зовнішнього вторгнення в даному варіанті атаки зловмиснику необхідний доступ до бездротового адаптера і необхідно, щоб він перебував у радіусі дії бездротової мережі. У на відміну від атаки за допомогою провідної лінії, маємо більш високий ступінь загрози та можливість нанесення максимальної шкоди.

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

Формується заздалегідь визначений (еталонний) мережевий профіль, який включає стандарти, що підтримуються, застосовні мережеві протоколи, використовувану політику трафіку і стан фізичних і канальних рівнів передачі даних, які постійно відстежуються:

- допустима кількість підключень до точки доступу;
- якість сигналу;
- кількість переданих прийнятих широкомовних пакетів;
- частота та кількість повторних передач пакетів;
- відсоткове співвідношення цілих та фрагментованих фреймів;
- параметри передачі даних (швидкість та її зміни);
- виникнення та частота помилок контрольної суми при передачі пакетів;
- використовуються для повідомлень автентифікації MAC-адреси;
- технології, що застосовуються при передачі даних, автентифікації та шифрування.

Для реалізації захисту інформації процедури реагування повинні бути сформовані таким чином, щоб максимально знижували можливі збитки як від реалізації вторгнення, так і від можливого збою взаємодії через точку доступу.

Модель протидії у графічному вигляді представлена на рис. 4.3, а відповідні даної моделі функції реалізації – у таблиці 4.2.

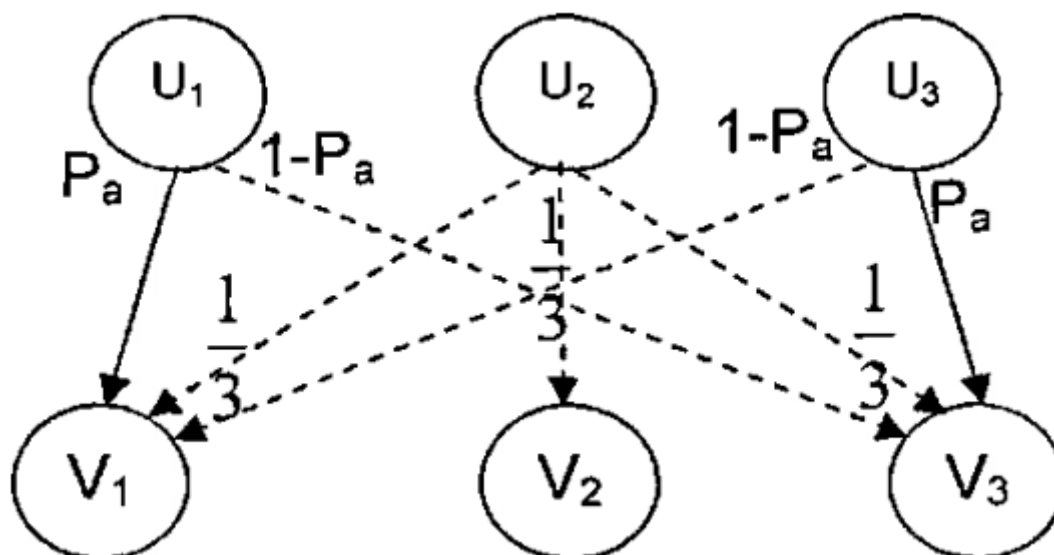


Рисунок 4.3 – Граф зв'язку варіантів реагування та наслідків

Таблиця 4.2 - 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 ₃)	C(V ₃)
U ₃	C(V ₁)	C(V ₁)	C(V ₁)	C(V ₁)	C(V ₁)	C(V ₁)	C(V ₃)	C(V ₃)	C(V ₃)	C(V ₃)	C(V ₃)	C(V ₃)

Маємо такі варіанти керуючих впливів (реагування системи):

U₁ - блокування точки доступу;

U₂ – здійснення DOS-атаки на станцію, що реалізує атаку; U₃ – відсутність реагування.

Розподілимо за величиною можливої шкоди можливі результати керуючого впливу:

C(V₁) – нульовий збиток; C(V₂) – середня шкода;

C(V₃) – максимальні збитки.

Якщо система реалізує реакцію (вплив) U₁, то з ймовірністю збитків P_a збитків системі не буде (канал повністю перекритий і дії зловмисника припинено). Ймовірність P_a, у разі, дорівнює ймовірності атаки. Якщо за реалізацію атаки були

помилково розпізнані сигнали сенсорів або відбулася помилка в діях користувача, то збитки при виборі впливу U_1 , що управляє, буде максимальним (блокування точки доступу відбулося безпідставно, стався збій в нормальній роботі системи). Імовірність $(1-P_a)$ такого результату відповідає ймовірності помилкової інтерпретації сигналів системою чи помилки користувача.

Якщо вибрано 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 вибраний у ситуації помилкового розпізнавання сигналів сенсорів як атаки, то збитки будуть нульовими – система захисту не втручається в роботу і продовжується робота в штатному режимі (ймовірність становитиме $(1-P_a)$ для цього результату).

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

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

при $P_a=0,3$: альтернатива U_3 : $J(U_{1,z})=0,699$; $J(U_{2,z})=0,36$; $J(U_{3,z})=0,3$;

при $P_a=0,4$: альтернатива U_2 : $J(U_{1,z})=0,6$; $J(U_{2,z})=0,3663$; $J(U_{3,z})=0,399$;

при $P_a=0,678$: альтернатива 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 $(V_1)=0$; $(V_2)=0,1$; $3(V_3)=1$.

Для цього варіанта загроз модель протидії проілюстрована на фіг. 4.4 функції реалізації, відповідні цієї моделі, наведені в додатку А.

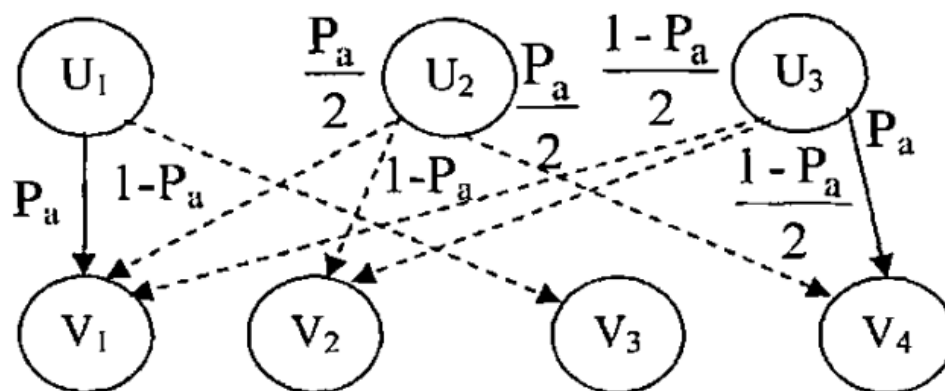


Рисунок 4.4 – Граф підключення варіантів відповіді та результатів

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

U_1 – блокування доступу користувачів до відповідної послуги мережі;

U_2 -Реконфігурація служби безпеки для блокування взаємодії з конкретною IP-адресою;

U_3 – надсилання оповіщення (попередження) відповідному користувачеві за його IP-адресою, надсилання інформації адміністратору про збільшення активності цього користувача.

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

$Z(V_1)$ – нульовий збиток;

$Z(V_2)$ - незначний урон (збиток, завданий тільки віддаленому користувачеві);

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

$Z(V_4)$ - максимальний урон (атака реалізована і система пошкоджено).

Якщо система вибирає варіант реагування U_1 , то з ймовірністю P_a , яка дорівнює ймовірності реалізації атаки, збиток інформаційної системи дорівнює нулю (тобто відсутня), так як система захисту припинила атаку.

Якщо ж здійснено цей керуючий вплив (U_1), але сталося помилкове спрацювання сенсорів або було зроблено помилку користувачем, то збитки будуть

середніми (безпідставно заблоковані системою безпеки пакети, що надходять за цим протоколом). Імовірність цього результату складе $(1-P_a)$.

Реалізація рішення U_2 може привести або печербудля віддаленого користувача (якщо аномальні події не були викликані реалізацією атаки) з ймовірністю $(1-P_a)$, або (якщо була реалізована атака) можливі два рівноймовірні $(P_a/2)$ за принципом Бернуллі результату.

Коли контрольна дія U_3 та атака здійснені, результатом буде максимальна шкода (реалізована атака не буде пригнічена системою захисту з ймовірністю P_a , рівної ймовірності атаки. У разі помилкового спрацьовування датчиків або помилка користувача, з рівною ймовірністю $(1-p_a)/2$ кінцевому користувачеві буде заподіяно незначну шкоду, інакше не буде жодної шкоди як системі, так і користувачеві.

За результатами чисельних розрахунків можна сказати, що мінімальне значення цільової функції досягається при виборі:

– при $P_a=0,05$: альтернативи U_3 : $J(U_1, z) = 0,4948$; $J(U_2, z) = 0,107$;
 $J(U_3, z) = 0,05948$;

– при $P_a=0,238$: альтернативи U_2 : $J(U_1, z) = 0,380$; $J(U_2, z) = 0,195$;
 $J(U_3, z) = 0,276$

– при $P_a=0,742$: альтернативи U_1 : $J(U_1, z) = 0,129$; $J(U_2, z) = 0,3968$;
 $J(U_3, z) = 0,7549$

Чисельні розрахунки зроблені для наступних чисельних значень:

$3(V_1) = 0$; $3(V_2) = 0,1$; $3(V_3) = 0,5$; $3(V_4) = 1$.

4.3 Розробка структури системи інтелектуальної підтримки прийняття рішень щодо оперативного управління 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 реалізацію інших функцій.

Оперативне управління є одним із ключових функцій у межах забезпечення захисту інформації, реалізація якої може забезпечити ефективне функціонування СЗІ.

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

Синтез структури СЗІ та параметрів системи управління для забезпечення захисту певних масивів інформації є одним із ключових завдань теорії управління. Залежно від наявної інформації про об'єкт управління, даних про середовищі, в якій функціонує система, а також про ступінь невизначеності даної інформації, структурна схема системи оперативного управління може різнитися. Невизначеність, що існує в системі, пов'язана з невідомими діями потенційних злоумисників.

Оперативне управління в умовах інформаційної невизначеності (недостатність даних про стан об'єкта або можливі загрози, що спричиняє високу невизначеність при прийнятті керуючих рішень) може бути ефективно організовано при реалізації ієрархічного принципу в структурі керуючої системи.

Важливу значущість у системах управління захистом інформації набувають процеси контролю та аналізу, оскільки така система не обмежується регулювальною функцією. Розподіл функціонального навантаження проводиться таким чином: процес регулювання покладається на керуючі модулі, а система підтримки прийняття рішень реалізує такі функції як аналіз, контроль, планування та прийняття рішень (тобто всі ті функції, які не належать 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 керуючими впливами, що виробляються, слабо формалізована;

– Існуюча інформація (що надходить від сенсорів чи інших систем) про стан контрольованого об'єкта у зв'язку з змінами середовища реальному часі може повною мірою відбивати стан об'єкта управління.

Усе це зумовлює необхідність створення багаторівневої системи управління зменшення ступеня невизначеності після прийняття рішень та підвищення надійності системи.

Щоб побудувати ієрархічну структуру, виберіть такі елементи керування:

– засоби управління - засіб та заходи безпеки;
– модулі управління, вбудовані в захисне обладнання або мережеве обладнання;

– система підтримки прийняття рішень щодо оперативного управління ЗІ,

Введемо позначення інформаційних потоків, що циркулюють у системі:

$U^{ЗВН}$ – зовнішні загрози

$U'^{ЗВН}$ – інформація про стан навколишнього середовища доступна

U – інформація про команду на виході ОУ, $U_{ум}$ – контрольна дія,

X - інформація про стан ОУ - контрольовані параметри,

X' – інформація про контрольовані параметри доступна в СППР ОУ. На рис. 4.4 показано ієрархічну структуру системи управління.

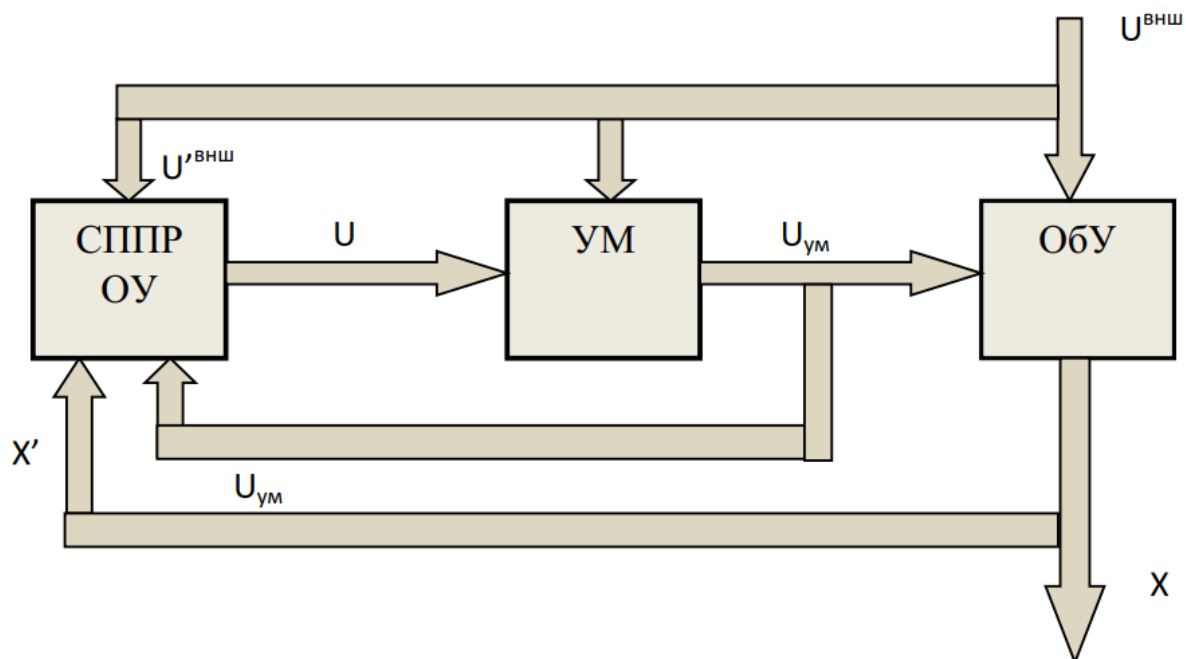


Рисунок 4.4 – Ієрархічна структура керуючої системи

Зниження інформаційної невизначеності є ключовим чинником підвищення якості рішень, прийнятих СППР ОУ. Прийняття рішень в СППР ОУ - це реалізація багатокрокового процесу за допомогою керуючих модулів, в процесі якого на підставі наявних даних про результати контролю рішень вибирається варіант реакції на одну або набір аномальних подій. Вхідні дані називаються у разі змінними вибору (оскільки впливають вибір керуючого рішення), які вплив можна як посилення позитивних і послаблення негативних реакцій у керуючої системі.

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

Крім безпосереднього управління, в СУЗІ забезпечується накопичення та аналіз інформації про процеси управління та результати реалізації різних рішень. Таким чином, знижується невизначеність при прийнятті рішень, підвищується їх

ефективність, так як система, що управляє, накопичує дані, що дозволяють точніше передбачити результат застосування того чи іншого управляючого впливу.

Розробка архітектурного рішення СППР ОУ відповідно до вищесказаного передбачає використання інтелектуальних інформаційних технологій, а саме:

- реалізація чисельної оцінки ймовірності того, що аномальна подія є атакою, виконується з використанням механізму нечіткого висновку;
- інформація та дані про систему, а також дані про події безпеки, які накопичуються системою в процесі роботи, упорядковуються в базі знань керуючої системи;
- система реалізує інтелектуальні алгоритми вибору рішень про реалізований керуючий вплив у разі виникнення аномальних подій у системі.

Завданням СППР ОУ 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 самої інформаційної системи.

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

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

На рис. 4.5 представлена пропонована архітектурна побудова СППР ОУ.

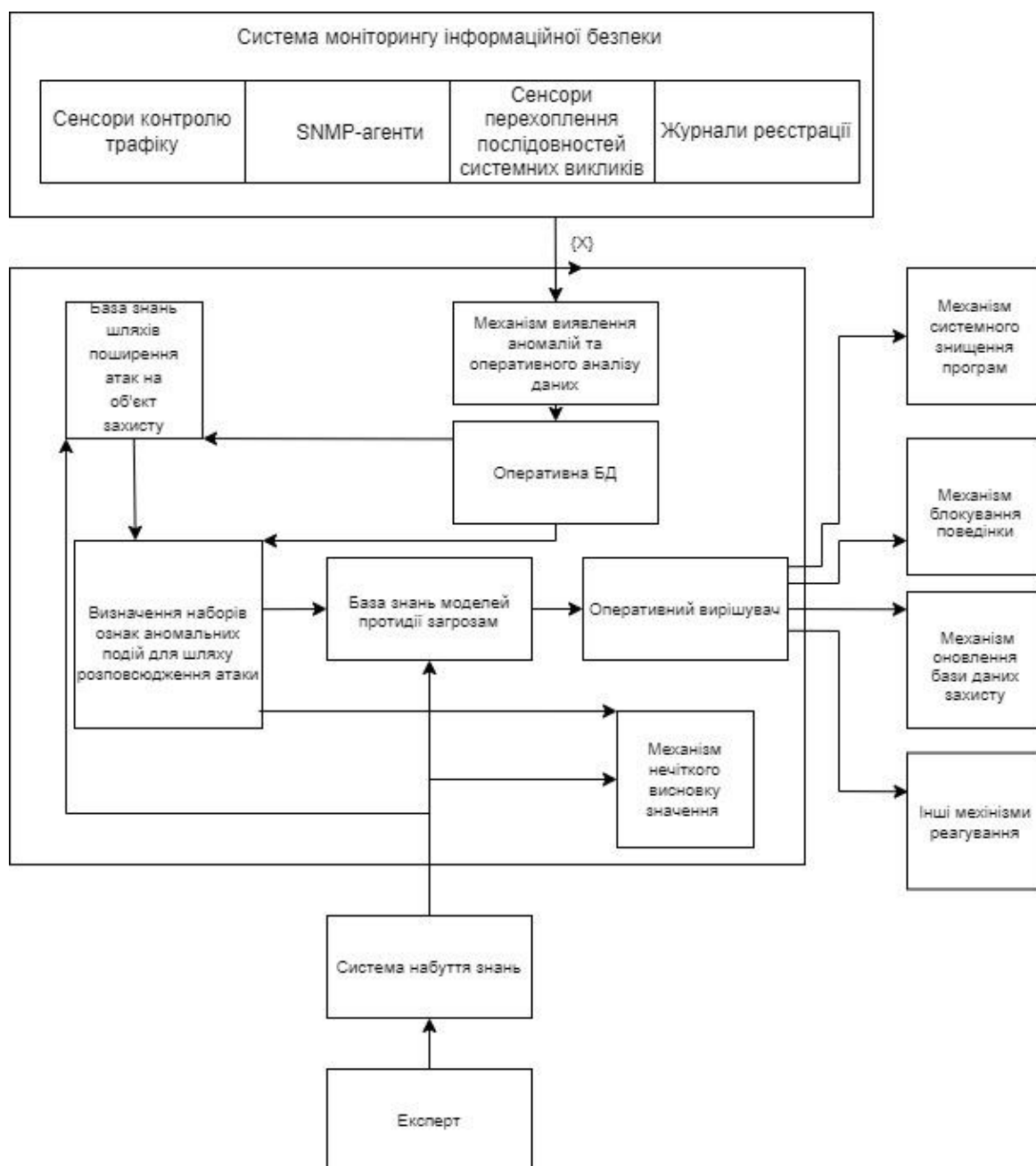


Рисунок 4.5 – Структура системи інтелектуальної підтримки прийняття рішень на контурі оперативного управління ЗІ

Для отримання даних застосовуються датчики, які у різних сегментах мережі (точки виходу глобальну мережу, окремі сегменти локальної мережі інформаційної системи, комутатори, маршрутизатори та інших.). Кожен датчик збирає інформацію про події безпеки, які відбуваються у відповідному вузлі, і передає їх для протоколювання у відповідних журналах. Також інформація від

датчиків може передаватися безпосередньо, а через додаткові програмні компоненти.

Аналізуючи відомості, що надходять 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 реєструватися атаки, але ті, які системі не відомі як зовнішні, так і внутрішні (наприклад, порушення користувачами допусків на доступ до інформації).

Проте слід зазначити, що не кожен випадок аномальних подій пов'язаний зі спробою реалізації атаки. Такі події можуть бути пов'язані, наприклад, з помилками користувачів, неправдивими спрацьовування датчиків і т.д. В результаті формування керуючого впливу, що відповідає атаці, може вивести систему зі штатного режиму роботи за відсутності загрози безпеці (хибна тривога).

Для вирішення цієї проблеми в запропонованій СППР ОУ керуючі рішення приймаються на підставі розрахунку ймовірності того, що подія, що розглядається, 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 кількісний вираз.

Реалізацію цього механізму у запропонованій архітектурі СППР ОУ здійснює модуль «Механізм нечіткого виведення ймовірності атаки». Реалізований за допомогою такого підходу механізм прийняття рішень дозволяє максимально ефективно використовувати досвід та напрацювання експертних знань та подолати властиві інформаційному середовищу проблеми неповноти та суперечливості інформації про її стан, тим самим скоротивши невизначеність при прийнятті рішень.

У системі може бути використана різна кількість датчиків, сенсорів, підсистем виявлення та 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

$$S = (I_0, I_p, T), \quad (4.1)$$

де I_0 – системний ідентифікатор виявника,

I_p – ідентифікатор шляху атаки,

T – системний час.

Ефективність алгоритму при виборі керуючого рішення має критичне значення для ефективності роботи всієї системи захисту інформації. У запропонованому варіанті СППР ОУ варіант реагування формується в оперативному решителі, 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 у табличній формі зберігає функції реалізації для кожного типу шляху поширення атаки, вказаної експертом.

Розглянемо процеси накопичення знань автоматизованою системою СППРОУ. У цьому вся процесі можна назвати кілька ключових етапів.

На етапі концептуалізації реалізуються такі:

- вибір та формалізація наборів змінних, що описують (характеризують) події безпеки, що відбуваються в системі;
- експертне завдання функцій належності, визначення характеристик подій безпеки, які можна віднести до класу атак;
- формування експертом правил, що задають реакцію системи у відповідь виявлення потенційно небезпечних подій;
- формування бази даних про можливі джерела та шляхи
- поширення атак;

- формування структури інформаційних джерел про можливі загрози та атаки;

- аналіз варіантів реагування, альтернатив дій системи (U_i) та зіставлення цих варіантів з ймовірними наслідками (V_j) та потенційною шкодою від даних наслідків (C_j).

Усі знання задаються у основі знань у єдиної формалізованої формі уявлення.

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

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

Інформація в базі знань повинна доповнюватись та актуалізуватись в міру оновлення та 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 поставляється датчиками і сигнальними системами про атаки, що реалізуються, і далі ця інформація використовується для актуалізації бази знань і подальшого застосування при обчисленні «коефіцієнта впевненості» та вибору функції реалізації реакції системи з наявної бази знань моделей протидії загрозам. У ході такої актуалізації всі сигнали, що надходять від аналізаторів, прив'язуються до єдиної тимчасової осі та формується шлях поширення атаки. Таким чином, кожна послідовність подій безпеки, які можуть бути кваліфіковані як атака, має послідовність повідомлень від сигналізаторів, упорядковану за часом. Відповідно,

кожен шлях поширення атак обробляється індивідуально і вироблення впливу, що управляє, проводиться в залежності від цього шляху.

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

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

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

Математична модель ІС, побудована на основі теоретичного підходу до наборів, є інформаційною системою у вигляді набору елементів, розподілених за трьома рівнями конфіденційності та взаємопов'язаних певними відносинами. Такий підхід дозволяє визначити безліч джерел загроз для елементів кожного сегмента та шляхи можливих атак. Для кожного сегмента отримано оцінки кількості шляхів

поширення атак у кількісному вираженні. Щоб приймати обґрунтовані рішення щодо управління операціями, можна впровадити систему функціональних показників, що відповідають реалізації атаки на кожному шляху.

Вводиться поняття «коефіцієнта впевненості», що дозволяє ідентифікувати подію як атаку чи ймовірність атаки, з урахуванням механізму нечіткого логічного висновку. Використовуючи досвід кваліфікованих експертів, узагальнений у вигляді бази правил та сформульований на основі лінгвістичних змінних, що відповідають ненормальним подіям, ми маємо можливість кількісно оцінити ймовірність атаки.

У запропонованому методі прийняття рішень раціональним варіантом прийняття полягає в тому, що ймовірність результату не встановлюється на основі статистичних даних, а розраховується відповідно до ймовірності атаки з використанням механізму нечіткого висновку, що підвищує ступінь достовірності рішення про наявність факту атаки, а також знижує ризик прийняття нерациональних рішень.

Розроблена структура системи підтримки прийняття рішень для оперативного управління включає модулі, що базуються на інтелектуальних технологіях, що ефективно вирішують слабо формалізовані завдання вибору раціонального реагування на події безпеки.

ВИСНОВКИ

У магістерській роботі розглянуто методологічні засади управління інформаційною безпекою у сегменті КІС із використанням принципів системного аналізу та загальних прав на 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 та реагування самої системи захисту інформації.

На основі трирубіжної моделі захисту інформації проведено розрахунки, що дозволяють отримати в кількісному вираженні оцінку кількості шляхів розповсюдження атак до вузлів у сегментах. Введено показник

«Коефіцієнт впевненості», що дозволяє віднести сукупність аномальних подій інформаційної системи до атак з використанням механізму нечіткого логічного висновку.

Ієрархічна структура системи інтелектуальної підтримки ухвалення рішень для оперативного управління інформаційною безпекою, а також структура системи інтелектуальної підтримки ухвалення рішень в оперативному управлінні захистом інформації. Запропонована структура рішень, що приймаються системою, про вибір раціонального варіанта реагування на події безпеки за рахунок застосування інтелектуальних технологій для вирішення слабо формалізованих завдань класифікації подій безпеки в системі та вибору шляхів реагування ними. Таким чином, поставлені перед магістерською роботою завдання повністю виконані.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. ISO/IEC 27001 – Інформаційні технології. Методи забезпечення безпеки. Системи управління інформаційною безпекою».
2. ISO/IEC 27002 – Інформаційні технології. Методи забезпечення безпеки. Практичні правила управління інформаційною безпекою»
3. ISO/МЕК 15408-2002. Інформаційна технологія. Методи та засоби забезпечення безпеки. Критерії оцінки безпеки інформаційних технологій. - М.: Видавництво стандартів, 2002.
4. ISO/МЕК 51583-2000 «Захист інформації. Порядок створення автоматизованих систем у захищеному виконанні»
5. Астахова Л.В., Цимбол В.І. Застосування самонавчання систем кореляції подій інформаційної безпеки на основі нечіткої логіки при автоматизації систем менеджменту інформаційної безпеки // Вісник Південно-Уральського державного університету. Комп'ютерні технології, керування, радіоелектроніка, 2016.
6. Баженов Р.І. Інформаційна безпека та захист інформації. Практикум/Біробміджан, 2011. - 278 с.
7. Бікмаєва Є.В., Баженов Р.І. Про оптимальний вибір системи захисту інформації від несанкціонованого доступу // Apriori/ Серія: Природні та технічні науки, 2014. - №6. - С. 5.
8. Галицький О. В. Захист інформації у мережі: аналіз технологій та синтез рішень / О. В. Галицький, С. Д. Рябко, В. Ф. Шаньгін. - М.: ДМК Прес, 2004. - 616 с.
9. Гаскаров Д. В. Інтелектуальні інформаційні системи: підручник для вишів. - М.: Вищ. шк., 2003. - 431 с.
10. Груздєва Л.М., Абрамов К.Г., Монахов Ю.М. Експериментальне дослідження корпоративної мережі передачі з адаптивної системою захисту // Вісті вищих навчальних закладів. Приладобудування, 2012.

11.Добрушський С.UEBA, або поведінкова аналітика.Базова функція всіх систем безпеки майбутнього // Інформаційна безпека, 2017. - № 4. Електронний доступ:http://www.itsec.com/articles2/Inf_security/ueba--ilipovedencheskaya-analitika-bazova-funkciya-vsikh-sistem-bezpeki/ (дата звернення 22.10.2022)

12.Дудоров О.М. Можливі варіанти створення інтелектуальної системи виявлення несанкціонованої роботи програмного забезпечення. // Математичні структури та моделювання 2005, вип. 15, с. 116-124

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

14.Ліпаєв В. В. Функціональна безпека програмних засобів / В. В. Ліпаєв. - М.: СИНТЕГ, 2004. - 348 с.

15.Машкіна К. В., Васильєв В. І. Підхід до розробки інтелектуальної системи захисту інформації // Інформаційні технології, 2007. - № 6. - С. 2-6.

16.Машкіна І. В., Гузаїров М. Б. Інтелектуальна підтримка прийняття рішень щодо управління захистом інформації в критично важливих сегментах інформаційних систем // Інформаційні технології, 2009. - №7. - 32 с.

17.Машкіна І. В., Рахімов, Є. А. Система підтримки прийняття рішень щодо управління захистом інформації // Безпека інформаційних технологій, 2006. - №2. - С. 62-67.

18.Мур М. Управління інформаційними ризиками // Фінансовий директор, 2003. - С.64-69.

19.Нестеренко В. А. Статистичні методи виявлення порушень безпеки в мережі // Інформаційні процеси, 2006. - Т. 6. - Вип. 3. - С. 208-217.

20.Система захисту інформації від несанкціонованого доступу

21.«DallasLock7.0».Опис застосування Електронний доступ:http://www.confident.com/isc/assets/files/secured_area/dl70_doc.zip.Система захисту інформації від несанкціонованого доступу "Блокхост-мережа". Керівництво адміністратора. Електронний доступ:

http://www.gaz-is.com/products/windows/winbhnet.php?down=bhnet_adm.rar. (дата звернення 22.10.2022)

22. Система захисту інформації від несанкціонованого доступу

23. "Вартовий NT". Опис застосування. Електронний доступ: http://www.guardnt.com/download/dor/App-Guide_NT_2_5.pdf (дата звернення 22.10.2022)

24. Система виявлення вторгнень «ФОРПОСТ 1.1». Електронний доступ: http://www.id_46/lang_ua/ (дата звернення 22.10.2022)

25. Сканер безпеки SecPointPenetrator. Електронний доступ: <http://ftp.technoserv.com/off-line/it/products/secur/secpoint/secpoint.pdf> (дата звернення 22.10.2022)

26. Основні науково-теоретичні проблеми розроблення систем захисту інформації. / Актуальні проблеми підготовки інженерних кадрів. Матеріали регіональної конференції. URL: <https://pandia.org/text/78/534/90615-7.php> (дата звернення: 12.11.2022)

27. Соколов А.В., Шаньгін В.Ф. Захист інформації у розподілених корпоративних мережах та системах. - М.: ДМК Прес, 2002.

28. Засоби адаптивного керування безпекою. Електронний доступ: <http://www.rnt.com/price/> (дата звернення 22.10.2022)

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

30. Тюрнев Д. Грамотне обслуговування технічних засобів безпеки. Практичні рекомендації // Системи безпеки, 2016. - № 6

31. Шумський А. А. Системний аналіз захисту інформації: навч. посібник / А. А. Шумський, А. А. Шелупанов. - М.: Геліос АРВ, 2005. - 224 с.

32. Цибулін А. М., Шипільова А. В. Математична модель зловмисника у корпоративній мережі. Управління великими системами. Випуск 19. - М: ІГТУ РАН, 2007. - С. 127-133.

33. Черемних С.В. Моделювання та аналіз систем: IDEF-технології: практикум / С. В. Черемних, І.О. Семенов, В. С. Ручкін. - М.: Фінанси та статистика. 2006. - 192 с.

- 34.Щорічний звіт Cisco з кібербезпеки за 2021 р.: топ-менеджери у сфері безпеки роблять ставку на автоматизацію, машинне самонавчання та штучний інтелект. [Електронний ресурс]:Офіційний сайт компанії Cisco: URL:https://www.cisco.com/c/com_ua/about/press/press-releases/2022/03-12.html (дата звернення: 19.11.2022)
- 35.Miller, DR Security Information and Event Management (SIEM) implementation / DR Information Technology. Information Security. Information Assurancy. Електронний доступ:<http://www.isaca.org>. (дата звернення: 19.11.2022)
- 36.Jones JA An Introduction to FAIR / JA Jones - Trustees of Norwich University, 2005. - 67 p.
- 37.Zadeh LA Fuzzy sets / LA Zadeh. - Information and Control, 1965. - №8. - P. 338-353.
- 38.Zadeh LA On optimalний контроль і linear programming / LA Zadeh, BH Whalen. - IRE Trans. Automaticcontrol, Ac-7, 1962. - P. 45-46.
- 39.Zimmermann H.-J. Fuzzy Sets, Decision Making and Expert Systems / H.-J. Zimmermann. - Kluwer: Dordrecht, 1987. - 335 p.

The diagram illustrates the components of a Security System (СЗІ). At the center is a dark hexagon labeled "СЗІ". It is surrounded by six light gray hexagons, each representing a component:

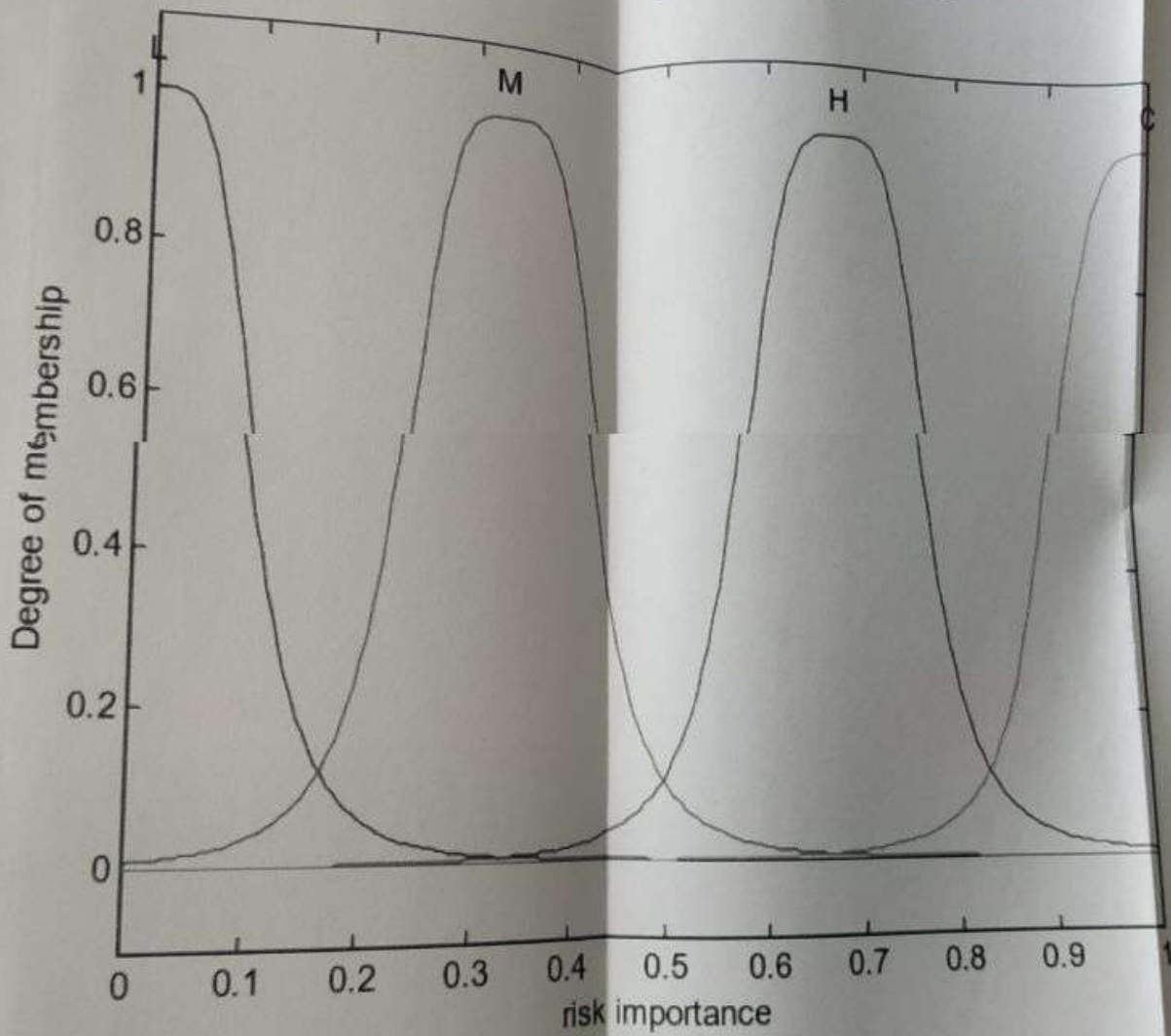
- Правові нормативні документи, стандарти
- Засіб управління контролю
- Об'єкт захисту
- Засоби захисту інформації
- Співробітники відділу інформаційної безпеки
- Апаратне забезпечення (ПК, сервери, принтер, сканер)

Additional components are listed on the right side, connected by lines to the central "СЗІ" hexagon:

- Комунікаційне обладнання, канали та лінії зв'язку
- Програмні об'єкти (операційні системи, мережеві програми, СКБД)
- Інформаційні об'єкти (електронні документи, бази даних)

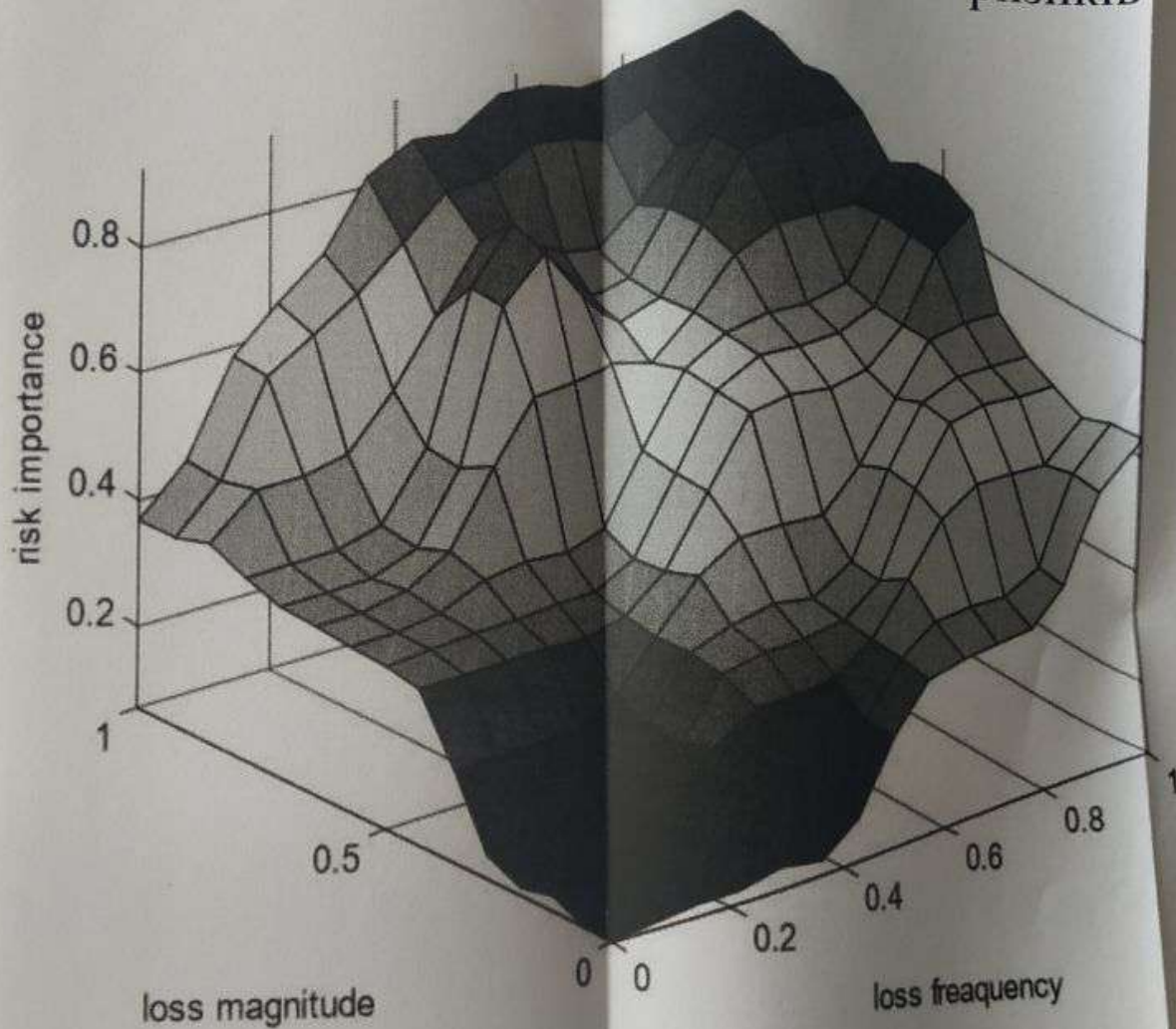
					13.02070849.51111 ПЛ1		
					Комп'ютерна система з підвищеним рівнем безпеки на основі інтелектуальних технологій		
					Модель сходу системи захисту інформації СГ КІС		
					Дат.		Мес.
					Дист. 1		Дист. 1
					НУ «Запорізька політехніка		
					КНТ-511М		

Графіки функцій належності показника рівня інформаційних ризиків у КІС



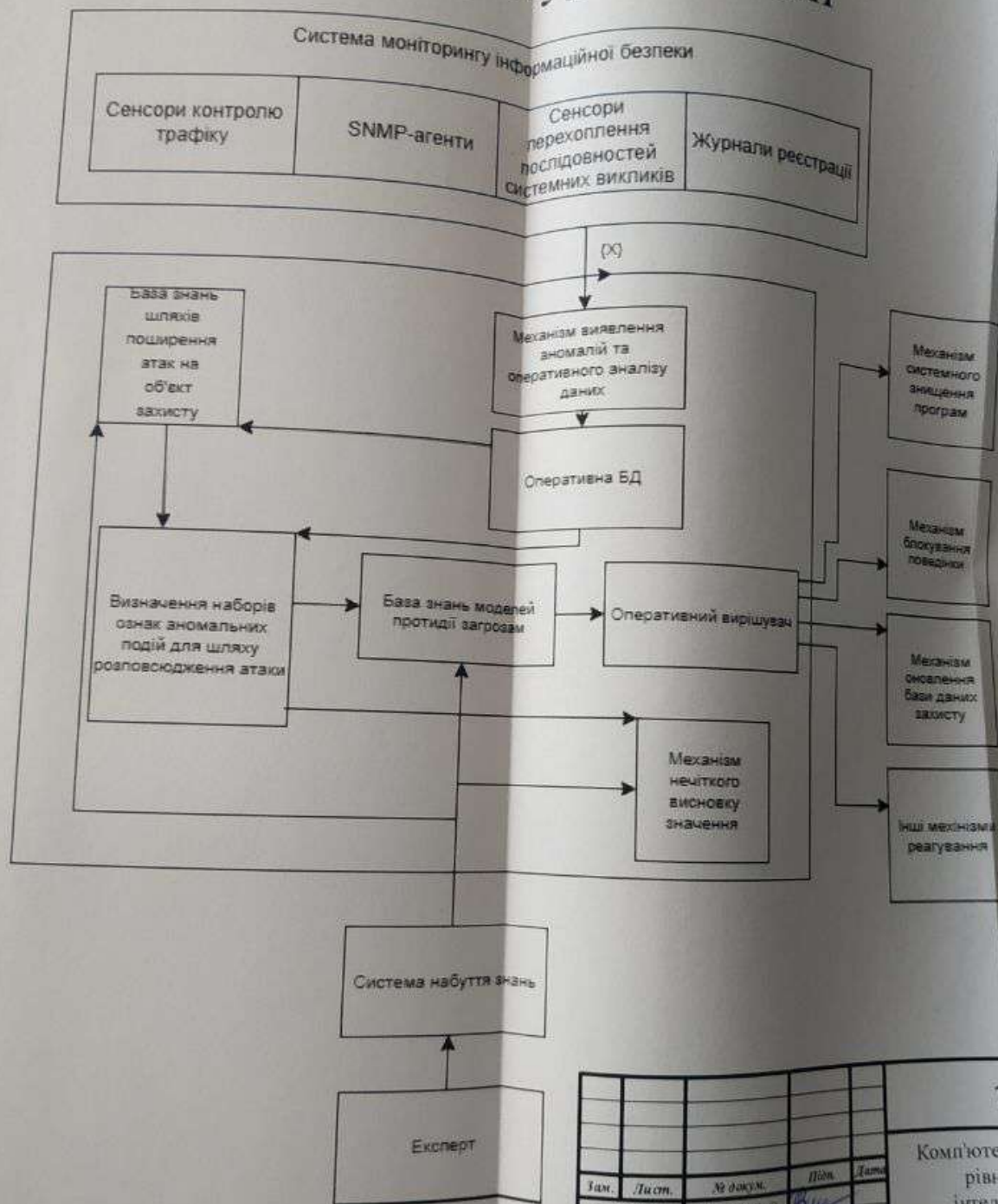
13.02070849.51111 ПЛ2				
Комп'ютерна система з підвищеним рівнем безпеки на основі інтелектуальних технологій				
Графіки функцій належності показника рівня інформаційних ризиків у КІС				
Зам.	Лист	№ докум.	Підп.	Дата
Розроб.		Поліщук В.О.		
Перев.		Пилипенко М.В.		
Т.контр.				
Н.контр.		Щербак Н.В.		
Зам.		Кузьмичов Р.К.		
Лист 1				
Листів 1				
НУ «Запорізька політехніка»				
КНТ-511м				

Графічне представлення системи нечіткого висновку показника рівня інформаційних ризиків



13.02070849.51111 ПЛЗ				
Зам.	Лист.	М. док.	Підп.	Дата
Розроб.	Поліщук В. О.			
Перев.	Пилипенко М. Б.			
Т. контр.				
Н. контр.	Щербак Н. В.			
Затв.	Кузьменко Р. К.			
Комп'ютерна система з підвищенням рівнем безпеки на основі інтелектуальних технологій. Графічне представлення системи нечіткого висновку показника рівня інформаційних ризиків.				
Лист	Маса	Масит.		
Лист 1	Листів 1			
НУ «Запорізька політехніка» КНТ-511М				

Структура системи



13.02070849.51111 ПЛ4

Комп'ютерна система з підвищеним рівнем безпеки на основі інтелектуальних технологій.
Структура системи

Лист	Маса	Масшт.
Лист 1	Листів 1	
НУ «Запорізька політехніка»		
КНТ-511м		

Зам.	Лист	№ докум.	Підп.	Дата
Розроб.		Попишук В. О.	В. О. Попишук	
Перев.		Попишук М. Б.	М. Б. Попишук	
Т.контр.				
Н.контр.		Шербаков Н. В.	Н. В. Шербаков	