НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Радіотехнічний факультет

Кафедра радіоконструювання та виробництва радіоапаратури

«На правах рукопису»
УДК 510.004

«До захисту допущено»
Завідувач кафедри
_____ Є. А. Нелін
(підпис) (ініціали, прізвище)
"17" 12 2018 р.

Магістерська дисертація

за спеціальністю 172 Телекомунікації та радіотехніка
за спеціалізацією Інтелектуальні технології мікросистемної радіоелектронної техніки

на тему: Система захисту інформації на основі динамічного програмування

Виконав: студент 6 курсу, групи РІ-з71мп
Погорський Владислав Олександрович
(підпис)

Науковий керівник к.т.н., доцент Євграфов Д.В.
(підпис)

Консультант з охорони праці к.т.н., доцент Каштанова С.Ф.
(назва розділу) (посада, вчене звання, науковий ступінь, прізвище, ініціали) (підпис)

Рецензент доцент кафедри Декарта-
(посада, науковий ступінь, вчене звання, наукова ступінь, прізвище та ініціали) (підпис)
менту, к.т.н., Бодров С.В.

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2018

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Факультет радіотехнічний

Кафедра радіоконструювання та виробництва радіоапаратури

Рівень вищої освіти – другий (магістерський)

Спеціальність 172 – телекомунікації та радіотехніка

Спеціалізація інтелектуальні технології мікросистемної радіоелектронної техніки

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Є.А. Нелін
(підпис) (ініціали, прізвище)
«11» 12 2018 р.

ЗАВДАННЯ
на магістерську дисертацію студенту

Погорєлому Владиславу Олександровичу
(прізвище, ім'я, по батькові)

1. Тема дисертації Система захисту інформації на основі динамічного програмування,
науковий керівник дисертації Єфіменко Д.В. К.Т.Н. доцент,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом по університету від «6» листопада 2018 р. №4094-с

2. Термін подання студентом дисертації 21 грудня 2018р

3. Об'єкт дослідження Показники ефективності системи комплексу захисту інформації

4. Предмет дослідження Динамічне програмування як засіб оптимізації комплексної системи захисту інформації за показниками ефективності

5. Перелік завдань, які потрібно розробити Показники ефективності комплексної системи захисту інформації. Побудова динамічного програмування для обґрунтування комплексної системи захисту інформації. Практично реалізувати комплексну систему захисту інформації.

6. Орієнтовний перелік ілюстративного матеріалу
Електронна презентація в Microsoft PowerPoint, кількість слайдів 6

7. Орієнтовний перелік публікацій Міжнародна наукова інтернет - конферен

8. Консультанти розділів дисертації

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Кашбанов С.Ф., к.т.н., доцент		

9. Дата видачі завдання 01.09.2017

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1.	Показники ефективності комплексної системи захисту інформації	березень 2017 - листопад 2017	виконано
2.	Метод динамічного програмування для підвищення ефективності комплексної системи захисту інформації	листопад 2017 - березень 2018	виконано
3.	Практична реалізація комплексної системи захисту інформації в інформаційно-бездротовій системі АМКУ	березень 2018 - червень 2018	виконано

Студент _____ (підпис) В.О. Погорський (ініціали, прізвище)

Науковий керівник дисертації _____ (підпис) Д.В. Євграфов (ініціали, прізвище)

РЕФЕРАТ

Структура й обсяг дипломної роботи

Магістерська дисертація: 114 с., 6 рис., 42 табл., 2 додатка, 7 джерел.

Ключові слова. *ІНФОРМАЦІЯ, ЕФЕКТИВНІСТЬ, ОПТИМІЗАЦІЯ, ЗАХИСТ ІНФОМРАЦІЇ.*

Актуальність теми. Комплексний характер системи безпеки для протидії різноманітним загрозам інформаційної системи має забезпечувати контроль за діяльністю службовців, які використовують різноманітні внутрішні ресурси систем.

Мета дослідження. Метою роботи є оптимізація показників ефективності та практична реалізація.

Для реалізації поставленої мети були сформульовані такі **завдання дослідження**, що визначили логіку дослідження та його структуру: дослідити показники ефективності; проаналізувати технічне завдання; практично реалізувати в ІТС.

Об'єкт дослідження — показники ефективності системи комплексу захисту інформації.

Предмет дослідження — динамічне програмування, як засіб оптимізації комплексної системи захисту інформації за показниками ефективності.

Методи дослідження: При вирішенні задач роботи застосовувались наступні методи: динамічне програмування, комп'ютерне моделювання в середовищі Mathcad.

Наукова новизна одержаних результатів. Наукова новизна полягає в розробці оптимізації ефективності на високому технічному рівні та її реалізації.

Практичне значення одержаних результатів роботи полягає в реалазіції комплексної системи захисту інформації в ІТС АМКУ.

ABSTRACT

Structure and volume of thesis

Master's dissertation: 113 c., 6 rites, 42 tables, 2 appendixes, 7 sources.

Keywords. INFORMATION, EFFICIENCY, OPTIMIZATION, PROTECTION OF INFOMATION.

Actuality of theme. The complex nature of the security system to counter the various threats to the information system should provide control over the activities of employees who use the various internal systems of the systems.

The aim of the study. The aim of the work is to optimize performance and practical implementation.

To achieve this goal, the following research objectives were formulated, which determined the logic of the research and its structure: to investigate performance indicators; analyze the technical task; practically realize in ITS.

Object of research - indicators of efficiency of the system of information security complex.

The subject of research - dynamic programming, as a means of optimizing a comprehensive information security system by performance indicators.

Methods of research: When solving problems of work, the following methods were used: dynamic programming, computer simulation in the environment of Mathcad.

Scientific novelty of the obtained results. Scientific novelty is to develop optimization of efficiency at a high technical level and its implementation.

The practical significance of the results of the work is to implement a comprehensive system of information security in the ITS AMCU.

ПОЯСНЮВАЛЬНА ЗАПИСКА
до магістерської дисертації

на тему: Система захисту інформації на основі динамічного програмування

Київ – 2018

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

АПЗ – Апаратно-програмний засіб
АЦСК – Акредитований центр сертифікації ключів
БД – База даних
ДБЖ – Джерело безперебійного живлення
ДССЗЗІ – Державна служба спеціального зв'язку і захисту інформації України
ЕК – Електронний ключ
ЕОМ – Електронна обчислювальна машина
ІТС – Інформаційно-телекомунікаційна система
КЗЗ – Комплекс засобів захисту
КЗІ – Криптографічний захист інформації
КСЗІ – Комплексна система захисту інформації
КТЗ – Комплекс технічних засобів
ЛОМ – Локальна обчислювальна мережа
НЖМД – Накопичувач на жорстких магнітних дисках
НКІ – Носій ключової інформації
НСД – Несанкціонований доступ
ОЗП – Оперативних запам’ятовуючий пристрій
ОС – Операційна система
ПД – Персональні дані
ПЕОМ – Персональна електронна обчислювальна машина
ПЗ – Програмний засіб
ПК – Програмний комплекс
РМ – Робоче місце
РС – Робоча станція
СЗІ – Служба захисту інформації
СКБД – Система керування базами даних
ФПЗ – Функціональне програмне забезпечення

ТЗ – Технічне завдання

ТЗІ – Технічний захист інформації

ЦСК – Центр сертифікації ключів

BIOS – Basic input/output system

CD – Compact Disk (компакт-диск)

DVD – Digital Versatile Disk (Цифровий багатоцільовий диск)

FDD – Floppy Disk Drive (Привід для гнучких магнітних дисків)

IDS – Intrusion Detection System

IPS – Intrusion Prevention System (система протидії мережним вторгненням)

RDP – Remote Desktop (віддалений робочий стіл)

SQL – Structured Query Language (мова структурованих запитів)

TCP – Transmission Control Protocol (протокол керування передачею)

VLAN – Virtual Local Area Network (віртуальна локальна мережа)

ВСТУП

Захист інформації в сучасних умовах стає усе більш складною проблемою, що обумовлено такими основними причинами:

- масове поширення засобів електронної обчислювальної техніки (ЕОТ);
- ускладнення шифрувальних технологій;
- необхідність захисту не тільки державної і військової таємниці, але і промислової, комерційної і фінансової таємниць;
- можливості несанкціонованих дій, що розширюються, над інформацією.

Крім того, у даний час одержали широке поширення засоби і методи несанкціонованого отримання інформації.

Побудова комплексної системи захисту інформації на об’єкті, здійснюється згідно НД ТЗІ 3.7-003-05. НД ТЗІ 3.7-003-05 визначає порядок прийняття рішень щодо складу КСЗІ в залежності від умов функціонування ІТС і видів оброблюваної інформації, визначення обсягу робіт і зміст робіт, етапності робіт, основних завдань та порядку виконання робіт кожного етапу.

Процес створення КСЗІ полягає у здійсненні комплексу взаємоузгоджених заходів, спрямованих на розроблення і впровадження інформаційної технології, яка забезпечує обробку інформації в ІТС згідно з вимогами, встановленими нормативно-правовими актами та НД у сфері захисту інформації.

РОЗДІЛ 1 - ПОКАЗНИКИ ЕФЕКТИВНОСТІ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

1.1 Аналіз технічного завдання комплексної системи захисту інформації та визначення об’єктів витоку інформації.

Основою для проведення аналізу ризиків і формування вимог до КСЗІ є розробка моделі загроз для інформації та моделі порушника.

Для створення моделі загроз необхідно скласти перелік суттєвих загроз, описати методи і способи їхнього здійснення.

Необхідно визначити, якими з можливих способів можуть здійснюватися загрози в АС:

– технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо- та радіотехнічні, хімічні та інші канали;

– каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;

– несанкціонованим доступом шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав’язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп’ютерних вірусів.

Загрози для інформації, що обробляється в АС, залежать від характеристик ОС, фізичного середовища, персоналу, технологій обробки та інших чинників і можуть мати об'єктивну або суб'єктивну природу. Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні. Мають бути визначені основні види загроз для безпеки інформації, які можуть бути реалізовані стосовно АС і повинні враховуватись у моделі загроз, наприклад:

– зміна умов фізичного середовища (стихійні лиха і аварії, як землетрус, повінь, пожежа або інші випадкові події);

– збої і відмови у роботі обладнання та технічних засобів АС;

– наслідки помилок під час проектування та розробки компонентів АС (технічних засобів, технології обробки інформації, програмних засобів, засобів захисту, структур даних тощо);

– помилки персоналу (користувачів) АС під час експлуатації;

– навмисні дії (спроби) потенційних порушників.

Необхідно визначити перелік можливих загроз і класифікувати їх за результатом впливу на інформацію, тобто на порушення яких властивостей вони спрямовані (конфіденційності, цілісності та доступності інформації), а також порушення спостережності та керованості АС.

Випадковими загрозами суб'єктивної природи (дії, які здійснюються персоналом або користувачами по неуважності, недбалості, незнанню тощо, але без навмисного наміру) можуть бути:

– дії, що призводять до відмови АС (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв'язку, видалення даних, програм та ін.);

– ненавмисне пошкодження носіїв інформації;

– неправомірна зміна режимів роботи АС (окремих компонентів, обладнання, ПЗ тощо), ініціювання тестуючих або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації);

– неумисне зараження ПЗ комп'ютерними вірусами;

– невиконання вимог до організаційних заходів захисту чинних в АС розпорядчих документів;

– помилки під час введення даних в систему, виведення даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо;

– будь-які дії, що можуть призвести до розголошення конфіденційних відомостей, атрибутів розмежування доступу, втрати атрибутів тощо;

– неправомірне впровадження і використання забороненого політикою безпеки ПЗ (наприклад, навчальні та ігрові програми, системне і прикладне забезпечення та ін.);

– наслідки некомпетентного застосування засобів захисту;

Навмисними загрозами суб'єктивної природи, спрямованими на дезорганізацію роботи АС (окремих компонентів) або виведення її з ладу, проникнення в систему і одержання можливості несанкціонованого доступу до її ресурсів, можуть бути:

– порушення фізичної цілісності АС (окремих компонентів, пристроїв, обладнання, носіїв інформації);

– порушення режимів функціонування (виведення з ладу) систем життєзабезпечення АС (електроживлення, заземлення, охоронної сигналізації, вентиляції та ін.);

– порушення режимів функціонування АС (обладнання і ПЗ);

– впровадження і використання комп'ютерних вірусів, закладних (апаратних і програмних) і підслуховуючих пристроїв, інших засобів розвідки;

– використання засобів перехоплення побічних електромагнітних випромінювань і наводів, акусто-електричних перетворень інформаційних сигналів;

– використання (шантаж, підкуп тощо) з корисливою метою персоналу АС;

– крадіжки носіїв інформації, виробничих відходів (роздруків, записів, тощо);

– несанкціоноване копіювання носіїв інформації;

– читання залишкової інформації з оперативної пам'яті ЕОМ, зовнішніх накопичувачів;

– одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача (“маскарад”);

– неправомірне підключення до каналів зв’язку, перехоплення даних, що передаються, аналіз трафіку тощо;

– впровадження і використання забороненого політикою безпеки ПЗ або несанкціоноване використання ПЗ, за допомогою якого можна одержати доступ до критичної інформації (наприклад, аналізаторів безпеки мереж);

В таблиці 1.1 подано класифікацію потенційних загроз інформації, за джерелами, природою, загрозами, наслідками порушення та ресурсами, які необхідні для подолання зазначених загроз. В таблиці використовуються наступні скорочення:

Таблиця 1.1 - Класифікація потенційних загроз інформації, що обробляється в АС

№	Джерело	Природа		Загроза	Наслідки порушення				Ресурси
					К	Ц	Д	С	
1	Зовнішні	Об’єктивна		Стихійні явища		+	+		Всі
2	Зовнішні	Об’єктивна		Збої та відмови системи електроживлення		+	+		Всі
3	Внутрішні	Об’єктивна		Збої та відмови обчислювальної техніки		+	+		Всі
4	Внутрішня	Об’єктивна		Збої, відмови та пошкодження носіїв інформації		+	+		Всі
5	Внутрішня	Об’єктивна		Збої та відмови програмного забезпечення		+	+		Всі
6	Внутрішня	Об’єктивна		Відмова в доступі користувачу АС в результаті помилки ПЗ			+		ІК_КЗЗ, ІЗК
7	Зовнішня	Суб’єктивна	Навмисна/ ненавмисна	Ураження програмного забезпечення комп’ютерними вірусами	+	+	+	+	всі
8	Внутрішня	Суб’єктивна	Навмисна/ ненавмисна	Несанкціоноване внесення змін до технічних засобів, в програмне забезпечення, що призводять до зміни режиму роботи чи відмови АС		+	+	+	ЗАЗ_КЗЗ, СПЗ_ КЗЗ, ТІ_КЗЗ

9	Внутрішня	Суб'єктивна	Навмисна/ ненавмисна	Порушення адміністратором безпеки реалізації ПРД	+	+	+	+	ТІ_КЗЗ,І_ ЖР, ІК, ІЗК
10	Внутрішня	Суб'єктивна	Ненавмисна	Втрата атрибутів розмежування доступу	+	+	+		всі
11	Внутрішня	Суб'єктивна	Навмисна	Неправомірне впровадження і використання забороненого політикою безпеки ПЗ	+	+	+	+	всі
12	Зовнішня	Суб'єктивна	Навмисна	Використання з корисливою метою персоналу АС	+	+	+	+	{ІК}, {ІЗК}
13	Зовнішня	Суб'єктивна	Навмисна	Несанкціонований доступ до приміщення АС	+	+	+	+	всі
14	Зовнішня	Суб'єктивна	Навмисна	Вербування працівників підприємства	+	+			всі
15	Зовнівшня/ Внутрішня	Суб'єктивна	Навмисна	Розкрадання матеріальних носіїв інформації	+	+			всі
16	Внутрішня	Суб'єктивна	Навмисна	Читання залишеної інформації	+				{ІК}, {ІЗК}
17	Внутрішня	Суб'єктивна	Ненавмисна	Ненавмисне псування матеріальних носіїв інформації			+		всі

1.2 Формування моделі порушника об’єкта інформаційної діяльності

Під порушником розуміється особа, яка зробила спробу виконання заборонених операцій помилково, не знаючи або навмисно зі злим помислом (корисним інтересом) або без таких (заради гри, самоствердження), заради самоствердження або помсти, використовуючи для цього різні способи і методи, можливості і засоби.

Порушник може використовувати різноманітні методи та засоби для доступу до ІзОД. Якщо порушник діє навмисне, з корисних мотивів, то будемо називати його зловмисником. Зловмисники винятково якісно вивчають системи безпеки в ІТС перед проникненням до неї.

Необхідно оцінити збитки, які можуть мати місце у випадку витоку інформації або при будь-якому іншому порушенні системи безпеки, а також ймовірність нанесення подібних збитків. Для визначення адекватності вартості системи захисту, слід зіставити розміри збитків і ймовірність їх нанесення з розмірами затрат на забезпечення захисту. Проте, реальну вартість інформації оцінити дуже важко, тому зазвичай використовують не кількісні, а якісні експертні оцінки. Найчастіше будується неформалізована модель порушника (зловмисника), що відображає причини й мотиви дій, його можливості, знання, цілі, основні шляхи досягнення поставлених цілей – способи реалізації загроз, місце і характер дії, можлива тактика і т. д. Для досягнення поставлених цілей зловмисник повинен прикласти деякі зусилля і затратити деякі ресурси.

Порушником по відношенню до АС можуть бути особи з персоналу і користувачів системи; сторонні особи.

Можливі внутрішні порушники :

– кінцеві користувачі (оператори системи); персонал;(перший рівень)

– особи, що обслуговують технічних засобів (третій рівень);

– співробітники відділу розробки і супроводження програмного забезпечення (четвертий рівень);

– співробітники служби безпеки АС (перший рівень);

– керівники різних рівнів (перший рівень).

Можливі зовнішні порушники (сторонні особи):

– технічний персонал, обслуговуючий будівлю (перший рівень);

– клієнти (перший рівень);

– представники організацій-конкурентів (другий рівень);

– відвідувачі запрошені з будь-якого приводу (другий рівень).

Порушники класифікуються за рівнем можливостей, що надаються їм штатними засобами КС. Виділяються чотири рівні цих можливостей. Класифікація є ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього:

– перший рівень визначає найнижчий рівень можливостей проведення діалогу з КС – можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;

– другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;

– третій рівень визначається можливістю управління функціонуванням КС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;

– четвертий рівень визначається всім обсягом можливостей осіб, що здійснюють проектування, реалізацію і ремонт апаратних компонентів КС, аж до включення до складу КС власних засобів з новими функціями обробки інформації.

Припускається, що в своєму рівні порушник – це фахівець вищої кваліфікації, який має повну інформацію про КС і КЗЗ.

Порушник може здійснювати несанкціонований доступ до інформації або під час роботи автоматизованої системи, або в період неактивності автоматизованої системи, або ж суміщаючи робочий і не робочий час.

У КСЗІ на виділеному об’єкті передбачаються, розглядаються і розробляються усі чотири рівні порушників.

РОЗДІЛ 2 - МЕТОД ДИНАМІЧНОГО ПРОГРАМУВАННЯ ДЛЯ ОБГРУНТУВАННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

2.1 Метод динамічного програмування

2.1.1 Термін “динамічне програмування”

Термін *динамічне програмування* був запроваджений в 40-х роках Річардом Беллманом для характеристики процесу розв'язування проблем, при якому потрібно знаходити найкращі рішення, одне за одним. Пізніше, в 1953 році, він уточнив його в сучасному розумінні, називаючи так задачі, безпосередньо пов'язані з розв'язуванням вкладених підзадач для пошуку розв'язку всієї задачі і ця сфера була пізніше визнана Інститутом інженерів з електротехніки та електроніки як підрозділ системного аналізу та інженерії. Відзначивши внесок Беллмана, його ім'ям назвали рівняння Беллма — основну формулу динамічного програмування, яка інтерпретує задачу оптимізації в рекурсивній формі.

Слово *динамічне* було обране Беллманом, тому що звучало більш переконливо і краще підходило для передачі того факту, що проблема оптимального управління, яку він розв'язував цим методом, має аспект залежності від часу. Слово *програмування* в цьому словосполученні в дійсності до «традиційного» програмування (написання тексту програм) майже ніякого відношення не має. Це використання таке саме як і в словосполученнях *лінійне програмування* та *математичне програмування*, які фактично є синонімами для математичної оптимізації. Тут воно означає оптимальну послідовність дій, оптимальну *програму* для отримання розв'язку задачі. Наприклад, певний розклад подій на виставці чи в театрі теж називають програмою. Програма в даному випадку розуміється як запланована послідовність подій. Хоча, динамічне програмування, як алгоритм, часто використовується при програмуванні для розв'язку відповідних задач (див. Нижче).

Динамічне програмування - метод оптимізації, пристосований до операцій, в яких процес прийняття рішень може бути розділений на окремі етапи (кроки). В основі методу лежить принцип оптимальності, сформульований Р.Беллманом.

Оптимальне управління характеризується такими властивостями, що незалежно від початкового стану на будь-якому кроці управління і наступне управління повинно обиратися оптимальним відносно стану, до якого прийде система в кінці цього кроку.

Метод, побудований на використанні принципу оптимальності, дозволяє встановити співвідношення між екстремальними значеннями цільової функції в задачах, що характеризуються різною тривалістю процесу і різними початковими станами. При цьому необхідно враховувати наслідки реалізації знайденого оптимального рішення і для наступних рішень. Такий підхід обумовлений розробкою оптимальної стратегії. Процес прийняття рішення в цьому випадку є багатокроковим.

Найбільш доцільно динамічне програмування застосувати для вирішення таких практичних задач, в яких пошук оптимального рішення вимагає поетапного підходу.

На практиці часто доводиться зустрічатись з випадками, коли метою (ціллю) оптимізації є встановлення найкращої послідовності тих чи інших робіт (виробничих операцій, етапів будівництва різних споруд тощо). З подібною метою зустрічаються при розв'язанні задач динамічного програмування. Однією з перших задач такого роду, що привернули увагу математиків, була задача про комівояжера (мандрівного торговця).

Суть її така: є n+1 міст $A_0, A_1, \dots A_n (n \geq 1)$ з заданими між ними відстанями $d_{ij} (i, j = 0,1, \dots, n)$.

Потрібно, відправившись з A_0, вибрати такий маршрут пересування $A_0, A_{i1}, A_{i2} \dots A_n, A_0$, при якому комівояжер, побувавши в кожному місті по одному разу, повернувся б до вихідного пункту A_0, пройшовши при цьому мінімально можливий сумарний шлях.

Основний спосіб динамічного програмування полягає в знаходженні правил домінування, які дозволяють робити порівняння варіантів розвитку послідовностей і завчасне відсіювання безперспективних варіантів. У ряді

випадків в задачах динамічного програмування вдається одержати такі сильні правила домінування, що вони визначають елементи оптимальної послідовності однозначно один за одним. В такому випадку правила домінування називають розв'язувальними правилами.

Розв'язувальні правила звичайно виводяться за допомогою принципу оптимальності Беллмана. Суть принципу оптимальності така. Нехай критерій *F* (задається формулою або алгоритмом), який дає числову оцінку якості варіанта (послідовності) $A_n = A_{i1}, A_{i2} \dots A_{in}$, можна застосовувати не тільки до всієї послідовності, але і до будь-якого її початкового відрізку $A_R = A_{i1}, A_{i2} \dots A_{iR}$. Послідовність A_n, якій відповідає екстремальне значення критерію *F*, називається оптимальною. Якщо будь-який початковий відрізок оптимальної послідовності також оптимальний (в класі всіх послідовностей, складених з тих же елементів, і можливо, такий, що має ті ж початок і кінець, що і даний відрізок), то вважають, що для відповідної задачі справедливий принцип оптимальності.

Розглянемо зразок розв'язання задачі про комівояжера методом динамічного програмування:

1. Введення даних про пункти $A_0 \dots A_n$ і відстані між пунктами *i* та *j* d_{ij} (d_{ij} =0 при *i=j)* .

2. Обчислення всіх можливих варіантів відстаней, що складаються з трьох дільниць A_0, A_{i1}, A_{i2}, A_{i3}. Вони групуються по останньому пункту *i* з них залишаються ті варіанти, що об'єднують однакові пункти, але мають найменший шлях.

3. До тих варіантів, що залишились додають ще четверту дільницю і повторюють процедуру з пункту 2. Це повторюється для п'ятої, шостої і т. д. дільниць, доки не повертається в пункт A_0. Той варіант (чи варіанти), що залишилися, і визначають найкоротший шлях, по якому комівояжеру можна об'їздити всі міста A_i *(i=0,…,n)*, якщо він почне та закінчить свою подорож

2.1.2 Системна оптимізація

В практиці проектування великих систем і управління такими системами, як правило, використовується багато критеріїв. В ряді випадків їх вдається в той чи іншій спосіб звести до одного критерію і тим самим повернутися до вже дослідженого випадку однокритеріальної оптимізації.

Найпростіший спосіб такого зведення – так зване зважування критеріїв. Якщо $f_1(x),...f_n(x)$ функції, що виражають значення використовуваних критеріїв, то кожній з них, відповідно до відносної важливості критеріїв, вибирається додатний ваговий коефіцієнт λ_i. Операція зважування критеріїв (цільових функцій) $f_1(x),...f_n(x)$ полягає в заміні їх єдиним критерієм (цільовою функцією) $f(x)=\lambda_1 f_1(x)+...+\lambda_n f_n(x)$.

Але для багатьох задач, що пов'язані з великими системами, подібне зведення виявляється практично неможливим, так що в процесі оптимізації доводиться мати справу з векторною (багатокритеріальною) цільовою функцією. При цьому припустима область M може змінюватись в процесі оптимізації. Більше того, в її цілеспрямованій зміні як раз і полягає основна змістовна сутність процесу оптимізації для подібного класу задач.

Наведемо одну з характерних формалізованих постановок задачі системної оптимізації.

Розв'язок відшукується безпосередньо в просторі K критеріїв оптимізації, які ми позначимо x_1 і x_2. Процес розв'язання починається з того, що в заданому просторі K вибирається деяка точка A_0 з координатами a_0, b_0 – бажаний розв'язок задачі. За цим будуються початкові обмеження $F_1^{(0)}(x_1,x_2)\geq 0,...,F_n^{(0)}(x_1,x_2)\geq 0$, що задають початкову припустиму область P_0. Прямою перевіркою встановлюється, чи належить точка A_0 області P_0. В першому випадку в принципі може бути застосована звичайна (класична) процедура оптимізації або за одним з критеріїв x_1, x_2, або за тією чи іншою їх комбінацією.

Але при системному підході застосовується звичайно запропонований Л. С. Понтрягіним спосіб, а саме: відповідно до моделі M вищого рівня, що управляє вибором критеріїв, точка A_0 виводиться з границь припустимої області P_0, як це показано на рисунку 2.1.

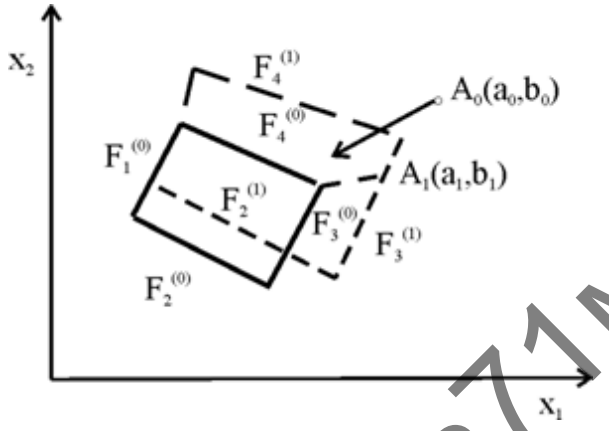

Рисунок 2.1 – Виведення точки A_0

Після цього виділяються ті обмеження, які не виконуються в точці A_0 (в випадку, що розглядається, ними будуть $F_3^{(0)}$ і $F_4^{(0)}$). Звертаючись до моделей M_3і M_4, які формують ці обмеження, в діалоговому режимі опробовуються ті чи інші рішення, що змінюють відповідні обмеження в потрібному напрямку (якщо така зміна можлива). Оптимальним при цьому вважається той напрямок, що зменшує абсолютну величину від'ємних відхилень $F_i^{(0)}(a_0,b_0)$(в випадку, який розглядається, $F_3^{(0)}(a_0,b_0)$ і $F_4^{(0)}(a_0,b_0)$.

2.1.3 Застосування теорії графів до розв'язання оптимізаційних задач

Розв'язання багатьох технічних задач можливо методами теорії графів. Основні поняття та визначення теорії графів розглянуті в відповідних підручниках, які є в списку літератури в кінці цієї книжки. Тут ми обмежимося розглядом підходів до транспортної задачі та задачі комівояжера з застосуванням теорії графів.

Ці підходи базуються на відомій задачі з теорії графів про знаходження найкоротшого шляху між двома вершинами зв'язного неорієнтованого графу. До цієї задачі зводяться не тільки задача про комівояжера чи транспортна, а також, наприклад, багато задач оптимальної обробки деталей, оптимізації

програмування, управління динамічними системами і т.д. В загальному вигляді задача формулюється так. Дано неорієнтований граф $G=(X,U)$, де X – множина вершин, U – множина ребер. Кожному ребру приписане деяке число $l(U)\geq 0$, що називається довжиною ребра (в транспортних задачах це може бути час чи вартість проїзду цим ребром).

Загальне правило виявлення найкоротшого шляху в графі полягає в тому, щоб кожній вершині X приписати індекс λ_i, який дорівнює довжині найкоротшого шляху з даної вершини до кінцевої. Якщо, наприклад, спочатку взяти граф з ребрами одиничної довжини, то порядок дій буде такий:

- кінцевій вершині X_0 присвоюється індекс 0;

- усім вершинам, з котрих йде ребро до кінцевої вершини, присвоюється індекс 1;

- усім вершинам, що не мають індексів, та з котрих йде ребро в вершину з індексом λ_i, приписується індекс λ_i+1, до тих пір, поки не буде помічена початкова вершина.

Після закінчення цього процесу індекс початкової вершини буде дорівнювати довжині найкоротшого шляху, а найкоротший шлях знаходиться, якщо пересуватися з початкової вершини в напрямку зменшення індексів. Приклад наведено на рисунку 2.2. Подвійною лінією наведені два найкоротших шляхи.

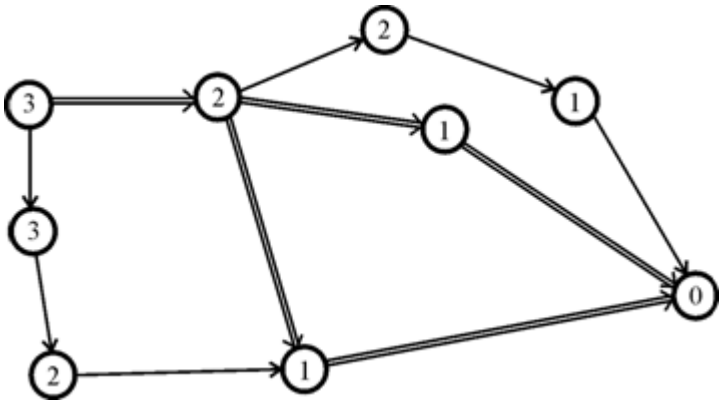

Рисунок 2.2 – Знаходження найкоротшого шляху в графі з ребрами одиничної довжини

Тепер розглянемо випадок, коли ребра мають довільну довжину. Процес присвоювання індексів ускладнюється, і порядок дій може бути зведений до такого:

– кожній вершині X_i присвоюється індекс λ_i.: спочатку кінцевій вершині X_0 присвоюється індекс $\lambda_0 = 0$, для інших вершин беремо на першому кроці $\lambda_0 = \infty \ (i \neq 0)$;

– Шукаємо таку дугу (x_i, x_j), що $\lambda_j - \lambda_i > l(x_i, x_j)$, й замінюємо індекс λ_j на індекс $\lambda_j = \lambda_i + l(x_i, x_j) < \lambda_j$ (де $l(x_i, x_j)$ - довжина дуги , процес заміни індексів продовжується до тих пір, поки залишиться хоча б одна дуга, для якої можна зменшити λ_j).

Відзначимо дві важливі властивості індексів:

– Нехай (X_k, X_s) – довільне ребро. Для нього обов'язково виконується умова $\lambda_s - \lambda_k \leq l(X_k, X_s)$. Це виходить з того, що при невиконанні умови індекс λ_s треба було б зменшити.

– Якщо X_p – довільна вершина. При реалізації алгоритму присвоювання індексів індекс λ_p монотонно зменшується. Нехай X_q – остання вершина, що була використана для його зменшення. Тоді $\lambda_p = \lambda_q + l(X_q, X_p)$. Це приводить до висновку, що для будь-якої вершини X_p з індексом λ_p може бути знайдено вершину X_q, що з'єднується ребром з X_p, таку, що $\lambda_p - \lambda_q = l(X_q, X_p)$.

Виявлені властивості дають можливість сформулювати такий спосіб знаходження найкоротшого шляху.

Нехай $X_n = a$ – початкова вершина з індексом λ_n. Шукаємо вершину X_{p_1} таку, що $\lambda_n - \lambda_{p_1} = l(X_{p_1}, X_n)$. Далі шукаємо вершину X_{p_2} таку, що $\lambda_{p_1} - \lambda_{p_2} = l(X_{p_2}, X_{p_1})$, і т.д. до тих пір, поки не дійдемо до кінцевої вершини. Шлях $\mu_0 = (X_n, X_{p_1}, \ldots, X_{p_k}, X_0)$ – найкоротший. Приклад використання цього способу поданий на рисунку 2.3. Найкоротший щлях виділений подвійною рискою.

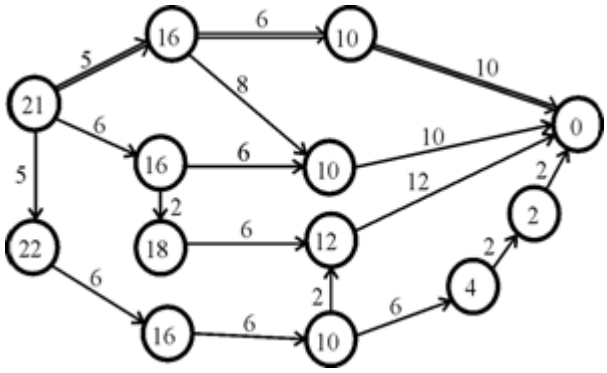

Рисунок 2.3 – Знаходження найкоротшого шляху в графі з ребрами довільної довжини

Очевидно, ці задачі про пошук найкоротшого шляху в графі аналогічні деяким задачам, що виникають в різних практичних областях. До неї зводяться задачі про побудову доріг, що з’єднують декілька міст найдешевшим чином, задачі про розбудову електромережі, нафтопроводів та ін. За допомогою графових підходів можна розв’язавши транспортну задачу та задачу комівояжера. Розглянемо задачу про комівояжера у вигляді графу. Вершини цього графу відповідають містам, а шляхи - дорогам, що ці міста з’єднують. Кожній дузі можна приписати довжину, що дорівнює відстані між містами. І далі дуже просто звести задачу комівояжера до задачі про пошук найкоротшого шляху. До задачі про комівояжера зводиться багато транспортних задач, задач оптимізації програмування, оптимізації порядку оброблення деталей та ін.

2.2. Аналіз алгоритмів виявлення порушника за допомогою засобів виявлення

2.2.1. Ймовірнісні показники одного засобу виявлення (ЗВ)

Чутлива зона (або зона чутливості) засобу виявлення - це ділянка або об'єкт, поява в якому об'єкта виявлення (найчастіше це людина-порушник) спричинює виникнення корисного сигналу з рівнем, що перевищує рівень шуму або перешкоди.

Усередині зони чутливості розташовується зона відчуження – це зона, поява в якій людей, техніки чи інших об'єктів виявлення може призвести до перевищення корисним сигналом порогового значення і видачу ЗВ сигналу "Тривога".

Усередині зони відчуження розташовується зона виявлення ЗВ – зона, де ЗВ забезпечує задану (описану в паспорті на виріб) ймовірність виявлення $P_в$.

Ймовірність виявлення - це ймовірність того, що ЗВ видасть обов'язково сигнал "Тривога" (як правило, це замикання або перемикання сухих контактів реле) при перетині чи вторгнення в зону виявлення порушника (іноді застосовується термін "об'єкта виявлення"), в умовах і способами, обумовленими в нормативній документації. Як правило, закордонні фірми вказують як ймовірності виявлення ЗВ незміщене оцінку ймовірності виявлення:

$$P_в = \frac{N_{вип} - M - 1}{N_{вип}}$$

де $N_{вип}$ - число випробувань з подолання зони виявлення ЗВ; М - число пропусків порушника (експериментів, в яких не спрацювало ЗВ).

Наприклад, якщо при перетині ЗВ у кількості 100 раз не було пропусків порушника, тобто ЗВ видало 100 разів сигнал "Тривога", то про це ЗВ можна сказати, що його вірогідність виявлення становить 0,99 (не 1 тому, що це незміщена оцінка математичного сподівання ймовірності виявлення порушника).

У вітчизняній практиці під імовірністю виявлення, як правило, розуміється нижня межа довірчого інтервалу, в якому з довірчою ймовірністю (як правило, від 0,8 до 0,95) лежить справжнє значення ймовірності виявлення.

Тобто під імовірністю виявлення розуміється величина

$$P_в = \frac{P^* + \frac{1}{2}\frac{t_\gamma^2}{N_{вип}} - t_\gamma \sqrt{\frac{P^*(1-P^*)}{N_{вип}} + \frac{1}{4}\left(\frac{t_\gamma}{N_{вип}}\right)^2}}{1 + \frac{t_\gamma^2}{N_{вип}}}$$

де Р * - середнє частотне значення ймовірності виявлення, визначається виразом:

$$P^* = 1 - \frac{M}{N_{вип}}$$

t_γ-коефіцієнт Стьюдента для даного числа випробувань і вибраної довірчої ймовірності.

Корисним називають сигнал, що виникає на виході чутливого елемента при подоланні чи вторгнення в зону виявлення порушника (при відсутності збурюючих чинників будь-якої природи, не пов'язаних з вторгненням чи подоланням порушником зони виявлення).

Іншим важливим параметром ЗВ є частота помилкових спрацьовувань $N_{пс}$, обумовлена виразом:

$$N_{пс} = \frac{1}{T_{пс}}$$

де $T_{пс}$ - час (період) напрацювання на помилкове спрацьовування.

Довірчий інтервал для оцінки середнього напрацювання на помилкове спрацьовування задається граничними значеннями T_1 і T_2, обумовленими зі співвідношень:

$$T_1 = \frac{T_{вип} N}{\lambda_1},$$

$$T_2 = \frac{T_{вип} N}{\lambda_2}$$

де $T_{вип}$ - тривалість випробувань; N - кількість випробовуваних зразків; λ_1 - нижня оцінка параметра розподілу Пуассона; λ_2 - верхня оцінка параметра розподілу Пуассона.

Перешкоджаючі сигнали (далі по тексту іменується перешкодою) називається залежність електричної величини (напруги або струму) від часу на виході ЧЕ ЗВ при впливі на нього збурюючих чинників будь-якої природи, не пов'язаних з вторгненням чи подоланням об'єктами виявлення зони виявлення.

Обурюючим впливом називається вплив на ЧЕ СВ, що є причиною виникнення перешкоди або спотворює форму корисного сигналу.

Прикладом обурюючого впливу можуть служити: порив вітру, сніг, дощ; кішки, собаки, що переміщаються в чутливій зоні (ЧЗ); транспорт, що переміщається поблизу ЧЗ, та ін

Флюктуаціоної перешкодою називають перешкоду, що є безперервним випадковим процесом, описуваних своїми багатовимірними функціями розподілу.

Імпульсної перешкодою називають перешкоду, що представляє собою випадкову послідовність імпульсів, описувану моментами появи імпульсів і їх видом.

Причиною пропуску корисного сигналу є маскуюча дія перешкоди, що повністю або частково компенсує корисний сигнал, або відсутність в корисному сигналі характерних ознак, що дозволяють відрізнити його від сигналу перешкоди, що призводить до неспрацьовування ЗВ.

При визначенні ймовірності виявлення ЗВ, що випускаються у великих обсягах, можуть застосовуватися методики, які використовують крім довірчого інтервалу і довірчої ймовірності ризик замовника і ризик виробника. Наприклад, за вітчизняною методикою аналогічне ЗВ буде мати можливість виявлення не більше 0,9.

2.2.2 Формалізація вибору різних варіантів комбінування засобів виявлення на одному рубежі охорони

Аналіз схем побудови КЗВ показав, що в даний час серед розробляються і розроблених систем (комплексів) найбільшого поширення набули схеми логічної обробки (бінарних сигналів тривоги з окремих ЗВ) K із N.

Функціонування всіх розроблених до теперішнього часу схем логічної обробки бінарних сигналів (тобто за формулою «є чи ні сигналу тривоги на виході ЗВ») для КЗВ засноване на тому, що число спрацювавших протягом часу пам'яті (час, протягом якого мають прийти сигнали від ЗВ) ЗВ має досягти або перевищити задану величину К. У цьому випадку формується загальний сигнал тривоги. Перевагою такого алгоритму обробки сигналів від різних ЗВ є його безсумнівна простота, однак відсутність обліку індивідуальних особливостей і характеристик кожного окремо взятого ЗВ не дозволяє досягти найкращого співвідношення між імовірністю виявлення та частотою помилкової тривоги КЗВ в цілому. У той же час різні окремі ЗВ володіють різними значеннями

ймовірності виявлення та ймовірності помилкової тривоги, у зв'язку з чим поява на виході ЗВ сигналу тривоги говорить про появу порушника з різним ступенем достовірності для різних ЗВ. Таким чином, виникає необхідність застосовувати алгоритми логічної обробки для КЗВ, що дозволяють за рахунок врахування індивідуальних особливостей ЗВ досягати зменшення ймовірності помилкової тривоги ЗВ при збереженні можливості забезпечення заданої ймовірності виявлення. Сигнали тривоги від окремих ЗВ будуть в цьому випадку оброблятися не як однаково достовірні і алгоритм обробки буде змінюватися в залежності від застосовуваних ЗВ.

В даний час відомі два таких алгоритму обробки бінарних сигналів від ЗВ:

– на основі можливих комбінацій спрацювавших ЗВ,

– на основі присвоєння ЗВ вагових коефіцієнтів.

2.2.3 Комбінації ймовірностей

Розглянемо перший алгоритм на прикладі трьох ЗВ, для кожного з яких відомі їх ймовірності виявлення P_1, P_2, P_3 та ймовірності помилкової тривоги $\overline{P_1}, \overline{P_2}, \overline{P_3}$. Поява довільній комбінації при проході порушника (наприклад, 101 - спрацювали перше і третє ЗВ, а друге не спрацювало) відбувається для ЗВ, що працюють на різних фізичних принципах дії і характезується статистичною незалежністю виникнення сигналів тривоги з певною ймовірністю (в даному випадку вона становить $P_{\text{рез}} = P_1 \ (1\text{-}P_2)\, P_3$. Поява тієї ж комбінації від завадового впливу відбудеться з вірогідністю

$$\overline{P_{\text{рез}}} = \overline{P_1}\,(1 - \overline{P_2})\overline{P_3}$$

Всі можливі комбінації для випадку трьох ЗВ представлені в таблиці 2.1.

Таблиця 2.1- Можливі комбінації з трьох ЗВ

	Комбінація	ΔP_j	$\Delta\overline{P}_j$
	111	$P_1\ P_2\ P_3$	$P_1\ P_2\ P_3$
	110	$P_1\ P_2\ (1\text{-}P_3)$	$P_1\ P_2\ (1\text{-}P_3)$
	101	$P_1\ (1\text{-}P_2)P_3$	$P_1\ (1\text{-}P_2)P_3$
	011	$(1\text{-}P_1)P_2P_3$	$(1\text{-}P_1)P_2P_3$
	100	$P_1\ (1\text{-}P_2)(1\text{-}P_3)$	$P_1\ (1\text{-}P_2)(1\text{-}P_3)$
	010	$(1\text{-}P_1)P_2(1\text{-}P_3)$	$(1\text{-}P_1)P_2(1\text{-}P_3)$
	001	$(1\text{-}P_1)(1\text{-}P_2)P_3$	$(1\text{-}P_1)(1\text{-}P_2)P_3$
	000	$(1\text{-}P_1)(1\text{-}P_2)(1\text{-}P_3)$	$(1\text{-}P_1)(1\text{-}P_2)(1\text{-}P_3)$

Тут же для кожної з комбінацій наведені ймовірності їх появи при проході порушника ΔP_j і за наявності завадового впливу ΔP_j (j - номер комбінації).

Імовірність виявлення для схеми логічної обробки 2 з 3 складається з ймовірностей тих комбінацій, в яких присутні дві або три одиниці:

$$P_{2/3} = \sum_{J=0}^{4} \Delta P_J$$

Імовірність помилкової тривоги

$$P_{2/3} = \sum_{J=0}^{4} \Delta \overline{P}_J$$

У разі застосування схеми логічної обробки АБО, коли загальну тривогу КЗВ викличе будь-яка комбінація, окрім восьмої, ймовірність виявлення

$$P_{\text{або}} = \sum_{J=0}^{7} \Delta P_J$$

ймовірність помилкової тривоги

$$P_{\text{або}} = \sum_{J=0}^{7} \Delta \overline{P}_J$$

При синтезі довільної схеми логічної обробки, в якій загальний сигнал тривоги формується при появі будь-якої комбінації з числа наперед заданих (наприклад, тільки у разі появи комбінацій 1, 2 і 5), її вірогідність виявлення і ймовірність помилкової тривоги складуть:

$$P = \sum_{J=0}^{3} \Delta P_J,$$

$$\bar{P} = \sum_{J=0}^{3} \Delta \bar{P}_J$$

де підсумовування проводиться за номерами тих комбінацій з табл. 2.1, які наводять для досліджуваної схеми логічної обробки до формування загального сигналу тривоги. Відзначимо, що безліч комбінацій у табл. 2.1 є повним.

Найкращою схемою логічної обробки КЗВ слід визнати ту, яка при забезпеченні заданої ймовірності виявлення володіє найменшою вірогідністю помилкової тривоги, у зв'язку з чим для синтезу такого алгоритму можна запропонувати наступну процедуру: розставити в табл. 2.1 комбінації в порядку убування відносно ΔP_J / $\Delta \overline{P}_J$, і вибрати з отриманої таблиці стільки перших комбінацій, скільки забезпечують задану ймовірність виявлення. Якщо алгоритм функціонування КЗВ побудувати таким чином, щоб саме ці комбінації приводили до формування загального сигналу тривоги, то зрозуміло, що будь-який алгоритм, що забезпечує не гіршу ймовірність виявлення, володітиме більшою ймовірністю помилкової тривоги, так як він може бути отриманий з вихідного тільки шляхом виключення комбінацій з великим відношенням вкладу в імовірність виявлення до внеску в імовірність помилкової тривоги і включення комбінацій з меншим відношенням.

Запропоновану процедуру пояснює табл. 2.2, в якій всі комбінації розставлені в порядку зменшення величини $\Delta P_J / \Delta \overline{P}_J$ для вибраних значень ймовірностей виявлення та ймовірностей помилкових тривог трьох ЗВ, а саме: $P_1 = 0{,}7$; $P_2 = 0{,}7$; $P_3 = 0{,}99$; $\overline{P_1} = 0{,}1$; $\overline{P_2} = 0{,}2$; $\overline{P_3} = 0{,}01$.

При цьому видно, що при синтезі оптимального алгоритму доцільніше, щоб загальний сигнал тривоги формувався при спрацьовуванні тільки третього ЗВ (j = 4), ніж при спрацьовуванні першого і другого (j= 5), що й обумовлює переваги алгоритму за пропонованою процедурі в порівнянні з алгоритмом 2 з 3. Запропонована схема формування алгоритмів логічної обробки дає в даному випадку (див. табл. 2.2) можливість синтезу семи різних алгоритмів (коли загальний сигнал тривоги викликає появу першої комбінації (j= 1), першою або другою(j = 1 або j = 2) і т. д. Кожен з семи алгоритмів відрізняється своєю імовірністю виявлення і при цьому забезпечує мінімальну ймовірність помилкової тривоги. Велика кількість варіантів побудови вирішального правила (в порівнянні з трьома традиційними: І, 2 з 3, АБО) забезпечує більшу гнучкість при виборі конкретного алгоритму.

Таблиця 2.2 - Комбінації, впорядковані по відношенню $\Delta P_J / \Delta \overline{P}_J$

j	Комбінація	ΔP_J	$\Delta \overline{P}_J$	$\Delta P_J / \Delta \overline{P}_J$
1	111	0,4851	0,0002	2400
2	101	0,2079	0,0008	260
3	011	0,2079	0,0018	116
4	001	0,0891	0,0072	12
5	110	0,0049	0,0198	0,25
6	100	0,0021	0,0792	0,027
7	010	0,0021	0,1782	0,012
8	000	0,0009	0,7128	0,0013

в найбільш важливій галузі між крайніми значеннями характеристик схем логічної обробки І і АБО. На рис. 2.1 показані отримані з табл. 2.2 значення ймовірності виявлення Р і ймовірності помилкових тривог $\overline{P}$, забезпечувані традиційними схемами логічної обробки І, 2 з 3, АБО (з'єднані суцільною лінією) і пропонуються (штрихова лінія). Видно, що досягається позитивний ефект обумовлений тим, що послідовний перехід від точки 1 до 2, від 2 до 3 і т.д. завжди відбувається по прямій з найбільшим тангенсом кута нахилу (в нормальному масштабі), тобто шляхом найбільшого відношення приросту ймовірності виявлення до величини збільшення ймовірності помилкової тривоги. Проведений аналіз показує, що при обробці бінарних сигналів від ЗВ за логічною схемою І доцільно, щоб всі ЗВ забезпечували однакові ймовірності виявлення (а ймовірності помилкових тривог були не гірше заданих). При обробці сигналів від ЗВ за схемою АБО доцільно, щоб (в одиницю часу) збігалися величини ймовірностей помилкових тривог всіх ЗВ, а ймовірності виявлення були б не нижче заданих.

2.3 Присвоєння вагових коефіцієнтів

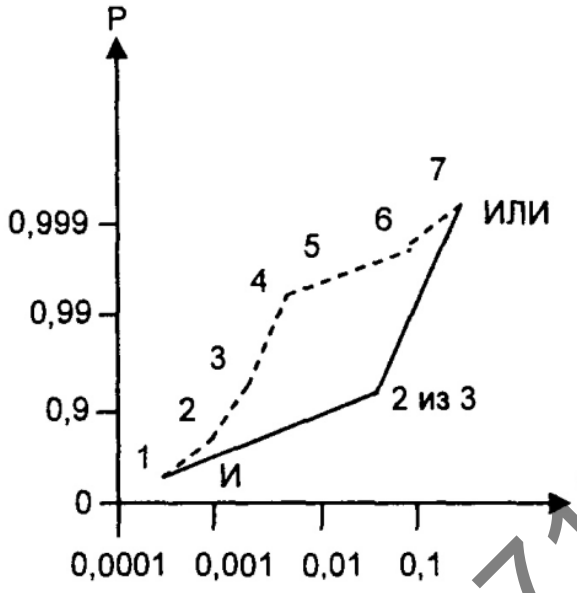

Рисунок 2.4. Графіки залежності P від $\overline{P}$

Розглянемо алгоритм на основі присвоєння кожному ЗВ вагових коефіцієнтів.

Нехай є N розташовані на одному рубежі ЗВ, на виході кожного з яких формується бінарний сигнал u_i, приймає (з певною ймовірністю) або значення u_i =1 (є сигнал тривоги від i-го ЗВ), або значення u_i =0 (сигнал тривоги з і-го ЗВ немає), де і = 1, 2… N. Ці сигнали характеризуються густиною ймовірностей розподілів їх появи при наявності порушника $\omega_{Si}(u_i)$ і за наявності завадового впливу $\omega_{Pi}(u_i)$. Оскільки за наявності порушника сигнал і u_i =1 формується з імовірністю, рівною імовірності виявлення P_i то можна для щільності ймовірності записати:

$$\omega_{Si}(u_i)_{(i=1,2\ldots N)} = \begin{cases} P_i \text{ при } u_i = 1 \\ 1 - P_i \text{ при } u_i = 0 \end{cases} \quad (2.1)$$

Аналогічно щільність ймовірності при наявності завадового впливу:

$$\omega_{Si}(u_i)_{(i=1,2\ldots N)} = \begin{cases} \overline{P_i} \text{ при } u_i = 1 \\ 1 - \overline{P_i} \text{ при } u_i = 0 \end{cases} \quad (2.2)$$

де $\overline{P_J}$ - імовірність помилкової тривоги i-го ЗВ.

Відомо, що оптимальне за критерієм Неймана-Пірсона вирішальне правило може бути записано у вигляді:

$$\log\left(\frac{\omega_{Si}(u_i \dots u_N)}{\omega_{Pi}(u_i \dots u_N)}\right) > C \qquad (2.3)$$

де $\omega_{Si}(u_i \dots u_N)$ - спільна щільність ймовірності сигналів від ЗВ при проході порушника; $\omega_{Pi}(u_i \dots u_N)$ - те ж при наявності завадового впливу; С - довільна постійна, значення якої визначає ймовірність виявлення алгоритму (2.3); $u_i \dots u_N$ - аналізована сукупність сигналів.

При виконанні нерівності (2.3) приймається рішення про наявність порушника (формується загальний сигнал тривоги).

Оптимальність вирішального правила полягає в тому, що при забезпеченні заданої ймовірності виявлення пристрою в цілому *P* (яка регулюється зміною величини С) досягається мінімальна ймовірність помилкової тривоги $\overline{P}$. Якщо всі ЗВ працюють на різних фізичних принципах дії, то сигнали статистично незалежні:

$$\omega_{Si}(u_i \dots u_N) = \prod_{i=1}^{N} \omega_{Si}(u_i),$$

$$\omega_{Pi}(u_i \dots u_N) = \prod_{i=1}^{N} \omega_{Pi}(u_i)$$

Тоді вирішальний правило може бути записано у вигляді:

$$\sum_{j=1}^{N} \log\left(\frac{\omega_{Si}(u_i)}{\omega_{Pi}(u_i)}\right) > C.$$

Віднімаючи з обох частин нерівності одну і ту ж постійну величину

$$\sum_{j=1}^{N} \log\left(\frac{1-(P_i)}{1-\overline{P}}\right) > C$$

і вводячи нове позначення :

$$C_1 = C - \sum_{j=1}^{N} \log\left(\frac{1-(P_i)}{1-\overline{P}}\right),$$

отримаємо

$$\sum_{j=1}^{N} \log\left(\frac{\omega_{Si}(u_i)(1-P_i)}{\omega_{Si}(u_i)(1-\overline{P})}\right) > C_1.$$

Після чого можна остаточно написати вирішальне правило у вигляді:

$$\sum_{i=1}^{N} V_i(u_i) > C_1 \qquad (2.4)$$

Якщо виконується нерівність (2.4), то формується загальний сигнал тривоги. При цьому з (2.1) і (2.2) видно:

$$V_i(u_i)_{(i=1,2\ldots N)} = \begin{cases} q_i & \text{при } u_i = 1 \\ 0 & \text{при } u_i = 0 \end{cases} \qquad (2.5)$$

де $q_i = \frac{P_i(1-\overline{P_i})}{\overline{P_i}(1-P_i)}$ постійна для i - го ЗВ величина.

Таким чином, оптимальний у зазначеному сенсі алгоритм побудови КЗВ згідно (2.4) і (2.5) полягає у формуванні за сигналом тривоги від i-го ЗВ сигналу заданої амплітуди q_i і тривалості τ (τ - час пам'яті) з наступним підсумовуванням сигналів і порівнянням одержуваної суми з фіксованим пороговим рівнем, перевищення якого призводить до формування загального сигналу тривоги.

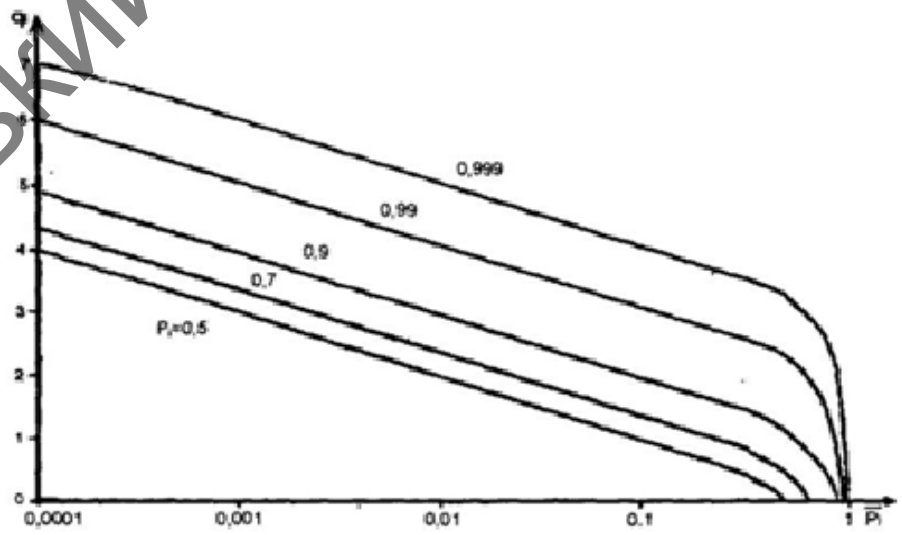

Рисунок 2.5. Графік залежності P_i від $\overline{P_i}$

Значення q_i можуть бути розраховані заздалегідь за ймовірністю виявлення P_i і ймовірності помилкової тривоги $\overline{P_i}$ і-го ЗВ. На рис. 2.5. наведені графіки залежностей «ваги» до ЗВ від його характеристик P_i і $\overline{P_i}$. Видно, що «вага» ЗВ тим більше, чим більше його вірогідність виявлення і чим менше його ймовірність помилкової тривоги.

2.3.1. Простота реалізації

Неважко переконатися, що цей алгоритм повністю ідентичний описаному раніше алгоритму впорядкування комбінацій по величині відношення$\Delta P_J/\ \Delta\overline{P_J}$, однак має більш простий вигляд і зручніше для практичної реалізації. При цьому, незважаючи на те, що загальний сигнал тривоги формується при перевищенні заданого порогового рівня сумою сигналів тривоги від окремих ЗВ (2.4), кожен з яких має свою амплітуду (2.5), зберігається логічний алгоритм КЗВ, тому що при заданій величині порогового рівня перевищення його можуть викликати лише певні комбінації сигналів тривоги від окремих ЗВ. Відзначимо, що значення (2.5) визначені з точністю до постійного множника, тобто алгоритм не зміниться, якщо всі q_i одночасно збільшити або зменшити в одно і те ж число раз (змінивши в те ж число раз значення порогу C_1).

2.3.2 Оптимальність алгоритму

Алгоритм (2.4) і (2.5) завжди оптимальний, тобто при заданій імовірності виявлення забезпечує мінімально можливу (на даному рівні інформації) ймовірність помилкової тривоги, що безпосередньо випливає з вихідного виразу (2.3). Відзначимо також, що той же алгоритм забезпечує і максимально можливу вірогідність виявлення при заданій імовірності помилкових тривог. Іншими словами, неможливо синтезувати алгоритм, який поліпшував б одну з двох вказаних характеристик (у порівнянні з алгоритмом (2.4) і (2.5)), не погіршуючи одночасно іншу.

Схеми логічної обробки K із N з перерахунком використовують додаткову інформацію про послідовність надходження сигналів тривоги від окремих ЗВ при проході порушника, тобто цей принцип може бути використаний і в

пропонованому алгоритмі для додаткового зменшення ймовірності помилкової тривоги.

Зміна порогового рівня C_1 дозволяє встановлювати різні ймовірності виявлення алгоритму в цілому. При цьому в загальному випадку забезпечується (2^N-1) різних градацій, в той час як традиційні схеми логічної обробки K із N забезпечують тільки N різних градацій (K = 1,2, ..., N). Установка порогового рівня C_1 в межах

$$\sum_{i=1}^{N} q_i - \min q_i < C_1 < \sum_{i=1}^{N} q_i$$

дає алгоритм, тотожний алгоритмом I (N з N), що забезпечує гранично низьку ймовірність помилкової тривоги, але і невисоку ймовірність виявлення. Інше крайнє значення розглянутого алгоритму $0 < C_1 < \sum_{i=1}^{N} q_i$ тотожне алгоритму АБО (1 з N), що забезпечує гранично високу ймовірність виявлення, а й високу ймовірність помилкової тривоги. Таким чином, велике число градацій алгоритму (2.4) і (2.5) знаходиться в найбільш важливою для практичних застосувань області між схемами I і АБО, що полегшує підбір конкретного значення порогового рівня C_1, забезпечує задані характеристики КЗВ. Причому, в процесі підбору значення C_1 для заданої ймовірності виявлення мінімальна ймовірність помилкової тривоги буде забезпечена автоматично.

Те ж саме відноситься і до можливості регулювання характеристик КЗВ в умовах експлуатації (наприклад, у зв'язку зі зміною тактичної обстановки) шляхом зміни порогового рівня C_1 в межах $0 < C_1 < \sum_{i=1}^{N} q_i$, Що забезпечує оптимальність алгоритму для будь-якого значення C_1.

2.3.3 Спрощення алгоритму в окремих випадках

У випадку, якщо функція втрат лінійна, сумарні втрати

$$L = L_1 V_1 (1 - P) + L_2 V_2 \bar{P}$$

де $\bar{P}$-ймовірність помилкової тривоги; $(1 - P)$ - ймовірність пропуску порушника; V_1, V_2- частота появи порушника і помехового впливу відповідно; L_1, L_2 - втрати від одного пропуску і помилкової тривоги відповідно.

При необхідності забезпечити мінімум втрат його легко отримати шляхом диференціювання. Величина відношення правдоподібності

$$\frac{dP(\bar{P})}{dP} = \frac{\omega_S}{\omega_P} = \frac{L_2 V_2}{L_1 V_1}$$

повинна бути постійною, тобто відповідно до (2.3) пороговий рівень С повинен бути незмінним (при заміні одного ЗВ іншим, при виході частини ЗВ з ладу, при включенні до складу КЗВ додаткових ЗВ і т.п.).

2.3.4 Надійність алгоритму

Найбільш складним є вибір значення параметра C_1 у вирішальному правилі (2.4) таким чином, щоб забезпечувалася задана ймовірність виявлення Р (або ймовірність помилкової тривоги $\bar{P}$). Зв'язок цих параметрів записується у вигляді:

$$P = \sum \omega_s (u_1, u_2, \dots, u_N)$$
$$\bar{P} = \sum \omega_P (u_1, u_2, \dots, u_N) \qquad (2.6)$$

де підсумовування проводиться за тими комбінаціями $u_1, u_2, \dots u_N$ для яких виконується нерівність (2.4). Для випадку необхідності якісної оцінки значень імовірнісних характеристик алгоритму за значенням параметра C_1 неважко отримати оцінку, скориставшись тим, що виконання нерівності (2.4) тотожне виконання (2.3) і тотожне виконання нерівності $\frac{\omega_s(u)}{\omega_P(u)} > A$, де

$$A = 10^C = 10^{C_1 + \sum_{j=1}^{N} \log \frac{1-P_j}{1-\bar{P}_j}}$$

Тоді неважко отримати:

$$\frac{P}{\bar{P}} = \frac{\sum \omega_S}{\sum \omega_P} > A$$

або остаточно:

$$\bar{P} = \frac{1}{A} = \frac{1}{C_1 + \sum_{i=1}^{N} \lg \frac{1-P_i}{1-\bar{P}_i}}$$

Аналогічно легко отримати:

$$\frac{1-\mathrm{P}}{1-\overline{\mathrm{P}}} \geq \frac{1}{\mathrm{A}}$$

або для ймовірності пропуску порушника:

$$1 - P \leq 10^{C_1 + \sum_{j=1}^{N} \log \frac{1-P_j}{1-\overline{P_j}}}$$

Слід зазначити, що отримані нерівності виконуються зазвичай з великим запасом (права і ліва частини відрізняються на порядок і більше). У разі визначення точного зв'язку характеристик P і $\bar{P}$ з параметром зміни величини порогового рівня C_1 необхідно користуватися більш складними в обчислювальному плані співвідношеннями (2.6) з урахуванням (2.4).

2.4 Використання метода динамічного програмування для забезпечення мінімальної хибної тривоги для заданої ймовірності правильного виявлення загрози і вартості комплексної системи охорони

Ефективність можна подати у вигляді:

$$E_i = 1 - \sum_{j=1}^{n_i} \Delta \bar{P}_j^i \qquad (2.7)$$

де $\Delta \bar{P}_j^i$ – упорядкований добуток із i - ймовірностей,

$$(f_i(n))_i \sum_{j=1}^{n} \Delta P \leq P_{\text{рез}} \qquad (2.8)$$

Припустимо, що початковий варіант системи комплексного захисту передбачає безліч давачів, розташованих в кожній зоні охорони таким чином, щоб забезпечити супернадійну охорону. Зрозуміло, що ціна такого вибору занадто велика:

$$C_i \gg C \qquad (2.9)$$

і потребує суттєвого зменшення кількості давачів. Робитиме таке зменшення покроковим методом динамічного програмування. На кожному і- му кроці будемо по черзі прибирати один із давачів і відшукувати всі

$$E_{i-1} = 1 - \sum_{j=1}^{n_{i-1}} \Delta \bar{P}_j^i$$

які призводять до найменшого зменшення

$$\Delta E_i = E_i - E_{i-1}$$

Таким чином на кожному кроці управління ми будемо виключати той давач, який зменшує ефективність системи найменшим чином. Будемо це робити до тих пір, поки

$$C_{i\,min} \leq C \qquad (2.10)$$

Оскільки початкова ефективність (2.7) є максимальною, кожний крок управління $u_1, u_2, \ldots u_{i-i_{min}}$, який відповідає викресленню з загальної системи того, або іншого давача відповідає принципам оптимальності Белмана [1], а завдання вирішено так, що залащаться саме кращі давачі, які виявлятиме порушника із заданою ймовірністю $P_{\text{рез}}$ і мінімальною ймовірністю хибної тривоги

$$\overline{P_{\text{рез}}} = \sum_{j=1}^{n_{i\,\min}} \Delta \overline{P_J^{i\,\min}} \qquad (2.11)$$

2.4.1 Вирішення задачі

Згідно з алгоритмом проведемо розрахунок ймовірності виявлення та ймовірності хибної тривоги для приміщення. В ньому знаходиться 5 давачів (3 давачі руху, 1 звуковий давач і 1 магніторконтактний давач).У таблиці 2.3 подані ймовірності виявлення та хибної тривоги для кожного з давачів.

Вирішимо задачу оптимізації для абстрактного приміщення.

Таблиця 2.3 - Розрахунок ймовірності виявлення та ймовірності хибної тривоги для приміщення

№ давача	Ймовірність виявлення	Ймовірність помилкового спрацювання
1	0,78	0,0001
2	0,8	0,0002
3	0,75	0,00025
4	0,9	0,0003

5	0,95	0,0004

$$\Delta P_j = \prod_{i=1}^{5}(1 + 2K_iP_i - K_i - P_i)$$

$$\overline{\Delta P_j} = \prod_{i=1}^{5}(1 + 2K_iP_i - K_i - P_i)$$

Таблиця 2.4 - Розрахунок хибної тривоги

Комбінаця	ΔP_J	$\Delta \overline{P_J}$	$\Delta P_J / \Delta \overline{P_J}$	Правильне виявлення	Хибна тривога
11111	0,40014	$6*10^{-19}$	$6,7*10^{17}$	0,40014	$6*10^{-19}$
11011	0,13338	$2,3994*10^{-15}$	$5,6*10^{13}$	0,53352	$2,4*10^{-15}$
10111	0,100035	$2,9994*10^{-15}$	$3,3*10^{13}$	0,633555	$5,3994*10^{-15}$
11101	0,04446	$1,9994*10^{-15}$	$2,2*10^{13}$	0,678015	$7,3988*10^{-15}$
01111	0,11286	$5,9994*10^{-15}$	$1,9*10^{13}$	0,790875	$1,33982*10^{-14}$
11110	0,02106	$1,4994*10^{-15}$	$1,4*10^{13}$	0,811935	$1,48976*10^{-14}$
10011	0,033345	$1,19946*10^{11}$	$2,8*10^{9}$	0,84528	$1,20095*10^{-11}$
11001	0,01482	$7,9956*10^{-12}$	$1,9*10^{9}$	0,8601	$2,00051*10^{-11}$
01011	0,03762	$2,39916*10^{-11}$	$1,6*10^{9}$	0,89772	$4,39967*10^{-11}$
11010	0,00702	$5,9961*10^{-12}$	$1,2*10^{9}$	0,90474	$4,99928*10^{-11}$
10101	0,011115	$9,995*10^{-12}$	$1,1*10^{9}$	0,915855	$5,99878*10^{-11}$
00111	0,028215	$2,9991*10^{-11}$	$9,4*10^{8}$	0,94407	$8,99788*10^{-11}$
10110	0,005265	$7,4955*10^{-12}$	$7*10^{8}$	0,949335	$9,74743*10^{-11}$
01101	0,01254	$1,9992*10^{-11}$	$6,3*10^{8}$	0,961875	$1,17466*10^{-10}$
11100	0,00234	$4,9965*10^{-12}$	$4,7*10^{8}$	0,964215	$1,22463*10^{-10}$
01110	0,00594	$1,49925*10^{-11}$	$4*10^{8}$	0,970155	$1,37455*10^{-10}$
10001	0,003705	$3,997*10^{-8}$	92694,5	0,97386	$4,01075*10^{-8}$

00011	0,009405	$1{,}19934*10^{-7}$	78418,1	0,983265	$1{,}60041*10^{-7}$
10010	0,001755	$2{,}99745*10^{-8}$	58549,8	0,98502	$1{,}90016*10^{-7}$
01001	0,00418	$7{,}9948*10^{-8}$	52284	0,9892	$2{,}69964*10^{-7}$
11000	0,00078	$1{,}9981*10^{-8}$	39037,1	0,98998	$2{,}89945*10^{-7}$
01010	0,00198	$5{,}9955*10^{-8}$	33024,8	0,99196	$3{,}499*10^{-7}$
00101	0,003135	$9{,}994*10^{-8}$	31368,8	0,995095	$4{,}4984*10^{-7}$
10100	0,000585	$2{,}49775*10^{-8}$	23421,1	0,99568	$4{,}74818*10^{-7}$
00110	0,001485	$7{,}49475*10^{-8}$	19813,9	0,997165	$5{,}49765*10^{-7}$
01100	0,00066	$4{,}996*10^{-8}$	13210,6	0,997825	$5{,}99725*10^{-7}$
00001	0,00045	0,00039966	2,61472	0,99887	0,0004006
10000	0,000195	$9{,}9885*10^{-5}$	1,95224	0,99905	0,000500145
00010	0,000495	0,000299715	1,65157	0,99956	0,00079986
01000	0,00022	0,00019979	1,10116	0,99978	0,00099965
00100	0,000165	0,00024975	0,66066	0,999945	0,0012494
00000	0,000055	0,9987506	$5{,}5*10^{-5}$	1	1

Задавшись мінімальним коефіцієнтом виявлення 0.99 виберемо найбільш ефективні комбінації.

На першому кроці оптимізації викреслюємо по черзі кожен давач з 1,2,3,4,5.

У таблиці 2.5 наведені результати змін у системі безпеки при викресленні давача №1, у таблиці 2.6 – давача №2, у таблиці 2.7 – давача №3, у таблиці 2.8 – давача №4 , у таблиці 2.9 – давача №5.

Таблиця 2.5- для викресленого давача № 1

Комбінації	ΔP_J	$\Delta \bar{P}_J$	$\Delta P_J / \Delta \bar{P}_J$	Правильне виявлення	Хибна тривога
1111	0,513	$6*10^{-15}$	$8{,}55*10^{13}$	0,513	$6*10^{-15}$
1011	0,171	$2{,}3994*10^{-11}$	7126781695	0,684	$2{,}4*10^{-11}$
0111	0,12825	$2{,}9994*10^{-11}$	4275855171	0,81225	$5{,}3994*10^{-11}$
1101	0,057	$1{,}9994*10^{-11}$	2850855257	0,86925	$7{,}3988*10^{-11}$
1110	0,027	$1{,}4994*10^{-11}$	1800720288	0,89625	$8{,}8982*10^{-11}$

0011	0,0275	$1,19946*10^{-7}$	356410,3668	0,939	$1,20035*10^{-7}$
1001	0,019	$7,9956*10^{-8}$	237630,6791	0,958	$1,99991*10^{-7}$
1010	0,009	$5,9961*10^{-8}$	150097,5484	0,967	$2,59952*10^{-7}$
0101	0,01425	$9,995*10^{-8}$	142571,2771	0,98125	$3,59902*10^{-7}$
0110	0,00675	$7,4955*10^{-8}$	90054,02521	0,988	$4,34857*10^{-7}$
1100	0,003	$4,9965*10^{-8}$	60042,02221	0,991	$4,84822*10^{-7}$
0001	0,00475	0,0003997	11,88391073	0,99575	0,000400185
0010	0,00225	0,000299745	7,506378696	0,998	0,00069993
1000	0,001	0,00019981	5,004753039	0,999	0,00089974
0100	0,00075	0,000249775	3,002701651	0,99975	0,001149515
0000	0,00025	0,998850485	0,000250288	1	1

Таблиця 2.6. для викресленого давача № 2

Комбінації	ΔP_J	$\Delta \overline{P}_J$	$\Delta P_J / \Delta \overline{P}_J$	Правильне виявлення	Хибна тривога
1111	0,500175	$3*10^{-15}$	$1,6673*10^{14}$	0,500175	$3*10^{-15}$
1011	0,166725	$1,1997*10^{-11}$	$1,3897*10^{10}$	0,6669	$1,2*10^{-11}$
1101	0,055575	$9,99710^{-12}$	5559167750	0,722475	$2,2*10^{-11}$
0111	0,141075	$2,999710^{-11}$	4702970297	0,86355	$5,2*10^{-11}$
1110	0,026325	$7,49710^{-12}$	3511404562	0,889875	$5,95*10^{11}$
1001	0,018525	$3,9978*10^{-8}$	463379,824	0,9084	$4*10^{-8}$
0011	0,047025	$1,1996*10^{-7}$	392012,194	0,955425	$1,6*10^{-7}$
1010	0,008775	$2,9981*10^{-8}$	292690,219	0,9642	$1,9*10^{-7}$
0101	0,015675	$9,996*10^{-8}$	156812,72	0,979875	$2,9*10^{-7}$
1100	0,002925	$2,4983*10^{-8}$	117081,943	0,9828	$3,15*10^{-7}$
0110	0,007425	$7,4963*10^{-8}$	99049,5208	0,990225	$3,9*10^{-7}$
0001	0,005225	0,00039974	13,0709944	0,99545	0,0004
1000	0,000975	9,9905E-05	9,75926843	0,996425	0,0005
0010	0,002475	0,00029978	8,25619078	0,9989	0,0008
0100	0,000825	0,0002498	3,30264149	0,999725	0,00105
0000	0,000275	0,99895039	0,00027529	1	1

Таблиця 2.7. для викресленого давача № 3

Комбінації	ΔP_J	$\Delta \overline{P}_J$	$\Delta P_J / \Delta \overline{P}_J$	Правильне виявлення	Хибна тривога
1111	0,53352	$2,4*10^{-15}$	$2,223*10^{14}$	0,53352	$2,4*10^{-15}$
1011	0,13338	$1,2*10^{-11}$	$1,1117*10^{10}$	0,6669	$1,2*10^{-11}$
1101	0,05928	$7,998*10^{-12}$	7412223667	0,72618	$1,99976*10^{-11}$
0111	0,15048	$2,4*10^{-11}$	6270627063	0,87666	$4,39952*10^{-11}$
1110	0,02808	$5,998*10^{-12}$	4681872749	0,90474	$4,99928*10^{-11}$
1001	0,01482	$3,998*10^{-8}$	370685,32	0,91956	$4,003*10^{-8}$

0011	0,03762	$1,2*10^{-7}$	313594,072	0,95718	$1,59994*10^{-7}$
1010	0,00702	$2,998*10^{-8}$	234140,466	0,9642	$1,89976*10^{-7}$
0101	0,01672	$7,997*10^{-8}$	209083,627	0,98092	$2,69944*10^{-7}$
1100	0,00312	$1,999*10^{-8}$	156109,258	0,98404	$2,8993*10^{-7}$
0110	0,00792	$5,997*10^{-8}$	132066,028	0,99196	$3,499*10^{-7}$
0001	0,00418	0,0003998	10,4562726	0,99614	0,00040011
1000	0,00078	$9,991*10^{-5}$	7,80702429	0,99692	0,00050002
0010	0,00198	0,0002998	6,60462231	0,9989	0,00079981
0100	0,00088	0,0001998	4,40352198	0,99978	0,00099965
0000	0,00022	0,9990003	0,00022022	1	1

Таблиця 2.8. для викресленого давача № 4

Комбінації	ΔP_j	$\Delta \bar{P}_j$	$\Delta P_j / \Delta \bar{P}_j$	Правильне виявлення	Хибна тривога
1111	0,4446	$2*10^{-15}$	$2,223*10^{14}$	0,4446	$2*10^{-15}$
1101	0,1482	$8*10^{-12}$	18529632408	0,5928	$8*10^{-12}$
1011	0,11115	$1*10^{-11}$	11117223445	0,70395	$1,7998*10^{-11}$
1110	0,0234	$5*10^{-12}$	4681872749	0,72735	$2,2996*10^{-11}$
1001	0,03705	$4*10^{-8}$	926666,9538	0,7644	$4,0005*10^{-8}$
1100	0,0078	$2*10^{-8}$	390253,6258	0,7722	$5,9992*10^{-8}$
1010	0,00585	$2,5*10^{-8}$	234140,4655	0,77805	$8,4977*10^{-8}$
1000	0,00195	$9,99*10^{-5}$	19,51658461	0,78	$1*10^{-4}$
0111	0,1254	$2*10^{-11}$	6270627063	0,9054	0,0001
0101	0,0418	$8*10^{-8}$	522682,926	0,9472	0,00010008
0011	0,03135	$1*10^{-7}$	313594,0719	0,97855	0,00010018
0110	0,0066	$5*10^{-8}$	132066,0277	0,98515	0,00010023
0001	0,01045	0,0004	26,13937417	0,9956	0,00050001
0100	0,0022	0,0002	11,00825437	0,9978	0,00069986
0010	0,00165	0,00025	6,604622311	0,99945	0,000949685
0000	0,00055	0,99905	0,000550523	1	1

Таблиця 2.9. для викресленого давача № 5

Комбінації	ΔP_j	$\Delta \overline{P}_j$	$\Delta P_j / \Delta \overline{P}_j$	Правильне виявлення	Хибна тривога
1111	0,4212	$1,5*10^{-15}$	$2,81*10^{14}$	0,4212	$1,5*10^{-15}$
1101	0,1404	$6*10^{-12}$	2,34E+10	0,5616	$6*10^{-12}$
1011	0,1053	$7,5*10^{-15}$	1,4E+10	0,6669	$1,35*10^{-11}$
1110	0,0468	$5*10^{-12}$	9,36E+09	0,7137	$1,85*0^{-11}$
0111	0,1188	$1,5*10^{-11}$	7,92E+09	0,8325	$3,35*10^{-11}$
1001	0,0351	$3*10^{-8}$	1170527	0,8676	$3*10^{-8}$
1100	0,0156	$2*10^{-8}$	780429,2	0,8832	$5*10^{-8}$
0101	0,0396	$6*10^{-8}$	660231,1	0,9228	$1,1*10^{-7}$
1010	0,0117	$2,5*10^{-8}$	468234,1	0,9345	$1,35*10^{-7}$
0011	0,0297	$7,5*10^{-8}$	396118,8	0,9642	$2,1*10^{-7}$
0110	0,0132	$5*10^{-8}$	264105,6	0,9774	$2,6*10^{-7}$
1000	0,0039	$9,99*10^{-5}$	39,02926	0,9813	0,0001
0001	0,0099	0,0003	33,01816	0,9912	0,0004
0100	0,0044	0,0002	22,01431	0,9956	0,0006
0010	0,0033	0,00025	13,20792	0,9989	0,00085
0000	0,0011	0,99915	0,001101	1	1

Порівняння ефективність між нульовим і першим кроком				
1	2	3	4	5
$1,349*10^{-8}$	$3,9981*10^{-8}$	0	0,00049966	0,00039967

Викреслюємо на першому кроці оптимізації давач під номером 3, оскільки його ефективність найменша. У таблиці 2.10 – 2.13 подані результати оптимізації системи на другому кроці.

На другому кроці оптимізації викреслюємо по черзі кожен давач з 1,2,4,5.

Таблиця 2.10. для викресленого давача № 5

Комбінації	ΔP_j	$\Delta \overline{P}_j$	$\Delta P_j / \Delta \overline{P}_j$	Правильне виявлення	Хибна тривога
111	0,5616	$6*10^{-12}$	93600000000	0,5616	$6*10^{-12}$
101	0,1404	$2,9994*10^{-8}$	4680936,187	0,702	$3*10^{-8}$
110	0,0624	$1,9994*10^{-8}$	3120936,281	0,7644	$5*10^{-8}$
011	0,1584	$5,9994*10^{-8}$	2640264,026	0,9228	$1,1*10^{-7}$
100	0,0156	$9,995*10^{-5}$	156,0780297	0,9384	0,0001
001	0,0396	0,00029991	132,0396092	0,978	0,0004
010	0,0176	0,00019992	88,03521144	0,9956	0,0006
000	0,0044	0,99940011	0,004402641	1	1

Таблиця 2.11. для викресленого давача № 4

Комбінації	ΔP_j	$\Delta \overline{P}_j$	$\Delta P_j / \Delta \overline{P}_j$	Правильне виявлення	Хибна тривога
111	0,5928	$8*10^{-12}$	74100000000	0,5928	$8*10^{-12}$
101	0,1482	$3,9992*10^{-8}$	3705741,148	0,741	$4*10^{-8}$
011	0,162	$7,9992*10^{-8}$	2090209,021	0,9082	$1,1999*10^{-7}$
110	0,0312	$1,9992*10^{-8}$	1560624,25	0,9394	$1,3998*10^{-7}$
001	0,0418	0,00039988	104,5313573	0,9812	0,00040002
100	0,0078	$9,994*10^{-5}$	78,04682185	0,989	0,00049996
010	0,0088	0,0001999	44,02200924	0,9978	0,00069986
000	0,0022	0,99930014	0,002201541	1	1

Таблиця 2.12. для викресленого давача № 2

Комбінації	ΔP_j	$\Delta \overline{P}_j$	$\Delta P_j / \Delta \overline{P}_j$	Правильне виявлення	Хибна тривога
111	0,6669	$1,2*10^{-11}$	$5,56*10^{10}$	0,6669	$1,2*10^{-11}$
101	0,0741	$3,9988*10^{-8}$	1853056	0,741	$4*10^{-8}$
011	0,1881	$1,19988*10^{-7}$	1567657	0,9291	$1,6*10^{-7}$
110	0,0351	$2,9988*10^{-8}$	1170468	0,9642	$1,9*10^{-7}$
001	0,0209	0,00039984	52,27091	0,9851	0,0004
100	0,0039	$9,993*10^{-5}$	39,02731	0,989	0,0005
010	0,0099	0,00029985	33,01651	0,9989	0,0007998
000	0,0011	0,99920019	0,001101	1	1

Таблиця 2.13 для викресленого давача № 1

Комбінації	ΔP_j	$\Delta \overline{P}_j$	$\Delta P_j / \Delta \overline{P}_j$	Правильне виявлення	Хибна тривога
111	0,684	$1,2*10^{-11}$	$5,7*10^{10}$	0,684	$1,2*10^{-11}$
101	0,076	$3,9988*10^{-8}$	1900570	0,76	$4*10^{-8}$
011	0,171	$1,19988*10^{-7}$	1425143	0,931	$1,6*10^{-7}$
110	0,036	$2,9988*10^{-8}$	1200480	0,967	$1,9*10^{-7}$
001	0,019	0,00039984	47,51901	0,986	0,0004
100	0,004	$9,993*10^{-5}$	40,02801	0,99	0,0005
010	0,009	0,00029985	30,01501	0,999	0,0008
000	0,001	0,99920019	0,001001	1	1

Порівняння ефективність між першим і другим кроком			
1	2	4	5
0,00049961	0,00079946	0,00069951	0,00059954

На другому кроці оптимізації відкинемо давач під номером 1

На третьму кроці оптимізації викреслюємо по черзі кожен давач з 2,4,5

Таблиця 2.14. для викресленого давача № 5

Комбінації	ΔP_j	$\Delta \overline{P}_j$	$\Delta P_j / \Delta \overline{P}_j$	Правильне виявлення	Хибна тривога
11	0,72	$6*10^{-8}$	12000000	0,72	$6*10^{-8}$
01	0,18	0,00029994	600,120024	0,9	0,0003
10	0,08	0,00019994	400,120036	0,98	0,00049994
00	0,02	0,99950006	0,020010004	1	1

Таблиця 2.15 для викресленого давача № 4

Комбінації	ΔP_j	$\Delta \overline{P}_j$	$\Delta P_j / \Delta \overline{P}_j$	Правильне виявлення	Хибна тривога
11	0,76	$8*10^{-8}$	9500000	0,76	$8*10^{-8}$
01	0,19	0,0003999	475,095019	0,95	0,0004
10	0,04	0,0001999	200,080032	0,99	0,00059992
00	0,01	0,9994001	0,010006003	1	1

Таблиця 2.16 для викресленого давача № 2

Комбінації	ΔP_j	$\Delta \overline{P}_j$	$\Delta P_j / \Delta \overline{P}_j$	Правильне виявлення	Хибна тривога
11	0,855	$1,2*10^{-7}$	7125000	0,855	$1,2*10^{-7}$
10	0,095	0,0004	237,5712714	0,95	0,0004
01	0,045	0,0003	150,06002	0,995	0,00069988
00	0,005	0,9993	0,005003502	1	1

Порівняння ефективність між другим і третім кроком		
2	4	5
0,00019992	$9,996*10^{-5}$	0,9995

Викреслюємо на третьму кроці оптимізації давач під номером 4.

Якщо при однаковій ціні на давачі грошей вистачає лише на два, то краще залишити давачі 2 і 5.

РОЗДІЛ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В АНТИМОНОПОЛЬНОМУ КОМІТЕТІ УКРАЇНИ

3.1.Опис ІТС АМКУ

До складу комплексу технічних засобів (далі – КТЗ) обчислювальної системи ІТС-АМКУ входять:

- сервери;
- робочі станції (далі - РС);
- системи зберігання даних;
- кероване та некероване комутаційне обладнання;
- шлюзи захисту;
- міжмережевий екран;
- термінали відеоконференцзв’язку та панелі для відображення відео;
- апаратно-програмні засоби (далі - АПЗ) криптографічного захисту інформації (КЗІ);
- пристрої друку.

За функціональним призначенням сервери ІТС-АМКУ поділяються на:

- сервери контролерів домену;
- поштові сервери;
- сервери технологічного ЦСК;
- сервери системи документообігу;
- сервери реєстру державної допомого суб’єктам господарювання;
- сервери фінансово-кадрової системи;
- сервери системи "Концентрація";
- сервери інформаційно-правових систем;
- сервери резервного копіювання;
- сервери відеоконференцій;
- сервери спільного доступу до файлів та директорій;
- сервери антивірусного захисту;

– сервер технологічного ЦСК;

– сервери друку.

Сервери контролерів домену (Microsoft Active Directory) призначено для централізованого керування доменними обліковими записами користувачів, ресурсами домена та налаштуваннями (у т.ч. налаштуваннями безпеки) операційних системам (далі - ОС) РС, введених до його складу. Основний контролер домена також виконує функцію DNS та DHCP сервера.

Поштовий сервер призначено для підтримки функціонування підсистеми корпоративної електронної пошти АМКУ, яка забезпечує прийом, зберігання та відправку поштових повідомлень.

Сервери технологічного ЦСК призначено для обслуговуванням сертифікатів відкритих ключів (далі – сертифікатів) мережного обладнання ІТС-АМКУ, засобів КЗІ та інших потреб АМКУ. Таке обслуговування включає:

– реєстрацію користувачів;

– сертифікацію відкритих ключів користувачів;

– управління статусом сертифікатів;

– генерацію відкритих та особистих ключів користувачів.

Сервери документообігу забезпечують функціонування системи внутрішнього документообігу, а також ведення БД документообігу ІТС-АМКУ.

Сервери ФПЗ кадрів та бухгалтерії призначено для роботи системного та функціонального ПЗ, яке реалізує бізнес-логіку обробки інформації щодо бухгалтерського обліку та кадрового діловодства ІТС-АМКУ. На цих серверах також розміщується СКБД система бухгалтерського обліку та кадрового діловодства (далі – фінансово-кадрова система). На даних серверах розміщається серверна частина ФПЗ фінансово-кадрової підсистеми з метою надання доступу до інформації користувачам відповідно до посадових

обов'язків. Доступ до цих серверів отримують тільки користувачі фінансово-кадрової системи.

Сервери реєстру державної допомого суб’єктам господарювання призначені для автоматизації процесів контролю та моніторингу державної допомоги. На цих серверах розміщується:

– портал державної допомоги, що дозволяє отримувати дані Повідомлень з веб-форм передавати їх для реєстрації та опрацювання до Системи електронного документообігу та накопичувати дані;

– бази даних реєстру державної допомоги, яка містить всю необхідну інформацію про надавачів та отримувачів державної допомоги, програми державної допомоги, індивідуальну державну допомогу з аналітичними інструментами та генераторами звітів для контролю та моніторингу державної допомоги, прийняття управлінських рішень;

– внутрішній портал Департаменту моніторингу та контролю державної допомоги АМКУ (далі ДМКДД), який призначено для підвищення ефективності внутрішніх процесів ДМКДД.

Сервери інформаційно-правових підсистем призначені надання користувачам ІТМ-АМКУ можливостей щодо пошуку та аналізу та систематизації правової інформації, що використовується в процесі виконання посадових обов’язків.

Сервер резервного копіювання призначено для зберігання резервних копій інформаційних баз даних, а також резервні копії операційних середовищ фізичних серверів.

Сервер спільного доступу до файлів та директорій призначено для надання користувачам ІТС-АМКУ віддаленого доступу до файлів та принтерів за протоколом SMB, FTP, а також для керування правами доступу користувачів до цих ресурсів.

Сервер антивірусного захисту призначено для централізованого керування програмним забезпеченням (далі - ПЗ) антивірусного захисту в складі ІТС-АМКУ.

Сервер друку забезпечує контрольований доступ користувачів до мережевих принтерів, а також здійснює автентифікацію користувачів при спробі друку документів.

Сервер технологічного ЦСК призначено для обслуговуванням сертифікатів відкритих ключів (далі – сертифікатів) для організації захищених каналів обміну центрального апарата з територіальними відділеннями та інших потреб АМКУ. Таке обслуговування включає:

- реєстрацію користувачів;
- сертифікацію відкритих ключів користувачів;
- управління статусом сертифікатів;
- генерацію відкритих та особистих ключів користувачів.

Сервери системи "Концентрація" призначено для накопичення, обробки та видачі інформації ФПЗ системи "Концентрація", що розміщується на РС користувачів. Дані між серверами БД синхронізуються з використанням механізму реплікації для збільшення доступності цих серверів.

Міжмережевий екран призначено для захисту компонентів ІТС-АМКУ від мережевих атак з боку зловмисників та шкідливого ПЗ. У якості міжмережного екрану повинен використовуватись технічний засіб, що має позитивний експертний висновки Держспецзв'язку у сфері технічного захисту інформації (далі – ТЗІ).

Джерела безперебійного живлення (автоматичні пристрої електроживлення) призначені для забезпечення безперебійного постачання електричною енергією компонентів ІТС в межах норми (у випадках стрибків напруги або повного відключення електроенергії).

Комунікаційне обладнання – мережні керовані та некеровані пристрої (активне мережне обладнання), що призначені для забезпечення обміну інформацією між компонентами ІТС-АМКУ.

Адміністратори та користувачі у складі відповідних структурних підрозділів АМКУ мають вільний доступ до мережі Інтернет, сервери зі складу ІТС-АМКУ мають вихід у мережу Інтернет з метою отримання оновлень ОС та програмного забезпечення.

Узагальнена структурна схема КТЗ ІТС-АМКУ наведена на рис.3.1.

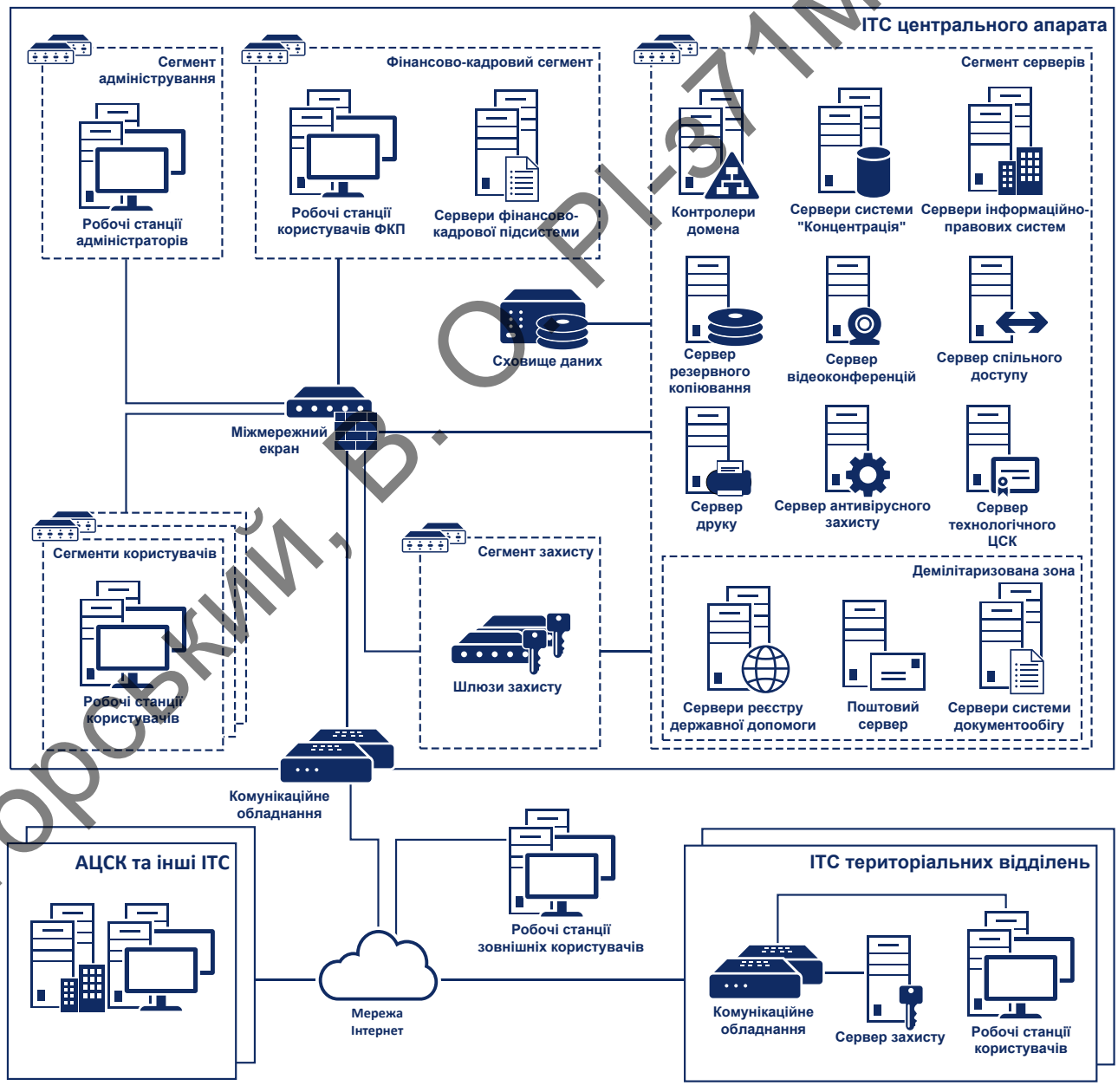

Рисунок 3.1 – Узагальнена структура ІТС-АМКУ

3.2 Програмне забезпечення

3.2.1 Загальний опис програмного забезпечення

Програмне забезпечення (далі – ПЗ) ІТС-АМКУ складається з системного та функціонального.

До системного програмного забезпечення ІТС-АМКУ відносяться:

- операційні система серверів (П_ОСС);
- операційні системи РС (П_ОСР);
- системи керування базами даних (П_СБД);
- ПЗ антивірусного захисту (П_ПАЗ).

До складу функціонального програмного забезпечення (далі - ФПЗ) ІТС-АМКУ відноситься:

- ПЗ сервера електронної пошти (П_СЕП);
- ПЗ технологічного ЦСК (П_ЦСК);
- програмний комплекс – (далі – ПК) клієнта захисту (П_КЛЗ);
- ПК віддаленого управління шлюзом захисту (П_ШЛЗ);
- ФПЗ системи електронного документообігу (П_ДОК);
- ФПЗ реєстру державної допомоги (П_РДД);
- ФПЗ фінансово-кадрової системи (П_ФКС);
- ФПЗ засідань комітету (П_ЗКМ);
- ФПЗ роботи з правовою інформацією (П_ПРІ);
- засоби адміністрування серверів та мережного обладнання (П_АДМ);
- веб-браузер (П_ВЕБ);
- текстові та графічні редактори загального призначення (П_РЕД).

Системне ПЗ ІТС-АМКУ забезпечує виконання наступних основних функцій:

- колективну роботу користувачів;
- адміністрування компонентів ІТС-АМКУ;
- збереження структурованої і неструктурованої інформації ІТС-АМКУ;

– доступ до файлів, баз даних і електронних документів колективного користування ІТС-АМКУ.

Середовище віртуалізації призначено для розгортання віртуальних ОС серверів у своєму складі, а також для керування розподілом ресурсів фізичного серверу та захисту ресурсів віртуальних серверів від НСД.

Серверні ОС із штатними комплексами засобів захисту (далі – КЗЗ) призначені для забезпечення загальносистемного функціонування ФПЗ, СКБД, і крім того ОС серверів забезпечують управління ресурсами сервера та організації взаємодії з користувачем.

ОС робочих станцій призначена для управління ресурсами РС та організації взаємодії з користувачем, а також для забезпечення загальносистемного функціонування іншого ПЗ РС.

СКБД – комплекс програмних застосувань, що забезпечують обробку запитів від ПЗ серверів, функціонального ПЗ на читання або модифікацію інформації, що зберігається в БД. Варто зауважити, що ЦСК ІТС-АМКУ має свою БД та СКБД, що обробляється у складі серверів ЦСК.

ПЗ антивірусного захисту – комплекс програмних модулів для виявлення і знешкодження комп'ютерних вірусів і шкідливих програм в режимі реального часу.

ПК клієнта захисту призначений для здійснення автентифікації користувачів на шлюзі захисту і встановлення захищеного з'єднання для передачі даних між ІТС територіальних відділень АМКУ і шлюзів захисту (зі складу ІТС-АМКУ). ПК віддаленого управління шлюзами захисту призначено для здійснення налаштувань в шлюзів захисту.

ПК віддаленого управління шлюзами захисту призначено для здійснення налаштувань відповідних засобів.

ПЗ сервера електронної пошти забезпечує обмін поштовими повідомленнями між користувачами ІТС-АМКУ (у тому числі між

користувачами ІТС-АМКУ та поштовими серверами зовнішніх телекомунікаційних мереж), а також забезпечує зберігання отриманих/відправлених поштових повідомлень. Підсистему електронної пошти ІТС-АМКУ інтегровано до домену на базі Microsoft Active Directory.

ФПЗ системи електронного документообігу автоматизує весь комплекс потоків документообігу АМКУ: введення у систему документів, їх реєстрацію, розподіл і розсилання, редагування, оперативне збереження, пошук і перегляд, відтворення, контроль виконання, розмежування доступу до документів, прискорення термінів опрацювання документів, удосконалення механізмів зберігання та виконання документів, тощо.

ФПЗ системи електронного документообігу підтримує використання електронного цифрового підпису, що забезпечує організацію якісно нового юридично-значущого документообігу.

ФПЗ реєстру державної допомоги - комплексне веб-орієнтоване рішення з автоматизації процесів контролю та моніторингу державної допомоги. ФПЗ реєстру державної допомоги дозволяє отримувати дані повідомлень з веб-форм передавати їх для реєстрації та опрацювання до Системи електронного документообігу (ФПЗ системи електронного документообігу) та накопичувати дані.

ФПЗ фінансово-кадрової системи є комплексним програмним забезпеченням, компоненти якого реалізовано в моделі трирівневої клієнт-серверної архітектури. Забезпечує централізоване управління бізнес-процесами підприємства (або групи підприємств) шляхом обліку його виробничої, фінансової та господарської діяльності. ФПЗ фінансово кадрової системи складається з множини підсистем (модулів), кожна з яких призначена для автоматизації певних завдань.

Усі підсистеми ФПЗ фінансово кадрової системи згруповані у контури управління. Кожен контур управління складається з декількох підсистем.

Допускається як ізоляція одне від одного функціональних підсистем, так і їх комбінування, в залежності від потреб на реальному об’єкті.

Складові модулі ФПЗ фінансово кадрової системи можна згрупувати у наступні контури управління:

- управління виробництвом;
- логістикою
- бюджетуванням і контролінг;
- управлінням персоналом;
- бухгалтерськргр та податкового обліку;
- аналізом та оптимізацією діяльності;

Всі модулі ФПЗ фінансово кадрової системи базуються на єдиному системному і функціональному ядрі, до якого входять модулі управління доступом та безпекою, адміністрування системи і бази даних, інструментальні засоби розширення функціональних можливостей системи.

Засоби адміністрування серверів, мережного обладнання призначено для віддаленого чи локального налаштування параметрів, а також моніторингу працездатності технічних та програмних засобів зі складу ІТС-АМКУ.

Веб-браузер використовується користувачами для доступу до функцій та інформації ІТС-АМКУ, а також для доступу до інших веб-сайтів у внутрішній мережі та мережі Інтернет.

Текстові та графічні редактори загального призначення використовується співробітниками організації для роботи з текстовими та графічними документами при виконанні своїх посадових обов'язків.

ПЗ технологічного ЦСК, у складі ПК центральних серверів ЦСК, ПК серверів взаємодії, 5 ПК адміністраторів, ПК користувача ЦСК забезпечує виконання основних функціональних завдань ЦСК, визначених в п.2.1.

3.2.2 Відомості щодо розміщення програмного забезпечення на засобах комплексу технічного засобів.

Відомості щодо розміщення ПЗ на засобах КТЗ наведено в таблиці 3.1.

Таблиця 3.1- Розміщення програмного забезпечення в компонентах ІТС-АМКУ

ПЗ / КТЗ	П_ОСС	П_ОСР	П_СБД	П_ПАЗ	П_СЕП	П_ЦСК	П_КЛЗ	П_ШЛЗ	П_ДОК	П_РДД	П_ФСК	П_ЗКМ	П_ПРІ	П_АДМ	П_ВЕБ	П_РЕД
Сервери контролерів домену	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Поштові сервери	+	-	-	+	+	-	-	-	-	-	-	-	-	-	-	-
Сервери технологічного ЦСК	+	-	+	+	-	+	-	-	-	-	-	-	-	-	-	-
Сервери системи документообігу	+	-		-	-	-	-	-	+	-	-	-	-	-	-	-
Сервери реєстру державної допомого суб'єктам господарювання	+	-	+	-	-	-	-	-	+	+	-	-	-	-	-	-
Сервери фінансово-кадрової системи	+	-	+	+	-	-	-	-	-	-	+	-	-	-	-	-
Сервери системи "Концентрація"	+	-	+	-	-	-	-	-	-	-	-	-	-	-	-	-
Сервери інформаційно-правових систем	+	-	+	-	-	-	-	-	-	-	-	+	+	-	-	-
Сервери резервного копіювання	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Сервери відеоконференцій	+	-	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Сервери спільного доступу до файлів та директорій	+	-	-	+	-	-	-	-	-	-	-	-	-	-	-	-	-
Сервери антивірусного захисту	+	-	-	+	-	-	-	-	-	-	-	-	-	-	-	-	-
Сервери друку	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Робочі станції	-	+	-	+	-	+	+	-	-	-	+	+	+	+	+	+	+

3.2.3 Опис програмних об'єктів захисту

Склад та вимоги безпеки до програмних ресурсів, що виконуються функції КЗЗ, наведено в таблиці 3.2.

Таблиця 3.2 – Склад та вимоги безпеки до програмних ресурсів

№	Назва програмного ресурсу	Вимоги безпеки	
		Цілісність	Доступність
1.	Операційні система серверів	+	+
2.	Операційні системи РС	+	+
3.	Системи керування базами даних	+	+
4.	ПЗ антивірусного захисту	+	+
5.	ПЗ сервера електронної пошти	+	-
6.	ПЗ технологічного ЦСК	+	-
7.	ПК клієнта захисту	+	+
8.	ПК віддаленого управління шлюзом захисту	+	-
9.	ФПЗ системи електронного документообігу	+	+
10.	ФПЗ реєстру державної	+	-

№	Назва програмного ресурсу	Вимоги безпеки	
		Цілісність	Доступність
	допомоги		
11.	ФПЗ фінансово-кадрової системи	+	+
12.	ФПЗ засідань комітету	+	-
13.	ФПЗ роботи з правовою інформацією	+	-
14.	Засоби адміністрування серверів та мережного обладнання	+	-
15.	Веб-браузер	+	-
16.	Текстові та графічні редактори загального призначення	+	-

3.3 Інформаційне забезпечення

3.3.1 Зміст вимог щодо захисту

- відкрита інформація;
- конфіденційна інформація;
- технологічна інформація.

У ІТС-АМКУ передбачена обробка персональних даних (ступінь обмеження доступу – «конфіденційно») та відкрита інформація.

Перелік інформаційних об’єктів, які обробляються у ІТС-АМКУ, ступінь обмеження доступу наведені у таблиці 3.3.

Таблиця 3.3- Перелік інформаційних об’єктів, які обробляються у ІТС-АМКУ

Позначення	Назва	Ступінь обмеження доступу	Представлення в ІТС
Інформаційні ресурси технологічних підсистем програмних та апаратних компонентів ІТС-АМКУ			

Позначення	Назва	Ступінь обмеження доступу	Представлення в ІТС
Д_ТІК	Технологічна інформація КЗЗ ІТС-АМКУ	Конфіденційна інформація	Об’єкти ФС, об’єкти БД
Д_ЖУР	Журнали аудиту ІТС-АМКУ	Конфіденційна інформація	Об’єкти ФС, об’єкти БД
Д_ТІУ	Технологічна інформація управління – дані налаштувань ОС та ПЗ	Конфіденційна інформація	Об’єкти ФС, об’єкти БД
Д_ВРМ	Файлові системи віртуальних машин, конфігурація та технологічна інформація віртуальних машин	Конфіденційна інформація	Об’єкти ФС серверів, дискового сховища
Д_РБД	Резервні копії інформаційних БД	Конфіденційна інформація	Об’єкти ФС серверів, дискового сховища
Д_РБС	Резервні копії файлів, стану та параметрів ОС серверів, що створені штатними засобами резервного копіювання та відновлення ОС	Конфіденційна інформація	Об’єкти ФС серверів, дискового сховища
Д_ТКЗ	Особисті ключі	Конфіденці	Об’єкти ФС ОС сервера

Позначення	Назва	Ступінь обмеження доступу	Представлення в ІТС
	(технологічні), що використовуються підсистемою КЗІ для забезпечення конфіденційності та цілісності інформації, що передається між ІТС-АМКУ та ІТС-ТВ	йна інформація	захисту ІТС-ТВ, запис в АПЗ КЗІ, ПЗП шлюзу захисту, ОС сервера технологічного ЦСК
Інформаційні ресурси функціональних систем обробки інформації ІТС-АМКУ			
Д_ВПД	Відомості, що складають персональні дані фізичних осіб – суб'єктів господарювання	Конфіденці йна інформація	Об'єкти БД (вміст полів таблиць) реєстру державної допомоги, системи електронного документообігу, БД системи "Концентрація"
Д_ДКТ	Файли електронних документів, що містять персональні дані осіб – суб'єктів господарювання (під час обробки або зберігання у відповідній системі)	Конфіденці йна інформація	Об'єкти БД реєстру державної допомоги, БД системи електронного документообігу
Д_ДКФ	Файли електронних документів, що містять персональні дані осіб –	Конфіденці йна інформація	Об'єкти ФС ОС для РС

Позначення	Назва	Ступінь обмеження доступу	Представлення в ІТС
	суб’єктів господарювання (під час обробки та зберігання у середовищі ОС РС користувачів)		
Д_ДВТ	Електронні документи, що містять відкриту інформацію, оприлюднену інформацію та інформацію на запити (під час обробки або зберігання у відповідній системі)	Відкрита інформація	Об’єкти БД реєстру державної допомоги, БД системи електронного документоо біг,БД поштових повідомлень БД засідань комітету, БД роботи з правовою інформацією
Д_ДВФ	Електронні документи, що містять відкриту інформацію, оприлюднену інформацію та інформацію на запити (під час обробки та зберігання у середовищі ОС РС користувачів)	Відкрита інформація	Об’єкти ФС ОС для РС
Д_ППС	Поштові повідомлення (під час обробки та зберігання на сервері)	Відкрита інформація	Об’єкти БД поштових повідомлень, об’єкти ФС ОС поштового сервера
Д_ППК	Копії поштових	Відкрита	Об’єкти ФС ОС для РС

Позначення	Назва	Ступінь обмеження доступу	Представлення в ІТС
	повідомлень (під час обробки та зберігання на РС користувача)	інформація	
Д_ІДС	Інформаційно-довідкові, нормативно-правові, аналітичні та статистичні відомості АМКУ	Відкрита інформація	Об’єкти БД засідань комітету, БД системи "Концентрація", БД системи бухгалтерського обліку та кадрового діловодства БД системи роботи з правовою інформацією БД реєстру державної допомоги
Інформаційні ресурси системи бухгалтерського обліку та кадрового діловодства			
Д_ЗВТ	Звіти користувачів фінансово кадрових підрозділів (під час обробки та зберігання у системі бухгалтерського обліку та кадрового діловодства)	Відкрита інформація	Об’єкти БД системи бухгалтерського обліку та кадрового діловодства, БД поштових повідомлень
Д_ПДС	Відомості, що складають персональні дані співробітників АМКУ	Конфіденційна інформація	Об’єкти БД системи бухгалтерського обліку та кадрового діловодства

Позначення	Назва	Ступінь обмеження доступу	Представлення в ІТС
Д_ЗВФ	Звіти користувачів фінансово кадрових підрозділів (під час обробки та зберігання у середовищі ОС РС користувачів)	Відкрита інформація	Об’єкти ФС ОС для РС
Д_ВБО	Відомості бухгалтерського обліку	Конфіденційна інформація	Об’єкти БД системи бухгалтерського обліку та кадрового діловодства
Д_ВКД	Відомості кадрового діловодства	Конфіденційна інформація	Об’єкти БД системи бухгалтерського обліку та кадрового діловодства
Д_СЕР	Сертифікати ЦСК, користувачів, списки відкликаних сертифікатів	Відкрита інформація	Об’єкти ФС
Інформаційні ресурси користувачів			
Д_ОКС	Особисті ключі внутрішніх користувачів – співробітників АМКУ	Конфіденційна інформація	Об’єкти ФС, об’єкти ФС АПЗ КЗІ

3.3.2 Відкрита інформація

До відкритої відносяться інформація, яка обробляється у ІТС-АМКУ і є доступною для читання всім користувачам, а доступ на модифікацію якої мають вповноважені користувачі ІТС-АМКУ згідно своїх посадових обов’язків. Відкрита інформація є інформацією вимога щодо захисту такої

встановлена законом. До інформації цієї категорії висуваються підвищені вимоги із забезпечення цілісності та доступності.

До відкритої інформації відноситься:

- електронні документи, якщо не містять персональних даних;
- інформація щодо діяльності АМКУ;
- довідники;
- звітність;
- відомості бухгалтерського обліку;
- інформаційно-довідкові відомості;
- шаблони документів;
- сертифікати відкритих ключів (якщо користувачем надана згода про публікацію сертифіката).

3.3.3 Конфіденційна інформація

Конфіденційна інформація, яка обробляється в ІТС-АМКУ, складається з персональних даних співробітників АМКУ та з персональних даних суб'єктів господарювання. Персональні дані співробітників АМКУ консолідовано у інформаційних БД фінансово-кадрової системи, персональні дані суб'єктів господарювання – у інформаційних БД реєстру державної допомоги та БД системи електронного документообігу.

Джерелами документованої інформації про особу є видані на її ім'я документи, підписані нею документи, а також відомості про особу, зібрані державними органами влади та органами місцевого і регіонального самоврядування в межах своїх повноважень.

Персональні дані співробітників АМКУ вносяться до ІТС-АМКУ з метою нарахування їм заробітної плати, ведення кадрового діловодства, а також інших задач, що передбачені задачами фінансово кадрових підрозділів АМКУ.

Персональні дані фізичних осіб, що не є співробітниками АМКУ, обробляються в ІТС-АМКУ в рамках виконання функціональних завдань, покладених на працівників АМКУ.

Персональні дані – конфіденційна інформація фізичних осіб, яка збирається та обробляється в рамках виконання завдань, покладених на АМКУ. Ця інформація відповідно до частини 2 статті 5 Закону України "Про захист персональних даних" може бути віднесена до конфіденційної інформації про особу законом або відповідною особою.

До конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження (частина 2 статті 11 Закону України «Про інформацію»).

До конфіденційної інформації відноситься:

- персональні дані суб’єктів господарювання;
- персональні дані співробітників АМКУ, які вони надають для ведення кадрового діловодства, нарахування заробітної плати, а також інших задач АМКУ у частині бухгалтерського обліку та кадрового діловодства;
- сертифікати відкритих ключів (якщо користувачем не надана згода про публікацію сертифіката).

3.3.4 Технологічна інформація

Технологічна інформація (далі – ТІ) складається з ТІ комплексу засобів захисту та ТІ щодо адміністрування та управління компонентами ІТС-АМКУ. Технологічна інформація призначена для використання тільки уповноваженими користувачами з числа адміністраторів ІТС-АМКУ, що забезпечує функціонування ІТС-АМКУ. До інформації цієї категорії висуваються підвищені вимоги із забезпечення доступності, конфіденційності та цілісності.

До технологічної відноситься інформація наступного змісту:

- налаштування операційних систем, СКБД, правил розмежування доступу, параметрів безпеки домена;
- особисті ключі, відповідні відкриті ключі яких сертифіковано технологічним ЦСК ІТС-АМКУ;
- налаштування ФПЗ фінансово-кадрової системи;
- налаштування міжмережевого екрану та активного мережевого обладнання;
- налаштування параметрів антивірусного захисту для робочих станцій;
- налаштування параметрів взаємодії з СКБД;
- атрибути доступу доступу адміністраторів та користувачів ІТС-АМКУ;
- журнали подій та налаштування щодо фіксації подій у журналах.

3.4 Технологія обробки інформації

Обробка інформації в ІТС-АМКУ здійснюється за допомогою множини функціональних підсистем за принципами клієнт-серверної технології обробки інформації.

ІТС-АМКУ забезпечує роботу наступних основних функціональних підсистем, які забезпечують обробку та зберігання інформації, пов'язаної з діяльністю АМКУ:

- система корпоративної електронної пошти;
- система бухгалтерського обліку та кадрового діловодства;
- система роботи з правовою інформацією;
- система електронного документообігу;
- система засідань комітету;
- реєстр державної допомоги суб’єктам господарювання;
- система спільного доступу до файлів та директорій.

Система електронної пошти призначена для забезпечення прозорої та оперативної комунікації між співробітниками АМКУ, а також для ведення співробітниками АМКУ електронного листування з іншими організаціями та державними установами в рамках виконання посадових обов’язків.

Підсистема побудована на базі платформи Microsoft Exchange Server та інтегрована в домен Microsoft Active Directory. Користувачі отримують доступ до власних повідомлень, що зберігаються на сервері, а також до функції отримання/відправлення повідомлень за допомогою поштових клієнтів, що відносяться до програмного забезпечення загального призначення. Поштовий сервер АМКУ доступний у мережі Інтернет за доменним іменем @amcu.gov.ua.

Система бухгалтерського обліку має клієнт-серверну архітектуру та призначена для автоматизації завдань бухгалтерського, податкового, виробничого та складського обліку. Підсистема кадрового діловодства призначена для автоматизації діяльності відділу кадрів.

Підсистема роботи з правовою інформацією призначена для пошуку та аналізу та систематизації правової інформації, що використовується співробітниками АМКУ в процесі виконання посадових обов’язків..

Система електронного документообігу призначена для побудована на базі рішень "megapolis.Діловодство" та "АСКОД", призначена для автоматизації процесів діловодства АМКУ, поточний стан використання - архівний.

Система засідань комітету на базі рішення MS SharePoint призначена для формування та накопичення інформаційних матеріалів для забезпечення проведення засідань Комітету.

Система спільного доступу до файлів та директорій призначена для надання користувачам ІТС-АМКУ віддаленого доступу до файлів та принтерів за протоколом SMB, а також для керування правами доступу користувачів до цих ресурсів.

ІТС-АМКУ також забезпечує функціонування службових підсистем:

- антивірусного захисту;
- резервного збереження інформації.

Підсистема антивірусного захисту складається з антивірусного програмного забезпечення, розміщеного на серверах та РС, щодо якого здійснюється централізоване керування параметрами, оновлення та слідкування за станом його функціонування.

Підсистема резервного збереження інформації забезпечує створення та зберігання резервних копій операційних систем серверів та інформаційних баз даних. Резервне копіювання налаштовано на фізичних серверах ІТС-АМКУ. Використовується програмне забезпечення "Система архівації даних Windows Server, версія 1". Резервне копіювання здійснюється щоденно. У якості сховища для зберігання резервних копій використовуються два фізичні сервери.

Маршрутизація мережного трафіку в ІТС-АМКУ забезпечується за рахунок впровадження апаратних маршрутизуючих пристроїв виробництва Cisco. Функції з фільтрації мережного трафіку згідно визначених правил, а також функції захисту від кіберзагроз покладено на міжмережевий екран зі складу ІТС-АМКУ.

3.4.1Технологія адміністрування ІТС

Адміністрування компонентів ІТС-АМКУ (у тому числі функціональних підсистем) здійснюється працівниками відділу забезпечення розвитку інформаційних систем Департаменту організаційної роботи АМКУ в межах контрольованої зони. Для централізованого керування обліковими записами користувачів, а також для централізованого розгортання програмного забезпечення та його налаштування на рівні ОС використовуються механізми Microsoft Active Directory.

Сегмент адміністрування використовує програмне забезпечення для керування програмними та апаратними засобами. Крім цього використовуються засоби для моніторингу та аудиту ІТС-АМКУ. Сегмент

адміністраторів відділений від сегменту інших засобів користувачів в корпоративній мережі АМКУ.

Діяльність адміністраторів регламентується положеннями та посадовими інструкціями працівників відповідних структурних підрозділів АМКУ.

3.5 Обмін інформації з іншими ІТС

Обмін інформацією ІТС-АМКУ з іншими ІТС здійснюється на підставі укладених угод, спільних наказів або інших аналогічних документів, що регламентують обмін інформацією між ІТС.

Обмін інформацією ІТС-АМКУ з іншими ІТС здійснюється з використанням засобів КЗІ. Міжмережені екрани зі складу інфраструктури забезпечують фільтрацію даних та компонентів, які можуть взаємодіяти з іншими ІТС АМКУ. На міжмережних екранах прописані чіткі правила по вхідним та вихідним заданням з іншими ІТС.

Обов’язковою умовою здійснення обміну інформацією ІТС-АМКУ з іншими ІТС, які не входять до складу інфраструктури АМКУ, є впровадження обома сторонами обміну заходів щодо захисту інформації з обмеженим доступом, що передається.

В ІТС-АМКУ відповідальним за дотримання організаційно-технічних заходів із захисту інформації в ході організації обміну є адміністратор безпеки або інша відповідальна особа, визначена керівником організації або підрозділу.

Отримувачі інформації з обмеженим доступом за її розголошення несуть відповідальність відповідно до чинного законодавства.

3.6 Характеристика користувачів

3.6.1 Перелік користувачів

Всі адміністративні ролі розділені між співробітниками АМКУ, відповідно до займаних посад. До визначених керівником АМКУ відділів і їх співробітників прив'язані відповідні ролі користувачів з ІТС-АМКУ. Таким чином в ІТС-АМКУ адміністраторів кожної ролі може бути декілька, що дасть змогу швидко реагувати на інциденти безпеки, а самі адміністратори будуть взаємозамінні.

Принцип розподілу на ролі в ІТС-АМКУ організовано наступним чином, що всі адміністративні ролі займаються забезпеченням функціонування ІТС-АМКУ, відповідно до покладених на конкретну роль задач.

Користувачі ІТС-АМКУ за рівнем повноважень доступу до інформації, що обробляється у ІТС-АМКУ, характеру й змісту робіт, які виконуються в процесі функціонування, підрозділяються на такі ролі:

- адміністратор безпеки;
- системний адміністратор;
- користувач центрального апарата;
- користувач територіального відділення;
- відповідальний за захисті інформації на ІТС-ТВ;
- користувач фінансово-кадрової системи;
- оператор реєстру державної допомоги;
- зовнішній користувач.

3.6.2 Функції користувачів

Основними функціями користувача з роллю "адміністратор безпеки" є:

- організація та контроль якісного виконання організаційно-технічних заходів з захисту інформації в ІТС-АМКУ;
- відстеження подій безпеки та реагування на інциденти безпеки;

- контроль функціонування КЗЗ ІТС-АМКУ;
- організація забезпечення антивірусного та мережного захисту в ІТС-АМКУ.

Основними функціями користувача з роллю "системний адміністратор" є:

- створення облікових записів користувачів;
- редагування облікових записів користувачів;
- налаштування групових політик Active Directory;
- налаштування механізмів безпеки компонентів ІТС-АМКУ;
- керування атрибутами доступу користувачів в ІТС-АМКУ, які використовуються для доступу до ресурсів ІТС-АМКУ;
- керування журналами аудиту подій в ІТС-АМКУ;
- налаштування, моніторинг працездатності та модернізація КТЗ ІТС-АМКУ;
- установка, модернізація, налаштування та моніторинг працездатності системного і функціонального (прикладного) ПЗ у ІТС-АМКУ;
- налаштування, контроль працездатності комунікаційного (мережного) обладнання;
- виконання робіт з відновлення функціонування компонентів ІТС-АМКУ;
- перегляд журналів реєстрації подій компонентів ІТС;
- призначення мережевих адрес компонентам ІТС-АМКУ;
- налаштування правил маршрутизації;
- налаштування та підтримка мережевих сервісів;
- організація та здійснення заходів з резервного копіювання та відновлення у ІТС-АМКУ.

Основними функціями користувача з роллю "користувач центрального апарата" є:

- створення, редагування та видалення електронних документів;
- приймання та відправлення електронної пошти;
- виконання інших задач в ІТС, що передбачені посадовими інструкціями співробітників.

Основними функціями користувача з роллю "користувач фінансово-кадрової системи" є:

- обробка інформації для підготовки бухгалтерської звітності;
- обробки бухгалтерської інформації щодо співробітників;
- обробка інформації по відносинам з іншими підприємствами;
- ведення кадрового діловодства;
- виконання інших задач, пов'язаних з бухгалтерською сферою та ведення кадрового діловодства.

Основними функціями користувача з роллю "користувач територіального відділення" є:

- створення, редагування та видалення електронних документів;
- приймання та відправлення електронної пошти;
- виконання інших задач в ІТС, що передбачені посадовими інструкціями співробітників.

Основними функціями користувача з роллю "відповідальний за захист інформації на ІТС-ТВ" є:

- встановлення, налаштування та модернізація програмного та апаратного забезпечення ІТС-ТВ, у тому числі КЗЗ складових ІТС-ТВ;
- реєстрація, блокування, видалення та підтримка в актуальному стану облікових записів користувачів в локальній ОС та визначення їм атрибутів та прав доступу в локальній ОС;
- аналіз журналів реєстрації подій;
- здійснення комплексу дій з контролю цілісності об’єктів захисту;
- оперативне реагування у випадку виникнення подій безпеки інформації;
- забезпечення працездатності програмного та апаратного забезпечення ІТС-ТВ.

3.6.3 Фізичні умови

Службові приміщення ІТС-АМКУ розміщуються на 1, 3-8 поверхах.

Службові приміщення центрального апарата АМКУ, де розміщується компоненти ІТС-АМКУ, знаходяться на контрольованій території і мають охорону. Вхід на контрольовану територію здійснюється через пропускний пункт, що контролюється черговим цілодобової охорони.

Межі контрольованої території встановлені наказом АМКУ.

Двері серверних та комутаційних кімнат обладнані механічними замками, ключі від яких зберігаються у співробітників відділу забезпечення розвитку інформаційних систем Департаменту організаційної роботи АМКУ. Двері кімнат обладнані сигналізацією на відкриття, що контролюється цілодобовою охороною.

Серверні шафи, в яких розташовано обладнання ІТС-АМКУ окремо не опечатується пломбами.

Серверне приміщення оснащене необхідними засобами енергозабезпечення, пожежної та охоронної сигналізації, газового пожежогасіння, кондиціювання, системою безперебійного живлення та допоміжними технічними засобами.

Доступ до обладнання надається тільки користувачам, яким надано повноваження тільки за письмовим розпорядженням або при належності відповідного наказу з доступу особи до обладнання.

Приміщення, де розміщуються РС адміністраторів та РС користувачів ІТС-АМКУ знаходяться в одній будівлі.

РС адміністраторів та користувачів не опечатуються та знаходяться в одній підмережі з серверами АМКУ.

3.6.4 Канали зв'язку

В ІТС-АМКУ локальну мережу побудовано на керованому комутаційному обладнанні, комутацію здійснено за допомогою структурованої кабельної системи зі швидкістю передачі даних до 1 Гбіт/с. Комутаційні вузли СКС

розташовані у спеціальних приміщеннях на другому, третьому, п’ятому, шостому та сьомому поверхах будівлі.

В якості комутаторів ядра використовуються пристрої Cisco Catalyst 2960s. Перелік комутаторів доступу наведено у відповідному додатку до цього акта.

Доступ до мережі Інтернет забезпечується з використанням послуг інтернет-провайдерів на договірних засадах. Захист/фільтрація інтернет-трафіка здійснюється засобами захищеного вузла інтернет-доступу ДП "УСС". Для підключення до мережі ДП "УСС" використовується окремо виділений канал зв’язку, наданий інтернет-провайдером в рамках надання телекомунікаційних послуг.

Доступ користувачів в мережу Інтернет контролюється міжмережним екраном Cisco ASA з сервісами Firepower, які фактично реалізують систему контролю мережного доступу та систему запобігання мережним вторгненням.

Підключення ІТС територіальних відділень до ІТС-АМКУ захищені з використанням засобів КЗІ, які відповідають вимогам ТЗ.

3.6.5 Організаційне забезпечення

Завданнями служби захисту інформації (далі – СЗІ) ІТС-АМКУ є:

- дослідження технології обробки інформації у ІТС-АМКУ з метою виявлення можливих напрямів атак та інших загроз для безпеки інформації, формування моделі загроз, визначення заходів, спрямованих на реалізацію політики безпеки інформації;
- забезпечення функціонування ІТС-АМКУ;
- організація та координація робіт, пов’язаних з захистом інформації у ІТС-АМКУ, необхідність захисту якої визначається чинним законодавством, підтримка необхідного рівня захищеності інформації, ресурсів і технологій;

- розроблення проектів нормативних і розпорядчих документів, чинних у межах організації, згідно з якими реалізується захист інформації у ІТС-АМКУ;
- організація робіт зі створення і використання КСЗІ на всіх етапах життєвого циклу ІТС-АМКУ;
- участь в організації професійної підготовки і підвищенні кваліфікації персоналу ІТС-АМКУ з питань захисту інформації;
- формування у персоналу розуміння необхідності виконання вимог нормативно-правових актів, нормативних і розпорядчих документів, що стосуються сфери захисту інформації;
- організація виконання персоналом вимог нормативно-правових актів, нормативних і розпорядчих документів з захисту інформації у ІТС-АМКУ та проведення контрольних перевірок їх виконання.

РОЗДІЛ 4 ОХОРОНА ПРАЦІ ТА ОРГАНІЗАЦІЯ БЕЗПЕКИ В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

У даному розділі визначено основні потенційно шкідливі та небезпечні виробничі фактори, які мають місце при магістерської дисертації. Оскільки ця робота має суто дослідницький напрям, пов'язаний, в основному, з використанням ВДТ ЕОМ, то основну увагу буде приділено питанню щодо забезпечення безпеки та комфортних умов на робочих місцях користувачів ВДТ ЕОМ з урахуванням вимог ДСТУ.9241:6-2004 та ДСанПІН 3.3.2.007-08

В цьому розділі запропоновані технічні рішення та організаційні заходи з безпеки і гігієни праці та виробничої санітарії, а також визначено основні заходи з безпеки в надзвичайних ситуаціях.

4.1 Визначення основних потенційно небезпечних і шкідлвих виробничих чинників при виконані науково—дослідної роботи.

Оскільки основу роботи складають дослідження із використанням електронно — обчислювальних машин (ЕОМ), існує небезпека ураження електричним струмом, можливий негативний вплив електромагнітного випромінювання ВДТ ПЕОМ.

Основні небезпечні та шкідливі фактори при проведенні наукових досліджень:

–незадовільні мікрокліматичні умови;

–недостатня освітленість робочих місць;

–небезпека ураження електричним струмом;

–наявність електромагнітного випромінювання;

–підвищений рівень шуму;

–наявність шкідливих речовин в повітрі робочої зони;

– можливість виникнення пожежі тощо;

–група психофізичних факторів: перевантаження фізичне та психологічне;

4.2 Технічне рішення та організаційні заходи з безпеки і гігієни працівника виробничої санітарії**.**

4.2.1 Електробезпека

Відповідно до ГОСТ 12.2.007.0-75 основне питання електроустаткування в робочому приміщенні (крім ВДТ ПЕОМ - II клас та вимірювальної техніки — 0I клас) відноситься до I класу, так як воно має робочу ізоляцію відповідно до ГОСТ 12.1.009-76 і підключається до електромережі за допомогою трьохконтактних вилок, один з виводів яких підключений до заземленого виводу розетки. Підключення устаткування виконане відповідно до вимог ПУЕ й ДНАОП 0.00-1.21-98.

Робоче приміщення нежарке, сухе, відноситься до класу приміщень без підвищеної небезпеки поразки персоналом електричним струмом, оскільки відносна вологість повітря не перевищує 75%, температура не більше 35ºС, відсутні хімічно агресивні середовища (ПУЕ-2017, ПБЕ й ОНТП24-86), а також відсутня можливість одночасного дотику до металоконструкцій будівлі, що мають контакт із землею, та до струмопровідних елементів електроустаткування. З іншого боку живлення електроприладів у робочому приміщенні здійснюється від трьохфазної мережі із глухозаземленоюнейтраллю напругою 220 В і частотою 50 Гц із використанням автоматів струмового захисту. У приміщенні застосована схема занулення.

Для зменшення значень напруг дотику й відповідних їм величин струму, при нормальному й аварійному режимах роботи електроустаткування має бути виконано повторне захисне заземлення нульового дроту. Виконаємо електричний розрахунок електромережі на перевірку вимикаючої здатності автоматів струмового захисту.

Розрахунок на вимикаючу здатність, включає визначення значення струму К.З. і перевірку кратності його стосовно номінального струму пристроїв максимального струмового захисту. Вихідні дані для розрахунку:

- $U_ф$ = 220В — фазова напруга;

- кабель чотирьох жильний, матеріал — алюміній (ρ=0,028 Ом*мм^2/м);

- відстань від трансформатора до споживача (L) =150м;

- номінальний струм спрацьовування автомата захисту ($I_{ном}$) =15 А. Струм однофазного К.З. визначається по формулі:

$$I_{к.з.} = \frac{U_ф}{R_ф + R_0 + \frac{Zm}{3}} = \frac{220}{2,3 + 2,4 + 0,16} = 45 \text{ А},$$

де:

$R_ф$= 2,3 Ом— активний опір фазного проводу;

R_0 = 2,4 Ом— активний опір нульового проводу;

$Zm/3$ = 0,16Ом— розрахунковий опір трансформатора потужністю 250 Вт.

Кратність струму однофазного короткого замикання стосовно номінального струму спрацьовування автомата захисту. Для надійної роботи автомату захисту повинна виконуватись наступні умови:

$$K_м = \frac{I_{к.з.}}{I_{ном}} > 1,45$$

Де $I_{К.З.}$ — струм короткого замикання; $I_{НОМ.}$— номінальний струм спрацювання автомату захисту.

$$K_м = 3$$

З розрахунків видно, що при однофазному К.З. автомат струмового захисту буде надійно спрацьовувати.

При однофазному К.З. максимальне значення напруги яка появиться на корпусі при аварійному режимі за час спрацювання максимального струмового захисту, $U_{max.}$ щодо землі: $U_{max.}$= $I_{к.з.} R_0$ = 45 · 2,4 = 108 В. Ця напруга менша $U_{доп}$ =500 В ($t_{дії}$< 0,1 сек.) згідно ГОСТ 12.1.038-88. З метою зниження $U_{max.}$ як у нормальному, так і у аварійному режимі варто використовувати повторне заземлення нульового дроту.

4.2.2 Правила безпеки під час експлуатації електронно-обчислювальних машин

Правила безпеки під час експлуатації ВДТ ЕОМ регламентуються ДСТУISO 9241:6-2004 та ДНАОП 0.00—1.31—99, які встановлюють вимоги безпеки та санітарно-гігієнічні вимоги до обладнання робочих місць користувачів ЕОМ і працівників, що виконують обслуговування, ремонт та налагодження ЕОМ, та роботи з застосуванням ЕОМ, відповідно до сучасного стану техніки та наукових досліджень у сфері безпечної організації робіт з експлуатації ЕОМ та з урахуванням положень міжнародних нормативно-правових актів з цих питань (директиви Ради Європейського союзу 90/270/ЄЕС, 89/391/ЄЕС, 89/654/ЄЕС, 89/655/ЄЕС, стандарти ISO, MPRII).

4.2.3 Вимоги до приміщень в якихрозміщені ВДТ ПЕОМ

Облаштування робочих місць, обладнаних ЕОМ, ВДТ, повинно забезпечувати:

— належні умови освітлення приміщення і робочого місця, відсутність відблисків;

— оптимальні параметри мікроклімату (температура, відносна вологість, швидкість руху, рівень іонізації повітря);

— належні ергономічні характеристики основних елементів робочого місця;

Будівлі та приміщення, в яких експлуатуються ЕОМ та виконуються їх обслуговування, налагодження і ремонт, повинні відповідати вимогам: СНиП 2.09.02-85 “Производственные здания”, СНиП 2.09.04-87 “Административные и бытовые здания”, “Правил устройства электроустановок”, затверджених Головдерженергонаглядом СРСР 1984 р. (ПВЕ), “Правил технической эксплуатации электро установок потребителей”, затверджених Головдерженергонаглядом СРСР 21.12.84 (ПТЕ, СНиП 2.08.02-89 “Общественныездания и сооружения” з доповненнями, затвердженими наказом Держкоммістобудування України від 29.12.94 № 106, СН 512-78 “Инструкция по проектированию зданий и помещений для электронно-вычислительных

машин", затверджених Держбудом СРСР, ДСанПіН 3.3.2.-007-98 ''Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин'', затверджених МОЗ України 10.12.98.

Заборонено розміщувати робочі місця з ВДТ, ЕОМ у підвальних приміщеннях, на цокольних поверхах, поряд з приміщеннями, в яких рівні шуму та вібрації перевищують допустимі значення (поряд з механічними цехами, майстернями тощо), з мокрими виробництвами, з вибухопожежонебезпечними приміщеннями категорій А і Б, а також над такими приміщеннями або під ними.

Приміщення мають бути обладнані системами водяного опалення, кондиціонування або припливно-витяжною вентиляцією відповідно до СНиП 2.04.05-91.

Згідно з ДНАОП 0.00-1.31-99 площу приміщень визначають із розрахунку, що на одне робоче місце вона має становити не менше ніж 6 м^2, а об'єм не менше ніж 20 м^3 з урахуванням максимальної кількості осіб, які одночасно працюють у зміні. Приміщення являє собою кімнату розміром 7 х 5 м., висотою 4 м. Розмір дверного прорізу 1,5м.

Площа й об'єм приміщення знаходимо по формулах:

$S = ab$,

$V = Sh$,

де a— довжина, b— ширина, h — висота приміщення.

Маємо:

S=7·5=35 м^2, V=35·4=140 м^3.

Зведемо нормативні та фактичні дані приміщення в таблицю 4.1.

Таблиця 4.1 — Параметри приміщення

Назва характеристики	Нормативн	Фактичне
Площа приміщення з розрахунку	>6 м^2	35 м^2
Об'єм приміщення з розрахунку на 1	>20 м^3	140 м^3
Висота приміщення	3,5 — 4 м	4 м
Розміри дверей	≥1,1х1.8м	1,5х2 м
Відстань від стіни зі світловими прорізами до ВДТ	≥1м	1,5 м

На підставі отриманих результатів можна зробити висновок, що геометричні розміри приміщення цілком відповідають нормативним вимогам.

Оздоблюють стіни, стелю, підлогу приміщення з матеріалів, які дозволені органами державного санітарно-епідеміологічного нагляду. Заборонено застосовувати полімерні матеріали (деревостружкові плити, шпалери, що можна мити, рулонні синтетичні матеріали, шаруватий паперовий пластик, тощо), що виділяють у повітря шкідливі хімічні речовини. За розміщенням робочих місць з ВДТ, ЕОМ потрібно витримувати такі відстані: від стін зі світловими прорізами не менше 1 м; між бічними поверхнями ВДТ не менше 1,2 м; між тильною поверхнею одного ВДТ та екраном іншого не менше 2,5 м; прохід між рядами робочих місць не менше 1 м. Робочі місця з ВДТ щодо світлових прорізів розміщують так, щоб природне світло падало збоку, переважно зліва. Екран ВДТ і клавіатура мають розміщуватися на оптимальний відстані від очей користувача, але не ближче 600 мм з урахуванням розміру алфавітно-цифрових знаків і символів. Розміщення екрана ВДТ має забезпечувати зручність зорового спостереження у вертикальній площині під кутом ± 30° від лінії зору працівника.

Усі вище перераховані вимоги відповідають робочому приміщенню, де проводяться дослідження.

4.2.4 Відповідність параметрів мікроклімату в робочій зоні санітарним нормам

Для нормалізації мікроклімату, згідно з ДСН 3.3.6.042—99. «Державні санітарні норми параметрів мікроклімату у виробничих приміщеннях», приміщення з ЗОТ обладнане системою опалення, а також системою кондиціювання повітря з індивідуальним регулюванням температури та об'єму повітря, що подається, у відповідності до СНиП 2.04.05—91 «Отопление, вентиляция и кондиционирование». Для захисту від перегрівання в теплий період року та радіаційного охолодження — в зимовий, приміщення обладнане жалюзі і екранами.

На робочому місці роботи виконуються сидячи і не потребуютьфізичного напруження. Таким чином їх можна віднести до категорії Іа, що охоплює види діяльності з витратами енергії до 120 ккал/год.

Відповідно до ДСН 3.3.6.042—99 «Державні санітарні норми параметрів мікроклімату у виробничих приміщеннях» та ГОСТ 12.005-88. «ССБТ.Общиесанитарно—гигиеническиетребования к воздухурабочейзоны» параметри мікроклімату, що нормуються: температура (*t,C*) і відносна вологість (*W,%)* повітря, швидкість руху повітря (*V,м/с*).

Оптимальні та допустимі параметри мікроклімату для умов, що розглядаються (категорія робіт та період року) наведені в табл.4.2.

Таблиця 4.2— Параметри мікроклімату.

Період Року	Оптимальні			Допустимі		
	t,С	*W*,%	*V*,м/с	*t*,С	*W*,%	*V*,м/с
Теплий	23-25	40-60	0,1	22-28	55	0,2-0,1
Холодний	22-24	40-60	0,1	21-25	75	≤ 0,1

Фактичні параметри мікроклімату в робочій зоні відповідають приведеним вище нормам ДСН 3.3.6.042—99.

4.2.5 Вимоги до освітлення робочих місць користувачів відеодисплейних терміналів персональних електронно—обчислювальних машин

Приміщення з ЕОМ повинні мати природне і штучне освітлення відповідно до ДБН В 2.5—28—2006. Природне світло повинно проникати через бічні світлопрорізи, зорієнтовані, як правило, на північ чи північний схід, і забезпечувати коефіцієнт природної освітленості не нижче 1,5 %. Розрахунки коефіцієнта природної освітленості проводяться відповідно до ДБН В.2.5—28— 2006. Приміщення з ВДТ, ЕОМ мають бути оснащені природним і штучним освітленням відповідно до ДБН В.2.5—28—2006. Природне освітлення має здійснюватись через світлові прорізи, які орієнтовані переважно на північ чи північний схід і обладнані регулювальними пристроями відкривання та жалюзями, завісками, зовнішніми козирками.

Приміщення має бічне природне та штучне освітлення, центральне водяне опалення. У приміщенні три вікна розміром 2х2,2 м. Штучне освітлення забезпечує чотири люмінесцентних світильники з лампами ЛБ —40, розміщених у ряд.

Отже, усі вимоги до освітлення робочого місця відповідають параметрам освітлення приміщення, де проводяться дослідження.

4.2.6 Виробничий шум

Для умов, що розглядаються в проекті характеру роботи, який можна класифікувати як роботу програміста обчислювальної машини у лабораторіїдля теоретичних робіт та обробки даних, рівні шуму визначені ДСН 3.3.6.037— 99. «Санітарні норми виробничого шуму, ультразвуку та інфразвуку» та ГОСТ

12.1.003—83. «ССБТ. Шум. Общиетребованиябезопасности». Допустимі рівні звуку і рівні звукового тиску в октавних смугах частот представлені у табл. 4.3.

Таблиця 4.3 — Допустимі рівні звукового тиску і рівні звуку для постійного (непостійного) широкосмугового (тонального) шуму

Характер робіт	Допустимі рівні звукового тиску (дБ) в стандартизованих									Допустимий рівень звуку (дБ)
	31	63	125	250	500	1000	2000	4000	8000	
Інженер лабораторії	86	71	61	54	49	45	42	40	38	50

Джерелами шуму в умовах робочого приміщення, що розглядається в роботі є вентилятори охолодження внутрішніх систем персонального комп'ютера (вентилятори блоку живлення, радіатора процесора та відеокарти) і система кондиціювання повітря.

Очікувані рівні звукового тиску і рівень звуку відповідно до шумових характеристик цих джерел:

—рівень шуму, створюваний внутрішніми елементами персонального комп'ютера дорівнює 35 дБ;

—рівень шуму системи кондиціювання на низьких/високих частотах дорівнює 30 дБ.

Оскільки одержанний рівень (36.2 дБ) звуку не перевищує допустимих норм, умови робочого приміщення повністю відповідають існуючим санітарним вимогам.

4.3 Безпека в надзвичайних ситуаціях

Безпека в надзвичайних ситуаціях регламентується ПЛАС. Основними складовими частинами ПЛАС є розробка технічних рішень та організаційних заходів щодо оповіщення, евакуації та дій персоналу у разі виникнення

надзвичайних ситуацій, а також визначення основних заходів з пожежної безпеки.

4.3.1 Обов’язки та дії персоналу у разі виникнення надзвичайної ситуації

У разі виявлення ознак НС працівник, який їх помітив повинен:

- негайно повідомити про це засобами зв’язку органи ДСНС, вказати при цьому адресу, кількість поверхів, місце виникнення пожежі, наявність людей, а також своє прізвище;
- повідомити про НС керівника, адміністрацію, пожежну охорону підприємства;
- організувати оповіщення людей про НС;
- вжити заходів щодо евакуації людей та матеріальних цінностей;
- вжити заходів щодо ліквідації наслідків НС з використанням наявних засобів.

Керівник та пожежна охорона установки, яким повідомлено про виникнення пожежі, повинні:

- перевірити, чи викликані підрозділи ДСНС;
- вимкнути у разі необхідності струмоприймачі та вентиляцію;
- у разі загрози життю людей негайно організувати їх евакуацію, та їх рятування, вивести за межі небезпечної зони всіх працівників, які не беруть участь у ліквідації НС;
- перевірити здійснення оповіщення людей про НС;
- забезпечити дотримання техніки безпеки працівниками, які беруть участь у ліквідації НС ;
- організувати зустріч підрозділів ДСНС та надати їм допомогу у локалізації і ліквідації НС.

Після прибуття на НС підрозділів ДСНС повинен бути забезпечений безперешкодний доступ їх до місця, де виникла НС.

4.3.2 Вимоги щодо організації ефективної роботи системи оповіщення персоналу при надзвичайних ситуаціях

Для підвищення безпеки в надзвичайних ситуаціях (НС) пропонується встановлення системи оповіщення (СО) виробничого персоналу.

Оповіщення виробничого персоналу у разі виникнення НС, наприклад при пожежі, здійснюється відповідно до вимог НАПБ А.01.003-2009.

Оповіщення про НС та управління евакуацією людей здійснюється одним з наступних способів або їх комбінацією:

— поданням звукових і (або) світлових сигналів в усі виробничі приміщення будівлі з постійним або тимчасовим перебуванням людей;

— трансляцією текстів про необхідність евакуації, шляхи евакуації, напрямок руху й інші дії, спрямовані на забезпечення безпеки людей;

— трансляцією спеціально розроблених текстів, спрямованих на запобігання паніці й іншим явищам, що ускладнюють евакуацію;

— ввімкненням евакуаційних знаків "Вихід";

— ввімкненням евакуаційного освітлення та світлових покажчиків напрямку евакуації;

— дистанційним відкриванням дверей евакуаційних виходів;

Як правило, СО вмикається автоматично від сигналу про пожежу, який формується системою пожежної сигналізації або системою пожежогасіння. Також з приміщення оперативного (чергового) персоналу СО (диспетчера пожежного поста) слід передбачати можливість запуску СО вручну, що забезпечує надійну роботу СО не тільки при пожежі, а і у разі виникнення будь-якої іншої НС.

Згідно з вимогами ДБН В.1.1-7-2002 необхідно забезпечити можливість прямої трансляції мовленнєвого оповіщення та керівних команд через мікрофон для оперативного реагування в разі зміни обставин або порушення нормальних умов евакуації виробничого персоналу.

Оповіщення виробничого персоналу про НС /пожежу/ здійснюється за допомогою світлових та/або звукових оповіщувачів — обладнуються всі виробничі приміщення.

СО повинна розпочати трансляцію сигналу оповіщення про НС (пожежу), не пізніше трьох секунд з моменту отримання сигналу про НС (пожежу).

Пульти управління СО необхідно розміщувати у приміщенні пожежного поста, диспетчерської або іншого спеціального приміщення (в разі його наявності). Ці приміщення повинні відповідати вимогам пунктів ДБН В.2.5-56-2014 "Інженерне обладнання будинків і споруд. Пожежна автоматика будинків і споруд".

Кількість звукових та мовленнєвих оповіщувачів, їх розміщення та потужність повинні забезпечувати необхідний рівень звуку в усіх місцях постійного або тимчасового перебування виробничого персоналу.

Звукові оповіщувачі повинні комбінуватися зі світловими, які працюють у режимі спалахування, у таких випадках:

— у приміщеннях, де люди перебувають у шумозахисному спорядженні;

— у приміщеннях з рівнем шуму понад 95 дБ.

Допускається використовувати евакуаційні світлові покажчики, що автоматично вмикаються при отриманні СО командного імпульсу про початок оповіщення про НС /пожежу/ та (або) аварійному припиненні живлення робочого освітлення.

Вимоги до світлових покажчиків "Вихід" приймаються відповідно до ДБН В.2.5-28-2006 «Систем протипожежного захисту».

СО в режимі "Тривога" повинна функціонувати протягом часу, необхідного для евакуації людей з будинку, але не менше 15 хвилин.

Вихід з ладу одного з оповіщувачів не повинен призводити до виведення з ладу ланки оповіщувачів, до якої вони під’єднанні.

Електропостачання СО здійснюється за І категорією надійності згідно з "Правилами устройстваэлектроустановок" (ПУЕ) від двох незалежних джерел

енергії: основного — від мережі змінного струму, резервного — від акумуляторних батарей тощо.

Перехід з основного джерела електропостачання на резервний та у зворотному напрямку в разі відновлення централізованого електропостачання повинен бути автоматичним.

Тривалість роботи СО від резервного джерела енергії у черговому режимі має бути не менш 24 годин.

Тривалість роботи СО від резервного джерела енергії у режимі "Тривога" має бути не менше 15 хвилин.

Звукові оповіщувачі повинні відповідати вимогам ДСТУ EN 54-3:2003 "Системи пожежної сигналізації. Частина 3. Оповіщувачі пожежні звукові".

Світлові оповіщувачі, які працюють у режимі спалахування, повинні бути червоного кольору, мати частоту мигтіння в межах від 0,5 Гц до 5 Гц та розташовуватись у межах прямої видимості з постійних робочих місць.

4.3.3 Пожежна безпека

Відповідно до НАПБ Б.03.002-2007 робоче приміщення лабораторії відноситься до категорії В по вибухопожежній небезпеці. Відповідно до ПУЕ (ДНАОП 0.00-1.32-01) клас робочих зон приміщення лабораторії по пожежонебезпеці — П-IIа. Можливими причинами пожежі в приміщенні є несправність електроустаткування, коротке замикання проводки, і порушення протипожежного режиму (використання побутових нагрівальних приладів, паління). У зв’язку з цим, відповідно до вимог ПБЕ та ПУЕ, необхідно передбачити наступні заходи:

1. Ретельну ізоляцію всіх струмоведучих провідників до робочих місць, періодичний огляд та перевірку ізоляції.

2. Строге дотримання норм протипожежної безпеки на робочих місцях.

3. Відповідні організаційні заходи (заборона паління, інструктаж).

Приміщення обладнане чотирма пожежними датчиками типу ДТЛ (площа, що знаходиться під захистом одного датчика, становить 15 м^2), відстань між датчиками рівна 4 м, що відповідає нормам ДБНВ 2.5-56-2014. Відповідно до ГОСТ 12.4.009-75 й ISO 3941-77 для гасіння пожежі в робочому приміщені лабораторії (клас пожежі „Е” — наявність електрообладнання під напругою) використовуються два вогнегасники вуглекислотно-брометиленові ОУБ-3. Вибір вогнегасної речовини ґрунтується на тому, що у вогні можуть опинитись електричні пристрої, що знаходяться під напругою.

Таким чином, кількість, розміщення й вміст первинних засобів гасіння пожеж цілком задовольняють всім вимогам ДСТУ 3675-98й ISO 3941-77. Крім того, у коридорі є 2 пожежних крана і ящик з піском. Дотримано усіх заходів безпеки відповідно до ГОСТ 12.3.019-80 і НАПБ А.01.001-2004 «Правила пожежної безпеки в Україні».

Дотримано усі вимоги ДБН В.1.1-7-2002 та СНиП 2.09.02-85 по вогнестійкості будинку і ширині евакуаційних проходів і виходів із приміщень назовні.

Значення основних параметрів шляхів евакуації приведені в таблиці 4.4.

Таблиця 4.4 — Характеристики і норми евакуаційних виходів

Параметр	Фактичне значення	Норма
Висота дверних прорізів	2,0 м	Не менше 2 м
Ширина дверних прорізів	1,5 м	Не менше 0,8 м
Ширина проходу для евакуації	Більше 1,5 м	Не менше 1 м
Ширина коридору	3 м	Не менше 2 м
Число виходів з коридору	2	Не менше 2
Ширина сходової клітки	1,5 м	Не менше 1 м
Висота поруччя сходів	1 м	Не менше 0,9 м

5 - РОЗРОБЛЕННЯ СТАРТАП-ПРОЕКТУ

Даний розділ має на меті проведення маркетингового аналізу стартап проекту задля визначення принципової можливості його ринкового впровадження та можливих напрямів реалізації цього впровадження.

5.1 Опис ідеї проекту

В межах цього підрозділу аналізується зміст ідеї, можливі напрямки застосування, основі вигоди які може отримати користувач товару та відмінності від існуючих аналогів та замінників.

Таблиця 5.1 — Опис ідеї стартап-проекту

Зміст ідеї	Напрямки застосування	Вигоди для користувача
Оптимізація показників надійності, що визначаються тепловими режимами в блоці радіоелектронної апаратури	Виробництво	Збільшення надійності окремих чарунок в блоці радіоелектронної апаратури
	Наука	

Основним конкурентом розроблюваному проекту є пакет прикладного програмного забезпечення Solidworks Flow Simulation, який дозволяє моделювати теплообмін . Пакет Solidworks Flow Simulationдозволяє виконувати ті ж речі, що і розроблюваний пакет, але в ньому більш складні вимоги до вихідних даних та відсутність оптимізації температур.

Таблиця 5.2 — Визначення сильних, слабких та нейтральних характеристик ідеї проекту

№ п/п	Техніко-економічні характеристики ідеї	Товари конкурентів		W (слабка сторона)	N (нейтральна сторона)	S (сильна сторона)
		Мій проект	Конкурент			

1	Простота					✔
2	Дешевизна					✔
3	Швидкодія					✔

5.2 Технологічний аудит ідеї проекту

В межах даного підрозділу проводиться аудит технології, за допомогою якої можна реалізувати ідею проекту.

Для реалізації цього проекту потрібно вибрати мову програмування чи середовище програмування. Оглянуто три варіанта:

1. Mathcad — система комп'ютерної алгебри з класу систем автоматизованого проектування, орієнтована на підготовку інтерактивних документів з обчисленнями і візуальним супроводженням, відрізняється легкістю використання і застосування для колективної роботи.
2. Мова програмування C++ — мова програмування високого рівня з підтримкою кількох парадигм програмування: об'єктно-орієнтованої, узагальненої та процедурної.
3. Мова програмування JavaScript — динамічна, об'єктно-орієнтована прототипна мова програмування. Реалізація стандарту ECMAScript. Найчастіше використовується для створення сценарії ввеб-сторінок, що надає можливість на стороні клієнта(пристрої кінцевого користувача) взаємодіяти з користувачем, керувати браузером, асинхронно обмінюватися даними з сервером, змінювати структуру та зовнішній виглядвеб-сторінки.

Таблиця 5.3 — Технологічна здійсненність проекту

№ п/п	Ідея проекту	Технології її реалізації	Наявність технології	Доступність технології
1	Оптимізація показників надійності, що визначаються тепловими режимами в блоці	Mathcad	Так	Так
2		C++	Так	Так
3		JavaScript	Ні	Так

	радіоелектронної апаратури			
Обрана технологія реалізації ідеї проекту:JavaScript				

Даний проект можливо реалізувати і в якості технологічного шляху обраноJavaScriptчерез наявність у автора проекту знань у мові програмування JavaScript та можливості розробки програми в браузере, що дозволяє виконувати розрахунки в браузере, що значно прискорює процес тренування мережі.

5.3 Аналіз ринкових можливостей запуску стартап-проекту

В межах даного підрозділу проводиться визначення ринкових можливостей, які можна використати під час ринкового впровадження проекту, та ринкових загроз, які можуть перешкодити реалізації проекту. Визначення ринкових можливостей дозволяє спланувати напрями розвитку проекту із урахуванням стану ринкового середовища, потреб потенційних клієнтів та пропозицій проектів-конкурентів.

Таблиця 5.4 — Попередня характеристика потенційного ринку стартап-проекту

№ п/п	Показники стану ринку	Характеристика
1	Кількість головних гравців, од	1
2	Загальний обсяг продаж, ум. од.	Невідомий
3	Динаміка ринку	Зростає
4	Наявність обмежень для входу	Невідома
5	Специфічні вимоги до стандартизації та сертифікації	Існують
6	Середня норма рентабельності в галузі, %	Невідома

За результатами аналізу важно зробити висновок щодо привабливості для входження за попереднім оцінюванням.

Визначимо потенційні групи клієнтів.

Таблиця 5.5 — Характеристика потенційних клієнтів стартап-проекту

№ п/п	Потреба, що формує ринок	Цільова аудиторія	Відмінності у поведінці різних потенційних цільових груп клієнтів	Вимоги споживачів до товару
1	Оптимізація показників надійності, що визначаються тепловими режимами в блоці радіоелектронної апаратури	Науковці, розробники радіоелектронної апаратури	Невідомі	Точність, швидкість обрахунку, адекватність результату

Проведемо аналіз ринкового середовища: складемо таблиці факторів, що сприяють ринковому впровадженню проекту, та факторів, що йому перешкоджають.

Таблиця 5.6 — Фактори загроз

№ п/п	Фактор	Зміст загрози	Можлива реакція компанії
1	Новий функціонал ПЗ конкурентів	Впровадження нового функціоналу у SolidworksFlowSimulation, аналогічного до розроблюваного у цьому проекті	Вихід з ринку

Таблиця 5.7 Фактори можливостей

№ п/п	Фактор	Зміст можливості	Можлива реакція компанії
1	Новий	Додавання нових моделей та	Розроблення

	функціонал у проекті що розробляється	можливостей у проект, що розроблюється	цього функціоналу

Проведемо аналіз пропозиції: визначимо загальні риси конкуренції на ринку.

Таблиця 5.8 — Ступеневий аналіз конкуренції на ринку

Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підприємства
Тип конкуренції — монополістична	Одне підприємство майже зайняло усю нішу	Значний
За рівнем конкурентної боротьби — національне	Дане підприємство відомо по усьому світу	Значний
За галузевою ознакою — внутрішньогалузева	Конкуренція виконується в рамках однієї галузі	Значний
Конкуренція за видами товарів — невідомо		
За характером конкурентних переваг — цінова	Товар даного підприємства має дуже високу вартість	Значний
За інтенсивністю — невідомо		

Проведемо більш детальний аналіз умов конкуренції у галузі.

Таблиця 5.9 — Аналіз конкуренції в галузі за М. Портером

Складові аналізу	Прямі конкуренти в галузі	Потенційні конкуренти	Постачальники	Клієнти	Товари-замінники

	SolidWorks Flow Simulation	Розрахунок теплообміну	Невідомо	Невідомо	Невідомо
Висновки	Маючи майже монопольне положення на ринку розробник цього ПЗ не буде приділяти уваги розробці	Є можливість виходу на ринок	Невідомо	Невідомо	Невідомо

За результатами аналізу можна зробити висновок, що працювати на даному ринку можна незважаючи на конкурентну ситуацію. Для поширення продукту він повинен володіти рядом факторів, які відрізняють його від існуючого конкурента.

Перелічимо фактори конкурентоспроможності

Таблиця 5.10 — Обґрунтування факторів конкурентоспроможності

№ п/п	Фактор конкурентоспроможності	Обґрунтування
1	Простота	Дана розробка не вимагає від користувача особливих знань у галузі
2	Дешевизна	Поширюється безкоштовно і кожний має можливість користуватися нею
3	Швидкодія	Розраховуються найкращі показники для конкретного проекту

Проведемо аналіз сильних та слабких сторін стартап-проекту.

Таблиця 5.11 — Порівняльний аналіз сильних та слабких сторін проекту

№ п/п	Фактор конкурентоспроможності	Бали 1-20	Рейтинг товарів —конкурентів у порівнянні з проектом, що розробляється						
			-3	-2	-1	0	+1	+2	+3
1	Простота								
2	Дешевизна								
3	Швидкодія								

Проведемо SWOT-аналіз

Таблиця 5.12 — SWOT-аналіз стартап-проекту

Сильні сторони: Простота Дешевизна Швидкодія	Слабкі сторони: Невідома компанія Відсутність стартового капіталу
Можливості: Розширення функціоналу Нові технології	Загрози: Продукти-замінники

З огляду на SWOT-аналіз можна прийти до висновку що нема потреби розробляти альтернативи ринкового впровадження цього проекту.

5.4 Розроблення ринкової стратегії проекту

Розроблення ринкової стратегії першим кроком передбачає визначення стратегії охоплення ринку, а саме опис цільових груп потенційних споживачів.

Таблиця 5.14 — Вибір цільових груп потенційних споживачів

№ п/п	Опис профілю цільової групи потенційних клієнтів	Готовність споживачів сприйняти продукт	Орієнтовний попит в межах цільової групи	Інтенсивність конкуренції в сегменті	Простота входу у сегмент
1	Науковці	Готові	Високий	У сегменті	Важко

				значна конкуренція	
2	Розробники радіоелектронної апаратури	Готові	Високий	У сегменті не значна конкуренція	Важко
Які цільові групи обрано: науковці, розробники радіоелектронної апаратури					

Для роботи в обраних сегментах ринку сформулюємо базову стратегію розвитку.

Таблиця 5.15 — Визначення базової стратегії розвитку

№ п/п	Стратегія охоплення ринку	Ключові конкурентоспроможні позиції	Базова стратегія ринку
1	Диференційований маркетинг	Простота, дешевизна, швидкодія	Стратегія спеціалізації

Виберемо конкурентну поведінку

Таблиця 5.16 — Визначення базової стратегії конкурентної поведінки

№ п/п	Чи є проект «першопроходьцем» на ринку?	Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів?	Чи буде компанія копіювати основні характеристики товару конкуренту?	Стратегія конкурентної поведінки
1	Так	Ні	Ні	Заняття конкурентної ніші

Розробимо стратегію позиціонування, що полягає у формуванні ринкової позиції, за яким споживачі мають ідентифікувати проект.

Таблиця 5.17 — Визначення стратегії позиціонування

№	Вимоги до	Базова	Ключові	Вибір асоціацій,

п/п	товару цільової аудиторії	стратегія розвитку	конкурентоспроможні позиції власного стартап-проекту	які мають сформувати комплексну позицію власного проекту
1	Точність			

5.5 Розроблення маркетингової програми стартап-проекту

Сформуємо маркетингову концепцію товару, який отримає споживач.

Таблиця 5.18 — Визначення ключових переваг концепції потенційного товару

№ п/п	Потреба	Вигода, яку пропонує товар	Ключові переваги перед конкурентами
1	Оптимізація показників надійності, що визначаються тепловими режимами в блоці радіоелектронної апаратури	Швидке створення розміщення чарунок в блоці радіоелектронної апаратури та швидка оптимізація показників надійності	Швидкодія, безкоштовність, точність

Таблиця 5.19 — Опис трьох рівнів моделі товару

Рівні товару	Сутність та складові
1. Товар за задумом	Оптимізація показників надійності, що визначаються тепловими режимами в блоці радіоелектронної апаратури
2. Товар у реальному виконанні	Властивості: 1. Простота 2. Дешевизна 3. Швидкодія

	Якість: апробація на готових фізичних моделях
	Пакування: відсутнє
	Марка: відсутня
3. Товар із підкріпленням	До продажу: невідомо
	Після продажу: невідомо

Товар не буде якимось чином захищатись від копіювання та буде поширюватись як є.

Визначимо цінові межі, якими необхідно керуватись при встановленні ціни на товар.

Таблиця 5.20 — Визначення меж встановлення ціни

№ п/п	Рівень цін на товари-замінники	Рівень цін на товари-аналоги	Рівень доходів цільової групи споживачів	Верхня та нижня межі встановлення ціни на товар
1	70-100 тис. ум. од.	До 10 тис ум. од.	Високий	Безкоштовно

Визначимо оптимальну систему збуту

Таблиця 5.21 — Формування системи збуту

№ п/п	Специфіка закупівельної поведінки цільових клієнтів	Функції збуту, які має виконувати постачальник товару	Глибина каналу збуту	Оптимальна система збуту
1	Невідома	Вільний доступ до товару	Невідома	Вільний доступ до товару

Розробимо концепцію маркетингових комунікацій

Таблиця 5.22 — Концепція маркетингових комунікацій

№ п/п	Специфіка поведінки цільових клієнтів	Канали комунікацій, якими користуються клієнти	Ключові позиції, обрані для позиціонування	Завдання рекламного повідомлення	Концепція рекламного звернення
1	Невідома	Інтернет, наукові публікації	Можливості проекту	Донести про можливості проекту	Донесення про можливості та сильні стороні проекту

5.6 Висновки за розділом

За результатами проведеного аналізу можна зробити висновок, що є можливість ринкової комерсалізації проекту оскільки на ринку є попит на таку продукцію.

ВИСНОВКИ

1. Істотна частина проблем забезпечення захисту інформації в АС може бути вирішена організаційними заходами. Для побудови КС при створенні КСЗІ використовуються програмні та апаратні компоненти.

2. Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею. Інформація зберігає цілісність, якщо дотримуються встановлені правила її модифікації (видалення). Інформація зберігає доступність, якщо зберігається можливість ознайомлення з нею або її модифікації відповідно до встановлених правил упродовж будь-якого певного (малого) проміжку часу. Загрози, реалізація яких призводить до втрати інформацією якої-небудь з названих властивостей, відповідно є загрозами конфіденційності, цілісності або доступності інформації.

3. Комп'ютерна система складається з безлічі компонентів. Деякі з них спеціально призначені для реалізації політики безпеки. Інші можуть впливати на безпеку опосередковано, наприклад, забезпечувати функціонування компонентів першого типу. І, нарешті, треті можуть взагалі не бути задіяні під час вирішення завдань забезпечення безпеки. Множина всіх компонентів перших двох типів називається комплексом засобів захисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Захист інформації в автоматизованих системах управління : навчальний посібник / Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.

2. Логінова Н. І. правовий захист інформації : навчальний посібник / Н. І. Логінова, Р. Р. Дробожур. – Одеса : Фенікс, 2015. – 264 с., іл.

3. Остапов С. Е. технологія захисту інформації : навчальний посібник / С. Е. Осапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.

4. Корякин-Черняк С.Л., Как собрать шпионские штучки своими руками,Наука и техника 2010,-224с.

5. Яковлев В.А., Шпионские и антишпионские штучки, Наука и техника 2016,-317с

6. Бахрушин В.Є. Методи аналізу даних : навчальний посібник для студентів / В.Є. Бахрушин. – Запоріжжя : КПУ, 2011. – 268с;

7. Грабовецький Б.Є., Навчальний посібник. – Вінниця: ВФ ТАНГ, 2000.

ДОДАТОК А

Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

Радіотехнічний факультет

Кафедра радіоконструювання та виробництва радіоапаратури

ПОГОДЖЕНО	**ЗАТВЕРДЖУЮ**
Науковий керівник, викладач кафедри конструювання і виробництва радіоапаратури НТУУ «КПІ»	Завідувач кафедри радіоконструювання та виробництва радіоапаратури НТУУ «КПІ»
_____	_____
Д.В. Євграфов к.т.н., доцент	Є.А.Нелін д.т.н,професор

ТЕХНІЧНЕ ЗАВДАННЯ

« » _____ 20 р.

на виконання магістерської дисертації

з теми: «Система захисту інформації на основі динамічного програмування»

Київ 2018

1 Назва магістерської дисертації.

Назва: Система захисту інформації на основі динамічного програмування.

2 Підстава для виконання роботи

Завдання на магістерську дисертацію видане кафедрою радіоконструювання і виробництва радіоапаратури видане від « »_____ 2018 року.

3 Виконавець магістерської дисертації

Виконавець: студент групи РІ-з71мп Погорський Владислав Олександрович.

Науковий керівник: кандидат технічних наук, доцент, старший науковий співробітник Євграфов Дмитро Вікторович.

4 Термін виконання

Початок – 01.09.2017

Закінчення – 21.12.2018

5 Мета, актуальність та призначення

Метою розроби КСЗІ є впровадження заходів та засобів, які реалізують способи, методи, механізми захисту інформації від:

– витоку технічними каналами, до яких відносяться канали побічних електромагнітних випромінювань і наведень, акустоелектричні та інші канали;

– несанкціонованих дій та несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав’язування хибної інформації, застосування закладних пристроїв чи програм, використання комп’ютерних антивірусів та ін.;

– спеціального впливу на інформацію, який може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту.

Комплексна система захисту інформації надає загальну характеристика автоматизованої системи установи і умов її функціонування. Метою комплексної системи захисту інформації є формування моделі загроз

інформації та моделі порушника об’єкта інформаційної діяльності, розробка політики безпеки та системи документів з забезпечення захисту інформації.

Комплексна система захисту інформації призначена для захисту інформації, що циркулює та зберігається у межах об’єкта інформаційної діяльності. КСЗІ створюється на основі Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», ДСТУ 3396.1-96, НД ТЗІ 1.1-002-99, НД ТЗІ 1.4-001-2000, НД ТЗІ 2.1-001-200, НД ТЗІ 3.7-001-99, НД ТЗІ 3.7-003-05

6 Вимоги до виконання магістерської дисертації

Вимоги:

- Дослідна робота проводиться на реалізації ситеми захисту інформації в Антимонопольному комітеті;
- Матеріали і розробки за темою мають бути виконані на достатньому науковому рівні та придатні для практичного використання у науково-технічній галузі, у тому числі в сфері виявлення закладних пристроїв;
- Наукові звіти, матеріали магістерської дисертації та інші текстові документи подаються на електронному і паперовому носіях за встановленими формами та відповідають сучасним нормам наукової лексики і оформлюються відповідно до ДСТУ 3008-95 «Документація. Звіти у сфері науки і техніки».

7 Приблизний зміст магістерської дисертації

Вступ

Розділ 1. Показники ефективності комплексної системи захисту інформації.

Розділ 2. Метод динамічного програмування для обгрунтування комплексної системи захисту інформації.

Розділ 3. Практична реалізація комплексної системи захисту інформації в інформаційно-телекомукаційній системі Антимонопольного комітету України.

Розділ 4. Охорона праці та організація безпеки в надзвичайних ситуаціях.

Розділ 5. Розроблення стартап-проекту.

Висновки

Перелік посилань

8 Вихідні дані для проведення роботи та обґрунтування теми

При виконанні НДР використовуються:

– матеріали монографій за темою дисертації;

5. Корякин-Черняк С.Л., Как собрать шпионские штучки своими руками, Наука и техника 2010,-224с.
6. Яковлев В.А., Шпионские и антишпионские штучки, Наука и техника 2016,-317с
7. Баскаков С.И, Радиотехнические цепи и сигналы, Высшая школа 2000,
8. Бахрушин В.Є. Методи аналізу даних : навчальний посібник для студентів / В.Є. Бахрушин. – Запоріжжя : КПУ, 2011. – 268с;
9. Грабовецький Б.Є., Навчальний посібник. – Вінниця: ВФ ТАНГ, 2000.

9 Очікувані результати

Практичне вирішення задачі комплексного захисту методом динамічного програмування. Використання метода динамічного програмування для забезпечення мінімальної хибної тривоги для заданої ймовірності правильного виявлення загрози.

10 Матеріали, які подаються по закінченні магістерської дисертації:

- завдання;
- технічне завдання;
- пояснювальна записка;
- електронна презентація

11 Етапи магістерської дисертації і терміни їх виконання

Шифр етапів	Назва етапів виконуваного завдання	Терміни виконання		Чим закінчується етап
		початок	закінчення	
1	Показники ефективності комплексної системи захисту інформації	вересень 2017	листопад 2017	Звіт магістра

2	Метод динамічного програ мування для обґрунтування ефективності комплексної системи захисту інформації	листопад 2017	березень 2018	Звіт магістра
3	Практична реалізація комп лексної системи захисту інформації в інформаційно-телекомукаційній системі Антимонопольного коміте ту України.	березень 2018	вересень 2018	Звіт магістра
4	Виконання пояснювальної записки	вересень 2018	грудень 2018	Звіт магістра

Термін виконання НДР: 1.09.2017 – 21.12.2018

12 Порядок розгляду приймання магістерської дисертації:

Визначають порядок приймання магістерської дисертації:

- Подання магістерської дисертації на попередній захист;
- Захист магістерської дисертації.

Виконавець
магістерської дисертації
студент групи РІ –з71мп _____ Погорський В.О.

(науковий ступінь,вчене звання) (підпис) (прізвище, ініціали)

ДОДАТОК Б

Погорський Владислав Олександрович, магістрант
КПІ ім. Ігоря Сікорського, м.Київ
Кафедра радіоконструювання
та виробництва радіоапаратури, студент

ОБГРУНТУВАННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ МЕТОДОМ ДИНАМІЧНОГО ПРОГРАМУВАННЯ

Створення комплексної системи захисту інформації є забезпечення захисту інформації, що циркулює в інформаційно-телекомунікаційних системах. Захист інформації має здійснюватися шляхом протидії загрозам, які можна очікувати внаслідок дій порушника на всіх технологічних етапах її обробки і в усіх режимах функціонування інформаційно-телекомунікаційної системи.

При розробці та впровадженні КСЗІ повинні бути враховані існуючі тенденції розвитку захищених інформаційних технологій, розробки відповідних засобів захисту інформації, розвитку державної нормативної бази з технічного захисту інформації.

Для здійснення захисту інформації на всіх стадіях життєвого циклу ІТС у КСЗІ має бути передбачено застосування наступних заходів та засобів захисту інформації:

- організаційно-правові заходи, які реалізуються поза обчислювальною системою ІТС;
- інженерно-технічні заходи, що реалізуються поза обчислювальною системою ІТС;
- апаратні, програмно-апаратні та програмні засоби захисту від несанкціонованого доступу, реалізації функцій криптографічного захисту інформації (далі – КЗІ) та забезпечення доступності інформації, яка обробляється й зберігається у ІТС.

КСЗІ призначена для:

реалізації політики розмежування доступу, заданої у ІТС;

- ідентифікації та автентифікації користувачів у ході надання їм доступу до функцій та інформації ІТС;
- забезпечення конфіденційності, цілісності та доступності інформації, яка обробляється в ІТС;
- розмежування доступу користувачів до інформації та функцій ІТС;
- забезпечення конфіденційності та цілісності технологічної інформації, що обробляється та передається каналами зв'язку у ІТС;
- реалізації функцій криптографічного захисту інформації (КЗІ),
- створення механізму та умов оперативного реагування на зовнішні та внутрішні загрози з метою забезпечення безпеки інформації;
- ефективного попередження, своєчасного виявлення та знешкодження загроз для ресурсів обчислювальної системи ІТС, причин та умов, які спричиняють або можуть призвести до порушення її нормального функціонування;
- керування засобами захисту інформації, контроль за їхньою роботою з боку осіб, які відповідають за забезпечення безпеки інформації у ІТС;

Науковою новизною роботи є запропонований метод, який дозволяє на більш технічному рівні захистити обробку інформації в різних підприємствах.

Література

1. Захист інформації в автоматизованих системах управління : навчальний посібник / Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.

2. Логінова Н. І. правовий захист інформації : навчальний посібник / Н. І. Логінова, Р. Р. Дробожур. – Одеса : Фенікс, 2015. – 264 с., іл.

3. Остапов С. Е. технологія захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.