Форма № Н-9.02

Національний університет «Полтавська політехніка імені Юрія Кондратюка»
(повне найменування закладу вищої освіти)
Навчально-науковий інститут інформаційних технологій і робототехніки
(повне найменування інституту, назва факультету (відділення))
Кафедра автоматики, електроніки та телекомунікацій
(повна назва кафедри (предметної, циклової комісії))

Пояснювальна записка

до кваліфікаційної роботи

магістра
(ступінь вищої освіти)

на тему «**Розробка проекту кампусної комп'ютерної мережі підприємства «СВ АЛЬТЕРА»**

Виконав: студент 6 курсу, групи 601ТТ
спеціальності 172 «Телекомунікації та радіотехніка»
(шифр і назва напряму підготовки, спеціальності)
Баландін А. В.
(прізвище та ініціали)
Керівник Жученко О.С.
(прізвище та ініціали)
Рецензент Галай В.М.
(прізвище та ініціали)

Полтава - 2023 рік

Національний університет «Полтавська політехніка імені Юрія Кондратюка»
Інститут **Навчально-науковий інститут інформаційних технологій і робототехніки**
Кафедра Автоматики, електроніки та телекомунікацій
Освітній рівень магістр
Спеціальність 172 «Телекомунікації та радіотехніка»

ЗАТВЕРДЖУЮ
завідувач кафедри автоматики, електроніки та телекомунікацій
_____ д.т.н., проф. О.В. Шефер
"04" 09 2023 р.

З А В Д А Н Н Я

НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Баландіну Артему Володимировичу

1. Тема проекту (роботи) **«РОЗРОБКА ПРОЕКТУ КАМПУСНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ПІДПРИЄМСТВА «СВ АЛЬТЕРА» »**

керівник проекту (роботи) Жученко Ллександр Сергійович, к.т.н., доцент
затверджена наказом вищого навчального закладу від 04.09. 2023 року № 986-фа

2. Строк подання студентом проекту (роботи) 13.12. 2023 р.

3. Вихідні дані до проекту (роботи). Вихдними даними до кваліфікаційної роботи магістра є матеріали опрацьовані під час переддипломної практики.

4. зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Вступ з обґрунтуванням теми кваліфікаційної роботи. Аналітичний огляд проблеми та постановка задачі дослідження. Аналіз правил забезпечення захисту інформації. Опис об'єкта «СВ. АЛЬТЕРА». Апаратне та програмне забезпечення обєкта та підбір мережевого обладнання. Трасування роботи корпоративної комп'ютерної мережі. Основні принципи захисту інформації в локальній мережі підприємства. Інженерно-технічний та програмний захистінформації. Висновки.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових плакатів): Актуальність та мета роботи. Визначення об'єкта та предмета досліджень. Особливості захисту інформації. Опис підприємства «СВ. Альтера» та специфіка його роботи. Аналіз локації підприємства. Структурні особливості компанії. Аналіз розміщення мережевого обладнання та плану будівлі. Аналіз апаратного забезпечення мережі. Аналіз параметрів комунікаційної інформації. Механізми аудита і протоколювання облікових записів. Кібернетичні та криптологічні особливості захисту інформації. Висновки.

7. Дата видачі завдання 04.09.23

КАЛЕНДАРНИЙ ПЛАН

ор. №	Назва етапів магістерської роботи	Термін виконання етапів роботи			Прим (плак
1	**Вступ з обґрунтуванням теми кваліфікаційної роботи.**	11.10.23		15%	Пл.
2	Аналітичний огляд проблеми та постановка задачі дослідження.	18.10.23	I	30%	Пл.
3	Аналіз правил забезпечення захисту інформації. опис об'єкта «св. альтера».	25.10.23		40%	Пл.
4	Аналіз розміщення існуючого апаратного забезпечення.	14.11.23		50 %	Пл.
5	Апаратне та програмне забезпечення обєкта та підбір мережевого обладнання.	21.11.23	II	60%	Пл.
6	Трасування роботи корпоративної комп'ютерної мережі.	28.11.23		70%	Пл.
7	Основні принципи захисту інформації в локальній мережі підприємства. інженерно-технічний та програмний захист інформації.	06.12.23		90%	Пл.
8	Висновки. Оформлення кваліфікаційної роботи та формування додатків.	13.12.23	III	100%	Пл. 9

Студент _____ Баландін
(підпис) (прізвище та і

Керівник роботи _____ Жученко
(підпис) (прізвище та і

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

АС – автоматизована система;

КСЗІ – комплексна система захисту інформації;

КЗЗ – комплекс засобів захисту від несанкціонованого доступу;

ІЗОД – інформація з обмеженим доступом;

Об'єкт ЕОТ – об'єкт електронно-обчислювальної техніки;

ТЗІ – Технічний захист інформації

НСД – Несанкціонований доступ

ОС – операційна система.

ЗУ – Закон України.

ВСТУП

Сучасній людині досить складно уявити своє життя без різноманітних засобів зв'язку та пристроїв для обробки інформації, різноманітних обчислень. Ще досить недавно цими засобами зв'язку були стаціонарні телефони, пошта, телевізор, радіо та величезні електронно-обчислювальні машини (ЕОМ), які, досить часто, займали не одну кімнату чи, навіть, не один поверх будівлі. Зараз майже кожен вдома має комп'ютер в сотні разів потужніший за ці ЕОМ та здатний замінити майже всі засоби зв'язку які використовувало людство протягом свого існування.

На сьогодні комунікаційні засоби та інформаційні технології застосовуються у всіх сферах життя та майже у всіх галузях виробництва, адже, за допомогою комп'ютерних мереж, інформаційні технології можуть пов'язувати певні групи користувачів у певні простори.

Метою проектування КМ є забезпечення вільного доступу до мережі Internet для користувачів певної мережі. КМ являє собою сукупність комп'ютерів та обчислювальних пристроїв (принтери, роутери, модеми та факси), які зв'язані каналами передачі даних та інформації. Іншими словами, комп'ютерна мережа може з'єднати комп'ютери та інші пристрої у одну структуру через повітряне чи кабельне середовище. Корпоративна мережа – це КМ, яка підтримує працездатність підприємства, яке володіє даною мережею. Користувачами корпоративної КМ можуть бути лише робітники певного підприємства [1].

Серед всіх топологій КМ базовими є топології зірка, шина та кільце. Топологія зірка має середню вартість організації, захист від прослуховування, середню надійність передачі даних, високе масштабування, добру зручність та простоту обслуговування. Саме це й посприяло її використанню в даній дипломній роботі [1].

Застосування комп'ютерів майже у всіх галузях виробництва та сферах життя призвело до зросту інтересу абонентів КМ до забезпечення захисту своєї

інформації від сторонніх користувачів. Захист інформації являє собою певну групу заходів, правових норм та методів для уникнення завдання шкоди власникам інформації та її користувачам можливим випадковим чи навмисним впливам. Захист інформації зводиться до забезпеченні її доступності, цілісності та конфіденційності.

Концепція обчислювальних мереж є логічним результатом еволюції комп'ютерної технології. Перші комп'ютери 50-х років були великими, громіздкими і дорогими. Такі комп'ютери не були призначені для інтерактивної роботи, а використовувалися в режимі пакетної обробки [1].

На сьогоднішній день у світі існує безліч комп'ютерів, і понад 80% з них об'єднані в різні інформаційно-обчислювальні мережі, від малих локальних мереж в офісах, до глобальних мереж типу Internet [2].

Однак, масове використання окремих, не пов'язаних, комп'ютерів породжує ряд серйозних проблем: як зберігати використовувану інформацію, як зробити її загальнодоступною, як обмінюватися цією інформацією з іншими користувачами, як спільно використовувати дорогі декільком користувачам? Вирішенням цих проблем стало об'єднання цих комп'ютерів у одну систему – комп'ютерну мережу [3].

Комп'ютерна мережа – це сукупність комп'ютерів та інших пристроїв, зв'язаних каналами передачі даних[4].

Об'єднання комп'ютерів у мережі вирішило безліч важливих проблем, таких як прискорення передачі інформаційних повідомлень, можливість швидкого обміну інформацією між користувачами, одержання і передача повідомлень не відходячи від робочого місця, а так само обмін інформацією між комп'ютерами різних фірм виробників працюючих під різним програмним забезпеченням.

Такі можливості, які несе в собі обчислювальна мережа, а саме, прискорення виробничого процесу, спонукає прийняти це до розробки і застосувати їх на практиці.

Отже, необхідно розробити принципове рішення питання з організації інформаційно-обчислювальної мережі на базі вже існуючого комп’ютерного парку та програмного комплексу, що відповідає сучасним науково-технічним вимогами, з урахуванням зростаючих потреб і можливістю подальшого розвитку мережі у зв’язку з появою нових технічних і програмних рішень [5].

1 АНАЛІТИЧНИЙ ОГЛЯД ПРОБЛЕМИ ТА ПОСТАНОВКА ЗАДАЧІ ДОСЛІДЖЕННЯ

1.1 Теоретичні відомості

Комп'ютерна мережа – система зв'язку між двома чи більше комп'ютерами. У ширшому розумінні комп'ютерна мережа – це система зв'язку через кабельне чи повітряне середовище, самі комп'ютери різного функціонального призначення і мережеве обладнання. Для передачі інформації можуть бути використані різні фізичні явища, як правило – різні види електричних сигналів чи електромагнітного випромінювання [1].

Середовищами передавання у комп'ютерних мережах можуть бути телефонні кабелі, та спеціальні мережеві кабелі: коаксіальні кабелі, виті пари, волоконно-оптичні кабелі, радіохвилі, світлові сигнали.

Безпосередньою основою комп’ютерних мереж (КМ) були телефонні і телеграфні мережі, внаслідок розвитку мікроелектроніки з’явились потужні електронно–обчислювальні машини для взаємодії яких виникла необхідність у швидкому та надійному каналі передачі даних.

Сучасні комп’ютерні мережі забезпечують:

- колективне опрацювання даних користувачами
- обмінювання файлами та іншими даними між користувачами
- спільне використовувати програми
- спільне використання принтерів, модемів та ін.

Для класифікації комп’ютерних мереж використовуються різні ознаки, вибір яких полягає в тім, щоб виділити з існуючого різноманіття такі, які дозволили б забезпечити даній класифікаційній схемі унікальні якості [1].

Комп’ютерні мережі класифікують за наступними ознаками:

- за територіальним розташуванням – локальні, регіональні, глобальні;

- за сферою застосування – офісні, промислові, побутові;
- за комплексом архітектурних рішень – Ethernet, Token Ring, Arcnet;
- за топологією – шинна, кільцева, зіркоподібна, деревоподібна, повнозв'язна;
- за фізичним середовищем передавання – з симетричним кабелем, з коаксіальним кабелем, з кабелем "кручена пара", з волоконно–оптичним кабелем, з інфрачервоним каналом, з мікрохвильовим каналом;
- за методом доступу до фізичного середовища передавання – з опитуванням, з маркерним доступом, із суперництвом, з уставлянням регістра.
- за ознаками структурної й функціональної організації.[2]

Певна невідповідність вимог до класифікації робить завдання вибору раціональної схеми класифікації КМ досить складним. В основному КМ класифікують за ознаками структурної й функціональної організації.

По призначенню КМ розподіляються на:

- обчислювальні;
- інформаційні;
- змішані (інформаційно-обчислювальні)

До недавнього часу, побудова мережі обмежувалася лише територіальними масштабами, але сьогодні з розвитком технологій це змінилося, і тепер ці масштаби територій стали єдиними як для локальних мереж, так і для глобальних мереж, які відрізняються лише технологічними можливостями побудови мережі.

Комп'ютерної мережі поділяються на:

- локальна мережа;
- глобальна мережа.

Локальні мережі – мережі які мають максимальну відстань між вузлами не більше 1–2км.

Глобальні мережі– мережі, що охоплюють територію країни або кількохкраїн з максимаьною відстанню між окремими вузлами в

тисячікілометрів. Структура сучасних глобальних мереж наведена на рисунку 1.1 [2].

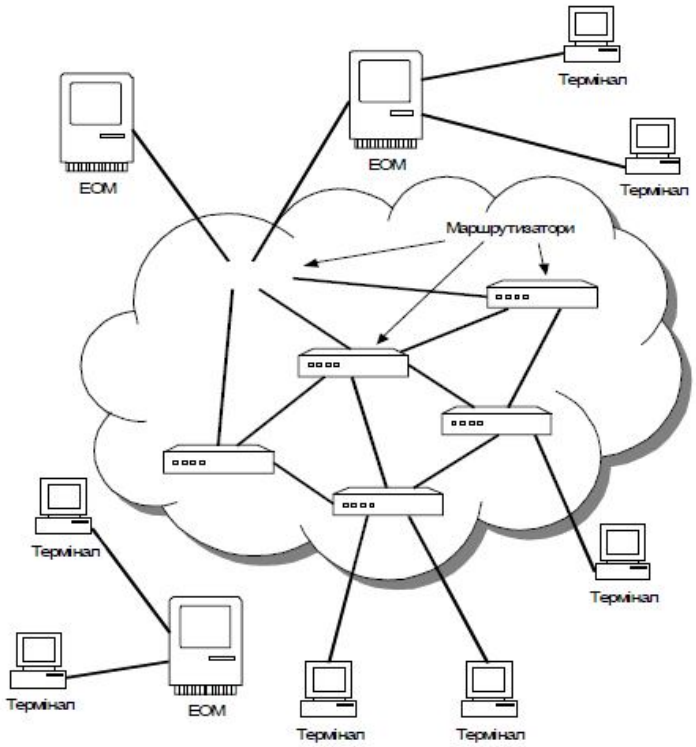

Рисунок 1.1 – Структура сучасних мереж

.

Комп'ютерна мережа — це сукупність комп'ютерів та інших пристроїв, зв'язаних каналами передавання даних [3].

Комп'ютерні мережі забезпечують спільний доступ до даних. У мережі виділяють комп'ютери, на яких розміщують великі масиви даних, а користувачі інших комп'ютерів мережі одержують доступ до них. Це дає можливість, наприклад, людям, котрі працюють над одним проектом, використовувати дані, створені іншими, тобто працювати над проектом одночасно.

За допомогою комп'ютерної мережі стає можливим спільне користування периферійними пристроями: принтерами, сканерами, модемами тощо. Невигідно мати їх біля кожного персонального комп'ютера, наприклад, у комп'ютерному класі або в банку [4].

Основне призначення всіх комп'ютерних мереж — це спільний доступ до мережних ресурсів (апаратного забезпечення комп'ютерів, периферійних

пристроїв), спільне використання даних та швидкий обмін ними, спільне використання програмного забезпечення.

Мережна взаємодія передбачає віддалений доступ до мережних ресурсів та відбувається за технологією. Залежно від повноважень комп'ютери в мережі розподіляються на сервери та клієнтів [4].

Клієнт — це комп'ютер користувача, який здійснює запит, сервер - комп'ютер, що обробляє цей запит і відповідає на нього [4].

Звертаємо вашу увагу: сервером та клієнтом називаються як комп'ютери в мережі, так і програмне забезпечення, що працює на цих комп'ютерах.

У централізованих мережах виділяється один потужний комп'ютер — виділений сервер, що виконує основні функції з організації роботи мережі. Такі мережі ще називаються „клієнт-виділений сервер". Усі клієнти отримують доступ до ресурсів мережі через сервер [4].

На сервері встановлюється спеціальна операційна система (наприклад, 52г). Операційна система дозволяє організувати і контролювати роботу комп'ютерів і користувачів у мережі, надавати кожному користувачеві певні права доступу до ресурсів і даних цієї мережі. Для цього кожен користувач отримує ім"я користувача (логін) та пароль для входу до мережі [5].

Прикладами такої мережі можуть бути комп'ютерні мережі банків, корпорацій, вищих навчальних закладів, деяких шкіл м. Києва та інші.

Перевагами централізованих комп'ютерних мереж є висока швидкість обміну даними і можливість розподіляти права доступу користувачів у них. Але суттєвим недоліком є те, що при виході з ладу сервера вся мережа перестає працювати [5].

У децентралізованих мережах немає виділеного сервера, будь-який комп'ютер може бути як сервером, так і клієнтом. Такі мережі ще називаються щоранговим . Як клієнт, комп'ютер в одноранговій мережі може здійснювати запит щодо доступу до ресурсів інши х комп'ютерів мережі. Як сервер, комп'ютер повинен обробляти запити від інших комп'ютерів мережі та надавати потрібні дані.

В одноранговій мережі всі комп'ютери мають однакові права (ранги) щодо доступу до ресурсів кожного й до периферійних пристроїв. Кожен користувач мережі може на своєму жорсткому диску визначити папки і файли, які він надає для загального користування [4].

У таких мережах на всі комп'ютери встановлюється операційна система, яка забезпечує їм рівні можливості.

Перевагою одиорангових мереж є працездатність мережі при виході з ладу будь-якого з комп'ютерів, а недоліком — неможливість розподіляти права клієнтів щодо роботи в мережі.

Прикладом такої мережі може бути мережа комп'ютерного класу у більшості шкіл.

Локальна мережа — комп'ютерна мережа, що об'єднує комп'ютери, які знаходяться в одному приміщенні або кількох приміщеннях, розташованих на невеликій відстані одне від одного [4].

Але локальні мережі не дозволяють забезпечити спільний доступ до даних тим користувачам, що знаходяться, наприклад, у різних частинах міста. На допомогу приходять регіональні мережі, що об'єднують комп'ютери в межах одного регіону (району, міста, країни). Прикладами такої мережі є комп'ютерна мережа, що об'єднує комп'ютери, які знаходяться в будинках одного або кількох кварталів, комп'ютери директорів шкіл району, комп'ютерна мережа «Воля» в Києві та інші [3].

1.2 Комплексна система захисту

Комплексна система захисту інформації (КСЗІ) – це взаємопов’язаний комплекс організаційних та інженерних заходів, засобів та методів захисту інформації.

Захист інформації в сучасних умовах стає дедалі складнішою проблемою через низку обставин, основними з яких є:

- широке використання електронних обчислень;

- ускладнення технологій шифрування;
- необхідність охорони не тільки державної та військової таємниці, а й виробничої, комерційної та фінансової таємниць;
- збільшення можливостей несанкціонованих дій щодо інформації [8].

Крім того, набули поширення інструменти та методи несанкціонованого та секретного пошуку інформації. Вони все частіше використовуються не тільки в діяльності державних правоохоронних органів, але і в діяльності різних злочинних груп. Слід пам’ятати, що природні канали витоку інформації формуються стихійно через специфічні обставини, що склалися на об’єкті захисту [8].

Захист державних секретів завжди була важливою складовою обороноздатності країни. З початком впровадження в різних, в першу чергу, силових, відомствах інформаційних систем виникла потреба забезпечити розмежування доступу до ресурсів цих систем за аналогією з паперовими носіями. Так, в 1970 році в США з'явилася перша теоретична модель розмежування доступу ADEPT-50, а в 1985 році Міністерство оборони США випустило перші критерії оцінки захищеності комп'ютерних систем, так звану «Помаранчеву книгу». Ці критерії, по суті, гуртувалися на узагальненому досвіді побудови систем захисту інформації в державних структурах. Таким чином, саме держсектор став локомотивом розвитку світового ринку інформаційної безпеки. Технології, успішно використовувалися в силових відомствах, були згодом поставлені на службу як приватному бізнесу, так і домашньому користувачеві [9].

В процесі еволюції технологій і систем захисту інформації виникла необхідність уніфікувати вимоги до їх створення і забезпечити деяку стандартизацію. Одним з найважливіших підсумків цієї роботи став міжнародний стандарт ISO / IEC 15408, так звані «Загальні критерії», який отримав визнання в багатьох країнах світу, включаючи наших сусідів. Україна вибрала власний шлях, розробивши серію нормативних документів системи

технічного захисту інформації, ключовим в яких є НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних систем від несанкціонованого доступу» і ґрунтується на «Канадських критеріях захищеності» 1993 року. Цей документ використовується при проектуванні та створенні комплексних систем захисту інформації державних інформаційних ресурсів, а також систем, в яких обробляється інформація з обмеженим доступом, вимога щодо захисту якої визначено законом. Визначення комплексної системи захисту інформації (КСЗІ) як взаємопов'язаної сукупності організаційних та інженерно-технічних заходів, засобів і методів захисту інформації наводиться в Законі України «Про захист інформації в інформаційно-телекомунікаційних системах» [9].

Головною метою створення КСЗІ є досягнення максимальної ефективності захисту за рахунок одночасного використання всіх необхідних ресурсів, методів і засобів, що виключають несанкціонований доступ до інформації, та створення умов обробки інформації відповідно до чинних нормативно-правових актів України у сфері захисту інформації: Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», «Про доступ до публічної інформації» та «Про захист персональних даних».

Комплексна система захисту інформації призначена для виконання наступних завдань:

- ефективна нейтралізація та запобігання загрозам ресурсам шляхом всебічного впровадження правових, морально-етичних, фізичних, організаційних, технічних та інших заходів безпеки;
- забезпечення властивостей політики безпеки інформації (конфіденційності, цілісності та доступності) під час створення та експлуатації інформаційної мережі;
- розмежування та контроль доступу користувачів відповідно до встановленої політики обмеження доступу;
- управління засобами інформаційної безпеки, доступом користувачів до ресурсів;

- контроль за роботою персоналу працівниками служби захисту інформації;
- оперативне повідомлення про спроби несанкціонованого доступу;
- виявлення вразливостей в операційних системах; захист від атак зловмисників безпеки;
- захист від проникнення та поширення комп'ютерних вірусів;
- контроль за функціонуванням КСЗІ;
- створення умов для локалізації збоїв і якнайшвидшого відновлення роботи після будь-якої несправності, спричиненої несанкціонованими діями фізичних та юридичних осіб, впливом зовнішнього середовища та іншими факторами [9].

Для побудови КСЗІ потрібно послідовно виконати 6 етапів (рис. 1.1).

Рисунок 1.1 – Етапи побудови комплексної системи захисту інформації

Мета і призначення КСЗІ. КСЗІ є невід'ємною складовою частиною автоматизованої системи. Метою створення КСЗІ в автоматизованій системі класу «1» є забезпечення захисту інформації, яка обробляється в автоматизованій системі, шляхом запобігання розголошенню, спотворенню і втратам при її обробці та експорті на зовнішні носії. Захист інформації повинен забезпечуватися на всіх технологічних етапах її обробки і в усіх режимах функціонування автоматизованої системи:

- захисту інформації з обмеженим доступом, яка обробляється засобами автоматизованої системи, та ресурсів автоматизованої системи від ознайомлення, розмноження, розповсюдження, копіювання, відновлення, витоку, модифікації та знищення за рахунок несанкціонованого доступу;

- блокування несанкціонованих дій інформації з обмеженим доступом;
- захисту інформаційних ресурсів, які обробляються засобами автоматизованої системи від впливу вірусів та інших зловмисних програм та кодів;
- реєстрації та контролю користувачів та носіїв інформації відповідно до встановленої політики безпеки;
- керування доступом користувачів до інформаційних ресурсів автоматизованої системи;
- здійснення однозначної ідентифікації та автентифікації кожного зареєстрованого користувача та його носія;
- моніторингу, реєстрації спроб реалізації загроз інформації та оперативного оповіщення адміністратора безпеки про факти несанкціонованих дій з інформацією з обмеженим доступом та протидії спробам реалізації загроз інформаційним ресурсам автоматизованої системи [9].

Цілі захисту інформації в автоматизованої системи розподілені на дві множини:

1. Цілі безпеки інформації для автоматизованої системи, що відображають необхідність протистояти загрозам безпеці ресурсів автоматизованої системи та реалізовувати політику безпеки під час обробки інформації засобами автоматизованої системи в частині:
   - середовища користувачів;
   - інформаційного середовища;
   - апаратного середовища автоматизованої системи;
   - програмного середовища автоматизованої системи;
   - технології обробки інформації.
2. Цілі безпеки інформації для фізичного середовища функціонування автоматизованої системи, що відображають вимоги щодо захисту забезпечень автоматизованої системи в частині:
   - фізичного середовища;

- середовища організаційного забезпечення [9].

Досягнення цілей безпеки для автоматизованої системи повинно сприяти запобіганню загрозам безпеки та реалізації вимог функціонального профілю захисту для автоматизованої системи. Для модулів комплексу засобів захисту, що забезпечують захист ресурсів автоматизованої системи, загальними є наступні цілі:

- ідентифікація й автентифікація суб'єктів і об'єктів системи в процесі забезпечення доступу та використання ресурсів автоматизованої системи;
- розмежування доступу до ресурсів автоматизованої системи;
- протоколювання й аудит подій інформаційної безпеки під час обробки інформації в автоматизованої системи;
- забезпечення коректного використання функцій безпеки виключно через інтерфейс комплексу засобів захисту автоматизованої системи;
- виконання резервного копіювання технологічної інформації, необхідної для відновлення роботи системи у випадку збоїв;
- забезпечення відновлення функціонування автоматизованої системи після збоїв і відмов обладнання автоматизованої системи;

контроль цілісності виконуваних модулів автоматизованої системи та комплексу засобів захисту та забезпечення їх само тестування [9].

Класифікація. На підставі НД ТЗІ 2.5-005-99 «Класифікація АС і стандартні функціональні профілі захищеності оброблюваної інформації від НСД» за сукупністю характеристик ІТС виділено три ієрархічні класи, вимоги до функціонального складу КЗЗ яких істотно відрізняються [9].

Клас «1» – одна робоча станція, яка обробляє конфіденційну інформацію. Можна виділити такі параметри:

- в будь-який момент часу з комп’ютером може працювати тільки один користувач, проте кількість осіб з доступом може бути більше, але всі вони мають одинакові права на доступ до інформації, яка оброблюється;

- технічні засоби з точки зору безпеки відносяться до однієї категорії і можуть застосовуватися для зберігання і всієї інформації [9].

Приклад – автономний ПК, доступ до якого контролюється з використанням організаційних заходів.

Клас «2» – локалізований багатомашинний багатокористувацький комплекс, який обробляючий інформацію різноманітних категорій конфіденційності. Важливою відмінністю від попереднього класу є існування користувачів з різними технічними засобами та правами доступу, які можуть одночасно обробляти інформацію різноманітних категорій конфіденційності. Приклад - локальна мережа.

Клас «3» – розподілений багатомашинний багатокористувацький комплекс, який обробляє інформацію різних категорій конфіденційності. Істотною відмінністю порівняно з попереднім класом є необхідність передавати інформацію через незахищене середовище. Прикладом є глобальна мережа [9].

1.3 Нормативно-правові акти про необхідність КСЗІ в ІТС

Розпочалася історія ТЗІ в Україні з Закону України «Про захист інформації в автоматизованих системах», прийнятого постановою Верховної Ради України № 81/94-ВР від 5 липня 1994 року.

У тому же році постановою Кабінету Міністрів України (далі - ПКМУ) від 9 вересня 1994 року № 632 було затверджене «Положення про технічний захист інформації в Україні» (далі - ТЗІ), згідно якого була створена Державна служба України з питань ТЗІ.

Через 3 роки постановою КМУ від 8 жовтня 1997 року № 1126 була затверджена «Концепція ТЗІ в Україні». Вона визначає поняття ТЗІ таким чином: це діяльність, спрямована на забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності інформації з обмеженим доступом, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави. А вже через 2 роки з’явилося нове «Положення

про ТЗІ в Україні», затверджене Указом Президента України від 27 вересня 1999 року № 1229. Пов’язане це було з тим, що питання ТЗІ були покладені на Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України (скорочено – ДСТСЗІ СБУ), до складу якого і увійшла Державна служба з питань ТЗІ. Старе положення втратило чинність згідно постанови КМУ від 13 березня 2002 року № 281 [9].

«Положення про ТЗІ в Україні» визначає поняття ТЗІ таким чином: це діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності важливої для держави, суспільства і особи інформації [5].

Він також визначає такі терміни:

- конфіденційність – властивість інформації, що захищається від несанкціонованого доступу;
- цілісність – властивість інформації, що захищається від несанкціонованого спотворення, знищення або знищення;
- доступність – властивість інформації, що захищається від несанкціонованого блокування;
- інформаційна система – автоматизована система, комп'ютерна мережа або система зв'язку [8].

1.4 Правила забезпечення захисту інформації в ІС.

Захисту в системі підлягає:

- відкрита інформація, яка належить до державних інформаційних ресурсів, а також відкрита інформація про діяльність суб'єктів владних повноважень, військових формувань, яка оприлюднюється в Інтернеті, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами (далі - відкрита інформація);

- конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених Законом України "Про доступ до публічної інформації";
- службова інформація;
- інформація, яка становить державну або іншу передбачену законом таємницю (далі - таємна інформація);
- інформація, вимога щодо захисту якої встановлена законом [8].

Відкрита інформація під час обробки в системі повинна підтримувати цілісність, що забезпечується захистом від несанкціонованих дій, які можуть призвести до її випадкового або навмисного модифікації або знищення.

Всім користувачам повинен бути наданий доступ до публічної інформації. Лише ідентифіковані та автентифіковані користувачі, яким надано відповідні повноваження, можуть змінювати або знищувати публічну інформацію. Спроби модифікувати або знищити публічну інформацію несанкціонованими користувачами, невстановленими користувачами або користувачами з непідтвердженою ідентифікацією ідентифікатора слід заблокувати. Під час обробки офіційної та секретної інформації повинен бути забезпечений її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, розповсюдження [8].

Доступ до службової інформації надається лише ідентифікованим та автентифікованим користувачам. Спроби отримати доступ до такої інформації невстановленими особами або користувачами з підтвердженою ідентифікацією представленого ідентифікатора під час автентифікації слід заблокувати. У системі забезпечується можливість надання користувачеві права на виконання однієї або кількох операцій з обробки конфіденційної інформації або позбавлення його такого права [8].

У системі здійснюється обов'язкова реєстрація:

- результатів ідентифікації та автентифікації користувачів;
- результатів виконання користувачем операцій з обробки інформації;

- спроб несанкціонованих дій з інформацією;
- фактів надання та позбавлення користувачів права доступу до інформації та її обробки; - результатів перевірки цілісності засобів захисту інформації.

Аналізувати реєстраційні дані можна лише користувач, який уповноважений управляти засобами захисту інформації та контролювати захист інформації в системі (адміністратор безпеки).

Реєстрація здійснюється автоматично, а дані реєстрації захищені від модифікацій та знищення користувачами, які не мають повноважень адміністратора безпеки. Реєстрація спроб несанкціонованих дій з інформацією, що становить державну таємницю, а також конфіденційною інформацією про фізичну особу, яка за законом віднесена до персональних даних, повинна супроводжуватися повідомленням адміністратора охорони [8].

Ідентифікація та автентифікація користувачів, надання та позбавлення їх права на доступ до інформації та її обробки, контроль за цілісністю засобів захисту в системі здійснюється в автоматизованому режимі. Передача офіційної та секретної інформації з однієї системи в іншу здійснюється у зашифрованому вигляді або захищених каналах зв'язку відповідно до вимог законодавства про технічний та криптографічний захист інформації. Порядок підключення систем, в яких обробляється офіційна та секретна інформація, до глобальних мереж передачі даних визначається законодавством.

Система контролює цілісність програмного забезпечення, що використовується для обробки інформації, запобігання несанкціонованим модифікаціям та усунення наслідків такої модифікації. Також контролюється цілісність інформаційної безпеки програмного та апаратного забезпечення. У разі порушення їх цілісності обробка в інформаційній системі припиняється [9].

1.5Висновки за розділом та постановка задач

Тема роботи присвячена розробці проекту комп'ютерної мережі та рекомендацій по захисту інформації підприємства «СВ АЛЬТЕРА»

Метою роботи є підвищення захищеності даних компанії «СВ АЛЬТЕРА» шляхом створення корпоративної комп'ютерної мережі, що з'єднає структурні підрозділи у єдину мережеву структуру, створення системи захисту інформації компанії.

Об'єкт дослідження є процес створення комп'ютерної мережі організації «СВ АЛЬТЕРА».

Організація корпоративної КМ повинна забезпечити надійність комп'ютерної підтримки компанії «СВ АЛЬТЕРА» та з'єднати структурні підрозділи у єдину мережеву структуру. Система шифрування передачі повідомлень повинна підвищити рівень захищеності даних компанії «СВ АЛЬТЕРА». Призначення створюваної комп'ютерної мережі – забезпечення спільного доступу користувачів мережі до загальних ресурсів та забезпечення вільного доступу до інтернету. Користувачами даної корпоративної мережі можуть бути тільки співробітники компанії ПП «СВ АЛЬТЕРА».

В ході виконання кваліфікаційнох роботи очікується одержати проект корпоративної комп'ютерної мережі для компанії «СВ АЛЬТЕРА» з системою захисту інформації.

2. АПАРАТНА СКЛАДОВА

2.2 Опис підприємства «СВ. АЛЬТЕРА»

Заснована в 1998 році, «СВ АЛЬТЕРА» сьогодні займає провідні позиції на українському ринку електротехніки і систем автоматизації технологічних процесів.

Мета компанії - максимально ефективно вирішувати задачі клієнта в області модернізації підприємства, автоматизації виробництва і управління, ресурсозбереження, підвищення продуктивності обладнання.

Рисунок. 2.1 Офісні приміщення

Ми пропонуємо клієнтам максимально ефективні рішення в галузі електропостачання та автоматизації виробництва, що в підсумку призводить до підвищення продуктивності обладнання та якості продукції наших замовників. За допомогою нашої продукції здійснюється розподіл електроенергії від РП (ТП) і головних розподільних щитів до кінцевого споживача, захист електричних мереж, компенсація реактивної потужності, спеціальні рішення для металургії та хімічної промисловості. Здійснюється керування екструдерами, термопластавтоматами, печами, кліматокамерами, системами опалення, водопостачання та вентиляції, холодильною технікою, компресорами, кондиціонерами, насосами, запірною арматурою, різним харчовим, пакувальним, деревообробним, нафтохімічних обладнанням і т.п.

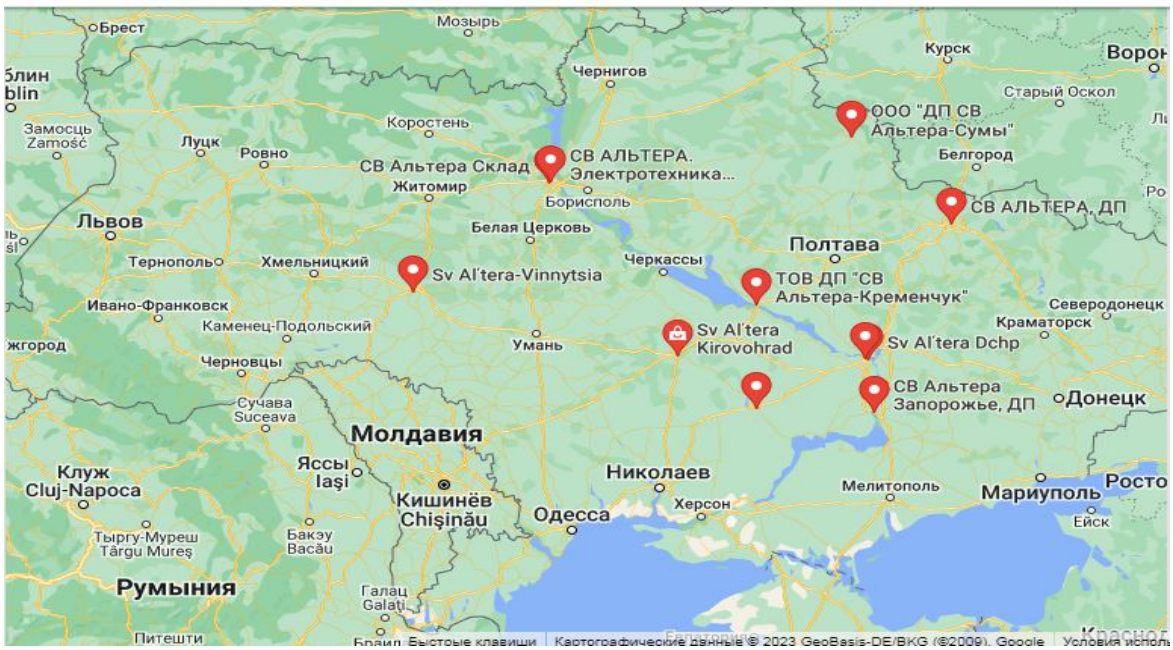

Рисунок. 2.2 Розміщення підприємства

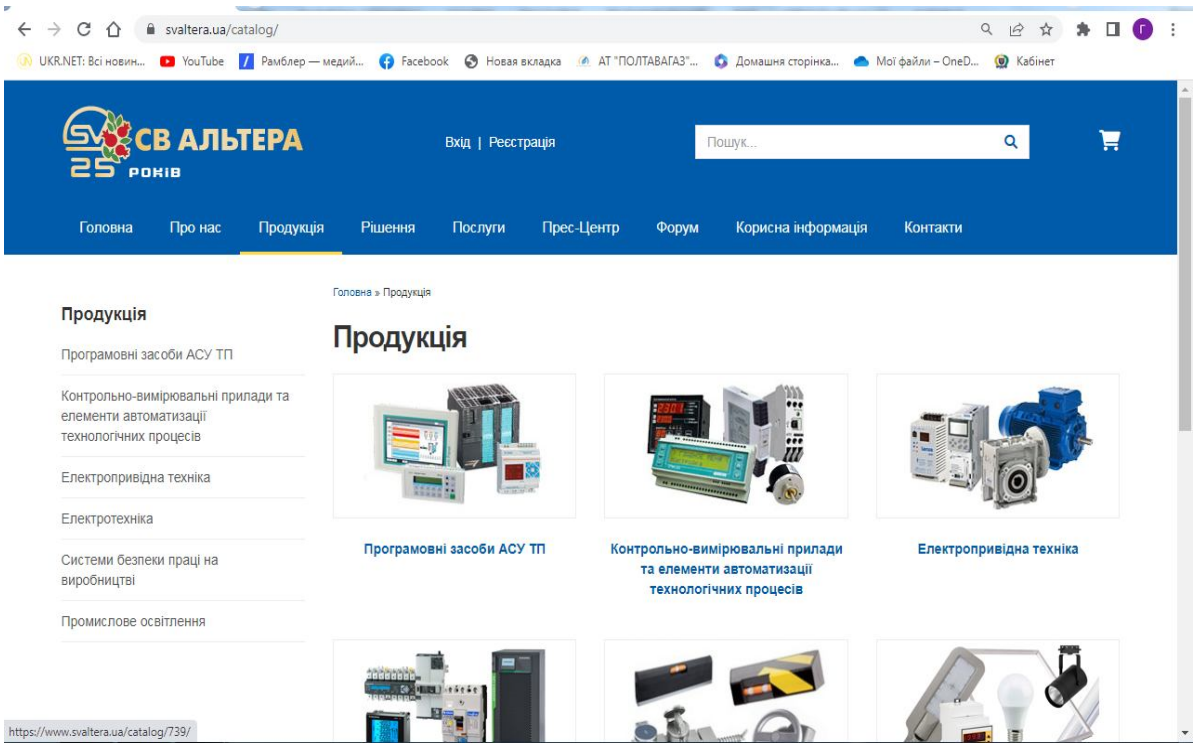

Рисунок. 2.3 Приклад сайту підприємства

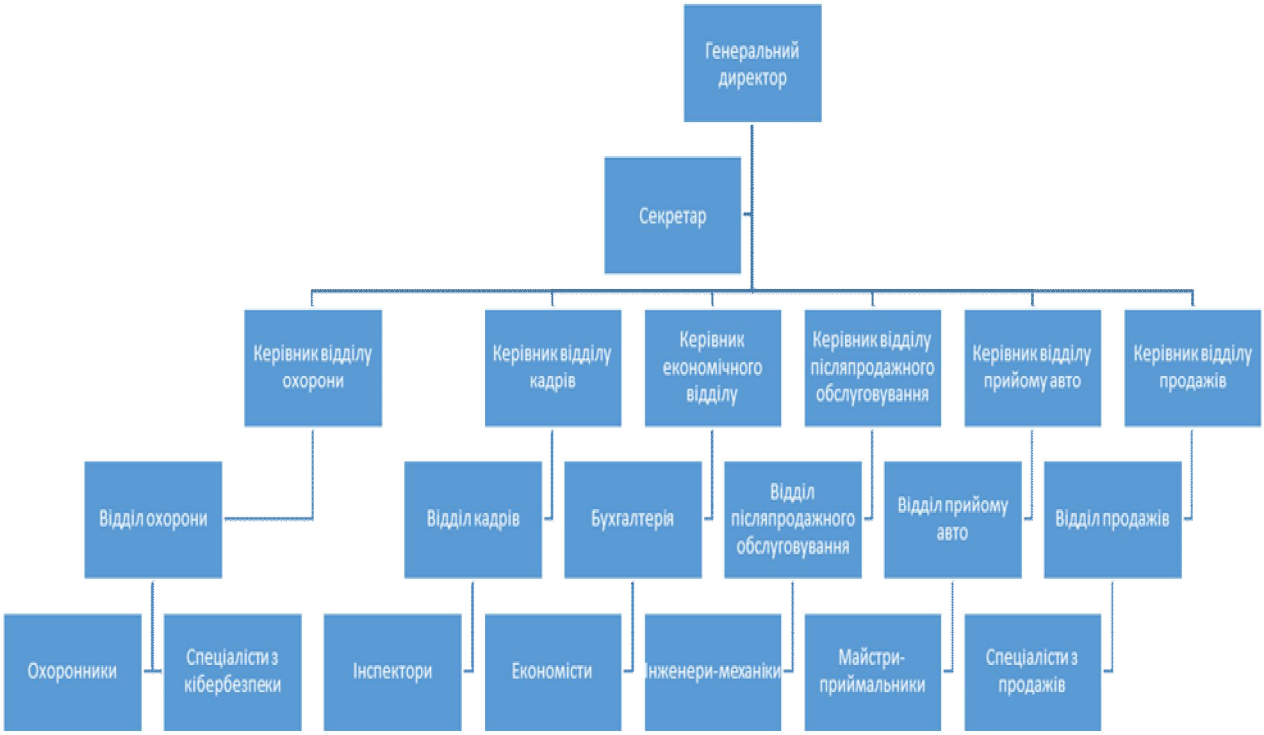

Рисунок. 2.4 – Структура компанії.

Таблиця 2.1. Кількість та види техніки необхідної длядіяльності кожного підрозділу.

Посада	**Техніка**	**К-сть**
Генеральний директор	Комп’ютер Принтер	1 1
Секретар	Комп’ютер Принтер	1 1
Керівник відділу охорони	Комп’ютер	1
Охоронники	Комп’ютер	3
Спеціалісти з кібербезпеки	Комп’ютер Сервер	3 1
Керівник відділу кадрів	Комп’ютер	1
Інспектори відділу кадрів	Комп’ютер	3
Керівник економічного відділу	Комп’ютер Принтер	1 1
Економісти	Комп’ютер	5

Керівник відділу післяпродажного обслуговування	Комп’ютер	1
Інженери-механіки	Комп’ютер	4
Керівник відділу прийому авто	Комп’ютер	1
Майстри-приймальники	Комп’ютер	3
Керівник відділу продажів	Комп’ютер	1
Спеціалісти з продажів	Комп’ютер	6
Всього	Комп’ютер Принтер Сервер	39 7 1

Фундамент будівлі - залізобетонний; зовнішні стіни цегляні товщиною 95 см. Перекриття між поверхами виконані із залізобетонних плит. Дах будівлі скатний, вкритий залізом. Вікна в приміщеннях будівлі металопластикові. Вікно приміщення № 129 орієнтовано у північно-східному напрямку. Огорожа навколо будинку відсутня, територія впорядкована, покриття виконано асфальтом та тротуарною плиткою.

Категорія об'єкта – «четверта», на базі якого спроектовано АС класу «1», що призначений для оброблення інформації з обмеженим доступом.

Для організації пропускного режиму, контролю за дотриманням внутрішньо об'єктового режиму та охорони будинку, організовано цілодобовий пост охорони, який розташовано на першому поверсі у вестибюлі. Прохід працівників та відвідувачів до будівлі здійснюється через центральний вхід.

ПЛАН БУДІВЛІ

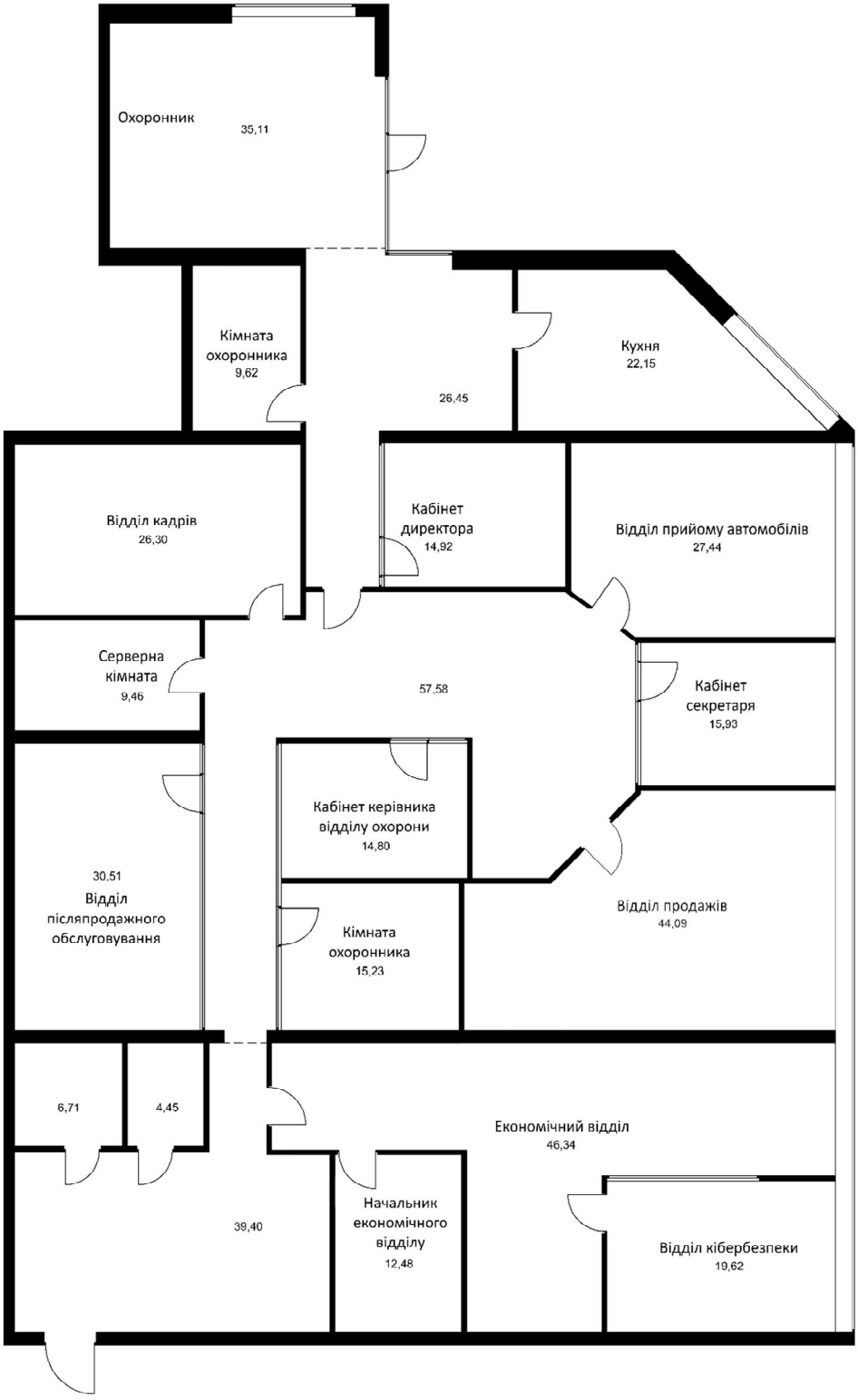

Рисунок 2.5– План будівлі

Таблиця 2.2. Експлікація приміщень.

Назва кімнати	**Довжина стін (м)**	**Загальна площа кімнати ($м^2$)**
Головний вхід	5,95 х 5,95	35,11
Кімната охоронника 1	2 х 4,5	9,62
Кімната охоронника 2	4 х 3,8	15,23
Відділ кадрів	4,6 х 5,8	26,30
Кабінет директора	3,5 х 4,2	14,92
Відділ прийому автомобілів	5 х 5,5	27,44
Кабінет керівника відділу охорони	4 х 3,7	14,80
Відділ продажів	6 х 7,35	44,09
Відділ післяпродажного обслуговування	5 х 6	30,51
Начальник економічного відділу	3 х 4,15	12,48
Економічний відділ	12 + 5 + 5 + 5 + 5 + 4,5 + 5 + 4,5	46,34
Відділ кібербезпеки	4 х 4,9	19,62
Вбиральня 1	2 х 2.225	6,71
Вбиральня 2	2 х 2.225	4,45
Кухня	8 + 5 + 4 + 5	22,15
Коридор 1	1,55 + 4 + 4 + 6 + 5 + 6	26,45
Коридор 2	54	57,58
Коридор 3	9 + 6 + 2 + 3 + 2,225 + 3 + 6 + 6 + 2	39,40
	Всього	453,2

2.2 Вибір топології мережі

Топологією КМ називають спосіб з'єднання в ній комп'ютерів (спосіб організації фізичних зв'язків). Іншими словами топологія - це конфігурація графа, вершинам якого відповідають комп'ютери мережі (іноді й інше обладнання, наприклад концентратори), а ребрам - фізичні зв'язки між ними.

Вибір топології істотно впливає на ряд характеристик мережі. Наприклад, наявність резервних зв'язків підвищує її надійність і робить можливим балансування завантаження окремих каналів. Простота приєднання нових вузлів, яка властива деяким топологіям, робить КМ легкорозширюваною. Економічні міркування часто приводять до вибору топологій, для яких характерна мінімальна сумарна довжина ЛЗ [5].

Повнозв'язна топологія відповідає мережі, в якій кожний комп'ютер мережі має зв'язки з усіма іншими її комп'ютерами. В загальному випадку це досить громіздкий і неефективний варіант КМ, оскільки потребує велику кількість комунікаційних портів для забезпечення такого зв'язку (кількість ЛЗ у такій КМ буде, n(n-1)/2, де n – кількість вузлів у мережі). Повнозв'язана топологія застосовуються дуже рідко. Найчастіше вона використовується в багатомашинних комплексах або ГКМ при невеликій кількості комп'ютерів.

Всі інші варіанти топологій засновані на неповнозв'язаних структуррах, коли для обміну даними між двома комп'ютерами може бути потрібна проміжна передача даних через інші вузли мережі [5].

Коміркова топологія (mesh) виходить з повнозв'язної шляхом видалення деяких можливих зв'язків. У мережі з комірковою топологією зв'язуються лише ті комп'ютери, між якими відбувається інтенсивний обмін даними. Для обміну даними між комп'ютерами, не сполученими прямими ЛЗ, використовуються транзитні передачі через проміжні вузли. Коміркова топологія допускає з'єднання великої кількості комп'ютерів і характерна, як правило, для ГКМ.

Загальна шина донедавна була дуже поширеною топологією для ЛКМ. Тут комп’ютери від’єднуються до одного коаксіального кабелю за схемою “монтажного АБО”. Інформація, що надсилається може розповсюджуватися в обидві сторони. Застосування загальної шини знижує вартість проводки, уніфікує підключення різних модулів, забезпечує можливість майже миттєвого широкомовного звернення до всіх станцій мережі [5].

Основними перевагами такої схеми є дешевизна і простота прокладки кабелю по приміщеннях. Основні недоліки - низька надійність (будь-який дефект кабелю або будь-якого з роз’ємів повністю паралізує всю КМ), невисока продуктивність (оскільки в кожний момент часу тільки один комп’ютер може надсилати дані у мережу). Тому пропускна спроможність каналу зв’язку тут завжди ділиться між усіма вузлами мережі [5].

В мережах з кільцевою конфігурацією дані передаються по кільцю від одного комп’ютера до іншого, як правило, в одному напрямку. Якщо комп’ютер розпізнає дані як “свої”, то він копіює їх у свій внутрішній буфер. У мережі з кільцевою топологією слід вживати спеціальних заходів, щоб у разі виходу з ладу або відключення будь-якої станції не розривався канал зв’язку між іншими станціями. Кільце є дуже зручною конфігурацію для організації зворотного зв’язку: дані, зробивши повний обіг, повертаються до вузла-джерела. Тому останній може контролювати процес доставки даних адресату. Часто ця властивість кільця використовується для тестування зв’язаності мережі і пошуку вузла, який працює некоректно. Для цього у мережу посилаються спеціальні тестові повідомлення.

В той час коли невеликі КМ, як правило, мають типову топологію зірка, кільце або загальна шина, для великих мереж характерна наявність довільних зв’язків між комп’ютерами. В таких мережах можна виділити окремі довільно зв’язані фрагменти (підмережі), що мають типову топологію, тому їх називають мережами зі змішаною топологією [5].

Для даного проекту локальної мережі було обрано топологію зірка. У цьому випадку кожний комп’ютер підключається окремим кабелем до

загального пристрою - концентратора, який знаходиться в центрі мережі і надсилає інформацію, що передається комп’ютером одному або всім іншим комп’ютерам мережі. Головна перевага цієї топології перед загальною шиною - набагато більша надійність (будь-які проблеми з кабелем стосуються лише того комп’ютера, до якого цей кабель приєднаний, і тільки несправність концентратора може вивести з ладу всю КМ). Крім того, концентратор може грати роль інтелектуального фільтра інформації, що надходить від вузлів у мережу, і при необхідності блокувати заборонені адміністратором передачі.

До недоліків топології типу зірка відноситься більш висока вартість мережевого обладнання (внаслідок необхідності придбання концентратора). Крім того, можливості по нарощуванню кількості вузлів у мережі обмежуються кількістю портів концентратора. Іноді доцільно будувати мережу з використанням кількох концентраторів, ієрархічно званих між собою у вигляді зірки [6].

В наш час ієрархічна (розширена) зірка є найпоширенішим типом топології зв’язків як в ЛКМ, так і ГКМ.

2.3 Розміщення апаратного забезпечення

Згідно з державними санітарними правилами та нормами «Влаштування і обладнання кабінетів комп'ютерної техніки» (ДСанШН 5.5.6.009-98) площа приміщення на одне робоче місце повинна становити 6 $м^2$, а об'єм - не менше 20 $м^3$. Площа приміщень з ПК повинна розраховуватись не більш як 12 чоловік.

Не дозволяється розміщувати кабінети обчислювальної техніки у підвальних приміщеннях та на цокольних поверхах. Кабінети, обладнані комп'ютерною технікою, повинні розміщуватись в окремих приміщеннях з природним освітленням та організованим обміном повітря.

Покриття підлоги, стін, стелі мають бути матовими з коефіцієнтами відбиття відповідно 0,2-0,3; 0,4-0,5; 0,7-0,8; робочого столу 0,4-0,5; корпусу

дисплея та клавіатури 0,3-0,5; шаф і стелажів 0,4-0,6. Поверхня підлоги повинна мати антистатичне покриття і бути зручною для вологого прибирання.

Забороняється застосовувати для оздоблення інтер'єру приміщень комп'ютерних класів полімерні матеріали (деревинно-стружкові плити, шпалери, що миються, рулонні синтетичні матеріали, шаруватий паперовий пластик тощо), які виділяють у повітря шкідливі хімічні речовини, що перевищують гранично допустимі норми.

При розташуванні елементів робочого місця користувача ПК слід враховувати робочу позу користувача, простір для розміщення користувача, можливість огляду елементів робочого місця, можливість ведення записів, розміщення документації і матеріалів, які використовуються користувачем.

Робочі місця з ПК повинні бути розташовані від стіни з вікнами на відстані не менш 1,5 м, від інших стін - на відстані 1 м, відстань між ними має становити не менш ніж 1,5 м [6].

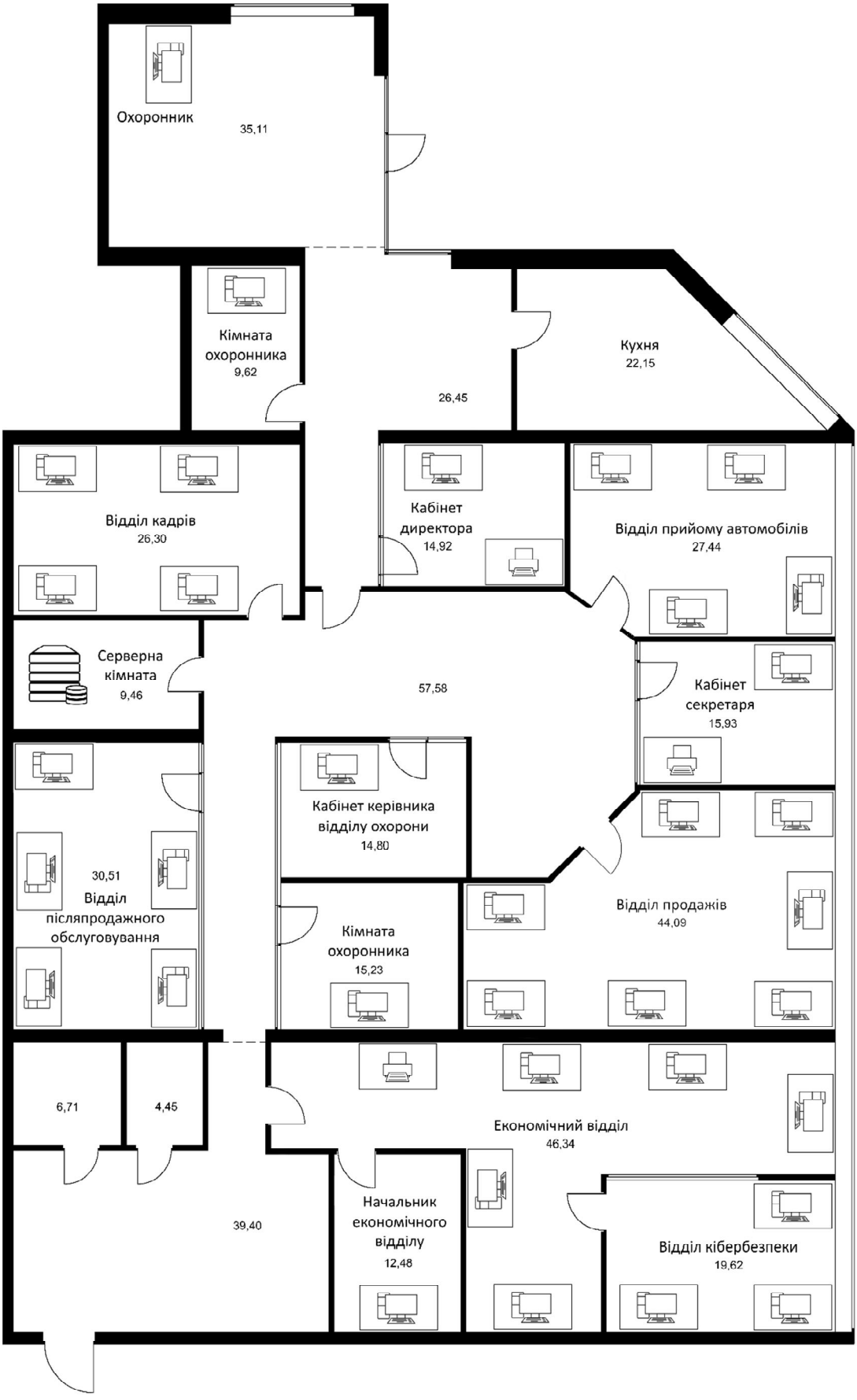

Рисунок. 2.6 – Розміщення апаратного забезпечення.

2.4. Апаратне та програмне забезпечення

Таблиця 2.4. Характеристики апаратного забезпечення.

Найменування	**Характеристика**
Моноблок HP Pavilion All-in-One 27-xa0110ur (7JU42EA) White (клавіатура + миша)	Процесор: Intel Core i7-9700T Чипсет мат. плати: Intel H370 Відеокарта: nVidia GeForce GTX 1050 Обсяг відеопам’яті: 3 ГБ Порти: • 2 x USB 3.1 Type-C Gen2 • 3 x USB 3.1 (1 з підтримкою прискореного заряджання HP Fast Charge 1.2) • 1 x LAN (RJ-45) • 1 x HDMI 1.4 вихід • 1 x HDMI 1.4 вхід • 1 x комбінований роз'єм для навушників і мікрофону • Кардридер Потужність БЖ: 150 Вт Обсяг оперативної пам’яті: 12 ГБ Обсяг SSD: 512 ГБ Дисплей: 27” Full HD (1920x1080) Тип матриці: IPS Бездротові технології: Wi-Fi, Bluetooth Аудіо: B&O PLAY (вбудоване)
Моноблок Lenovo IdeaCentre 3 24ALC6 (F0G100R5UO) Black (клавіатура + миша)	Процесор: AMD Ryzen 5 5625U Чипсет: AMD SoC Platform Відеокарта: AMD Radeon Graphics Порти:

	• 2 x USB 3.2 Gen 2 порти • 2 x USB 2.0 порти • 1 x HDMI 1.4 порт • 1 x LAN (RJ-45) • Аудіо Потужність БЖ: 90 Вт Обсяг оперативної пам’яті: 16 ГБ Обсяг SSD: 512 ГБ Дисплей: 23.8” Full HD (1920x1080) Тип матриці: IPS Бездротові технології: Wi-Fi, Bluetooth Аудіо: вбудоване
Принтер Canon i-SENSYS MF655Cdw EMEA, DADF (5158C004AA)	Технологія друку: лазерний друк Максимальна роздільна здатність друку: 1200x1200 dpi Тип пристрою: БФП Друк: кольоровий, чорно-білий Мережеві інтерфейси: Fast Ethernet, Wi-Fi Кількість кольорів: 4
Сервер Dell Enterprise EMC T40	Процесор: Intel Xeon E-2224G Тактова частота процесора: 4.7 ГГц Кількість ядер: 4 Форм-фактор: Mini-Tower Контролери SATA: Intel C246 Chipset (4 SATA 6Gb/s порти) Жорсткий диск: 2 x 2 Тб Об’єм оперативної пам’яті: 32 Гб Тип оперативної пам’яті: DDR-4 UDIMM ECC Порти:

	• 2 x PS/2 • 2 x DisplayPort • 1 x COMport • 1 x LAN Gbit • 4 x USB2.0 • 5 x USB3.0 • 1 x USB3.1 Type-C • Аудіо Швидкість LAN: 1 Гбіт/с
Жорсткий диск для сервера Western Digital Gold Enterprise	Місткість накопичувача: 8 Тб Інтерфейс підключення: SATA III Швидкість обертання шпинделя: 7200 об/хв Обсяг буфера: 256 Мб Швидкість передавання даних: 255 Мб/с Максимальний рівень шуму: 36 дБ Напрацювання на відмову: 2 000 000 годин

Таблиця 2.5. Вартість апаратного забезпечення.

Найменування	**Кількість**	**Вартість за одиницю, грн**	**Вартість усього, грн**
Моноблок HP Pavilion	3	30 999	92 997
Моноблок Lenovo IdeaCentre	32	28 999	927 968
Принтер Canon	3	17 349	52 047
Сервер Dell	1	99 999	99 999
Жорсткий диск WD Gold	2	9 159	18 318
Всього			1 191 329

2.5 Мережеве обладнання

Комутатор локальної мережі — пристрій, призначений для з'єднання декількох вузлів комп'ютерної мережі в межах одного сегмента.

Для локальної мережі компанії Volvo Poltava було обрано 2 комутатори **TP-LINK TL-SG1024DE**. Дана модель комутатора має 24 порти RJ-45 та підтримує швидкість LAN-портів до 1 Гбіт/с.

Вита пара — вид мережевого кабелю, з однією або декількома парами ізольованих провідників, скручених між собою (з невеликою кількістю витків на одиницю довжини) для зменшення взаємних наведень при передачі сигналу і покритих пластиковою оболонкою. Кабель приєднується до мережевих пристроїв за допомогою з'єднувача RJ-45. Підтримує передачу даних на відстань біля 100 метрів.

RJ-45 — фізичний інтерфейс, який загалом використовується для з'єднання комп'ютерних мереж за допомогою звитої пари через мережевий комутатор, або при створенні мережі з двох комп'ютерів до один одного через мережеву карту.

Таблиця 6. Вартість мережевого обладнання.

Найменування	**Кількість**	**Вартість за одиницю, грн**	**Вартість усього, грн**
Комутатор локальної мережі TP-Link	2	4 983	9 966
Кабель (1 Гбіт/с)	500 м	28	14 000
Конектор RJ-45	60	5.50	330
Всього			24 296

2.6 Програмне забезпечення

Таблиця 7. Вартість програмного забезпечення.

Найменування	**Кількість**	**Вартість за одиницю, грн**	**Вартість усього, грн**
Microsoft Windows 10 Enterprise	1	2 190	2 190
Microsoft Office Pro 2021 (коробкова версія)	1	17 714	17 714
Microsoft Windows Server 2022 Standard - 16 Core License Pack	1	48 323	48 323
BAS Бухгалтерія PROF (для 5 користувачів)	1	16 200	16 200
BAS Бухгалтерія PROF (для 1 користувача)	1	8 400	8 400
Autodesk AutoCAD 2024 (річна підписка)	5	67 543	337 715
Всього			430 542

Вартість мережі

Таблиця 8. Вартість локальної мережі.

Складова	**Вартість, грн**
Програмне забезпечення	430 542
Мережеве обладнання	24 296
Апаратне забезпечення	1 191 329
Вартість локальної мережі	1 646 167
Проектно-кошторисні роботи (10%)	164 616
Всього	1 810 783

2.7. Трасування роботи корпоративної комп'ютерної мережі

NetCracker – це система яка представляє собою CASE-ресурси автоматизованого проектування, моделювання та аналізу комп'ютерних мереж. Дозволяє провести дослідження, результати яких можуть бути використані для обгрунтування вибору типу мережі, середовищ передачі, мережевих складових обладнання та програмно-математичного забезпечення [7].

Програмні ресурси NetCracker дають можливість здійснити збір відповідних даних про існуючу мережу без зупинки її роботи, створити проект цієї мережі та виконати необхідні дослідження для визначення граничних характеристик, можливості розширення, зміни топології та модифікації мережевого обладнання з ціллю подальшого її вдосконалення та розвитку. Для перевірки роботи локальної мережі у програмі NetCracker потрібно:

1. Розташувати комп'ютери та сервери згідно з планом.
2. У двох кабінетах охоронників розташувати комутатори.
3. Встановити на всі ПК мережеві карти – Fast Ethernet Adapters.
4. Поставити драйвера на сервер: File Server, SQL Server, та HTTP Server.
5. Налаштувати трафік між комп’ютером та сервером: File, HTTP та SQL.
6. Запустити роботу локальної мережі, перевірити правильність роботи.

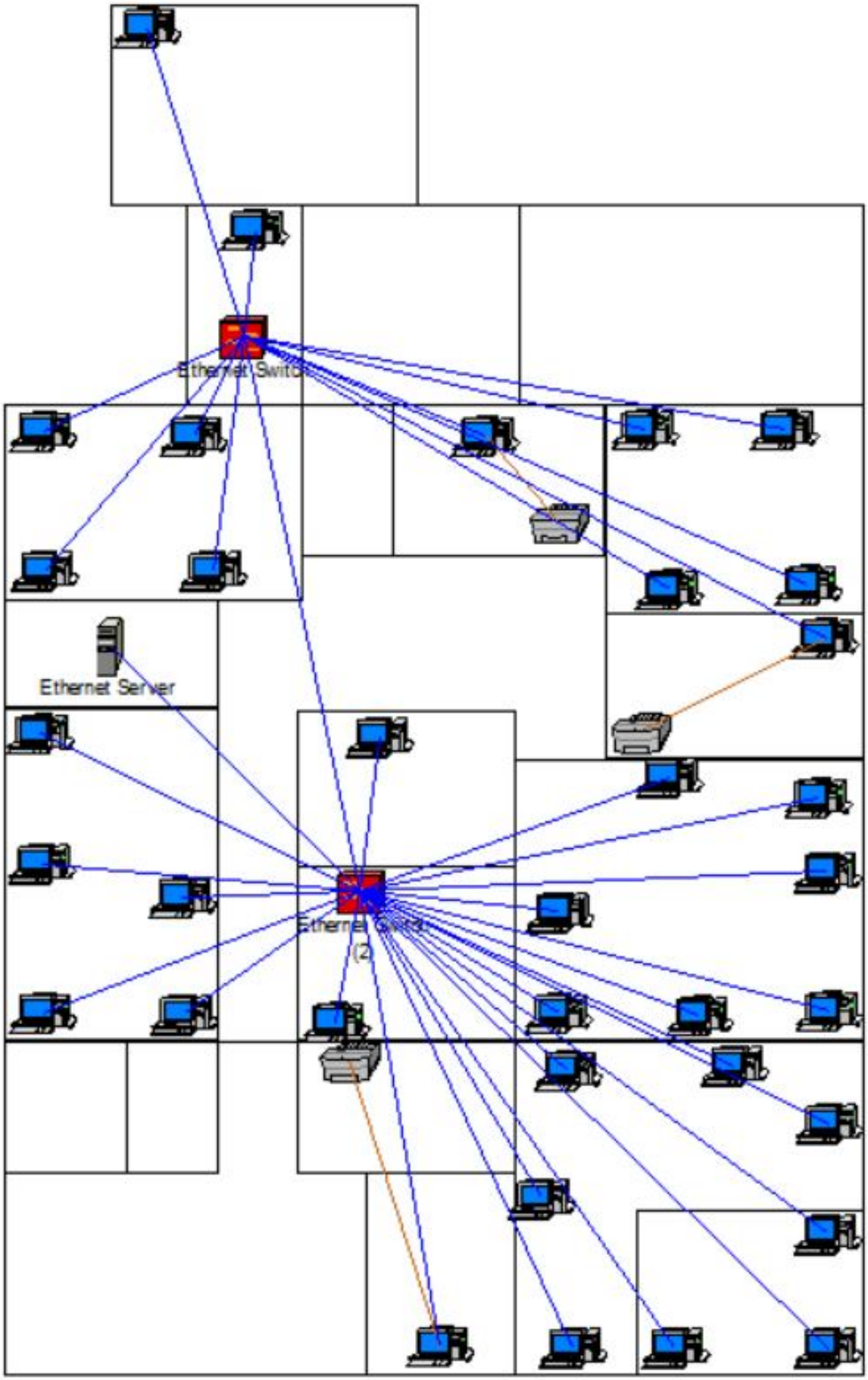

Рисунок. 2.7 Схема локальної мережі.

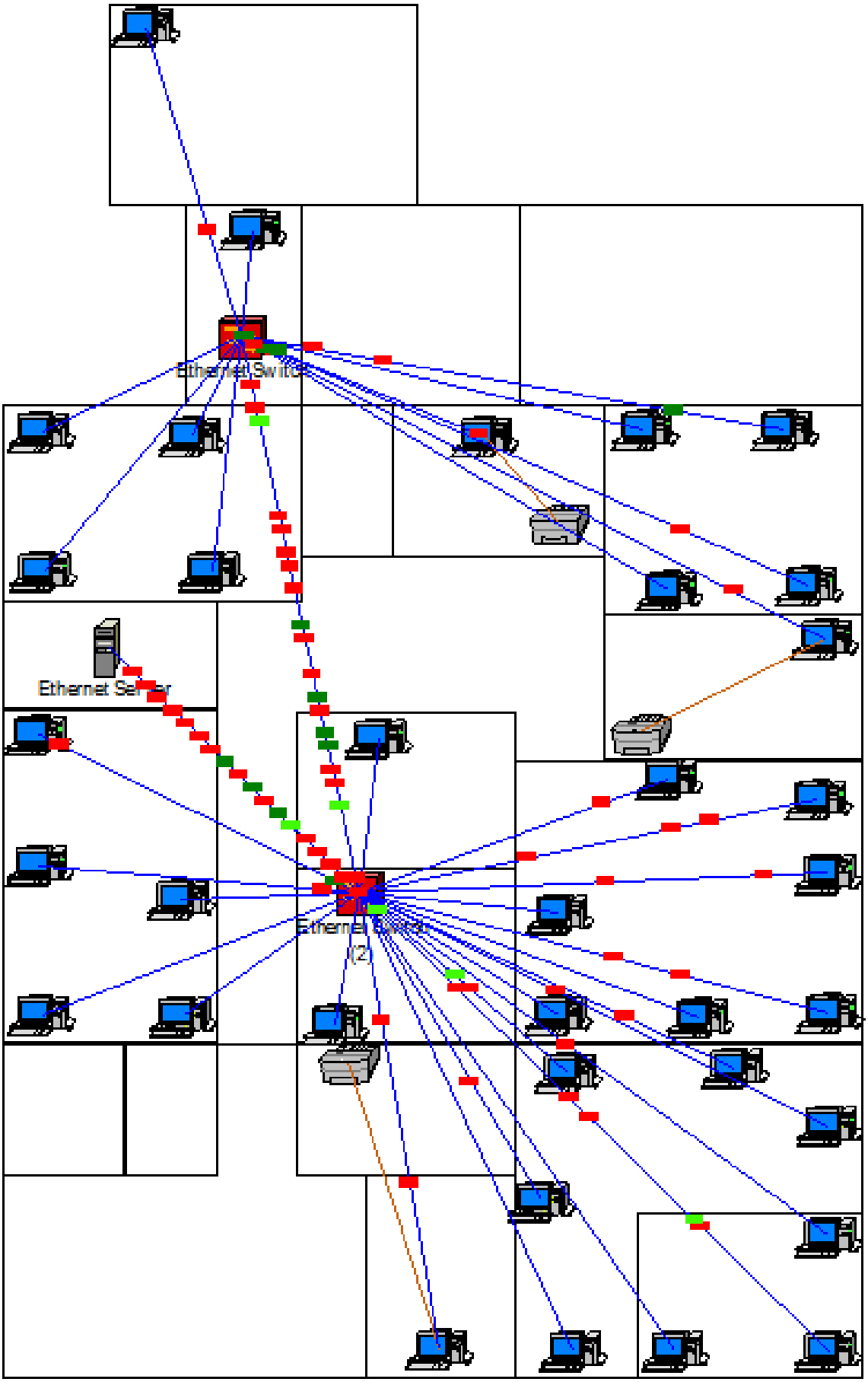

Рисунок. 2.8 Приклад роботи локальної мережі.

3 ПРОГРАМНА СКЛАДОВА РОБОТИ

3.1 Характеристика інформації

Відповідно до призначення, в АС передбачається обробка та зберігання таких видів інформації:

- службова інформація, при роздрукуванні якої матеріальним носіям присвоюється гриф обмеження доступу «Для службового користування», - повинна бути доступною авторизованим користувачам системи в ході виконання ними своїх функцій;
- відкрита інформація – повинна бути доступною авторизованим користувачам системи в ході виконання ними своїх функцій;
- технологічна інформація функціонування АС та бази даних комплексу засобів захисту АС (персональні ідентифікатори, паролі, інформація журналів аудиту тощо) – повинна бути доступною адміністраторам в ході виконання ними службових повноважень [8].

До службової інформації також відноситься технологічна інформація системи захисту, до якої відносяться такі дані:

- база облікових записів:
  - список користувачів (перелік користувачів із їхніми атрибутами доступу та даними, необхідними для автентифікації);
  - список груп користувачів, в якому для кожної групи вказаний перелік її членів;
- атрибути доступу об'єктів;
- журнал реєстрації;
- параметри конфігурації системи, у тому числі атрибути доступу програмних засобів КЗЗ та технологічної інформації;
- оперативні дані про роботу системи [8].

3.2 Захист інформації в локальній мережі

Взагалі, однією із най глобальніших загроз для безпеки інформаційного середовища на сьогодні постають витоки інформації з організацій та підприємств. Базові знання із захисту інформації, навички оперативного попередження витокам інформації в даний час досить цінні , враховуючи те, що у цій галузі особливо гостро відчувається нестача досвідчених кваліфікованих фахівців. Для попередження та протидії зовнішнім загрозам не достатня тільки наявність засобів захисту інформації, а й орієнтуватися та розуміти засади їх коректної роботи, вміти правильно налаштувати на збалансовану роботу згадані засоби, мати поняття про недоліки операційних систем вміти попереджувати її збої та оперативно усувати проблеми [8].

Досліджуючи питання захисту інформації в локальних мережах слід звернутись насамперед до поняття захисту даних, що виступає як діяльність , комплекс заходів щодо запобігання та попередження витоків, викрадення, втрати, підробки та зміни, несанкціонованої діяльності щодо захищеної інформації [8].

Підсумувавши вищезазначене можна сформулювати, що захист інформації в локальних мережах – це поєднання визначених одиниць комп'ютерів на відносно невеликій території, що має кілька вирізняльних специфічних характеристик, пов'язаних з тим, що інформація може легко та оперативно копіюватися та передаватися далі по каналах зв'язку.

На сьогоднішній день сформульовано головні принципи інформаційної безпеки, яка несе на меті забезпечення:

- Конфіденційності інформації;
- Цілісності даних;
- Захисту від збоїв, наслідком яких може бути повна або часткова втрата інформації;
- Доступності інформації для всіх авторизованих користувачів.

Проаналізувавши вітчизняну літературу можна стверджувати , що захист інформації буває:

- непрямим – без фізичної взаємодії із компонентами локальних мереж;
- прямим – з фізичним втручанням до елементів локальних мереж.

В даний час незаконний доступ до інформації, що знаходиться в локальних мережах відбувається шляхом:

- використання прослуховуючих пристроїв;
- портативного фотографування;
- незаконного застосування терміналів;
- несанкціонованого виведення з ладу засобів захисту;
- імітації носіїв інформації;
- активного застосування програмних пасток.

Для розв’язання проблеми захисту інформації, провідними засобами, що застосовуються для забезпечення дієвого захисту, варто звернути увагу на інженерно – технічні та програмні засоби захисту інформації [8].

3.3 Інженерно-технічний захист

Засоби інженерно – технічного захисту інформації – це різноманітні механічні, електронні або електронно-механічні пристрої, пристрої та складові елементи , що забезпечують ефективний захист від викрадення та незаконного доступу до інформації та запобігання її втрати як наслідок порушення функціонування, стихійних лих, диверсій тощо [8].

Я вважаю, що засоби інженерно-технічного захисту інформації в локальній мережі можна поділити на:

1. Фізичні засоби – це будь які апарати, гаджети, пристрої, конструкції, інструменти, що створюють перешкоди для зловмисників. До них належать конструкції та спорудження, що запобігають фізичному доступу чи проникненню злочинців до матеріальних носіїв інформації та на безпосередні

об’єкти захисту, здійснюють захист посадових осіб та причетних співробітників, інформації та матеріальних засобів від протиправної діяльності.

Умовно засоби фізичного захисту можна розмежувати на 3 категорії:

- попереджувальні засоби (посилені двері , грати);
- засоби виявлення (сигналізація);
- засоби ліквідації загроз.

До засобів фізичного захисту належать:

- природні та штучні перешкоди, які протидіють та попереджують незаконне проникнення на територію функціонування об’єкта. На сьогоднішній день можна нарахувати досить значний масив таких засобів (це можуть бути як досить прості сітчасті огорожі та наявність доповнень на них, так і достатньо складні комбінованих огородження, які дозволяють від лякати правопорушника та, в деякій мірі, попередити злочинне діяння);
- специфічні конструкції, проходів, периметрів, дверних та віконних плетінь, особлива будова сховищ та приміщень, наявність сейфів тощо має бути в наявності в обов’язковому порядку задля безпеки для будь-яких підприємств, установ та організацій. Ці структури мусять протистояти будь-яким способам прямого чи опосередкованого фізичного впливу з боку кримінальних елементів. Одним з ключових технічних способів захисту приміщень, сховищ та сейфів є замки. Вони бувають простими (передбачають наявність ключа), з програмними пристроями та кодовими ;
- зони безпеки, які зазвичай розташовуються на об’єкті послідовно, створюючи ланцюг перешкод, що доведеться здолати злочинцеві, починаючи свій шлях від огорожі навколо території об’єкта до сховища інформаційних та матеріальних цінностей [8].

2. Апаратні засоби – складають засоби, пристрої, та інші технічні пристосування, що використовуються з метою захисту інформації. Головною задачею апаратних засобів виступає забезпечення захисту інформації від витоку, розголошення та несанкціонованого доступу використовуючи технічні засоби забезпечення виробничої діяльності .

Як окремим структурним елементом, до групи інженерно – технічних засобів слід віднести:

- засоби захисту кабельної системи. Проаналізувавши статистику, слід зауважити, що більше половини збоїв та відмов локальної обчислювальної мережі (ЛОМ) спричиняють саме неполадки кабельної системи. Найкращим способом вирішення цієї проблеми та попередження подібних ексцесів у майбутньому є побудова структурованої кабельної системи, для якої застосовуються ідентичні кабелі для організації передачі даних, відеозаписів та звітної інформації від охоронної системи, попереджувальних сигналів та маячків від датчиків пожежної безпеки, а також локальної телефонної мережі.

- засоби захисту системи електроживлення. Найдивнішим та надійним засобом, що допомагає попередити витоки інформації у разі стрибків напруги в електромережі або короткочасних тимчасових вимкнень електроенергії є встановлення джерел безперебійного живлення;

- засоби дублювання та архівування інформації. При наявності у користувача значного об’єму інформації для архівації даних доцільним буде організувати віддалений відокремлений спеціалізований сервер. У випадку якщо така інформація є досить цінною то, її варто зберігати у спеціальному, добре захищеному приміщенні;

- засоби захисту від відпливу інформації по різних фізичних полях, що виникають під час роботи технічних засобів – спеціальні засоби розкриття та ліквідації прослуховувальної апаратури, активне радіотехнічне маскування із активним застосуванням спеціалізованих генераторів шумів, електромагнітне екранування приміщень тощо.

Слід зазначити, що найчастіше технічні засоби захисту ефективніше реалізуються в поєднанні з програмними [8].

3.4 Програмний захист

Програмні засоби захисту забезпечують аутентифікацію та ідентифікацію користувачів, диференціації доступу до інформаційних ресурсів відповідно до повноважень активних користувачів, формальну реєстрацію подій, захист інформації від комп'ютерних вірусів, криптографічний захист інформації тощо. Досліджуючи програмні засоби захисту, слід зосередити свою увагу на стенографічних методах. Найчастіше такий спосіб використовується для створення цифрових водяних знаків. На відміну від загальноприйнятих позначень, їх можна закарбувати та ідентифікувати тільки за допомогою спеціального програмного забезпечення – цифрові водяні знаки позначаються як випадково згенеровано по черговості шумових сигналів, сформованих на базі секретних ключів [8].

Системи розмежування доступу

Такі системи призначені для реалізації правил розмежування доступу суб'єктів до даних, мережевих пристроїв створення твердих копій і обміну даними між суб'єктами мереж, а також для управління потоками даних в цілях запобігання запису даних на носії і ін [9].

Розмежування доступу полягає в тому, щоб кожному зареєстрованими користувачу надати можливості безперешкодного доступу до інформації в межах його повноважень і виключити можливості перевищення цих повноважень. Для кожного користувача встановлюються його повноваження щодо файлів, каталогів, логічних дисків та інших системних ресурсів. Для розподілу повноважень суб'єктів по відношенню до об’єктів використовується матрична модель доступу, що може здійснюватися:

• за рівнями таємності (секретно, цілком таємно і т.п.). Користувачеві дозволяється доступ тільки до даних свого або більш низьких рівнів. Захищені дані розподіляються по масивах таким чином, щоб в кожному масиві містилися дані одного рівня таємності;

• спеціальними списками (при цьому розмежування доступу для кожного елемента даних, що захищаються файлу, програми, бази складається список всіх тих користувачів, яким надано право доступу до відповідного елементу. Можливий зворотний варіант, коли для кожного зареєстрованого користувача складається список тих елементів даних, що захищаються, до яких йому надано право доступу);

• матрицями повноважень.

При організації доступу до обладнання істотне значення мають ідентифікація і аутентифікація користувачів, а також контроль і автоматична реєстраціям їх дій. Для впізнання користувача можуть бути використані паролі і індивідуальні ідентифікаційні картки.

Такі системи призначені для реалізації правил розмежування доступу суб'єктів до даних, мережевих пристроїв створення твердих копій і обміну даними між суб'єктами мереж, а також для управління потоками даних в цілях запобігання запису даних на носії і ін [9].

Розмежування доступу полягає в тому, щоб кожному зареєстрованому користувачу надати можливості безперешкодного доступу до інформації в межах його повноважень і виключити можливості перевищення цих повноважень. Для кожного користувача встановлюються його повноваження щодо файлів, каталогів, логічних дисків та інших системних ресурсів.

Для розподілу повноважень суб'єктів по відношенню до об'єктів використовується матрична модель доступу. Розмежування може здійснюватися:

• за рівнями таємності (секретно, цілком таємно і т.п.). Користувачеві дозволяється доступ тільки до даних свого або більш низьких рівнів. Захищаються дані розподіляються по масивах таким чином, щоб в кожному масиві містилися дані одного рівня таємності;

• спеціальними списками. При цьому розмежування доступу для кожного елемента даних, що захищаються (файлу, програми, бази) складається список всіх тих користувачів, яким надано право доступу до відповідного елементу.

Можливий зворотний варіант, коли для кожного зареєстрованого користувача складається список тих елементів даних, що захищаються, до яких йому надано право доступу;

• матрицями повноважень [11].

Механізми аудита і протоколювання облікових записів

При організації доступу до обладнання істотне значення мають ідентифікація і аутентифікація користувачів, а також контроль і автоматична реєстрація їх дій. Для впізнання користувача можуть бути використані паролі і індивідуальні ідентифікаційні картки, а для управління доступом до устаткуванню такі прості, але ефективні заходи, як відключення живлення або механічні замки і ключі для пристроїв.

Організація доступу обслуговуючого персоналу до пристроїв інформаційної системи відрізняється від організації доступу користувачів тим, що пристрій звільняється від конфіденційної інформації і відключаються всі інформаційні зв'язки. Технічне обслуговування та відновлення працездатності пристроїв виконуються під контролем посадової особи.

За увазі управління доступом системи розмежування поділяють:

• на системи з дискреційним управлінням, що дозволяє контролювати доступ названих суб'єктів (користувачів) до пойменованим об'єктів (файлів, програм і т.п.) відповідно до матриці доступу. Контроль доступу застосуємо до кожного об'єкту і кожному суб'єкту (індивіду або групі рівноправних індивідів). Крім того, є можливість санкціонованого зміни списку користувачів і списку об'єктів, що захищаються, передбачені кошти управління, що обмежують поширення прав на доступ як для явних, так і для прихованих дій користувача;

• мандатні системи. Для реалізації мандатної принципу управління доступом кожному суб'єкту і кожному об'єкту призначаються класифікаційні мітки, що відображають їх рівень (уразливості, категорії секретності і т.п.) у відповідній ієрархії [11].

Забезпечують засоби для системи розмежування доступу виконують ідентифікацію та аутентифікацію суб'єктів; реєстрацію дій суб'єкта і його

процесу; зміна повноважень суб'єктів і включення нових суб'єктів і об'єктів доступу; тестування всіх функцій захисту інформації спеціальними програмними засобами та ряд інших функцій.

Обліку підлягають створювані захищаються файли, каталоги, томи, області оперативної пам'яті і інші об'єкти. Для кожної події повинна реєструватися інформація (суб'єкт, дата і час, тип події та ін.) З видачою друкованих документів відповідного зразка. Крім того, може автоматично оформлятися облікова картка документа із зазначенням дати видачі, облікових реквізитів, найменування, виду, шифру, коду і рівня конфіденційності документа [11].

Особливості реалізації системи. В системі розмежування доступу повинен бути використаний диспетчер, який здійснює розмежування доступу відповідно до заданого принципом розмежування. Розмежування доступу до інформаційних об'єктів здійснюється відповідно до повноважень суб'єктів. Основою такого розмежування є обрана модель управління доступом, що реалізується диспетчером доступу. Диспетчер забезпечує виконання правил розмежування доступу суб'єктів до об'єктів доступу, які зберігаються в базі повноважень і характеристик доступу. Запит на доступ суб'єкта до деякого об'єкту надходить в блок управління базою і реєстрації подій. Повноваження суб'єкта і характеристики об'єкта аналізуються в блоці прийняття рішень. За результатами аналізу формується сигнал дозволу або відмови в допуску ("Допустити", "Відмовити"). Якщо число сигналів "Відмовити" перевищить заданий рівень (наприклад, 5 разів), який фіксується блоком реєстрації, то блок прийняття рішень видає сигнал "Несанкціонований доступ". На підставі цього сигналу адміністратор системи безпеки може заблокувати роботу суб'єкта для з'ясування причини таких порушень [11].

Модель Бела-Ла Падули є моделлю розмежування доступу до інформації, що захищається. Вона описується скінченним автоматом з допустимим набором станів, у яких може знаходитись інформаційна система. Усі елементи у складі інформаційної системи поділені на суб'єкти і об'єкти. Кожному суб'єкту

приписується рівень доступу, який відповідає рівню конфіденційності. Аналогічно об'єкту надається рівень таємності. Поняття захищеної визначається наступним чином: кожен стан системи повинен відповідати політиці безпеки, встановленої для даної інформаційної системи. Перехід між станами описується функціями переходу. Система знаходиться у безпечному стані тільки у тому випадку, коли у кожного суб'єкта наявний доступ тільки до тих об'єктів, до яких від дозволений на основі поточної політики безпеки [12].

Таблиця 3.1 - Матриця доступу

Види інформації / Відділи	Загальна інформація	Особиста інформація	Фінансова інформація	Економічна інформація	Правова інформація	Технічна інформація
Сервер	+	+	+	+	+	+
Генеральний директор	+	-	-	-	-	+
Секретар	+	-	-	-	-	+
Керівник відділу охорони	+	-	-	-	-	+
Охоронник	+	-	-	-	-	+
Охоронник	+	+	-	-	+	+
Охоронник	+	+	-	-	+	+
Спеціаліст з кібербезпеки	+	-	-	-	-	+
Спеціаліст з кібербезпеки	+	+	-	-	-	+
Спеціаліст з кібербезпеки	+	-	-	-	-	-
Керівник відділу кадрів	+	-	-	-	-	-

Інспектор відділу кадрів	Н	Н	Т	Т	Т	ДСК

Н – нетаємна;

Т – таємна;

ДСК – для службового користування.

Таблиця 2 - Мандатна модель доступу

Види інформації / Відділи	Загальна інформація	Особиста інформація	Фінансова інформація	Економічна інформація	Правова інформація	Технічна інформація
Сервер	П	П	П	П	П	П
Генеральний директор	Ч	Н	Н	Н	Н	П
Секретар	Ч	Н	Н	Н	Н	Ч
Керівник відділу охорони	Ч	Н	Н	Н	Н	Ч
Охоронник	Ч	Н	Н	Н	Н	Ч
Охоронник	П	П	Н	Н	П	П
Охоронник	П	П	Н	Н	П	П
Спеціаліст з кібербезпеки	Ч	Н	Н	Н	Н	Ч
Спеціаліст з кібербезпеки	Ч	Ч	Н	Н	Н	Ч
Спеціаліст з кібербезпеки	Ч	Н	Н	Н	Н	Н
Керівник відділу кадрів	Ч	Н	Н	Н	Н	Н
Інспектор відділу кадрів	Ч	Н	Н	Н	Н	Н

Ч – читання;

ЧС – частковий доступ;

Н – немає доступу;

П – повний доступ;

Протоколювання – це процес збирання і накопичення інформації про події, що відбуваються в інформаційній системі.

У кожного сервісу свій набір можливих подій, але у будь-якому випадку їх можна розділити на:

- зовнішні (викликані діями інших сервісів);
- внутрішні (викликані діями самого сервісу);
- клієнтські (викликані діями користувачів і адміністраторів).

Аудит – це аналіз накопиченої інформації, що здійснюється оперативно, у реальному часі або періодично.

Оперативний аудит з автоматичним реагуванням на виявлені нештатні ситуації називається активним.

Протоколювання й аудит дозволяють розв’язати такі задачі:

- забезпечення підзвітності користувачів і адміністраторів. Якщо користувачі і адміністратори знають, що все їх дії фіксуються, вони, можливо, утримаються від незаконних операцій. Очевидно, якщо є підстави підозрювати якого-небудь користувача в нечесності, можна реєструвати всі його дії, аж до кожного натиснення клавіші. При цьому забезпечується не тільки можливість розслідування випадків порушення режиму безпеки, але і відміна некоректних змін (якщо в протоколі присутні дані до і після модифікації). Тим самим захищається цілісність інформації;
- забезпечення можливості реконструкції послідовності подій,що дозволяє виявити слабкості в захисті сервісів, знайти винуватця вторгнення, оцінити масштаби заподіяного збитку і повернутися до нормальної роботи;

- виявлення спроб порушень інформаційної безпеки– функція активного аудиту. Звичайний аудит дозволяє виявити подібні спроби із запізненням, але і це виявляється корисним;
- надання інформації для виявлення та аналізу проблем може допомогти поліпшити такий параметр безпеки, як доступність. Виявивши вузькі місця, можна спробувати переконфігурувати або перенастроїти систему [9].

Обліковий запис може містити також додаткові анкетні дані користувача: ім'я, прізвище, по батькові, псевдонім, стать, вік, дата народження, адреса e-mail, домашня і робоча адреса, номер домашнього, робочого та мобільного телефону, номер Viber, ідентифікатор Skype, інші контактні дані систем миттєвого обміну повідомленнями, адреса домашньої сторінки та/або блогу в інтернеті, відомості про хобі, про коло інтересів, про сім'ю, про перенесені хвороби, про політичні уподобання, про партійну приналежність, про культурні уподобання, про вміння спілкуватися іноземними мовами тощо. Конкретні категорії даних, які можуть бути внесені в таку анкету, визначаються творцями і (або) адміністраторами системи [9].

Обліковий запис може також містити одну або декілька фотографій або аватар користувача.

Обліковий запис користувача також може враховувати різні статистичні характеристики поведінки користувача в системі на основі відстежень системи: давність останнього входу в систему, тривалість останнього перебування в системі, адреса використаного при підключенні комп'ютера, інтенсивність використання системи тощо [11].

Таблиця 3. Облікові записи користувачів підприємства.

Посада	**Логін**	**Пароль**
Сервер	server-volvo	volvogorsaker
Генеральний директор	gd	gd1000

Секретар	secr	secr1001
Керівник відділу охорони	ohor-ker	ohor2000
Охоронник	ohor1	ohor2001
Охоронник	ohor2	ohor2002
Охоронник	ohor3	ohor2003
Спеціаліст з кібербезпеки	kiber1	ohor2004
Спеціаліст з кібербезпеки	kiber2	ohor2005
Спеціаліст з кібербезпеки	kiber3	ohor2006
Керівник відділу кадрів	hr-ker	hr3000
Інспектор відділу кадрів	hr1	hr3001
Інспектор відділу кадрів	hr2	hr3002
Інспектор відділу кадрів	hr3	hr3003
Керівник економічного відділу	econ-ker	econ4000
Економіст	econ1	econ4001
Економіст	econ2	econ4002
Економіст	econ3	econ4003
Економіст	econ4	econ4004
Економіст	econ5	econ4005
Керівник відділу післяпродажного обслуговування	service-ker	service5000
Інженер-механік	service1	service5001
Інженер-механік	service2	service5002
Інженер-механік	service3	service5003
Інженер-механік	service4	service5004
Керівник відділу прийому авто	carrec-ker	carrec6000
Майстер-приймальник	carrec1	carrec6001
Майстер-приймальник	carrec2	carrec6002
Майстер-приймальник	carrec3	carrec6003
Керівник відділу продажів	sales-ker	sales7000

Спеціаліст з продажів	sales1	sales7001
Спеціаліст з продажів	sales2	sales7002
Спеціаліст з продажів	sales4	sales7004
Спеціаліст з продажів	sales5	sales7005
Спеціаліст з продажів	sales6	sales7006

Для викриття, локалізації та подальшого попередження «електронних заражень» можна застосовувати загальноприйняті засоби та методи захисту інформації (резервне копіювання даних, диференціювання доступу до неї) а також заходи профілактики, що мінімізують можливість зараження та інших ризиків. Спираючись на статистичні дані останніх років, можна прослідкувати появу апаратних пристроїв антивірусного захисту, спеціальні антивіруси, як для прикладу.

Однак, найбільш відомим та найпоширенішим методом залишається використання антивірусних програм – спеціально розроблених програм, які призначені для пошуку, випадкового викриття та подальшої локалізації комп'ютерних вірусів [9].

Антивірусний програмний засіб можна ідентифікувати як – програмне забезпечення (комп’ютерна програма) антивірусного захисту , яке призначене для захисту об’єктів (ресурсів) інформаційно – телекомунікаційної системи від ушкодження комп’ютерними вірусами. В свою чергу можна виокремити поняття антивірусного захисту як діяльність, спрямована запобігання несанкціонованим діям з використанням комп’ютерних вірусів, їх копій, модифікацій щодо інформації в системі. Система антивірусного захисту в інформаційно – телекомунікаційних системах призначена для запобігання несанкціонованим діям з використанням комп’ютерних вірусів, визначення найменувань та версій антивірусного програмного забезпечення, правил та порядку інсталяції, конфігурації та експлуатації антивірусних програмних засобів та контролю за їх функціонуванням, забезпечення та впровадження

антивірусних оновлень, а також контролю стану антивірусного захисту на підприємстві чи організації [10].

Система антивірусного захисту в інформаційно – телекомунікаційних системах складається з системи застосування антивірусних програмних засобів та системи антивірусних оновлень. До організаційного складу системи застосування антивірусного програмного засобу входять штатні та позаштатні підрозділи та спеціалізовані служби захисту інформації в інформаційно – телекомунікаційних системах, а також адміністратори та активні користувачі автоматизованих систем. Система антивірусних оновлень має дворівневу структуру та складається із системи забезпечення антивірусними оновленнями та системи впровадження антивірусних оновлень. Ефективне функціонування серверів та веб – сайтів антивірусного захисту, призначених для обробки інформаційних ресурсів , здійснюється із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. На веб – сайтах антивірусного захисту розміщуються активні посилання на актуальні бази та файли антивірусних оновлень, сигнатур, інсталяційні файли антивірусних програмних засобів, інструкції з антивірусного захисту та порядку активації антивірусних програмних засобів.

Для забезпечення ефективного захисту, коректної роботи антивірусної програми та уникнення шахрайських дій з боку недоброчесних користувачів мережею не рекомендується завантаження антивірусних оновлень та сигнатур з будь – яких невідомих чи підозрілих ресурсів мережі Інтернет, інших автоматизованих систем та джерел, в тому числі з незареєстрованих машинних носіїв інформації тощо. У разі виникнення ситуації, що призвела до неможливості знищення комп’ютерного вірусу та локалізації його наслідків наявним антивірусним програмним засобом з актуальним, на момент інциденту, антивірусним оновленням комп’ютерне обладнання повинно бути тимчасово відключене, а задіяні з цим обладнанням машинні носії інформації не повинні використовуватися до часу знайдення технічного рішення щодо знищення комп’ютерного вірусу.

Варто відмітити, що жоден із розглянутих у роботі з типів антивірусних програм не може забезпечити стовідсоткового захисту, тому не буде зайвим додержуватись загальноприйнятих норм та правил роботи і комп’ютером та користуватися останніми розробками версіями антивірусних файлів.

Я вважаю доречним буде окреслити головні заходи з антивірусного захисту:

- сучасні антивірусні програми слід використовувати комплексно та своєчасно оновлювати їх актуальні версії;
- комп'ютер, його системні області, пам'ять та файли слід регулярно перевіряти з невеликим інтервалом, завантаживши ОС із захищеної від запису диска ;
- носії інформації ,що взаємодіяли з іншими комп’ютерами слід перевіряти на наявність вірусів перед взаємодією із власним;
- файли, що надходять із комп’ютерних мереж також мають піддаватися антивірусній перевірці;
- якщо на носіях інформації не ведеться запис, їх завжди слід закривати від запису під час роботи на інших комп’ютерах;
- рекомендовано завжди робити архівні копії цінної інформації.

Система захисту файлових служб та служб баз даних має на меті забезпечити захист автоматизованої системи від комп'ютерних вірусів шляхом попередньої перевірки файлів та процесів на цих електронно-обчислювальних машинах антивірусним монітором, сканером, що встановлюються на цих машинах.

Отже, система антивірусного захисту повинна забезпечувати:

- можливість безперервного захисту об'єктів згідно із політикою безпеки та встановленими вимогами;
- можливість миттєвого реагування та автоматизованого блокування подальшого проникнення до системи комп'ютерних вірусів з усіх можливих джерел;

- ліквідування наслідків роботи та безпосередньо комп'ютерних вірусів із обов’язковим внесенням інформації про це у спеціальні протоколи для забезпечення моніторингу антивірусної роботи;
- можливість оперативного повідомлення причетних осіб щодо виникнення особливих чи критичних ситуацій;
- гнучке масштабування при появі нових об'єктів антивірусного захисту у АС;
- забезпечення ліцензійність застосованого антивірусного програмного забезпечення постачальниками.

Найбільш поширеним методом залишається використання антивірусних програм – спеціальних програм, призначених для виявлення і знищення комп'ютерних вірусів

Слід зазначити, що жодний з типів антивірусних програм не надає стовідсоткового захисту, тому слід додержувати загальних правил і користуватись останніми розробками антивірусних лабораторій.

Norton AntiVirus Plus.

Антивірусна програма сканує та допомагає видалити шкідливі файли, які потрапляють у комп'ютер, планшет чи смартфон. Технологія Norton AntiVirus використовує машинне навчання, щоб визначити, чи файл шкідливий, і може зробити це, навіть якщо стикається з цим файлом вперше.

Захист Norton також використовує «емуляцію» (запуск кожного файлу на спрощеній віртуальній машині), щоб змусити онлайн-загрози повідомити про себе. Це відбувається за мілісекунди, поки ви двічі клацаєте файл на робочому столі. Дані сигнатур файлів тепер зберігаються в хмарі, і захист Norton піддався сотням оптимізації антивірусного ядра, щоб мінімізувати вплив на взаємодію з користувачем.

Технологія безпеки Norton включає різні засоби захисту від вірусів та шкідливих програм. Наші технології засновані на штучному інтелекті та машинному навчанні. Ми є частиною найбільшої у світі мережі аналізу кібербезпеки. Захист включає наступне:

1. Система запобігання вторгненням аналізує інформацію, що надходить з мережі, і допомагає блокувати потенційні онлайн-загрози до того, як вони зможуть впливати на ваш комп'ютер.

2. Антивірус із розширеними можливостями машинного навчання сканує та видаляє файли шкідливих програм, що проникають на пристрій, використовуючи емуляцію для перевірки та аналізу дій файлів.

3. Захист репутації використовує інформацію про репутацію, отриману з глобальної мережі для класифікації файлів програм на основі їх атрибутів.

4. Поведінковий захист використовує штучний інтелект для класифікації програм на основі поведінки та автоматично блокує програми, які демонструють підозрілу поведінку.

5. Превентивний захист від експлойтів допомагає захистити від «атак нульового дня», які використовують уразливості у додатках чи операційній системі.

6. Power Eraser виявляє та допомагає видаляти програми з високим ступенем ризику та шкідливі програми, які можуть перебувати на вашому комп'ютері.

Безумовно, найкращим антивірусним програмним забезпеченням є рішення від перевіреного постачальника, яке пропонує надійні та ефективні технології захисту від вірусів та шкідливих програм та яке підтримується готовими завжди прийти на допомогу спеціалістами служби підтримки. Тому оцінивши різні продукти різних виробників для встановленя в архіві Полтавської політехніки ми рекомендуємо саме Norton AntiVirus Plus.

3.5. Криптологічний захист

Криптологія – наука про захист інформації, шляхом її перетворення. Криптологія поєднує два напрямки – криптографію й криптоаналіз. Слід зазначити, що ці дві науки – парна категорія. Розвиток однієї з них є поштовхом

для іншої. Розглядати окремо криптографію від криптоаналізу, значить порушити основи філософії й один з її законів єдності й боротьби протилежностей.

Криптосистема Рабіна — асиметрична криптографічна система, безпека якої забезпечується складністю пошуку квадратних коренів складеного числа. Безпека системи, як і безпека методу RSA, обумовлена складністю розкладання на множники великих чисел. Зашифроване повідомлення можна розшифрувати 4-а способами. Недоліком системи є необхідність вибору істинного повідомлення з 4-х можливих.[18]

Система Рабіна, як і будь-яка асиметрична криптосистема, використовує відкритий і закритий ключі. Відкритий ключ використовується для шифрування повідомлень і може бути опублікований для загального огляду. Закритий ключ необхідний для розшифровки і повинен бути відомий тільки одержувачам зашифрованих повідомлень.

Процес генерації ключів наступний:

- вибираються два випадкових числа **p** і **q** з урахуванням таких вимог:
- числа повинні бути великими (див. розрядність):
- числа повинні бути простими;
- повинна виконуватися умова: $\mathbf{P \equiv Q \equiv 3 \bmod 4}$.

Виконання цих вимог сильно прискорює процедуру вилучення коренів за модулем p і q:

- обчислюється число $\mathbf{n = p \cdot q}$;
- число n — відкритий ключ; числа **p** і **q** — закритий.

Початкове повідомлення **m** шифрується за допомогою відкритого ключа — числа **n** за такою формулою: $\mathbf{c = m^2 \bmod n.}$

Завдяки використанню множення по модулю швидкість шифрування системи Рабина більше, ніж швидкість шифрування за методом RSA, навіть якщо в останньому випадку вибрати невелике значення експоненти.

Для розшифровки повідомлення необхідно закритий ключ - числа **p і q**. Процес розшифровки виглядає наступним чином:

- спочатку, використовуючи алгоритм Евкліда, з рівняння $y_p \cdot p + y_q \cdot q = 1$ знаходять числа y_p і y_q ;
- далі, використовуючи китайську теорему про залишки, обчислюють чотири числа:

$$\begin{aligned} r &= (y_p \cdot p \cdot m_q + y_q \cdot q \cdot m_p) \bmod n \\ -r &= n - r \\ s &= (y_p \cdot p \cdot m_q - y_q \cdot q \cdot m_p) \bmod n \\ -s &= n - s \end{aligned}$$

Одне з цих чисел є істинним відкритим текстом m .[18]

Ефективність. Розшифровка тексту крім правильного наводить ще до трьох хибним результатам. Це є головною незручністю криптосистеми Рабіна і одним з факторів, які перешкоджали тому, щоб вона знайшла широке практичне використання.[19]

Якщо вихідний текст являє собою текстове повідомлення, то визначення правильного тексту не є важким. Однак, якщо повідомлення є потоком випадкових бітів (наприклад, для генерації ключів або цифрового підпису), то визначення потрібного тексту стає реальною проблемою. Одним із способів вирішити цю проблему є додавання до повідомлення перед шифруванням відомого заголовка або якоїсь мітки.

Швидкість обчислень. Алгоритм Рабіна схожий на кодування RSA, але замість зведення повідомлення в степінь e при шифруванні використовується операція піднесення блоку повідомлення в квадрат, що сприятливо позначається на швидкості виконання алгоритму без шкоди криптостійкості.

Для декодування китайська теорема про залишки застосована разом з двома зведення в степінь по модулю. Тут ефективність порівнянна RSA.

Вибір потрібного тексту з чотирьох призводить до додаткових обчислювальним затратам. І це послужило тому, що криптосистема Рабіна не отримала широкого практичного використання. [19]

Безпека. Велика перевага криптосистеми Рабіна полягає в тому, що випадковий текст може бути відновлений повністю від зашифрованого тексту

тільки за умови, що дешифрувальник здатний до ефективної факторизації відкритого ключа n.

Криптосистема Рабіна є доказовою стійкою до атаки на основі підібраного відкритого зашифрованого тексту в рамках підходу «все або нічого», тоді і тільки тоді, коли завдання про розкладання цілого числа на прості множники є важкою. [19]

Стійкість за принципом «все або нічого» полягає в тому, що, маючи текст, зашифрований певним алгоритмом, атакуючий повинен відновити блок вихідного тексту, розмір якого, як правило, визначається параметром безпеки криптосистеми. Маючи вихідний і зашифрований текст, атакуючий повинен відновити цілий блок секретного ключа. При цьому атакуючий або домагається повного успіху, або не отримує нічого. Під словом «нічого» мається на увазі, що атакуючий не має ніякої секретної інформації ні до, ні після безуспішної атаки.

Криптосистема Рабіна є абсолютно беззахисною перед атакою на основі обраного шифротекста. Як правило, атакуючий використовує всі наявні у нього можливості. Він вступає в контакт з атакованим користувачем, посилають йому зашифрований текст для подальшої розшифровки і вимагають повернути вихідний текст.

Наприклад, при додаванні надмірності, повторення останніх 64 біта, можна зробити корінь єдиним. Алгоритм розшифрування в цьому випадку видає єдиний корінь, який вже відомий атакуючому.

Процес додатково уразливий, оскільки при кодуванні використовуються тільки квадратні залишки.[18]

Практична частина

Для реалізації криптосистеми Рабіна було використано інтегроване програмне середовище VisualStudio 2017. Код написано мовою програмування C# з використанням частини бібліотеки .NET, а саме Windows Forms. Наведено лістинг створених класів (Додаток 1), зокрема класу Rabin, який відповідає саме за програмну реалізацію усіх необхідних функцій для роботи алгоритму.

Нижче наведено скріншоти роботи програми (Рис.1. – Рис.2.).

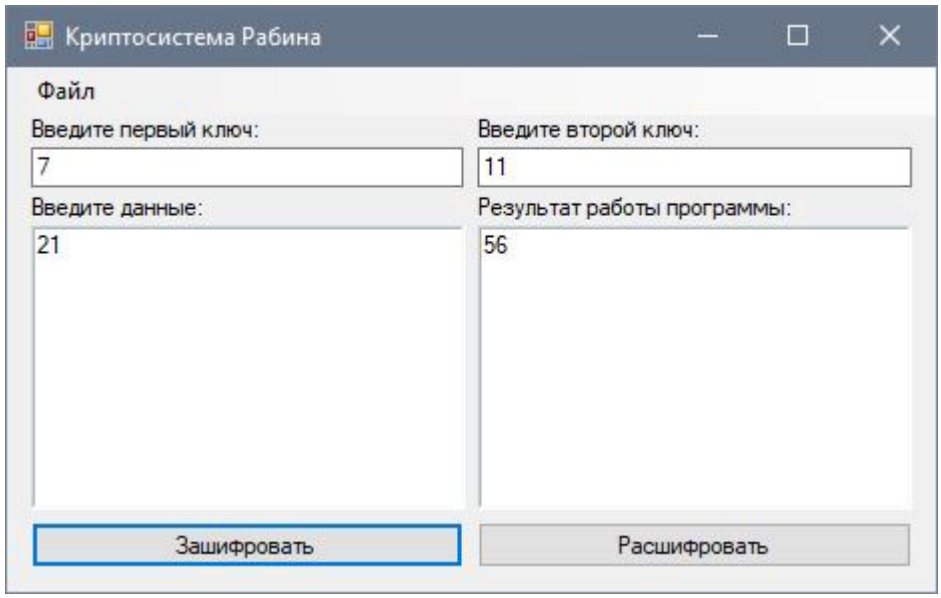

Рисунок 3.1. Режим «Зашифровати»

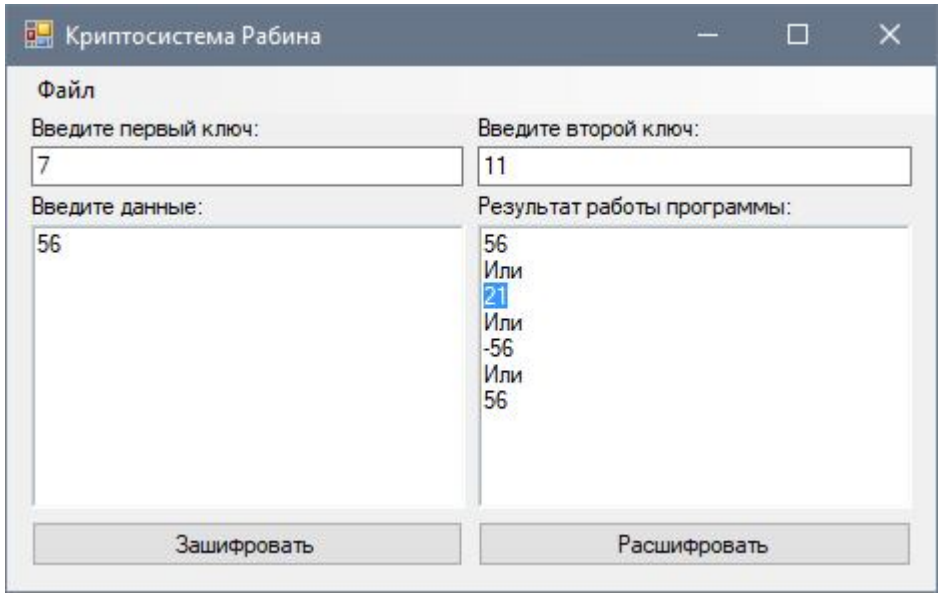

Рисунок 3.2. Режим «Розшифровати»

ВИСНОВКИ

У ході виконання кваліфікаційної роботи бакалавра було розроблено проект локальної комп’ютерної мережі для підприємства топології зірка:

1. Згідно плану будівлі було розміщено:

- 35 комп'ютерів;
- 3 принтери;
- 1 сервер.

2. Для побудови мережі було придбано:

- 2 комутатори;
- 500 метрів кабелю кручена пара;
- 80 конекторів роз'єму RJ-45.

3. На комп'ютери встановлено:

- операційна систему Windows 10 Enterprise;
- Windows Server 2022 на сервер.

4. Придбано програмне забезпечення:

- 1 коробкову версію Microsoft Office Pro 2021;
- 6 пакетів BAS Бухгалтерія PROF;
- 5 річних підписок на Autodesk AutoCAD.

5. Було використано розмежування доступу, побудовано матрицю доступу та мандатнумодельдоступудоінформації.

6. Також виконанозахист інформації на рівні паролю.

7. Рекомендовано використати Norton AntiVirus Plus.

8. Створено облікові записи користувачів та обрано антивірусну програму для захисту інформації підприємства від вірусів, враховуючи всі переваги та недоліки. Розроблено додаток, головною задачею якого є шифрування даних за допомогою криптосистеми Рабіна.

Загальна вартість проекту мережі становить 1 810 783 гривень (49 037,09 доларів США). Проектно-кошторисні роботи – 10% від вартості мережі. Тобто 164616,7 гривень (4 455,46 доларів США).

Трасирування роботи корпоративної локальної мережі було перевірено у програмі Net Cracker.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Інтернет-магазин Rozetka [Електронний ресурс] – Режим доступу: https://rozetka.com.ua/ua/

2. Вільна енциклопедія [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/

3. Розміщення комп’ютерів у приміщенні [Електронний ресурс] – Режим доступу: https://studopedia.com.ua/1_165969_vimogi-do-primishchen-ta-roztashuvannyarobochih-mists-z-pk.html

4. Комп'ютерні мережі та їх призначення [Електронний ресурс] – Режим доступу: http://edufuture.biz/

5. Топологія мережі [Електронний ресурс] – Режим доступу: ahttps://studfiles.net/preview/5263810/page:2/

6. NetCracker Professional 3.1 Portable [Електронний ресурс] – Режим доступу: https://www.twirpx.com/file/1314986/

7. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 02.08.1994 // Відомості Верховної Ради України. – 1994. – № 31. – Ст. 286.

8. Про доступ до публічної інформації: Закон України від 18.02.2011 // Відомості Верховної Ради України. – 2011. – № 32. – Ст. 1491.

9. Гребенніков В. Комплексні системи захисту інформації. Проектування, впровадження, супровід / В. Гребенніков. – Издательские решения, 2018. – 374 с.

10. Про місцеве самоврядування в Україні: Закон України від 12.06.1997 // Відомості Верховної Ради України. – 1997. – № 25. – Ст. 20.

11. Інформаційна безпека підприємства: нові загрози перспективи [Електронний ресурс] / О.А. Сороківська, В.Л. Гевко. – Режим доступу: http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf

12. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах

[Електронний ресурс] / постанова Кабінету Міністрів України від 29 березня 2006 р. № 373 // Урядовий портал. – Режим доступу: https://www.kmu.gov.ua/npas/32791826

13. Рибальський О. В. Основи інформаційної безпеки та технічного захисту інформації / О. В. Рибальський, В. Г. Хахановський, В. А. Кудінов – К.: Вид. Національної академії внутріш. справ, 2012. – 104 с.

14. НД ТЗІ 1.1–003–99 Термінологія у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. – К.: Держстандарт України, 1999.

15. НД ТЗІ 2.5–004–99 критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. – К.: Держстандарт України, 1999.

16. Вишняков В. М. Захист даних в інформаційних системах: навчальний посібник / В. М. Вишняков. – К.: КНУБА, 2010. – 128 с.

17. Шорошев В. В. Теоретичні і практичні аспекти організації і побудови архітектури захищених комп'ютерних систем. Монографія / В. В. Шорошев – К.: ДУПСТ, 2011. – 257 с.

18. Wikipedia [електронний ресурс] – Криптосистема Рабіна: https://uk.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D0%A0%D0%B0%D0%B1%D1%96%D0%BD%D0%B0

19. Романец Ю.В., Тимофєєв П.А., Шаньгин В.Ф. Захист інформації в комп'ютерних системах і мережах. Під ред. В.Ф. Шаньгина. - 2-і изд., перераб. і доп. - М.:Радіо і зв'язок, 2001. - 376 с.: іл.

20. Герасименко В.А., Размахнин М.К. "Криптографічні методи в автоматизованих системах" Закордонна радіоелектроніка,1982,N8

21. Сяо Д., Керр Д., С.Медник "Захист ЕОМ",М.,Світ,1982 - розглянуті практично всі аспекти захисту інформації в обчислювальних і автоматизованих системах.

Додатки

1 ANALYTICAL OVERVIEW OF THE PROBLEM AND STATEMENT OF THE RESEARCH PROBLEM

1.1 Theoretical information

A computer network is a communication system between two or more computers. In a broader sense, a computer network is a communication system through a cable or air medium, computers of various functional purposes and network equipment. Various physical phenomena can be used to transmit information, as a rule – various types of electrical signals or electromagnetic radiation [1].

Transmission media in computer networks can be telephone cables and special network cables: coaxial cables, twisted pairs, fiber optic cables, radio waves, light signals.

The immediate basis of computer networks (CM) were telephone and telegraph networks, as a result of the development of microelectronics, powerful electronic computing machines appeared, for the interaction of which there was a need for a fast and reliable data transmission channel.

Modern computer networks provide:

• collective data processing by users

• exchange of files and other data between users

• share applications

• shared use of printers, modems, etc.

To classify computer networks, various features are used, the choice of which is to select from the existing diversity those that would provide the given classification scheme with unique qualities [1].

Computer networks are classified according to the following characteristics:

• by territorial location – local, regional, global;

• by scope of application – office, industrial, household;

• by a complex of architectural solutions – Ethernet, Token Ring, Arcnet;

• by topology - bus, ring, star-shaped, tree-shaped, fully connected;

• according to the physical medium of transmission - with a symmetrical cable, with a coaxial cable, with a "twisted pair" cable, with a fiber-optic cable, with an infrared channel, with a microwave channel;

• according to the method of access to the physical transmission medium - with polling, with token access, with rivalry, with register setting.

• on the basis of structural and functional organization.[2]

A certain inconsistency of requirements for classification makes the task of choosing a rational classification scheme of CM quite difficult. Mainly, CMs are classified according to structural and functional organization.

By appointment, CMs are divided into:

• computing;

• informative;

• mixed (informational and computational)

Until recently, the construction of the network was limited only to territorial scales, but today, with the development of technology, this has changed, and now these scales of territories have become the same for both local networks and global networks, which differ only in the technological capabilities of network construction.

Computer networks are divided into:

• local network;

• global network.

Local networks are networks with a maximum distance between nodes of no more than 1–2 km.

Global networks – networks covering the territory of a country or several countries with a maximum distance between individual nodes of thousands of kilometers. The structure of modern global networks is shown in Figure 1.1 [2].

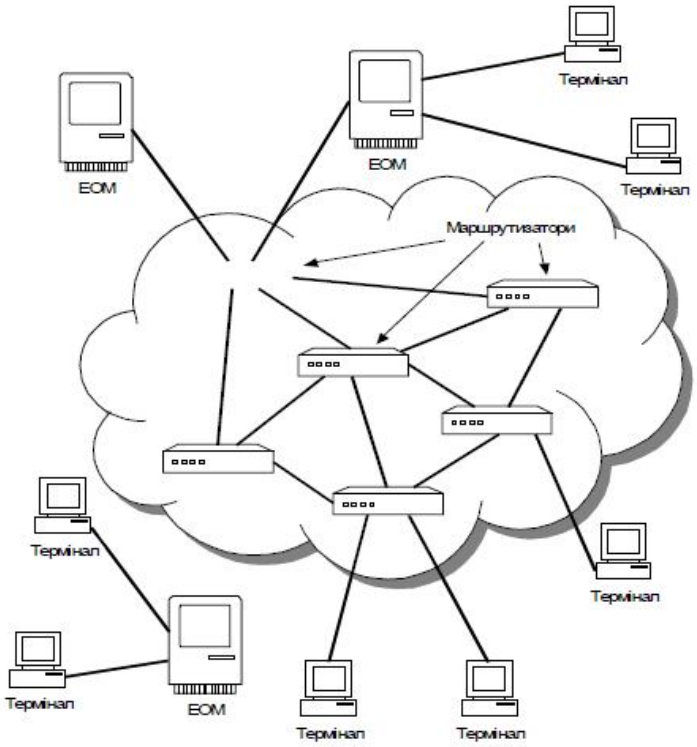

Figure 1.1 – Structure of modern networks

.

A computer network is a collection of computers and other devices connected by data transmission channels [3].

Computer networks provide shared access to data. In the network, computers are allocated, on which large data sets are placed, and users of other computers in the network get access to them. This makes it possible, for example, for people working on the same project to use data created by others, that is, to work on the project at the same time.

With the help of a computer network, it becomes possible to share peripheral devices: printers, scanners, modems, etc. It is not profitable to have them near each personal computer, for example, in a computer class or in a bank [4].

The main purpose of all computer networks is shared access to network resources (computer hardware, peripheral devices), shared use of data and their rapid exchange, shared use of software.

Network interaction involves remote access to network resources and occurs by technology. Depending on the authority, computers in the network are divided into servers and clients [4].

A client is a user's computer that makes a request, a server is a computer that processes this request and responds to it [4].

We draw your attention: both the computers in the network and the software running on these computers are called the server and the client.

In centralized networks, one powerful computer is allocated - a dedicated server, which performs the main functions of organizing the network. Such networks are also called "client-dedicated server". All clients access network resources through the server [4].

A special operating system (for example, 52g) is installed on the server. The operating system allows you to organize and control the work of computers and users in the network, to grant each user certain access rights to the resources and data of this network. For this purpose, each user receives a username (login) and a password for entering the network [5].

Examples of such a network can be the computer networks of banks, corporations, higher educational institutions, some schools in Kyiv, and others.

The advantages of centralized computer networks are the high speed of data exchange and the ability to distribute user access rights in them. But a significant drawback is that when the server fails, the entire network stops working [5].

In decentralized networks, there is no dedicated server, any computer can be both a server and a client. Such networks are also called peer-to-peer. As a client, a computer in a peer-to-peer network can request access to the resources of other computers in the network. As a server, the computer must process requests from other computers on the network and provide the required data.

In a peer-to-peer network, all computers have the same rights (ranks) to access each other's resources and peripheral devices. Each network user can define folders and files on his hard disk that he provides for public use [4].

In such networks, an operating system is installed on all computers, which provides them with equal opportunities.

The advantage of peer-to-peer networks is the ability of the network to function when any of the computers fails, and the disadvantage is the impossibility of distributing the rights of clients regarding work in the network.

An example of such a network can be a computer class network in most schools.

A local area network is a computer network that connects computers that are located in one room or several rooms located at a short distance from each other [4].

But local networks do not allow users who are located, for example, in different parts of the city, to share data. Regional networks that connect computers within one region (district, city, country) come to the rescue. Examples of such a network are a computer network that connects computers located in the houses of one or more blocks, computers of district school directors, the "Volya" computer network in Kyiv, and others [3].

1.2 Comprehensive protection system

A comprehensive system of information protection (CIS) is an interconnected complex of organizational and engineering measures, means and methods of information protection.

Information protection in modern conditions is becoming an increasingly difficult problem due to a number of circumstances, the main of which are:

• widespread use of electronic computing;

• complication of encryption technologies;

• the need to protect not only state and military secrets, but also industrial, commercial and financial secrets;

• increasing the possibilities of unauthorized actions regarding information [8].

In addition, tools and methods of unauthorized and secret information retrieval have become widespread. They are increasingly used not only in the activities of state law enforcement agencies, but also in the activities of various criminal groups. It should be remembered that natural channels of information leakage are formed

spontaneously due to specific circumstances that have developed at the object of protection [8].

Protection of state secrets has always been an important component of the country's defense capability. With the beginning of the introduction of information systems in various, first of all, law enforcement agencies, there was a need to ensure demarcation of access to the resources of these systems by analogy with paper media. Thus, in 1970, the first theoretical model of access delimitation, ADEPT-50, appeared in the USA, and in 1985, the US Department of Defense issued the first criteria for assessing the security of computer systems, the so-called "Orange Book". These criteria, in fact, were based on the generalized experience of building information protection systems in state structures. Thus, it was the state sector that became the locomotive of the development of the global information security market. Technologies that were successfully used in law enforcement agencies were subsequently put at the service of both private businesses and home users [9].

In the process of evolution of information protection technologies and systems, it became necessary to unify the requirements for their creation and ensure some standardization. One of the most important results of this work was the international standard ISO / IEC 15408, the so-called "General Criteria", which was recognized in many countries of the world, including our neighbors. Ukraine chose its own path by developing a series of normative documents of the technical information protection system, the key of which is ND TZI 2.5-004-99 "Criteria for evaluating the security of information in computer systems against unauthorized access" and is based on the "Canadian security criteria" of 1993. This document is used in the design and creation of complex information protection systems of state information resources, as well as systems that process information with limited access, the requirement for the protection of which is defined by law. The definition of a comprehensive information protection system (CIS) as an interconnected set of organizational and engineering measures, means and methods of information protection is given in the Law of Ukraine "On Information Protection in Information and Telecommunication Systems" [9].

The main goal of the creation of the CSZI is to achieve the maximum efficiency of protection due to the simultaneous use of all necessary resources, methods and means that exclude unauthorized access to information, and to create conditions for processing information in accordance with the current regulatory legal acts of Ukraine in the field of information protection: the Law of Ukraine "On protection of information in information and telecommunication systems", "On access to public information" and "On protection of personal data".

The comprehensive information protection system is designed to perform the following tasks:

• effective neutralization and prevention of threats to resources through comprehensive implementation of legal, moral and ethical, physical, organizational, technical and other security measures;

• ensuring the properties of the information security policy (confidentiality, integrity and availability) during the creation and operation of the information network;

• delineation and control of user access in accordance with the established access restriction policy;

• management of information security tools, user access to resources;

• control over the work of personnel by employees of the information protection service;

• prompt notification of unauthorized access attempts;

• detection of vulnerabilities in operating systems; protection against attacks by security attackers;

• protection against penetration and spread of computer viruses;

• control over the functioning of the KSZI;

• creation of conditions for the localization of failures and the fastest possible restoration of work after any malfunction caused by unauthorized actions of individuals and legal entities, the influence of the external environment and other factors [9].

To build a CSZI, 6 stages need to be performed sequentially (Fig. 1.1).

Figure 1.1 – Stages of building a comprehensive information protection system

Purpose and purpose of KSZI. KSZI is an integral part of the automated system. The purpose of creating the CSZI in the automated class "1" system is to ensure the protection of information processed in the automated system by preventing disclosure, distortion and losses during its processing and export to external media. Information protection must be ensured at all technological stages of its processing and in all modes of operation of the automated system:

• protection of information with limited access, which is processed by means of the automated system, and resources of the automated system from viewing, reproduction, distribution, copying, recovery, leakage, modification and destruction due to unauthorized access;

• blocking unauthorized actions of information with limited access;

• protection of information resources, which are processed by means of an automated system, against the influence of viruses and other malicious programs and codes;

• registration and control of users and media in accordance with the established security policy;

• managing user access to information resources of the automated system;

• implementation of unique identification and authentication of each registered user and his carrier;

• monitoring, registration of attempts to implement information threats and prompt notification of the security administrator about the facts of unauthorized actions with information with limited access and countering attempts to implement threats to the information resources of the automated system [9].

The goals of information protection in an automated system are divided into two sets:

1. Information security goals for the automated system, which reflect the need to resist threats to the security of the resources of the automated system and to implement a security policy during information processing by means of the automated system in terms of:

• user environment;

• information environment;

• hardware environment of the automated system;

• software environment of the automated system;

• information processing technologies.

2. Information security goals for the physical environment of the functioning of the automated system, which reflect the requirements for the protection of the automated system security in terms of:

• physical environment;

• environment of organizational support [9].

Achieving the security objectives for the automated system shall contribute to the prevention of security threats and the implementation of the requirements of the protection functional profile for the automated system. The following goals are common to the modules of the security system that protect the resources of the automated system:

• identification and authentication of subjects and objects of the system in the process of ensuring access and use of automated system resources;

• demarcation of access to the resources of the automated system;

• logging and auditing of information security events during information processing in the automated system;

• ensuring the correct use of security functions exclusively through the interface of the complex of automated system protection tools;

• performing backup copies of technological information necessary to restore system operation in case of failures;

• ensuring the restoration of the functioning of the automated system after failures and failures of the equipment of the automated system;

control of the integrity of the executable modules of the automated system and a set of protection tools and ensuring their self-testing [9].

Classification. On the basis of ND TZI 2.5-005-99 "Classification of AS and standard functional profiles of protection of processed information from NSD", three hierarchical classes are distinguished based on the totality of ITS characteristics, the requirements for the functional composition of KZZ are significantly different [9].

Class "1" - one workstation that processes confidential information. The following parameters can be selected:

• at any time, only one user can work with the computer, however, the number of persons with access may be larger, but they all have the same rights to access the information being processed;

• technical means from the point of view of security belong to the same category and can be used to store all information [9].

An example is a stand-alone PC, access to which is controlled using organizational measures.

Class "2" is a localized multi-machine multi-user complex that processes information of various confidentiality categories. An important difference from the previous class is the existence of users with different technical means and access rights who can simultaneously process information of various confidentiality categories. An example is a local network.

Class "3" is a distributed multi-machine multi-user complex that processes information of various confidentiality categories. A significant difference compared to the previous class is the need to transmit information through an unprotected environment. An example is the global network [9].

1.3 Regulatory and legal acts on the necessity of KSZI in ITS.

The history of ТИ in Ukraine began with the Law of Ukraine "On the Protection of Information in Automated Systems", adopted by the Resolution of the Verkhovna Rada of Ukraine No. 81/94-BP dated July 5, 1994.

In the same year, by resolution No. 632 of the Cabinet of Ministers of Ukraine (hereinafter referred to as the Cabinet of Ministers of Ukraine) dated September 9, 1994, the "Regulations on the Technical Protection of Information in Ukraine" (hereinafter referred to as the Technical Information Protection Service) was approved, according to which the State Service of Ukraine on Information Security was created.

After 3 years, the "Concept of ТЖИ in Ukraine" was approved by the Resolution of the CMU dated October 8, 1997 No. 1126. It defines the concept of TK as follows: it is an activity aimed at ensuring the order of access, integrity and availability of information with limited access, as well as the integrity and availability of open information, important for the individual, society and the state, by engineering and technical measures. And already 2 years later, a new "Regulation on ТРИ in Ukraine" appeared, approved by the Decree of the President of Ukraine No. 1229 dated September 27, 1999. This was due to the fact that TP issues were entrusted to the Department of Special Telecommunication Systems and Information Protection The Security Service of Ukraine (abbreviated as DSTSZI of the SBU), which includes the State Service for Criminal Investigation. The old provision became invalid according to the resolution of the CMU dated March 13, 2002 No. 281 [9].

"Regulations on TK in Ukraine" defines the concept of TK as follows: it is an activity aimed at ensuring the confidentiality, integrity, and availability of information important for the state, society, and the individual through engineering and technical measures [5].

It also defines the following terms:

• confidentiality – property of information that is protected from unauthorized access;

• integrity – property of information that is protected from unauthorized distortion, destruction or destruction;

• availability – property of information that is protected from unauthorized blocking;

• information system – automated system, computer network or communication system [8].

1.4 Rules for information protection in IS.

Protection in the system is subject to:

• open information that belongs to state information resources, as well as open information about the activities of subjects of power, military formations, which is made public on the Internet, other global information networks and systems or transmitted by telecommunication networks (hereinafter - open information);

• confidential information that is in the possession of information administrators, defined by the Law of Ukraine "On Access to Public Information";

• official information;

• information that constitutes a state or other legally prescribed secret (further - confidential information);

• information whose protection is required by law [8].

Open information during processing in the system must maintain integrity, which is ensured by protection against unauthorized actions that may lead to its accidental or intentional modification or destruction.

All users should be given access to public information. Only identified and authenticated users who are authorized to modify or destroy public information. Attempts to modify or destroy public information by unauthorized users, unidentified users, or users with unconfirmed ID identification should be blocked. During the processing of official and secret information, its protection against unauthorized and

uncontrolled reading, modification, destruction, copying, distribution must be ensured [8].

Access to service information is provided only to identified and authenticated users. Attempts to access such information by unidentified persons or users with verified identification of the presented identifier during authentication should be blocked. The system provides the ability to grant the user the right to perform one or more operations on the processing of confidential information or deprive him of such a right [8].

Mandatory registration is carried out in the system:

• results of user identification and authentication;

• the results of the user's performance of information processing operations;

• attempted unauthorized actions with information;

• facts of granting and depriving users of the right to access information and its processing; - the results of checking the integrity of information protection means.

Only a user who is authorized to manage information protection means and control information protection in the system (security administrator) can analyze registration data.

Registration is automatic and registration data is protected from modification and destruction by users who do not have security administrator authority. Registration of attempted unauthorized actions with information that constitutes a state secret, as well as confidential information about a natural person, which is classified as personal data by law, must be accompanied by a notification from the security administrator [8].

Identification and authenticationidentification of users, provision and deprivation of their right to access information and its processing, control over the integrity of protection means in the system is carried out in automated mode. Transfer of official and secret information from one system to another is carried out in encrypted form or protected communication channels in accordance with the requirements of the legislation on technical and cryptographic protection of information. The procedure for connecting systems in which official and secret

information is processed to global data transmission networks is determined by legislation.

The system controls the integrity of the software used to process information, preventing unauthorized modifications and eliminating the consequences of such modifications. The integrity of information security of software and hardware is also monitored. If their integrity is violated, processing in the information system is stopped [9].

1.5 Statement of the problem

The topic of the thesis is devoted to the development of a computer network project and recommendations for the protection of information of the enterprise "SV ALTERA"

The aim of the thesis is to increase the data security of the company "SV ALTERA" by creating a corporate computer network that will connect the structural units into a single network structure, creating a system for protecting the company's information.

Research object "ST ALTERA" and the organization's computer network.

The organization of the corporate KM should ensure the reliability of the computer support of the "SV ALTERA" company and connect the structural divisions into a single network structure. The message transmission encryption system should increase the level of data security of the SV ALTERA company. The purpose of the computer network being created is to ensure shared access of network users to common resources and to ensure free access to the Internet. Users of this corporate network can only be employees of the PE "SV ALTERA" company.

In the course of diploma design, it is expected to receive a project of a corporate computer network for the company "SV ALTERA" with an information protection system.

Лістинг 1. Файл Form1.cs

```
using System;
usingSystem.Collections.Generic;
usingSystem.ComponentModel;
usingSystem.Data;
usingSystem.Drawing;
usingSystem.Linq;
usingSystem.Text;
usingSystem.Threading.Tasks;
usingSystem.Windows.Forms;
usingSystem.Numerics;
using System.IO;


namespace Rabin
{
publicpartialclassForm1 : Form
    {
public Form1()
        {
InitializeComponent();
        }

// Зашифровать
privatevoid button1_Click(object sender, EventArgs e)
        {
try
            {
int p = int.Parse(textBox1.Text);
int q = int.Parse(textBox2.Text);
BigInteger value = BigInteger.Parse(richTextBox1.Text);

                richTextBox2.Text = Rabin.Encrypt(value, p,
q).ToString();
            }
catch (Exception ex)
            {
MessageBox.Show("Пожалуйставведитеобаключа.");
            }
        }

// Расшифровать
privatevoid button2_Click(object sender, EventArgs e)
        {
try
            {
int p = int.Parse(textBox1.Text);
int q = int.Parse(textBox2.Text);
BigInteger value = BigInteger.Parse(richTextBox1.Text);
```

```
                    richTextBox2.Text = Rabin.Decrypt(value, p, q);
                }
            catch (Exception ex)
                {
            MessageBox.Show("Пожалуйставведитеобаключа.");
                }
            }

            // Открытьфайл
            privatevoidоткрытьToolStripMenuItem_Click(object  sender,  EventArgs
e)
            {
            OpenFileDialogopenFile = newOpenFileDialog();

            openFile.Filter = "txt files (*.txt)|*.txt|All files (*.*)|*.*";

            if (openFile.ShowDialog() == DialogResult.OK)
                {
            try
                    {
                        richTextBox1.Text                                    =
File.ReadAllText(openFile.FileName);
                    }
            catch (Exception ex)
                    {
            MessageBox.Show("Ошибка! Пожалуйста выберите другой файл.");
                    }
                }
            }

            // Сохранить файл
            privatevoidсохранитьToolStripMenuItem_Click(object           sender,
EventArgs e)
            {
            SaveFileDialogsaveFile = newSaveFileDialog();

            saveFile.Filter = "txt files (*.txt)|*.txt|All files (*.*)|*.*";

            if (saveFile.ShowDialog() == DialogResult.OK)
                {
            try
                    {
            File.WriteAllText(saveFile.FileName, richTextBox2.Text);
                    }
            catch (Exception ex)
                    {
            MessageBox.Show("Ошибка! Пожалуйста выберите другое имя файла.");
            }
                }
            }
```

```
    }

publicclassRabin
    {
publicstaticBigInteger Encrypt(BigInteger value, int p, int q)
        {
int n = p * q;
return ((value * value) % (n));
        }

publicstaticstring Decrypt(BigInteger c, int p, int q)
        {
int n = p * q;

// START - АлгоритмЕвкліда
BigInteger x_1 = (BigInteger.Pow(c, ((p + 1) / 4)) % p);
BigInteger y_1 = (BigInteger.Pow(c, ((q + 1) / 4)) % q);

int q_1 = 0;
int p_1 = 0;

int l = 10;
for (int i = 0; i <= l; i++)
            {
if ((i * q) % p == 1) { q_1 = i; i = l + 100; } else { l += 1; }
            }
            l = 10;
for (int i = 0; i <= l; i++)
            {
if ((i * p) % q == 1) { p_1 = i; i = l + 100; } else { l += 1; }
}
// END

// START - Китайська теорема про залишки
BigInteger r1 = ((x_1 * q * q_1 + y_1 * p * p_1) % n);
BigInteger r2 = (-r1 + n) % n;
BigInteger r3 = ((x_1 * q * q_1 - y_1 * p * p_1) % n);
BigInteger r4 = (-r3 + n) % n;
// END

return (r1 + "\nИли\n" + r2 + "\nИли\n" + r3 + "\nИли\n" + r4);
}
    }
}
```

РЕФЕРАТ

Пояснювальна записка містить: __ с., ___ малюнків., ___ таблиць., __ джерел.

Об’єкт дослідження – приватне підприємство «СВ. АЛЬТЕРА».

Суб’єкт дослідження – локальна мережа підприємства, система захисту інформації на приватному підприємстві «СВ. АЛЬТЕРА», організаційний та технічний захист.

Мета роботи: проектування локальної мережі, розробка загальних засад захисту інформації на приватному підприємстві «СВ. АЛЬТЕРА».

Ключові слова: інформаційна система, інформаційна безпека, захист інформації, організаційний захист, технічний захист, проектування локальної мережі.

ANNOTATION

The explanatory note contains: ___ pages, __ figures, __tables, __ sources.

The object of the study is the private enterprise "SV. ALTERA".

The subject of the study is the local network of the enterprise, the information protection system at the private enterprise "SV. ALTERA", organizational and technical protection.

The purpose of the work: design of a local network, development of general principles of information protection at the private enterprise "SV. ALTERA".

Keywords: information system, information security, information protection, organizational protection, technical protection, local network design.