Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Стратія Гліба Івановича*

академічної групи *125-17з-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Обґрунтування засобів захисту інформації комп'ютерної мережі товариство з обмеженою відповідальністю «Євро полюс»*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.т.н., проф. Корнієнко В.І.			
розділів:				
спеціальний	ас. Ковальова Ю.В.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2021

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту *Стратію Глібу Івановичу* **академічної групи** *125-17з-1*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Обґрунтування засобів захисту інформації комп'ютерної мережі товариство з обмеженою відповідальністю «Євро полюс»***

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

Розділ	Зміст	Термін виконання
Розділ 1	Виконати класифікацію загроз безпеки інформації, навести заходи забезпечення безпеки комп'ютерної мережі підприємства	29.03.2021
Розділ 2	Розробка комплексної системи захисту інформації комп'ютерної мережі ТОВ «Євро полюс»	24.05.2021
Розділ 3	Виконати розрахунок економічного ефекту від впровадження та налагодження комплексів засобів захисту інформації комп'ютерної мережі	14.06.2021

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі: 08.01.2021р.

Дата подання до екзаменаційної комісії: 15.06.2021р.

Прийнято до виконання _____ _____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: __ с., __ рис., _ табл., __ додатків, __ джерел.

Мета роботи: за допомогою програмних, апаратних і організаційних заходів поліпшити захищеність інформації в комп'ютерній мережі ТОВ «Євро полюс» від несанкціонованого доступу.

У розділі Стан питання. Постановка задачі описані найпоширеніші загрози безпеки та основні положення захисту інформації від них.

У спеціальному розділі описана кратка характеристика об’єкту інформаційної діяльності ТОВ «Євро полюс», розроблені й описані методи підвищення захисту інформації від несанкціонованого доступу.

В економічному розділі наведені розрахунки й обґрунтовані всі заходи щодо вдосконалення системи захисту інформації в комп'ютерній мережі ТОВ «Євро полюс».

Практичне значення роботи полягає в підвищенні рівня інформаційної безпеки мережі шляхом програмних, апаратних і організаційних заходів.

ІНФОРМАЦІЙНА БЕЗПЕКА, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, МІЖМЕРЕЖЕВИЙ ЕКРАН, СИСТЕМА ВИЯВЛЕННЯ ТА ЗАПОБИГАННЯ АТАК.

РЕФЕРАТ

Пояснительная записка: стр., __ рис., табл., приложений, __ источников.

Цель работы: с помощью программных, аппаратных и организационных мероприятий улучшить защищенность информации в компьютерной сети ООО «Евро полюс» от несанкционированного доступа.

В разделе Состояние вопроса. Постановка задачи описаны наиболее распространенные угрозы безопасности и основные положения защиты информации от них.

В специальном разделе описана кратка характеристика объекта информационной деятельности ООО «Евро полюс», разработаны и описаны методы повышения защиты информации от несанкционированного доступа.

В экономическом разделе приведены расчеты и обоснованные все меры по совершенствованию системы защиты информации в компьютерной сети ООО «Евро полюс».

Практическое значение работы заключается в повышении уровня информационной безопасности сети путем программных, аппаратных и организационных мероприятий.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, МОДЕЛИ УГРОЗ, МОДЕЛЬ НАРУШИТЕЛЯ, МЕЖСЕТЕВОЙ ЭКРАН, СИСТЕМА ОБНАРУЖЕНИЯ И ЗАПОБИГАННЯ АТАК.

ABSTRACT

Explanatory note: __ p., __ fig., __ tab., __ additions, __ sources.

Purpose: To improve the security of information on the computer network of LLC "Euro Polus" against unauthorized access through software, hardware and organizational measures.

In the Question status section. The problem statement describes the most common security threats and the basic provisions for protecting information from them.

The special section describes a brief description of the object of information activity of LLC "Euro Polus", developed and describes methods to improve the protection of information from unauthorized access.

The economic section presents the calculations and substantiated all measures to improve the information security system in the computer network of LLC "Euro Polus".

The practical value of the thesis is to increase the level of information security of the network through software, hardware and organizational activities.

INFORMATION SECURITY, MODEL OF THREATS, MODEL OF VIOLENT, INTERMEDIATE SCREEN, SYSTEM OF DETECTION AND ATTACK AVOIDANCE.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ЕОМ – електронно-обчислювальна машина;

ІБ – інформаційна безпека;

ІС – інформаційна система;

КМ – комп’ютерна мережа;

ЛОМ – локальна обчислювальна мережа;

МЕ – між мережевий екран;

НСД – несанкціонований доступ;

ОС – операційна система;

ПЗ – програмне забезпечення;

ПК – персональний комп'ютер;

FTP – File Transfer Protocol;

HIPS – Host-based Intrusion Prevention System;

ICMP – Internet Control Message Protocol;

IP – internet protocol;

IT – Information technology;

SNMP – Simple Network Management Protocol;

TCP – Transmission Control Protocol;

WWW – World Wide Web;

YAST – Yet another Setup Tool.

ЗМІСТ

с.

ВСТУП 10

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ 12

1.1 Класифікація загроз безпеки інформації 12

1.2 Найбільш поширені загрози 13

1.3 Програмні атаки 16

1.4 Шкідливе програмне забезпечення 17

1.5 Класифікація заходів забезпечення безпеки КМ 18

1.6 Апаратні засоби захисту інформації в КМ 22

1.7 Програмні засоби захисту інформації в КМ 22

1.8 Криптографічні методи захисту 24

1.9 Шифрування дисків 24

1.10 Спеціалізовані програмні засоби захисту інформації 26

1.11 Архітектурні аспекти безпеки 29

1.12 Системи архівації і дублювання інформації 30

1.13 Аналіз захищеності 32

1.14 Висновки 33

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА 34

2.1 Характеристика об'єкту 34

2.2 Характеристика будівлі 34

2.3 Характеристика серверу 35

2.4 Встановлене ПЗ 36

2.5 Характеристика оброблюваної інформації в комп'ютерній мережі 36

2.6 Вхід в ОС 37

2.7 Модель загроз 38

2.8 Характеристика комп'ютерної мережі підприємства 44

2.9 Характеристика серверної ОС 45

2.10 Матриця доступу 47

2.11 Вибір антивірусного захисту 48

2.12 Вибір міжмережевого екрану 52
2.13 Система виявлення вторгнень 56
2.14 Організаційні заходи щодо забезпечення інформаційної безпеки мережі 65
2.14.1 Інструкція використання ЛОМ ТОВ «Євро полюс» 65
2.15 Висновки 71
РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ 72
3.1 Розрахунок (фіксованих) капітальних витрат 72
3.1.1 Розрахунок поточних витрат 75
3.2 Оцінка можливого збитку від атаки на вузол або сегмент мережі 77
3.2.1 Оцінка величини збитку 77
3.2.2 Загальний ефект від впровадження системи інформаційної безпеки 80
3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки 81
3.4 Висновок 82
ВИСНОВКИ 83
ПЕРЕЛІК ПОСИЛАНЬ 84
ДОДАТОК А 86
ДОДАТОК Б 87
ДОДАТОК В 88
ДОДАТОК Г 89
ДОДАТОК Д 90
ДОДАТОК Е 91

ВСТУП

У 21 столітті поняття інформації нерозривно пов'язане з комп'ютерними технологіями, системами і мережами зв'язку, то стає очевидною важливість питання захисту інформації в них. Винахід комп'ютера і подальший бурхливий розвиток інформаційних технологій в другій половині 20 століть зробили проблему захисту інформації настільки актуальною і гострою, наскільки актуальна сьогодні інформатизація для всього суспільства. Особливо актуально коштує це питання в області секретної інформації держави і приватної комерційної інформації.

У бізнесі добросовісна конкуренція припускає суперництво, засноване на дотриманні законодавства і загальновизнаних норм моралі. Проте нерідко підприємці, конкуруючи між собою, прагнуть за допомогою протиправних дій отримати інформацію в збиток інтересам іншої сторони і використовувати її для досягнення переваги на ринку. Криміналізація суспільства і недостатня ефективність державної системи охорони правопорядку примушує представників бізнесу самим приймати заходи для адекватного протистояння негативним процесам, що мають місце, завдають збитку конфіденційної інформації фірми.

Причин активізації комп'ютерних злочинів і пов'язаних з ними фінансових втрат достатні багато, істотними з них є:

– перехід від традиційної «паперової» технології зберігання і передачі відомостей на електронну і недостатній при цьому розвиток технології захисту інформації в таких технологіях;

– об'єднання обчислювальних систем, створення глобальних мереж і розширення доступу до інформаційних ресурсів;

– збільшення складності програмних засобів.

Отже головна тенденція, що характеризує розвиток сучасних інформаційних технологій, – зростання числа комп'ютерних злочинів і

пов'язаних з ними розкрадань конфіденційної і іншої інформації, а також матеріальних втрат.

У роботі вирішуються проблеми несанкціонованого доступу до інформації через комп'ютерну мережу підприємства або мережу Internet.

ТОВ «Євро полюс» фірма, яка на даному етапі свого існування прагне до розширення і економічного зростання. З цього виходить, що в даний час необхідно побудувати ефективну систему захисту комп'ютерної мережі.

У проекті передбачається підвищення безпечної роботи комп'ютерної мережі, поліпшення умов праці і економічне обґрунтування комплексів заходів захисту інформації в комп'ютерній мережі ТОВ «Євро полюс».

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Класифікація загроз безпеки інформації

Під загрозою безпеки інформації в комп'ютерній мережі (КМ) розуміють подію або дію, яка може викликати зміну функціонування КМ, пов'язану з порушенням захищеності оброблюваної в ній інформації.

Уразливість інформації – це можливість виникнення такого стану, при якому створюються умови для реалізації загроз безпеці інформації.

Атакою на КМ називають дію порушником, що робиться, яке полягає в пошуку і використанні тієї або іншої уразливості. Інакше кажучи, атака на КМ є реалізація загрози безпеці інформації в ній.

Проблеми, що виникають з безпекою передачі інформації при роботі в комп'ютерних мережах, можна розділити на три основні типи перехоплення інформації – цілісність інформації зберігається, але її конфіденційність порушена;

Специфіка комп'ютерних мереж, з погляду їх уразливості, пов'язана в основному з наявністю інтенсивної інформаційної взаємодії між територіально рознесеними і різнорідними (різнотипними) елементами.

Уразливими є буквально всі основні структурно-функціональні елементи КМ: робочі станції, сервери, між мережеві мости (шлюзи, центри комутації), канали зв'язку і так далі

Відома велика кількість різнопланових загроз безпеці інформації різного походження. У літературі зустрічається безліч різноманітних класифікацій, де як критерії ділення використовуються види породжуваних небезпек, ступінь злого наміру, джерела появи загроз і так далі Одна з найпростіших класифікацій приведена на рисунок 1.1.

Природні загрози – це загрози, викликані діями на КМ і її елементах об'єктивних фізичних процесів або стихійних природних явищ, незалежних від людини.

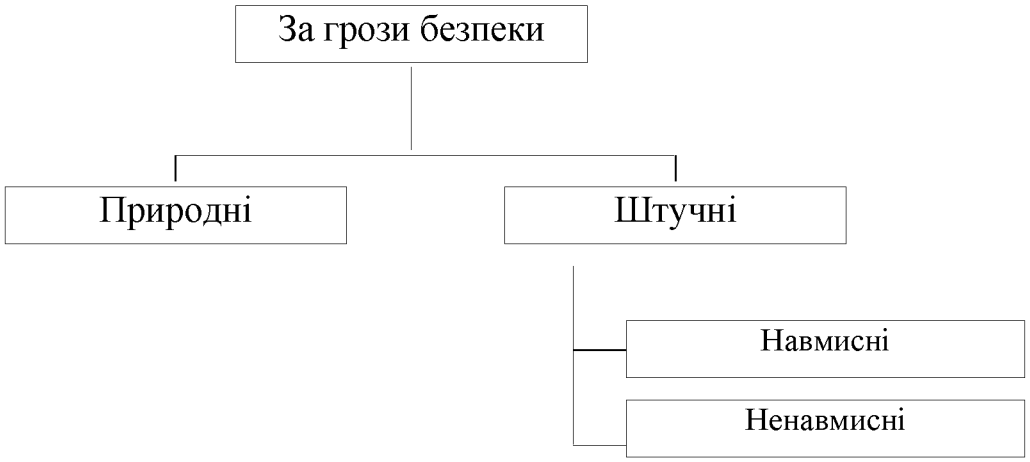

Рисунок 1.1 – Загальна класифікація загроз безпеці

Штучні загрози – це загрози КМ, викликані діяльністю людини. Серед них, виходячи з мотивації дій, можна виділити:

– ненавмисні (ненавмисні, випадкові) загрози, викликані помилками в проектуванні КМ і її елементів, помилками в програмному забезпеченні, помилками в діях персоналу тощо;

– навмисні (умисні) загрози, пов'язані з корисливими устремліннями людей (зловмисників).

Джерела загроз по відношенню до КМ можуть бути зовнішніми або внутрішніми (компоненти самої КМ - її апаратура, програми, персонал).

Джерела загроз по відношенню до КМ можуть бути зовнішніми або внутрішніми (компоненти самої КМ - її апаратура, програми, персонал).

Аналіз негативних наслідків реалізації загроз припускає обов'язкову ідентифікацію можливих джерел загроз, вразливостей , сприяючих їх прояву і методів реалізації. І тоді ланцюжок зростає в схему, представлену на рисунку 1.2.

Загрози класифікуються по можливості нанесення збитку суб'єктові стосунків при порушенні цілей безпеки. Збиток може бути причинний яким-небудь суб'єктом (злочин, провина або недбалість), а також стати слідством, не залежним від суб'єкта проявів. Загроз не так вже і багато.

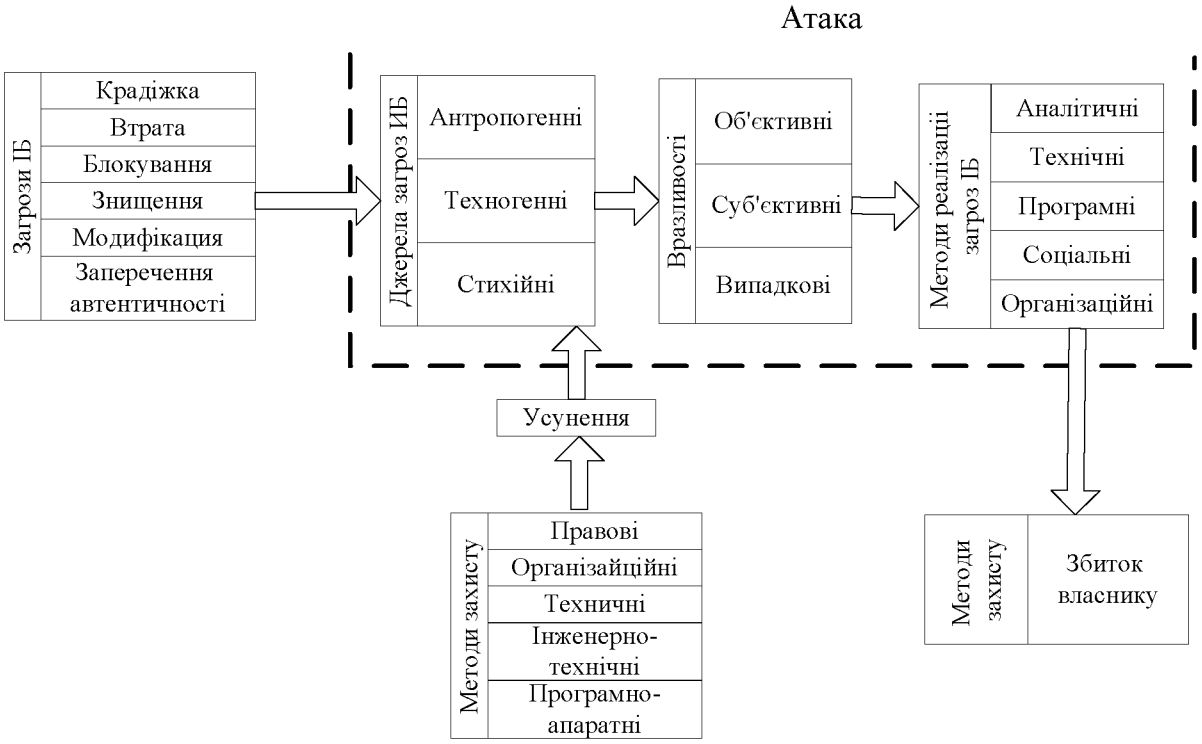

Рисунок 1.2 – Модель реалізації загроз інформаційній безпеці

При забезпеченні конфіденційності інформації це може бути розкрадання (копіювання) інформації і засобів її обробки, а також її втрата (ненавмисна втрата, витік). При забезпеченні цілісності інформації список загроз такий: модифікація (спотворення) інформації; заперечення достовірності інформації; нав'язування помилковій інформації. При забезпеченні доступності інформації можливе її блокування, або знищення самої інформації і засобів її обробки.

1.2 Найбільш поширені загрози

Найчастішими і найнебезпечнішими (з погляду розміру збитку) є ненавмисні помилки штатних користувачів, операторів, системних адміністраторів і інших осіб, обслуговуючих комп'ютерну мережу.

Іноді такі помилки і є власне загрозами (неправильно введені дані або помилка в програмі, що викликала крах системи), іноді вони створюють вразливі місця, якими можуть скористатися зловмисники. За деякими даними, до 65% втрат – наслідок ненавмисних помилок.

Пожежі і повені не приносять стільки бід, скільки неписьменність і недбалість в роботі.

Найрадикальніший спосіб боротьби з ненавмисними помилками – максимальна автоматизація і строгий контроль.

Інші загрози доступності можна класифікувати по компонентах КМ, на які націлені загрози:

– відмова користувачів;

– внутрішня відмова мережі;

– відмова підтримуючої інфраструктури.

Зазвичай стосовно користувачів розглядаються наступні загрози:

– небажання працювати з інформаційною системою (найчастіше виявляється при необхідності освоювати нові можливості і при розбіжності між запитами користувачів і фактичними можливостями і технічними характеристиками);

– неможливість працювати з системою через відсутність відповідної підготовки (недолік загальної комп'ютерної письменності, невміння інтерпретувати діагностичні повідомлення, невміння працювати з документацією і тому подібне);

– неможливість працювати з системою через відсутність технічної підтримки.

Основними джерелами внутрішніх відмов є:

– відступ (випадкове або умисне) від встановлених правил експлуатації;

– вихід системи з штатного режиму експлуатації через випадкові або навмисні дії користувачів або обслуговуючого персоналу (перевищення розрахункового числа запитів, надмірний об'єм оброблюваної інформації і тому подібне);

– помилки при (пері) конфігурації системи;

– відмови програмного і апаратного забезпечення;

– руйнування даних;

– руйнування або пошкодження апаратури.

По відношенню до підтримуючої інфраструктури рекомендується розглядати наступні загрози:

– порушення роботи (випадкове або умисне) систем зв'язку, електроживлення, водо- і/або теплопостачання, кондиціонування;

– руйнування або пошкодження приміщень;

– неможливість або небажання обслуговуючого персоналу і/або користувачів виконувати свої обов'язки (цивільні безлади, аварії на транспорті, терористичний акт або його загроза, страйк і тому подібне).

Вельми небезпечні так звані "скривджені" співробітники - нинішні і такі, що були. Як правило, вони прагнуть завдати шкоди організації - "кривдникові", наприклад:

– зіпсувати устаткування;

– вбудувати логічну бомбу, яка з часом зруйнує програми і/або дані;

– видалити дані.

Скривджені співробітники, що навіть були, знайомі з порядками в організації і здатні завдати чималого збитку. Необхідно стежити за тим, щоб при звільненні співробітника його права доступу (логічного і фізичного) до інформаційних ресурсів анулювалися.

1.3 Програмні атаки

Як засіб виведення мережі з штатного режиму експлуатації може використовуватися агресивне споживання ресурсів (зазвичай – смуги пропускання мереж, обчислювальних можливостей процесорів або оперативній пам'яті). По розташуванню джерела загрози таке споживання підрозділяється на локальне і видалене. При прорахунках в конфігурації системи локальна програма здатна практично монополізувати процесор і/або фізичну пам'ять, звивши швидкість виконання інших програм до нуля.

Простий приклад видаленого споживання ресурсів – атака, що отримала найменування "SYN-наводнення" [5]. Вона є спробою переповнити таблицю "напіввідкритих" TCP-з’єднання сервера (встановлення з'єднань починається,

але не закінчується). Така атака щонайменше утрудняє встановлення нових з'єднань з боку легальних користувачів, тобто сервер виглядає як недоступний.

По відношенню до атаки "Papa Smurf" уразливі мережі, що сприймають ping-пакети з широкомовними адресами. Відповіді на такі пакети "з'їдають" смугу пропускання.

Видалене споживання ресурсів останнім часом виявляється в особливо небезпечній формі – як скоординовані розподілені атаки, коли на сервер з безлічі різних адрес з максимальною швидкістю прямують цілком легальні запити на з'єднання і/або обслуговування. Часом почала "моди" на подібні атаки можна рахувати лютий 2000 року, коли жертвами виявилися декілька найбільших систем електронної комерції (точніше - власники і користувачі систем). Якщо має місце архітектурний прорахунок у вигляді розбалансованості між пропускною спроможністю мережі і продуктивністю сервера, то захиститися від розподілених атак на доступність украй важко.

Для виведення систем з штатного режиму експлуатації можуть використовуватися вразливі місця у вигляді програмних і апаратних помилок. Наприклад, відома помилка в процесорі Pentium давала можливість локальному користувачеві шляхом виконання певної команди "підвісити" комп'ютер, так що допомагає тільки апаратний RESET.

Програма "Teardrop" видалено "підвішує" комп'ютери, експлуатуючи помилку в збірці фрагментований IP-пакети [12].

1.4 Шкідливе програмне забезпечення

Одним з найнебезпечніших способів проведення атак є впровадження в системи шкідливого програмного забезпечення, що атакуються.

Виділяють наступні аспекти шкідливого ПЗ:

- шкідлива функція;
- спосіб розповсюдження;
- зовнішнє уявлення.
- частина, що здійснює руйнівну функцію, призначається для:

– впровадження іншого шкідливого ПЗ;

– отримання контролю над системою, що атакується;

– агресивного споживання ресурсів;

– зміни або руйнування програм і/або даних.

– по механізму розповсюдження розрізняють:

– віруси - код, що володіє здібністю до розповсюдження (можливо, із змінами) шляхом впровадження в інші програми;

– "черв'яки" – код, здатний самостійно, тобто без впровадження в інші програми, викликати розповсюдження своїх копій по мережі і їх виконання (для активізації вірусу потрібний запуск зараженої програми).

Віруси зазвичай розповсюджуються локально, в межах вузла мережі; для передачі по мережі їм потрібна зовнішня допомога, така як пересилка зараженого файлу. "Черв'яки", навпаки, орієнтовані насамперед на подорожі по мережі.

Іноді само розповсюдження шкідливого ПЗ викликає агресивне споживання ресурсів і, отже, є шкідливою функцією. Наприклад, "черв'яки" "з'їдають" смугу пропускання мережі і ресурси поштових систем.

Шкідливий код, який виглядає як функціонально корисна програма, називається троянським. Наприклад, звичайна програма, будучи ураженою вірусом, стає троянською.

1.5 Класифікація заходів забезпечення безпеки КМ

По способах здійснення всі заходи забезпечення безпеки комп'ютерних мереж підрозділяються на: правові (законодавчі), морально-етичні, організаційні (адміністративні), фізичні, технічні (апаратно-програмні) [6,22].

До правових заходів захисту відносяться закони, що діють в країні, укази і нормативні акти, що регламентують правила поводження з інформацією, що закріплюють права і обов'язки учасників інформаційних стосунків в процесі її обробки і використання, а також що встановлюють відповідальність за порушення цих правил, перешкоджаючи тим самим неправомірному

використанню інформації і що є стримуючим чинником для потенційних порушників.

До морально-етичних заходів протидії відносяться норми поведінки, які традиційно склалися або складаються у міру розповсюдження комп'ютерних мереж в країні або суспільстві. Ці норми переважно не є обов'язковими, як законодавчо затверджені нормативні акти, проте, їх недотримання веде зазвичай до падінню авторитету, престижу людини, групи осіб або організації.

Морально-етичні норми бувають як неписані (наприклад, загальновизнані норми чесності, патріотизму і тому подібне), так і писані, тобто оформлені в деяке зведення (статут) правив або розпоряджень.

Організаційні (адміністративні) заходи захисту - це заходи організаційного характеру, що регламентують процеси функціонування системи обробки даних, використання її ресурсів, діяльність персоналу, а також порядок взаємодії користувачів з системою так, щоб найбільшою мірою утруднити або унеможливити реалізації загроз безпеці. Вони включають:

– заходи, здійснювані при проектуванні, будівництві і устаткуванні мереж і інших об'єктів систем обробки даних;

– заходи щодо розробки правил доступу користувачів до ресурсів мереж (розробка політики безпеки);

– заходи, здійснювані при підборі і підготовці персоналу;

– організацію охорони і надійного пропускного режиму;

– організацію обліку, зберігання, використання і знищення документів і носіїв з інформацією;

– розподіл реквізитів розмежування доступу (паролів, ключів шифрування і тому подібне);

– організацію явного і прихованого контролю за роботою користувачів;

– заходи, здійснювані при проектуванні, розробці, ремонті і модифікаціях устаткування і програмного забезпечення і тому подібне.

Фізичні заходи захисту засновані на застосуванні різного роду механічних, електронно або електронно-механічних пристроїв і споруд, спеціально

призначених для створення фізичних перешкод на можливих шляхах проникнення і доступу потенційних порушників до компонентів мереж і інформації, що захищається, а також технічних засобів візуального спостереження, зв'язку і охоронної сигналізації.

Технічні (апаратні) заходи захисту засновані на використанні різних електронних пристроїв, що входять до складу КМ і виконують (самостійно або в комплексі з іншими засобами) функції захисту.

Програмні методи захисту призначаються для безпосереднього захисту інформації по трьом напрямам: а) апаратура; б) програмного забезпечення; в) даних команд, що управляють.

Для захисту інформації при її передачі зазвичай використовують різні методи шифрування даних перед їх введенням в канал зв'язку або на фізичний носій з подальшою розшифровкою. Як показує практика, методи шифрування дозволяють достатньо надійно приховати сенс повідомлення.

Всі програми захисту, що здійснюють управління доступом до машинної інформації, функціонують за принципом відповіді на питання: хто може виконувати, які операції і над якими даними.

Доступ може бути визначений як:

- загальний (що безумовно надається кожному користувачеві);
- відмова (безумовна відмова, наприклад дозвіл на видалення порції інформації);
- залежний від події (керований подією);
- залежний від змісту даних;
- залежний від стану (динамічного стану комп'ютерної системи);
- частотно-залежний (наприклад, доступ дозволений користувачеві тільки один або певне число разів);
- по імені або іншою ознакою користувача;
- залежний від повноважень;
- по дозволу (наприклад, по паролю);
- за процедурою.

Також до ефективних заходів протидії спробам несанкціонованого доступу відносяться засоби реєстрації. Для цих цілей найбільш перспективними є нові операційні системи спеціального призначення, що широко вживані в зарубіжних країнах і отримали назву моніторингу (автоматичного спостереження за можливою комп'ютерною загрозою).

Моніторинг здійснюється самою операційною системою (ОС), причому в її обов'язки входить контроль за процесами введення-виводу, обробки і знищення машинної інформації. ОС фіксує час несанкціонованого доступу і програмних засобів, до яких був здійснений доступ. Окрім цього, вона проводить негайне сповіщення служби комп'ютерній безпеці про посягання на безпеку комп'ютерної системи з одночасною виводом на друк необхідних даних (лістингу).

Останнім часом в США і низці європейських країн для захисту комп'ютерних систем діють також спеціальні підпрограми, що викликають самознищення основної програми при спробі несанкціонованого перегляду вмісту файлу з секретною інформацією аналогічно дії “логічної бомби”.

Завдання забезпечення безпеки:

– захист інформації в каналах зв'язку і базах даних криптографічними методами;

– підтвердження достовірності об'єктів даних і користувачів (аутентифікація сторін, що встановлюють зв'язок);

– виявлення порушень цілісності об'єктів даних;

– забезпечення захисту технічних засобів і приміщень, в яких ведеться обробка конфіденційної інформації, від витоку по побічних каналах і від можливо упроваджених в них електронних пристроїв знімання інформації;

– забезпечення захисту програмних продуктів і засобів обчислювальної техніки від впровадження в них програмних вірусів і закладок;

– захист від несанкціонованих дій з каналу зв'язку від осіб, не допущених до засобів шифрування, але переслідуючи цілі компрометації секретної інформації і дезорганізації роботи абонентських пунктів;

– організаційно-технічні заходи, направлені на забезпечення збереження конфіденційних даних.

1.6 Апаратні засоби захисту інформації в КМ

До апаратних засобів захисту інформації відносяться електронно і електронно-механічні пристрої, що включаються до складу технічних засобів

КМ і виконуючі (самостійно або в єдиному комплексі з програмними засобами) деякі функції забезпечення інформаційної безпеки. Критерієм віднесення пристрою до апаратних, а не до інженерно-технічних засобів захисту є обов'язкове включення до складу технічних засобів КМ.

До основних апаратних засобів захисту інформації відносяться:

– пристрої для введення, що ідентифікує користувача інформації (магнітних і пластикових карт, відбитків пальців і тому подібне);

– пристрою для шифрування інформації;

– пристрої для того, що перешкодило несанкціонованому включенню робочих станцій і серверів (електронні замки і блокують);

– пристрої фільтрації пакетів.

– Приклади допоміжних апаратних засобів захисту інформації:

– пристрої знищення інформації на магнітних носіях;

– пристрої сигналізації про спроби несанкціонованих дій користувачів КМ і ін.

Апаратні засоби привертають всю більшу увагу фахівців не тільки тому, що їх легко захистити від пошкоджень і інших випадкових або зловмисних дій, але ще і тому, що апаратна реалізація функцій вище по швидкодії, чим програмна, а вартість їх неухильно знижується.

1.7 Програмні засоби захисту інформації в КМ

Під програмними засобами захисту інформації розуміють спеціальні програми, що включаються до складу програмного забезпечення КМ виключно для виконання захисних функцій.

До основних програмних засобів захисту інформації відносяться:

– програми ідентифікації і аутентифікації користувачів КМ;

– програми розмежування доступу користувачів до ресурсам КМ;

– програми шифрування інформації;

– програми захисту інформаційних ресурсів (системного і прикладного програмного забезпечення, баз даних, комп'ютерних засобів навчання і т. п.) від несанкціонованої зміни, використання і копіювання.

Треба розуміти, що під ідентифікацією, стосовно забезпеченню інформаційної безпеки КМ, розуміють однозначне розпізнавання унікального імені суб'єкта КМ. Аутентифікація означає підтвердження того, що пред'явлене ім'я відповідає даному суб'єктові (підтвердження достовірності суб'єкта).

Також до програмних засобів захисту інформації відносяться:

– Програми знищення залишкової інформації (у блоках оперативної пам'яті, тимчасових файлах і т. п.);

– програми аудиту (ведення реєстраційних журналів) подій, пов'язаних з безпекою КМ, для забезпечення можливості відновлення і доказу факту події цих подій;

– програми імітації роботи з порушником (відвернення його на отримання нібито конфіденційній інформації);

– програми тестового контролю захищеності КМ і ін.

До переваг програмних засобів захисту інформації відносяться:

– Простота тиражування;

– гнучкість (можливість настроювання на різні умови використання, що зважають на специфіку загроз інформаційної безпеки конкретних КМ);

– простота застосування – одні програмні засоби, наприклад шифрування, працюють в «прозорому» (непомітному для користувача) режимі, а інші не вимагають від користувача ні яких нових (в порівнянні з іншими програмами) навиків;

– практично необмежені можливості їх розвитку шляхом внесення змін для обліку нових загроз безпеці інформації.

До недоліків програмних засобів захисту інформації відносяться:

– зниження ефективності КМ за рахунок споживання її ресурсів, потрібних для функціонування програм захисту;

– нижча продуктивність (в порівнянні з тими, що виконують аналогічні функції апаратними засобами захисту, наприклад шифрування);

– можливість зловмисної зміни програмних засобів захисту в процесі експлуатації КМ.

1.8 Криптографічні методи захисту

Криптографія - це наука про забезпечення безпеки даних. Вона займається пошуками вирішень чотирьох важливих проблем безпеки – конфіденційності, аутентифікації, цілісності і контролю учасників взаємодії. Шифрування – це перетворення даних в нечитабельну

форму, використовуючи ключі шифрування-розшифровки. Шифрування дозволяє забезпечити конфіденційність, зберігаючи інформацію в таємниці від того, кому вона не призначена.

Криптографія займається пошуком і дослідженням математичних методів перетворення інформації.

Сучасна криптографія включає чотири крупні розділи:

– симетричні криптосистеми;

– криптосистеми з відкритим ключем;

– системи електронного підпису;

– управління ключами.

Основні напрями використання криптографічних методів - передача конфіденційній інформації по каналах зв'язку (наприклад, електронна пошта), встановлення достовірності переданих повідомлень, зберігання інформації (документів, баз даних) на носіях в зашифрованому вигляді.

1.9 Шифрування дисків

Зашифрований диск – це файл-контейнер, усередині якого можуть знаходитися будь-які інші файли або програми (вони можуть бути встановлені і запущені прямо з цього зашифрованого файлу). Цей диск доступний тільки після

введення пароля до файлу-контейнера – тоді на комп'ютері з'являється ще один диск, що пізнається системою як логічний і робота з яким не відрізняється від роботи з будь-яким іншим диском. Після відключення диска логічний диск зникає, він просто стає «невидимим».

На сьогоднішній день найбільш поширені програми для створення зашифрованих дисків – DriveCrypt, BestCrypt і PGPdisk. Кожна з них надійно захищена від видаленого злому.

Загальні риси програм:

– всі зміни інформації у файлі-контейнері відбуваються спочатку в

– оперативній пам'яті, тобто жорсткий диск завжди залишається зашифрованим. Навіть у разі зависання комп'ютера секретні дані так і залишаються зашифрованими;

– програми можуть блокувати прихований логічний диск після закінчення певного проміжку часу;

– всі вони недовірливо відносяться до тимчасових файлів (своп-файлам).

Є можливість зашифрувати всю конфіденційну інформацію, яка могла потрапити в своп-файл. Дуже ефективний метод утаєння інформації, що зберігається в своп-файле, – це взагалі відключити його, при цьому не забувши наростити оперативну пам'ять комп'ютера;

– фізика жорсткого диска така, що навіть якщо поверх одних даних записати інші, то попередній запис повністю не зітреться. За допомогою сучасних засобів магнітної мікроскопії (Magnetic Force Microscopy – MFM) їх все одно можна відновити. За допомогою цих програм можна надійно видаляти файли з жорсткого диска, не залишаючи ніяких слідів їх існування;

– всі три програми зберігають конфіденційні дані в надійно зашифрованому вигляді на жорсткому диску і забезпечують прозорий доступ до цих даних з будь-якої прикладної програми;

– вони захищають зашифровані файли-контейнери від випадкового видалення;

– відмінно справляються з троянськими застосуваннями і вірусами.

1.10 Спеціалізовані програмні засоби захисту інформації

Спеціалізовані програмні засоби захисту інформації від несанкціонованого доступу володіють в цілому кращими можливостями і характеристиками, чим вбудовані засоби мережевих ОС. Окрім програм шифрування, існує багато інших доступних зовнішніх засобів захисту інформації. З найчастіше згадуваних слід зазначити наступні дві системи, що дозволяють обмежити інформаційні потоки.

Firewalls (дослівно firewall – вогненна стіна) – між локальною і глобальною мережами створюються спеціальні проміжні сервера, які інспектують і фільтрують весь трафік, що проходить через них, транспортного рівнів. Це дозволяє різко понизити загрозу несанкціонованого доступу ззовні в корпоративні мережі, але не усуває цю небезпеку зовсім.

Розглянемо докладніше роботу брандмауера. Це метод захисту мережі від загроз безпеки, витікаючи від інших систем і мереж, за допомогою централізації доступу до мережі і контролю за ним апаратно-програмними засобами. Брандмауер є захисним бар'єром, що складається з декількох компонентів (наприклад, маршрутизатора або шлюзу, на якому працює програмне забезпечення брандмауера). Брандмауер конфігурується відповідно до прийнятої в організації політики контролю доступу до внутрішньої мережі. Всі вхідні і витікаючи пакети повинні проходити через брандмауер, який пропускає тільки авторизовані пакети.

Брандмауер з фільтрацією пакетів [packet-filtering firewall] - є маршрутизатором або комп'ютером, на якому працює програмне забезпечення, конфігуровано так, щоб відбраковувати певні види вхідних і витікаючи пакетів. Фільтрація пакетів здійснюється на основі інформації, що міститься в TCP- і IP-заголовках пакетів (адреси відправника і одержувача, їх номери портів і ін.).

Брандмауер експертного рівня [stateful inspecthion firewall] - перевіряє вміст пакетів, що приймаються, на трьох рівнях моделі OSI - мережевому, сеансовому і прикладному. Для виконання цього завдання використовуються спеціальні алгоритми фільтрації пакетів, за допомогою яких кожен пакет порівнюється з відомим шаблоном авторизованих пакетів.

Створення брандмауера відноситься до рішення задачі екранування. Формальна постановка завдання екранування полягає в наступному. Хай є дві безліч інформаційних систем. Екран - це засіб розмежування доступу клієнтів з однієї множини до серверів з іншої множини. Екран здійснює свої функції, контролюючи всі інформаційні потоки між двома безліччю систем (рисунок 3). Контроль потоків полягає в їх фільтрації, можливо, з виконанням деяких перетворень.

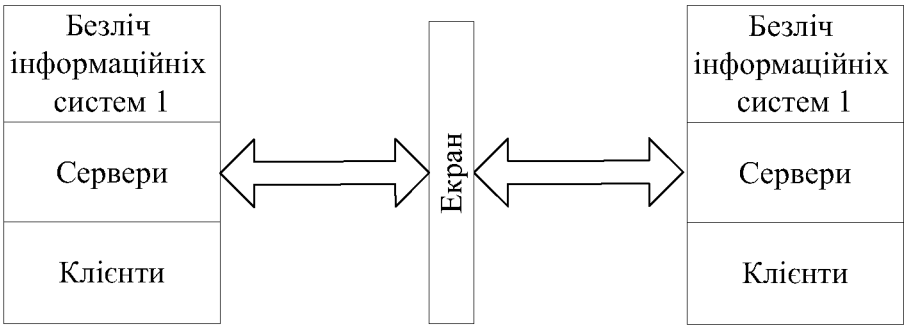

Рисунок 1.3 – Екран як засіб розмежування доступу

На наступному рівні деталізації екран зручно представляти як послідовність фільтрів. Кожен з фільтрів, проаналізувавши дані, може затримати (не пропустити) їх, а може і відразу "перекинути" за екран. Крім того, допускається перетворення даних, передача порції даних на наступний фільтр для продовження аналізу або обробка даних від імені адресата і повернення результату відправникові (рисунок 4).

Окрім функцій розмежування доступу, екрани здійснюють протоколювання обміну інформацією.

Зазвичай екран не є симетричним, для нього визначені поняття "усередині" і "зовні". При цьому завдання екранування формуються як захист внутрішньої області від потенційно ворожої зовнішньої. Так, міжмережеві екрани (МЕ) найчастіше встановлюють для захисту корпоративної мережі організації, що має вихід в Internet.

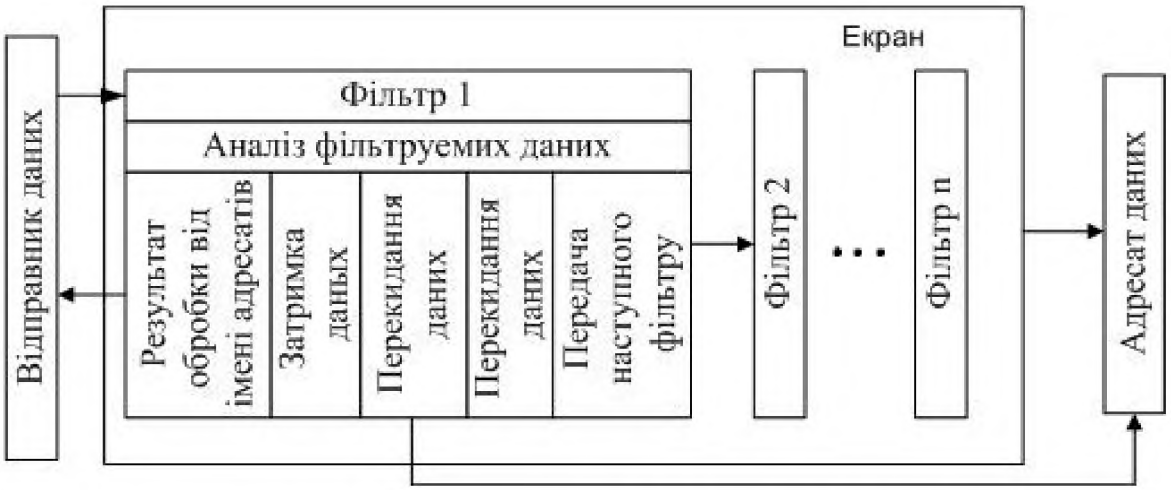

Рисунок 1.4 – Екран як послідовність фільтрів

Екранування допомагає підтримувати доступність сервісів внутрішньої області, зменшуючи або взагалі ліквідовуючи навантаження, викликане зовнішньою активністю. Зменшується уразливість внутрішніх сервісів безпеки, оскільки спочатку зловмисник повинен подолати екран, де захисні механізми конфігуровано особливо ретельно. Крім того, екрануюча система, на відміну від універсальної, може бути влаштована простішим і, отже, безпечнішим чином.

Екранування дає можливість контролювати також інформаційні потоки, направлені в зовнішню область, що сприяє підтримці режиму конфіденційності в ІС організації.

Екранування може бути частковим, захищаючим певні інформаційні сервіси (наприклад, екранування електронної пошти).

Обмежуючий інтерфейс також можна розглядати як різновид екранування. На невидимий об'єкт важко нападати особливо за допомогою фіксованого набору засобів. У цьому сенсі Web-інтерфейс володіє природним захистом, особливо у тому випадку, коли гіпертекстові документи формуються динамічно. Кожен користувач бачить лише те, що йому належить бачити. Можна провести аналогію між динамічно формованими гіпертекстовими документами і уявленнями в реляційних базах даних, з тією істотною обмовкою, що у разі Web можливості істотно ширше.

Екрануюча роль Web-сервиса наочно виявляється і тоді, коли цей сервіс здійснює посередницькі (точніше, інтегруючі) функції при доступі до інших ресурсів, наприклад таблицям бази даних. Тут не тільки контролюються потоки запитів, але і ховається реальна організація даних.

1.11 Архітектурні аспекти безпеки

Боротися з загрозами, властивими мережевому середовищу, засобами універсальних операційних систем не представляється можливим.

Універсальна ОС – це величезна програма, що напевно містить, окрім явних помилок, деякі особливості, які можуть бути використані для нелегального отримання привілеїв. Сучасна технологія програмування не дозволяє зробити такі великі програми безпечними. Крім того, адміністратор, що має справу з складною системою, далеко не завжди в змозі врахувати всі наслідки вироблюваних змін. Нарешті, в універсальній багатокористувацький системі пролому в безпеці постійно створюються самими користувачами (слабкі і/або рідко змінні паролі, невдало встановлені права доступу, залишений без нагляду термінал і тому подібне). Єдиний перспективний шлях пов'язаний з розробкою спеціалізованих сервісів безпеки, які через свою простоту допускають формальну або неформальну верифікацію. Міжмережевий екран якраз і є таким засобом, що допускає подальшу декомпозицію, пов'язану з обслуговуванням різних мережевих протоколів.

Міжмережевий екран розташовується між мережею, що захищається (внутрішньою), і зовнішнім середовищем (зовнішніми мережами або іншими сегментами корпоративної мережі). У першому випадку говорять про зовнішній МЕ, в другому – про внутрішній. Залежно від точки зору, зовнішній міжмережевий екран можна вважати за першу або останню (але ніяк не єдиною) лінію оборони. Першою – якщо дивитися на світ очима зовнішнього зловмисника. Останньою – якщо прагнути до захищеності всіх компонентів корпоративної мережі і припинення неправомірних дій внутрішніх користувачів.

Міжмережевий екран – ідеальне місце для вбудовування засобів активного аудиту. З одного боку, і на першому, і на останньому захисному рубежі виявлення підозрілої активності по-своєму важливе. З іншого боку, МЕ здатний реалізувати скільки завгодно могутню реакцію на підозрілу активність, аж до розриву зв'язку із зовнішнім середовищем. Правда, потрібно усвідомлювати той, що з'єднання двох сервісів безпеки в принципі може створити пролом, сприяючий атакам на доступність.

На міжмережевий екран доцільно покласти дентифікацію/аутентифікацію зовнішніх користувачів, що потребують доступу до корпоративних ресурсів (з підтримкою концепції єдиного входу в мережу).

Через принципи ешелонованості оборони для захисту зовнішніх підключень зазвичай використовується двокомпонентне екранування. Первинна фільтрація (наприклад, блокування пакетів протоколу SNMP, що управляє, небезпечного атаками на доступність, або пакетів з певними IP-адресами, включеними в "чорний список") здійснюється граничним маршрутизатором за яким розташовується так звана демілітаризована зона (мережа з помірною довірою безпеці, куди виносяться зовнішні інформаційні сервіси організації - Web, електронна пошта і тому подібне) і основний МЕ, що захищає внутрішню частину корпоративної мережі.

Теоретично міжмережевий екран (особливо внутрішній) має бути багатопротокольним, проте на практиці домінування сімейства протоколів TCP/IP таке велике, що підтримка інших протоколів представляється надмірністю, шкідливою для безпеки (чим складніше сервіс, тим він більш уразливий).

1.12 Системи архівації і дублювання інформації

Організація надійної і ефективної системи архівації даних є одному з найважливіших завдань по забезпеченню збереження інформації в мережі. У невеликих мережах, де встановлені один - два сервери, найчастіше застосовується установка системи архівації безпосередньо у вільні слоти

серверів. У крупних корпоративних мережах найпереважніше організувати виділений спеціалізований сервер архівації.

Такий сервер автоматично проводить архівацію інформації з жорстких дисків серверів і робочих станцій у вказане адміністратором локальної обчислювальної мережі час, видаючи звіт про проведене резервне копіювання.

Зберігання архівної інформації, що представляє особливу цінність, має бути організоване в спеціальному приміщенні, що охороняється. Фахівці рекомендують зберігати дублікати архівів найбільш цінних даних в іншій будівлі, на випадок пожежі або стихійного лиха. Для забезпечення відновлення даних при збоях магнітних дисків останнім часом найчастіше застосовуються системи дискових масивів - групи дисків, що працюють як єдиний пристрій, відповідних стандарту RAID (Redundant Arrays of Inexpensive Disks). Ці масиви забезпечують найбільш високу швидкість запису/читанню даних, можливість повного відновлення даних і заміни дисків, що вийшли з ладу, в "гарячому" режимі (без відключення решти дисків масиву).

Організація дискових масивів передбачає різні технічні рішення, реалізовані на декількох рівнях:

RAID рівня 0 передбачає просте розділення потоку даних між двома або декількома дисками. Перевага подібного рішення полягає в збільшенні швидкості введення/виводу пропорційно кількості задіяних в масиві дисків.

RAID рівня 1 полягає в організації так званих "дзеркальних" дисків. Під час запису даних інформація основного диска системи дублюється на дзеркальному диску, а при виході з ладу основного диска в роботу тут же включається "дзеркальний".

RAID рівні 2 і 3 передбачають створення паралельних дискових масивів, при записі на які дані розподіляються по дисках на бітовому рівні.

RAID рівні 4 і 5 є модифікацією нульового рівня, при якому потік даних розподіляється по дисках масиву. Відмінність полягає в тому, що на рівні 4 виділяється спеціальний диск для зберігання надмірної інформації, а на рівні 5 надмірна інформація розподіляється по всіх дисках масиву.

Підвищення надійності і захист даних в мережі, заснований на використанні надмірної інформації, реалізуються не тільки на рівні окремих елементів мережі, наприклад дискових масивів, але і на рівні мережевих ОС. Наприклад, компанія Novell реалізує відмовостійкі версії операційної системи Netware - SFT (System Fault Tolerance):

- SFT Level I. Перший рівень передбачає, створення додаткових копій FAT і Directory Entries Tables, негайну верифікацію кожного знов записаного на файловий сервер блоку даних, а також резервування на кожному жорсткому диску близько 2% від об'єму диска.

- SFT Level II містила додатково можливості створення "дзеркальних" дисків, а також дублювання дискових контролерів, джерел живлення і інтерфейсних кабелів.

- Версія SFT Level III дозволяє використовувати в локальній мережі дубльовані сервери, один з яких є "головним", а другий, такий, що містить копію всієї інформації, вступає в роботу у разі виходу "головного" сервера з ладу.

1.13 Аналіз захищеності

Сервіс аналізу захищеності призначений для виявлення вразливих місць з метою їх оперативної ліквідації. Сам по собі цей сервіс ні від чого не захищає, але допомагає виявити (і усунути) пропуски в захисті раніше, ніж їх зможе використовувати зловмисник. Насамперед, маються на увазі не архітектурні (їх ліквідовувати складно), а "оперативні" проломи, що з'явилися в результаті помилок адміністрування або із-за неуваги до оновлення версій програмного забезпечення.

Системи аналізу захищеності (звані також сканерами захищеності), як і розглянуті вище засоби активного аудиту, засновані на накопиченні і використанні знань. В даному випадку маються на увазі знання про пропуски в захисті: про те, як їх шукати, наскільки вони серйозні і як їх усувати.

Відповідно, ядром таких систем є база вразливих місць, яка визначає доступний діапазон можливостей і вимагає практично постійної актуалізації.

В принципі, можуть виявлятися проломи самої різної природи: наявність шкідливого ПЗ (зокрема, вірусів), слабкі паролі користувачів, невдало зконфігуровані операційні системи, небезпечні мережеві сервіси, невстановлені латки, уразливості в застосуваннях і так далі проте найбільш ефективними є мережеві сканери (очевидно, через домінування сімейства протоколів TCP/IP), а також антивірусні засоби. Антивірусний захист ми зараховуємо до засобів аналізу захищеності, не вважаючи за її окремий сервіс безпеки.

Сканери можуть виявляти вразливі місця як шляхом пасивного аналізу, тобто вивчення конфігураційних файлів, задіяних портів і тому подібне, так і шляхом імітації дій того, що атакує. Деякі знайдені вразливі місця можуть усуватися автоматично (наприклад, лікування заражених файлів), про інших повідомляється адміністраторові.

Контроль, що забезпечується системами аналізу захищеності, носить реактивний характер, що запізнюється, він не захищає від нових атак, проте слід пам'ятати, що оборона має бути ешелонованою, і як один з рубежів контроль захищеності цілком адекватний. Відомо, що переважну більшість атак носить рутинний характер; вони можливі тільки тому, що відомі проломи в захисті роками залишаються неусуненими.

1.14 Висновки

У даному розділі проведений аналіз апаратних і програмних засобів захисту інформації загалом і в комп'ютерній мережі зокрема. Внаслідок чого були виявлені достоїнства і недоліки методів захисту інформації, їх можливості, а також можливості їх застосування.

Виконана постановка завдань, відповідно до яких головною метою даної роботи є підвищення ефективності заходів захисту інформації в комп'ютерній мережі.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Характеристика об'єкту

ТОВ «Євро полюс» було засноване в 2001 році і займається виробництвом ліків, дизайном етикеток, збут готовій продукції або інгредієнтів до них. Головний офіс знаходиться за адресою вул. Краснопільська 13б в двоповерховому на другому поверсі. Ситуаційний план представлений у додатку Б.

Співробітники головного офісу:

– Директор - 1 людина;
– Заступник директора - 1 людина;
– Менеджери - 6 чоловік;
– Бухгалтер - 2 людини;
– Системний адміністратор - 1 людина.

Так само можна віднести до штату охоронців (2 людини) і прибиральницю (1 людина), які найняті всіма фірмами, що знаходяться в будівлі.

Системний адміністратор є так само працівником іншого підприємства, які належить директорові ТОВ «Євро полюс».

Режим роботи фірми:

Робочий день для співробітників підприємства починається з 9 до 18. Охорона у свою чергу приходить за півгодини до робочого дня. Для прибиральниці робочий день з 8.30 до 9.00, окрім цього поверхневе прибирання приміщень і коридору під час обідньої перерви з 12.30 до 13.30. Системний адміністратор працює з 9:30 до 18:00. Охоронець працює з 8:30 до 18, зміна через добу.

2.2 Характеристика будівлі

Офіс ТОВ «Євро полюс» знаходиться на 2-му поверсі 2-х поверхової будівлі. Має 5 кімнат, які займають площу 213,5 кв.м.:

– кабінет директора;
– кабінет зам директорів;

– кабінет менеджерів;

– кабінет бухгалтерів;

– серверна.

План поверху представлений у додатку В.

Сусіди:

– 1 поверх: фірма по продажах квартир;

– 1 поверх під офісом: фінансова фірма;

– 2 поверх: фірма по установці кабельного телебачення;

– З півдня – на відстані 15 м. знаходиться житловий 10 поверховий будинок;

– Зі сходу – на відстані 5м. знаходиться проїжджа частина, після якої розташований 5 поверховий житловий будинок;

– Із заходу – на відстані 15 м знаходиться не крита автостоянка;

– З півночі – на відстані 16м знаходиться житловою п’ятиповерховий будинок.

2.3 Характеристика серверу і ПК

На підприємстві встановлений сервер Сервер ARTLINE Business T19 (T19v12) з харакристиками:

Процесор: Восьмиядерний Intel Core i7-9700F (3.0 - 4.7 ГГц)

Патеринська плата: Asus Prime H370-Plus

Пам'ять: 64 ГБ DDR4-2666 МГц;

Слоти PCI: 1 x PCIe 3.0/2.0 x16 (x16 mode), 1 x PCIe 3.0/2.0 x16 (max at x4 mode), 2 x PCIe 3.0/2.0 x1, 2 x PCI.

Жорсткі диски: HDD: 2 x 1 ТБ, SSD: 2 x 250 ГБ

RAID контроллер: 0/1/5/10;

Мережевий контроллер: Realtek RTL8111H;

Стандартні порти виводу/введення: порт RJ-45, 2 x USB 2.0, 2 x USB 3.1 (5 Гбит/с), 2 x USB 3.1 (10 Гбит/с);

Корпус: QUBE QB07A;

Джерела живлення: Seasonic 400 Вт 80+ Bronze.

У офісі для кожного співробітника встановлений окремий комп'ютер. Всі 10 комп'ютерів мають однакову характеристику HP ProOne 440 G4 (4YV99ES):

Екран 23.8" IPS (1920x1080) Full HD;

Процесор: Intel Core i3-8100T (3.1 ГГц);

Пам’ять: 4 ГБ DDR4-2666 МГц;

Жорсткі диски: HDD 1 ТБ;

Відео: Intel UHD Graphics 630;

Пристрої: DVD+/-RW / LAN / Wi-Fi / Bluetooth 5.0 / веб-камера;

Клавиатура: Logitech K120 USB UKR OEM;

Миша: Logitech M170 Wireless Black/Grey.

2.4 Встановлене ПЗ

Основні ПЗ встановленні на підприємстві:

- ОС Windows Server 2016 Standard Edition;
- ОС Microsoft Windows 7 Pro SP1 64-bit Russian;
- Microsoft Office 2016 Pro;
- Бухгалтерія 1С (тільки на комп’ютерах бухгалтерів та сервері);
- Антивірус NOD32 корпоративна версія на 15 ПК, ліцензія на 1 рік.

2.5 Характеристика оброблюваної інформації в комп'ютерній мережі

Інформація, яка циркулює на об'єкті за способом доступу ділиться на:

– відкриту: інформація про підприємство, рід діяльності, кількість робочих місць і персоналу, заробітна плата співробітників, інформація про послуги, які надається фірма – вся інформація, яка не потребує захисту.

– інформацією з обмеженим доступом – важне для підприємства, порушення цілісності або доступності яких може привести до морального або матеріального збитку: інформація про замовників і поставників, про проекти і розробки, фінансові відомості, про устаткування, про засоби реалізації продукції.

Директор підприємства самостійно встановлює ступінь допуску до циркулюючої інформації.

Найвищий гриф секретності інформації на підприємстві: конфіденційно.

Функціональні ПЗ і офісні пакети встановлюються на робочі станції тільки для підтвердження дозволу адміністратора сети.

Вся інформація друкарського, документованого, архівного вигляду, а також системні журнали, технічна, експлуатаційна і розпорядча документація, в не залежності від терміну зберігання знаходиться в сейфі в кабінеті директора.

На сервері зберігається вся інформація, яка є конфіденційною. Терміни зберігання даної інформації встановлює директор підприємства:

- інформація про співробітників - 2 роки;
- інформація про партнерів - 3 року;
- інформація про постачальників - 2 року;
- розробки, проекти, - 3 року;
- бізнес-плани -2 роки;
- інформація про клієнтів-3 року.

Документація, яка включає конфіденційну інформацію, дублюється – створюються резервні копії. Архівація даних проводиться один раз на тиждень засобами ОС. Під час процесу архівації запису користувачів на сервер припиняються, а сервер відключається. Архівація даних виконується стандартними засобами ОС Windows – «Майстер архівації і оновлення», який створює копію необхідних даних на жорсткому диску. Архівації підлягають: стан системи, системні служби і всі диски, пов'язані з компонентами ОС. Майстер архівації створює файл якій містить відомості про архівацію, конфігурацію дисків і інструкції, по виконанню відновлення.

2.6 Вхід в ОС

Конфіденційна інформація зберігається на сервері. Сервер знаходиться в серверній. Доступ до інформації на сервері мають системний мережі, директор, заст. директора. При вході в ОС на сервері, користувачі наділені правом доступу

до інформації, яка зберігається на сервері, використовують систему введення особливого облікового запису і пароля.

Вхід в систему через введення особливого облікового запису і паролю.

Пароль є послідовністю символів і спеціальних символів, довга яких обмежена мінімальним порогом в 8 символів і максимальним – 12 символів.

Кількість введення пароля обмежена 3 спробами. Між спробами невірного пароля є тимчасова затримка для зменшення кількості спроб взлому системи захисту.

Кожен працівник зберігає пароль в місці малодоступному зловмисникові або запам'ятовує його.

На робочій станції вхід в систему здійснюється після введення особливого облікового запису і пароля.

2.7 Модель загроз

Всі джерела загроз безпеці інформації, циркулюючої в корпоративній мережі можна розділити на три основні групи:

1) Загрози, обумовлені діями суб'єкта (антропогенні загрози);

2) Загрози, обумовлені технічними засобами (техногенні загрози);

3) Загрози, обумовлені стихійними джерелами.

Перша група найбільш обширна і представляє найбільший інтерес з погляду організації парирування цим загрозам, оскільки дії суб'єкта завжди можна оцінити, спрогнозувати і прийняти адекватні заходи. Методи протидії цим загрозам керовані і безпосередньо залежать від волі організаторів захисту інформації.

Суб'єкти, дії яких можуть привести до порушення безпеки інформації можуть бути як зовнішні:

- кримінальні структури;
- рецидивісти і потенційні злочинці;
- недобросовісні партнери;
- конкуренти;

так і внутрішні:

– персонал установи;
– персонал філій;
– обличчя з порушеною психікою;
– спеціально упроваджені агенти.

Дії суб'єктів можуть привести до ряду небажаних наслідків, серед яких стосовно корпоративної мережі, можна виділити наступні:

1) Крадіжка:

– технічних засобів (вінчестерів, ноутбуків, системних блоків);
– носіїв інформації (паперових, магнітних, оптичних і ін.);
– інформації (читання і несанкціоноване копіювання);
– засобів доступу (ключі, паролі, ключова документація і ін.).

2) Підміна (модифікація):

– операційних систем;
– систем управління базами даних;
– прикладних програм;
– інформації (даних), заперечення факту відправки повідомлень;
– паролів і правил доступу.

3) Знищення (руйнування):

– технічних засобів (вінчестерів, ноутбуків, системних блоків);
– носіїв інформації (паперових, магнітних, оптичних і ін.);
– програмного забезпечення (ОС, СУБД, прикладного ПЗ)
– інформації (файлів, даних)
– паролів і ключової інформації.

4) Порушення нормальної роботи (переривання):

– швидкості обробки інформації;
– пропускній спроможності каналів зв'язку;
– об'ємів вільної оперативної пам'яті;
– об'ємів вільного дискового простору;
– електроживлення технічних засобів.

5) Помилки:

– при інсталяції ПЗ, ОС, СУБД;
– при написанні прикладного ПЗ;
– при експлуатації ПЗ;
– при експлуатації технічних засобів.

6) Перехоплення інформації (несанкціонований)

– за рахунок ПЕМІ від технічних засобів;
– за рахунок наведень по лініях електроживлення;
– за рахунок наведень по сторонніх провідниках;
– по акустичному каналу від засобів виводу;
– по акустичному каналу при обговоренні питань;
– при підключенні до каналів передачі інформації;
– за рахунок порушення встановлених правил доступу (злом).

Друга група містить загрози менш прогнозована, безпосередньо залежна від властивостей техніка і тому що вимагають особливої уваги. Технічні засоби, що містять потенційні загрози безпеці інформації так само можуть бути внутрішніми:

– неякісні технічні засоби обробки інформації;
– неякісні програмні засоби обробки інформації;
– допоміжні засоби (охорона, сигналізації, телефонії);
– інші технічні засоби, вживані в установі;

і зовнішніми:

– засоби зв'язку;
– близько розташовані небезпечні виробництва;
– мережі інженерних комунікації (енерго-, водопостачання, каналізації).

Наслідками застосування таких технічних засобів, що безпосередньо впливають на безпеку інформації можуть бути:

1) Порушення нормальної роботи:

– порушення працездатності системи обробки інформації;
– порушення працездатності зв'язку і телекомунікацій;

– старіння носіїв інформації і засобів її обробки;
– порушення встановлених правил доступу;
– електромагнітна дія на технічні засоби.

2) Знищення (руйнування):
– програмного забезпечення, ОС, СУБД;
– засобів обробки інформації (кидки напруги, протечки);
– приміщень;
– інформації (розмагнічування, радіація, протечки та ін.);
– персоналу.

3) Модифікація (зміна):
– програмного забезпечення. ОС, СУБД;
– інформації при передачі по каналах зв'язку і телекомунікаціям.

Третю групу складають загрози, які абсолютно не піддаються прогнозуванню і тому заходи їх парирування повинні застосовуватися завжди. Стихійні джерела, що становлять потенційні загрози інформаційній безпеці як правило є зовнішніми по відношенню до даного об'єкту і під ними розуміються раніше всього природні катаклізми:

– пожежі;
– землетруси;
– повені;
– урагани;
– інші форс-мажорні обставини;
– різні непередбачені обставини;
– нез'ясовні явища.

Ці природні і нез'ясовні явища так само впливають на інформаційну безпеку, небезпечні для всіх елементів корпоративної мережі і можуть привести до наступних наслідків:

1) Знищення (руйнування):
– технічних засобів обробки інформації;
– носіїв інформації;

– програмного забезпечення (ОС, СУБД, прикладного ПЗ);
– інформації (файлів, даних);
– приміщень;
– персоналу.

2) Зникнення (пропажа):
– інформації в засобах обробки;
– інформації при передачі по телекомунікаційних каналах;
– носіїв інформації;
– персоналу.

На основі аналізу, що проводиться різними фахівцями в області комп'ютерних злочинів і спостереженнями, по частоті прояву загрози безпеці можна розставити так:

– крадіжка (копіювання) програмного забезпечення;
– підміна (несанкціоноване введення) інформації;
– знищення (руйнування) даних на носіях інформації;
– порушення нормальної роботи (переривання) в результаті вірусних атак;
– модифікація (зміна) даних на носіях інформації;
– перехоплення (несанкціоноване знімання) інформації;
– крадіжка (несанкціоноване копіювання) ресурсів;
– порушення нормальної роботи (перевантаження) каналів зв'язку;

У таблиці 1 наведені най можливіші загрози від персоналу підприємства.

Таблиця 2.1 – Аналіз загроз

Можливі загрози інформації	Директор	Заст. директора	Системний адміністратор	Менеджери	Бухгалтери
Пожежа, землетрус, ураган, різні непередбачені явища і обставини	0,16	0, 16	0,12	0,12	0,128
Відмови інженерно-технічних засобів захисту інформації	0,64	0,64	0,80	0,52	0,52

Продовження таблиці 2.1

Можливі загрози інформації	Директор	Заст. директора	Системний адміністрат	Менеджери	Бухгалтери
Відмови в мережі енергозабезпечення	0,064	0,064	0,32	0,16	0,16
Відмови компонентів комп'ютерів	0,08	0,08	0,8	0,8	0,8
Технічних засобів	1	1	0,64	0,52	0,52
Носіїв інформації	0,80	0,80	0,64	0,64	0,64
Засобів доступу	1	1	0,80	0,64	0,64
Програмних засобів	0,24	0,24	0,8	0,8	0,8
Даних	0,24	0,24	0,8	0,64	0,64
Паролів і правил доступу	1	1	0,8	0,8	0,8
Носіїв інформації	1	1	0,64	0,52	0,52
Програмного забезпечення	0,8	0,8	0,8	0,8	0,8
Інформації	1	1	0,8	0,8	0,8
Паролів і ключової інформації	1	1	0,8	0,8	0,8
Пропускній спроможності каналів зв'язку	0,04	0,04	0,8	0,8	0,8
Об'ємів вільної оперативної пам'яті	0,128	0,128	0,64	0,64	0,64
Об'ємів вільного дискового простору	0,8	1	0,8	1	1
За рахунок ПЕМІ від технічних засобів	0,8	1	0,8	1	1
За рахунок наведень по лініях електроживлення	0,024	1	0,8	0,8	0,8
За рахунок наведень по сторонніх провідниках	0,024	1	0,8	0,8	0,8
При підключенні до каналів передачі інформації	0,64	0,64	0,8	0,48	0,48
За рахунок порушення встановлених правил доступу (злом)	0,64	0,64	0,8	0,48	0,48
Разом	13,2	13,2	17,24	15,7	15,7

2.8 Характеристика комп'ютерної мережі підприємства

На підприємстві існує своя локальна мережа, доступ до якої мають тільки працівники «Євро полюс». В більшості випадків є доступ лише до обмеженого числа тек цієї мережі, необхідних в ході трудової діяльності. Так само в мережі має вихід в Internet. Інформація про кожен вихід в мережу і Internet фіксується системним адміністратором.

Кількість робочих станцій в мережі – 10, поодинці на кожного співробітника.

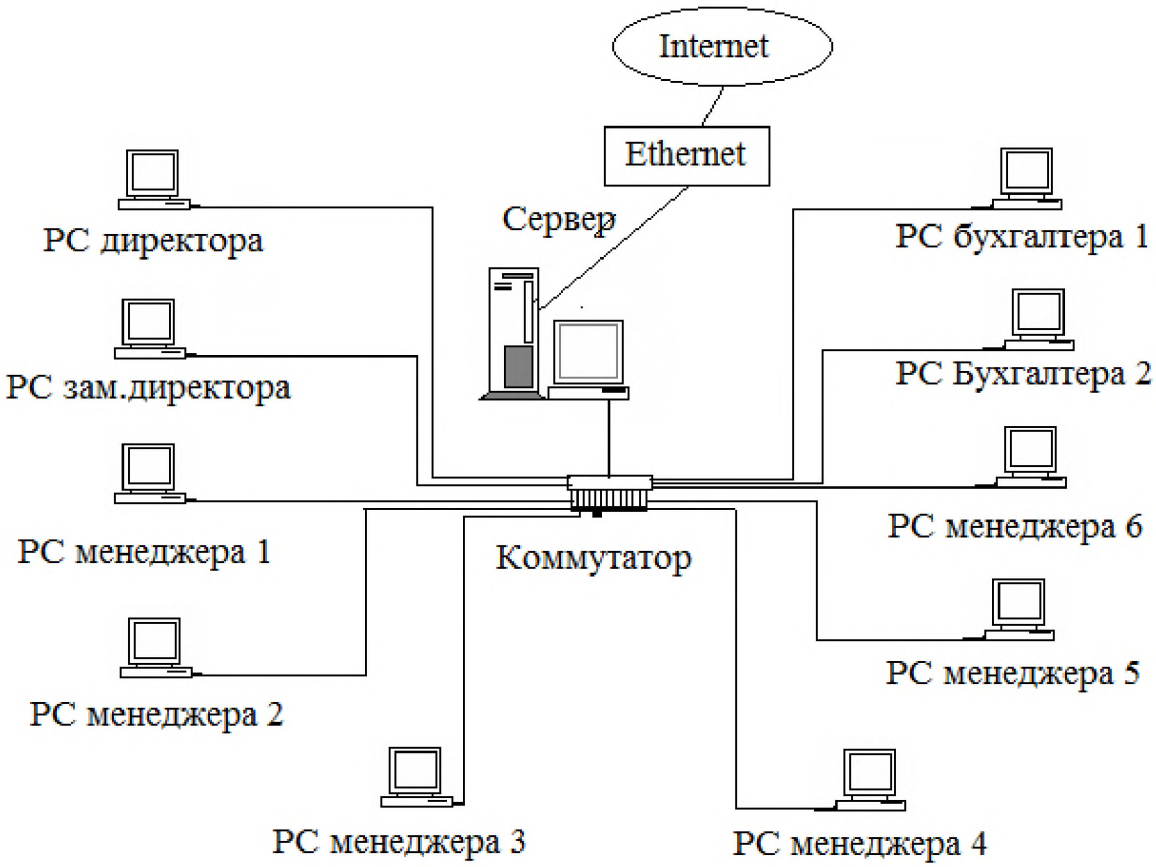

Рисунок 2.1 – Структура комп'ютерної мережі підприємства.

План приміщень, де розташовані робочі станції і сервер представлений у додатку В.

Мережа, як це видно з рисунку 5, має топологію «зірка».

Топологія типу «зірка» є продуктивнішою структурою, кожним комп'ютером, у тому числі і сервером, з'єднується окремим сегментом кабелю з центральним концентратором.

Основною перевагою такої мережі є її стійкість до збоїв, що виникають унаслідок неполадок на окремих ПК або із-за пошкодження мережевого кабелю.

Використовуваний метод доступу - CSMA/CD. Саме цей метод доступу застосовує мережева архітектура Ethernet, яка використовується на підприємстві. Мережа побудована на основі на основі витої пари з використанням кабелю стандарту UTP (Unshielded Twisted Pair) (неекранована витаючи пара) категорії 5е, міжнародного стандарту кабельних систем.

2.9 Характеристика серверної ОС

На сервері встановлена ОС Windows Server 2016.

Windows Server 2016 має засоби забезпечення безпеки, вбудовані в операційну систему. Нижче розглянуті найбільш значущі з них.

Стеження за діяльністю мережі:

Windows Server 2016 дає багато інструментальних засобів для стеження за мережевою діяльністю і використанням мережі. ОС дозволяє:

– проглянути сервер і побачити, які ресурси він використовує;

– побачити користувачів, підключених в даний час до сервера і побачити, які файли у них відкриті;

– перевірити дані в журналі безпеки;

– перевірити записи у журналі подій;

– вказати, про які помилки адміністратор має бути попереджений, якщо вони відбудуться.

Всякий раз, коли користувач починає сеанс на робочій станції, екран початку сеансу запрошує ім'я користувача, пароль і домен. Потім робоча станція посилає ім'я користувача і пароль в домен для ідентифікації. Сервер в домені перевіряє ім'я користувача і пароль в базі даних облікових карток користувачів домена. Якщо ім'я користувача і пароль ідентичні даним в обліковій картці,

сервер повідомляє робочу станцію про початок сеансу. Сервер також завантажує іншу інформацію при початку сеансу користувача, як наприклад установки користувача, свій каталог і змінні середовища.

Для всіх користувачів мережі підприємства передбачено своє ім'я і пароль.

Windows Server 2016 дозволяє визначити, що увійде до ревізії і буде записано в журнал подій безпеки всякий раз, коли виконуються певні дії або здійснюється доступ до файлів. Елемент ревізії показує виконана дія, користувача, який виконав його, а також дату і час дії. Це дозволяє контролювати як успішні, так і невдалі спроби яких-небудь дій. Журнал подій безпеки для умов підприємства є обов'язковим, оскільки у разі спроби злому мережі можна буде відстежити джерело.

Насправді протоколювання здійснюється тільки у відношенні підозрілих користувачів і подій. Оскільки якщо фіксувати всі події, об'єм реєстраційної інформації, швидше за все, ростиме дуже швидко, а її ефективний аналіз стане неможливим. Стеження важливе насамперед як профілактичний засіб. Можна сподіватися, що багато хто утримається від порушень безпеки, знаючи, що їх дії фіксуються.

Права користувача:

Права користувача визначають дозволені типи дій для цього користувача. Дії, регульовані правами, включають вхід в систему на локальний комп'ютер, виключення, установку часу, копіювання і відновлення файлів сервера і виконання інших завдань.

У домені Windows Server 2016 права надаються і обмежуються на рівні домена; якщо група знаходиться безпосередньо в домені, учасники мають права у всіх первинних і резервних контроллерах домена.

Для кожного користувача підприємства обов'язково встановлюються свої права доступу до інформації, дозвіл на копіювання і відновлення файлів.

Установка пароля і політика облікову сеансу:

Для домена визначені всі аспекти політики пароля: мінімальна довжина пароля (6 символів), мінімальний і максимальний вік пароля і винятковість

пароля, який оберігає користувача від зміни його пароля на той пароль, який користувач використовував недавно.

Якщо користувачі примусово відключаються від серверів, коли час його сеансу закінчився, то вони отримують попередження якраз перед кінцем встановленого періоду сеансу. Якщо користувачі не відключаються від мережі, то сервер проведе відключення примусово. Проте відключення користувача від робочої станції не відбудеться. Годинник сеансу на підприємстві не встановлений, оскільки співробітники можуть затриматися на роботі.

Якщо від користувача потрібно змінити пароль, то, коли він цього не зробив при простроченому паролі, він не зможе змінити свій пароль. При простроченні пароля користувач повинен звернутися до адміністратора системи за допомогою в зміні пароля, щоб мати можливість знову входити в мережу. Якщо користувач не входив в систему, а час зміни пароля підійшов, то він буде попереджений про необхідність зміни, як тільки він входитиме.

2.10 Матриця доступу

На підприємстві використовується такий варіант захисту інформації як опікунський захист даних. Опікун – це користувач, якому надані привілеї або права доступу до файлових інформаційних ресурсів.

Кожен співробітник має один з восьми різновидів:

- R - дозвіл на відкриття файлів тільки для читання;
- W - дозвіл на відкриття файлів для запису;
- C - дозвіл на створення файлів на диску;
- D - дозвіл на видалення файлів;
- N - дозвіл на перейменування файлів;
- X - дозвіл на запуск програм.

Таблиця 2.2 – Матриця доступу

Суб'єкти доступу	Об'єкти доступу				
	Доступ до файлів в комп'ютерах	Сервер	Стандартний набір службовим програм	Internet	Електронна пошта
Директор	R,W,C,D,N	R,W,C,D,N,X	R,W,C,D,N,X	R,W,C,D,N	R,W,C,D,N,X
Заст.директора	R,W,C,D,N	R,W,C,N	R,W,C,D,N,X	R,W,C,D,N	R,W,C,D,N,X
Системний адміністратор	R,W,C,D,N,X	R,W,C,D,N,X	R,W,C,D,N,X	R,W,C,D,N,X	R,W,C,D,N,X
Менеджери	R,W,C,D,N	R,W,D,N	R,W,C,D,N,X	R	R,W,C,N
Бухгалтери	R,W,C,D,N	R,W,D,N	R,W,C,D,N,X	R	R,W,C,N

2.11 Вибір антивірусного захисту

Віруси можуть проникати в машину різними шляхами (через глобальну мережу, через заражену дискету та ін). Наслідки їх проникнення вельми неприємні: від руйнування файлу до порушення працездатності всього комп'ютера. Достатньо всього лише одного зараженого файлу, щоб заразити всю інформацію, що є на комп'ютері, а далі заразити всю корпоративну мережу.

При організації системи антивірусного захисту на підприємстві враховувалися наступні чинники риски:

– обмежені можливості антивірусних програм:

Можливість створення нових вірусів з орієнтацією на протидію конкретним антивірусним пакетам і механізмам захисту, використання вразливостей системного і прикладного ПЗ приводять до того, що навіть тотальне застосування антивірусних засобів з актуальними антивірусними базами не дає гарантованого захисту від загрози вірусного зараження, оскільки можлива поява вірусу, процедури захисту від якого ще не додані в новітні антивірусні бази.

Наявність нових неусунених критичних вразливостей в системному ПЗ, створює канали масового розповсюдження нових вірусів по локальних і глобальних мережах. Включення до складу вірусів «троянських» модулів, що забезпечують можливість видаленого управління комп'ютером з максимальними привілеями, створює не тільки ризики масової відмови в обслуговуванні, але і ризики прямих розкрадань шляхом несанкціонованого доступу в автоматизовані банківські системи.

Установка оновлень без попереднього тестування створює ризики несумісності системного, прикладного і антивірусного ПЗ і може приводити до порушень в роботі. В той же час тестування приводить до додаткових затримок в установці оновлень і відповідно збільшує ризики вірусного зараження.

Можливість роботи окремих типів вірусів на різних платформах, здатність вірусів до розмноження з використанням корпоративних поштових систем або обчислювальних мереж, відсутність антивірусних продуктів для деяких конкретних платформ роблять у ряді випадків неможливою або неефективною застосування антивірусного ПЗ.

Сучасні мобільні засоби зв'язку дозволяють недобросовісним співробітникам провести несанкціоноване підключення автоматизованого робочого місця до мережі Internet, створивши тим самим пролом в периметрі безпеки корпоративної мережі і піддавши її інформаційні ресурси ризику масового зараження новим комп'ютерним вірусом. Наявність доступних компактних пристроїв зберігання і перенесення великих об'ємів інформації створює умови для несанкціонованого використання таких пристроїв і носіїв в особистих, не виробничих цілях. Несанкціоноване копіювання на комп'ютери підприємства інформації, отриманої з неперевірених джерел, істотно збільшує ризики вірусного зараження.

Некваліфіковані дії з віддзеркалення вірусної атаки можуть приводити до посилювання наслідків зараження, часткової або повної втрати критичної інформації, неповної ліквідації вірусного зараження або навіть розширення вогнища зараження.

У разі безпосередньої дії вірусу на систему, або при проведенні некваліфікованих лікувальних заходів може бути втрачена інформація або спотворено програмне забезпечення.

Таблиця 2.3 – Порівняння антивірусних програм

Тест/Антивірус	ESET Nod32	Symantec Norton Anti-Virus	Avast Premium	McAfee VirusScan
Помилкові спрацьовування	58%	38%	71%	61%
Самозахисти антивірусів	100%	62%	87%	100%
Лікування активного зараження	85%	40%	63%	53%
Швидкодія	мінімальний вплив на швидкість операційної системи	найшвидші антивірусні сканери на вимогу	найшвидші антивіруси для роботи з офісними програмами	середня швидкість
Виявлення сучасних поліморфних вірусів	26 з 33 балів	14 з 33 балів	31 з 33 балів	21 з 33 балів
Виявлення антивірусів і антируткитов на виявлення і видалення сучасних руткитов	6.5 з 8 балів	5.5 з 8 балів	6.5 з 8 балів	5 з 8 балів

В умовах дії вказаних чинників тільки вживання крутих комплексних заходів безпеки по всіх можливих видах загроз дозволить контролювати постійно зростаючі ризики повної або часткової зупинки бізнес процесів в результаті вірусних заражень.

За результатами тестів, які приведені у таблиці 2.3 був обраний антивірусній пакет ESET Nod32, який заняв перше місце.

ESET Nod32 (далі Nod32). Цей пакет забезпечує централізований захист корпоративної мережі будь-якого масштабу. Сучасне рішення на базі технологій Nod32 для корпоративних мереж, є унікальний технічний комплекс з вбудованою системою централізованого управління антивірусним захистом в масштабі підприємства. Nod32 дозволяє адміністраторові, що працює як

усередині мережі, так і на видаленому комп'ютері (через мережу Internet) здійснювати необхідні адміністративні завдання по управлінню антивірусним захистом організації.

Основні можливості:

– проактивний захист і точне виявлення загроз. Антивірус NOD32 розроблений на основі технології ThreatSense®. Ядро програми забезпечує проактивне виявлення всіх типів загроз і лікування заражених файлів (зокрема, в архівах) завдяки широкому застосуванню інтелектуальних технологій, поєднанню евристичних методів і традиційного сигнатурного детектування;

– Host Intrusion Prevention System (HIPS). Вдосконалена система захисту від спроб зовнішньої дії, здатних негативно вплинути на безпеку комп'ютера. Для моніторингу процесів, файлів і ключів реєстру HIPS використовується поєднання технологій поведінкового аналізу з можливостями мережевого фільтру, що дозволяє ефективно детектувати, блокувати і запобігати подібним спробам вторгнення;

– висока швидкість роботи. Робота Антівіруса NOD32 не відбивається на продуктивності комп'ютера – сканування і процеси оновлення відбуваються практично непомітно для користувача, не навантажуючи систему;

– зручність. Антивірус NOD32 розроблений за принципом мінімальної навантаження на систему і займає не більше 44 Мб пам'яті;

– простота використання. Компактний і інтуїтивно зрозумілий призначений для користувача інтерфейс, мінімальні звернення до користувача при роботі роблять використання NOD32 простим і зручним;

– персональний файервол. Персональний файервол NOD32 забезпечує захист від зовнішніх вторгнень. Використання функції низькорівневого сканування трафіку, дозволяє файерволу відображати більшість атак, які могли б пройти непоміченими.

2.12 Вибір міжмережевого екрану

Міжмережевий екран або мережевий екран – комплекс апаратних або

програмних засобів, що здійснює контроль і фільтрацію мережевих пакетів, що проходять через нього, на різних рівнях моделі OSI відповідно до заданих правил.

Основним завданням мережевого екрану є захист комп'ютерних мереж або окремих вузлів від несанкціонованого доступу. Також мережеві екрани часто називають фільтрами, оскільки їх основне завдання – не пропускати (фільтрувати) пакети, не відповідні під критерії, визначені в конфігурації.

Деякі мережеві екрани також дозволяють здійснювати трансляцію адресов – динамічну заміну внутримережевих (сірих) адресів або портів на зовнішніх, використовуваних за межами ЛОМ.

Для даної мережі і конфігурації сервера був вибраний апаратний міжмережевий екран Cisco PIX-535, який буде встановлений для захисту інформації, циркулюючої в комп'ютерній мережі ТОВ «Євро полюс», з боку Internet.

Міжмережевий екран Cisco PIX-535 дозволяє реалізувати захист корпоративних мереж на недосяжному раніше рівні, при цьому простий в експлуатації. PIX-535 може забезпечити абсолютну безпеку внутрішньої мережі, повністю приховавши її від зовнішнього світу. На відміну від звичайних proxy-серверів, що виконують обробку кожного мережевого пакету окремо з істотним завантаженням центрального процесора, Cisco PIX-535 використовує спеціальну не UNIX-подібну операційну систему реального часу, забезпечуючу вищу продуктивність. Основою високої продуктивності міжмережевого екрану Cisco PIX-535 є схема захисту, що базується на застосуванні алгоритму адаптивної безпеки (adaptive security algorithm – ASA), який ефективно приховує адреси користувачів від порушників. Цей стійкий алгоритм забезпечує безпека на рівні з'єднання на основі контролю інформації про адреси відправника і одержувача, послідовність нумерації пакетів TCP, номери портів і додаткові прапори TCP. Ця інформація зберігається в таблиці, перевірку на відповідність із записами якої проходять всі вхідні пакети.

Доступ через Cisco PIX-535 дозволений тільки в тому випадку, якщо

з'єднання успішно пройшло ідентифікацію. Цей метод забезпечує прозорий доступ для внутрішніх користувачів і авторизованих зовнішніх користувачів, при цьому повністю захищаючи внутрішню мережу від несанкціонованого доступу. Завдяки застосуванню технології "крізного посередника" (Cut-Through Proxy) міжмережевий екран Cisco PIX Firewall також забезпечує істотну перевагу в продуктивності в порівнянні з екранами-посередниками" на базі ОС UNIX. Як і звичайні proxy-сервери, Cisco PIX-535 контролює встановлення з'єднання на рівні застосування. Після успішного проходження користувачем авторизації доступу, відповідно до прийнятих правил безпеки, Cisco PIX-535 забезпечує контроль потоку даних між абонентами на рівні сесії. Така технологія дозволяє міжмережевому екрану працювати значно швидше, ніж звичайні proxy-екрани.

Окрім підвищення продуктивності, застосування спеціалізованої вбудованої операційної системи реального часу також забезпечує підвищення рівня безпеки. На відміну від операційних систем сімейства UNIX, початковий текст яких широко доступний, Cisco PIX – власна розробка компанії, створена спеціально для вирішення завдань забезпечення безпеки. Для підвищення надійності міжмережевий екран Cisco PIX-535 передбачає можливість установки в здвоєній конфігурації в режимі "гарячого резервування", за рахунок чого в мережі виключається наявність єдиної точки можливого збою. Якщо два PIX-екрана працюватимуть в паралельному режимі, і один з них вийде з ладу, то другою в прозорому режимі "підхопить" виконання всіх функцій забезпечення безпеки.

Міжмережевий екран Cisco PIX-535 підтримує більше 500000 одночасних з'єднань і, відповідно, забезпечує підтримку сотень і тисяч користувачів без зниження продуктивності. Повністю завантажений PIX Firewall може забезпечити пропускну спроможність 1,0 Гбіт/с, тобто істотно вище, ніж будь-який міжмережевий екран на базі ОС UNIX або ОС Microsoft Windows.

Міжмережевий екран Cisco PIX-535 забезпечує низьку вартість використання і супроводу. Користувачі, що не мають спеціальної підготовки, можуть швидко набудувати за допомогою простої графічної оболонки PIX

Device Manager (PDM), доступ до якої здійснюється за допомогою звичайного web-браузера. PDM – це застосування, що використовує http-сервер, вбудований в PIX, і що підтримує основний набір команд, необхідний для початкового налаштування міжмережевого екрану. PDM дозволяє настроювати міжмережевий екран практично з будь-якого комп'ютера, для захисту пристрою від "злому" під час конфігурації користувач може використовувати протокол SSL.

Міжмережевий екран Cisco PIX-535 також дозволяє уникнути проблеми браку адрес при розширенні і зміні IP-мереж, Технологія трансляції мережевих адрес Network Address Translation (NAT) робить можливим використання в приватній мережі, як існуючих адрес, так і резервних адресних просторів. Наприклад, це дозволяє використовувати всього лише одну реальну зовнішню IP-адрес для 64 тисяч вузлів внутрішньої приватної мережі. Cisco PIX-535 також може бути настроєний для сумісного використання трансльованих і нетрансльованих адрес, дозволяючи використовувати як адресний простір приватної IP-сети, так і зареєстровані IP-адреса.

Основні можливості :

- система захисту від несанкціонованого доступу на рівні з'єднання забезпечує безпеку ресурсів внутрішньої мережі;
- технологія Cut Through Proxy дозволяє контролювати як вхідні, так і витікаючі з'єднання на базі таких протоколів безпеки, як Terminal Access Controller Access Control System (TACACS+ або Remote Access Dial-In User Service (RADIUS);
- до шести мережевих інтерфейсів для застосування розширених правил захисту. Графічний інтерфейс адміністратора Security Manager призначений для налаштування до 100 міжмережевих екранів PIX Firewall з єдиної консолі;
- динамічна і статична трансляція адрес. Підтримка протоколу мережевого управління SNMP;
- облікова інформація з використанням ведення журналу системних подій (syslog);

- прозора підтримка всіх основних мережевих послуг, таких як World Wide Web (WWW), File Transfer Protocol (FTP), Telnet, Archie, Gopher.
- підтримка застосувань мультимедіа, включаючи Progressive Networks RealAudio & ReadVideo, Xing StreamWorks, White Pines CU-SeeMe, Vocal Tec Internet Phone, VDOnet VDOLive, Microsoft NetShow і VXtreme Web Theater.
- підтримка взаємодій Microsoft Networking сервер-клієнт, Oracle SQL Net-сервер-клієнт;
- безпечна вбудована операційна система реального часу;
- немає необхідності оновлення ПЗ на робочих станціях і маршрутизаторах;
- повний доступ до ресурсів мережі Інтернет для зареєстрованих користувачів внутрішньої мережі;
- сумісність з маршрутизаторами, що працюють під управлінням Cisco IOS™ ;
- підтримка відеоконференцій по протоколу H.323, включаючи Microsoft NetMeeting, Intel Internet Video Phone і White Pine Meeting Point;
- декілька можливих варіантів програмної і апаратної комплектації;
- засоби централізованого адміністрування;
- сповіщення про важливі події на пейджер або по електронній пошті.
- підтримка інтерфейсів Ethernet, Fast Ethernet, Token Ring і FDDI.
- підтримка віртуальних приватних мереж (Virtual Private Network) з використанням стандартної технології IPSec.
- висока продуктивність.

2.13 Система виявлення вторгнень

Підсистема моніторингу є базовим елементом багаторівневої системи захисту мережі і призначена для виявлення різних типів мережевих атак. Дана підсистема виявляє мережеві атаки за допомогою аналізу пакетів даних, що циркулюють в АС, а також подій, що відбуваються на серверах.

У якості можливих рішень даної підсистеми можуть виступати наступні:

- пакетний сніфер, встановлений на сервері;

- антивірусні засоби захисту, встановлено на серверах;
- система виявлення і запобігання атак, компоненти якої розподілено встановлені по мережі.

У таблиці 2.4 представлено аналіз кожного з типів виявлення мережевіх атак.

Таблиця 2.4 – Порівняльній аналіз досліджених рішень, розглянутих з точки зору системи моніторингу мережевих атак

Критерій	Система моніторингу		
	Система виявлення і запобігання атак	Антивірусні засоби захисту	Пакетні сніфери
Можливість виявлення мережевих атак в автоматичному режимі	+	+	-
Можливість блокування виявлених мережевих атак	+	-	-
Наявність модульного принципу побудови	+	+	+
Наявність розподіленої архітектури	+	+	-
Додатковій захист	+	-	-
Легкість реалізації	-	-	+
Кількість переваг	5	3	2

За підсумками порівняльного аналізу даних рішень в якості підсистеми моніторингу пропонується впровадження системи виявлення і запобігання атак. Пропоноване рішення в якості підсистеми моніторингу дозволяє своєчасно виявляти та блокувати мережеві атаки. Такий підхід до побудови підсистеми моніторингу не надає ніякого впливу на пропускну здатність мережевого обладнання, тому що весь аналіз мережевого трафіку здійснюється на сервері, а також даний підхід не вимагає переналаштування існуючого мережевого обладнання.

Система виявлення вторгнень (СОВ) програмний або апаратний засіб, призначений для виявлення фактів неавторизованого доступу в комп'ютерну систему або мережу або несанкціонованого управління ними в основному через

Internet. Системи виявлення вторгнень забезпечують додатковий рівень захисту комп'ютерних систем.

Системи виявлення вторгнень використовуються для виявлення деяких типів шкідливої активності, яке може порушити безпеку комп'ютерної системи. До такої активності відносяться мережеві атаки проти уразливих сервісів, атаки, направлені на підвищення привілеїв, неавторизований доступ до важливих файлів, а також дії шкідливого програмного забезпечення комп'ютерних вірусові

Зазвичай архітектура СОВ включає:

- сенсорную підсистему, призначену для збору подій, пов'язаних з безпекою системи, що захищається;
- підсистему аналізу, призначену для виявлення атак і підозрілих дій на основі даних сенсорів;
- сховище, що забезпечує накопичення первинних подій і результатів аналізу;
- консоль управління, що дозволяє конфігурувати СОВ, спостерігати за станом системи, що захищається, і СОВ, переглядати виявлені підсистемою аналізу інциденти.

За результатами порівняльного аналізу систем виявлення і запобігання атак (таблиця 2.5) обрано RealSecure.

Таблиця 2.5 – Таблиця порівнянь систем виявлення і запобігання атак

Критерій порівняння	OSSEC HIDS	IBM RealSecure	Snort
Метод виявлення	Сігнатурній	Сігнатурній, аналіз протоколів	Сігнатурній, аналіз протоколів
Наявність можливості віддаленого управління	+	+	-
Наявність розподіленої архітектури	+	+	-
Наявність механізмів відповідної реакції	-	+	+
Додатковій захист	SSL	SSL	SNMPv2

Система виявлення атак RealSecure розроблена американською компанією Internet Security Systems, Inc. і призначена для вирішення одного з важливих аспектів управління мережевою безпекою – виявлення атак. Система RealSecure – це інтелектуальний аналізатор пакетів з розширеною базою сигнатур атак, який дозволяє виявляти ворожу діяльність і розпізнавати атаки на корпоративній мережі. Система RealSecure побудована за технологією аналізу мережевих пакетів в реальному масштабі часу (real-time packet analysis) відноситься до систем виявлення атак, орієнтованих на захист цілого сегменту мережі (network-based).

Як тільки атака розпізнається відбувається сповіщення адміністратора через консоль управління або електронну пошту. Крім того, атака може бути зареєстрована в базі даних, а також всі операції при здійсненні атаки можуть бути записані для подальшого відтворення і аналізу. У разі здійснення атаки, яка може привести до виведення з ладу вузлів корпоративної мережі, можливе автоматичне завершення з'єднання з атакуючим вузлом або реконфігурація міжмережевих екранів і маршрутизаторів так, щоб надалі з'єднання з атакуючим вузлом були заборонені. Розподілена архітектура системи RealSecure дозволяє встановлювати компоненти системи так, щоб виявляти і запобігати атакам на мережу як зсередини, так і зовні.

Система RealSecure використовує розподілену архітектуру і містить два основні компоненти RealSecure Detector і RealSecure Manager. Перший компонент відповідає за виявлення і реагування на атаки, і складається з двох модулів - мережевого і системного агентів. Мережевий агент встановлюється на критичний сегмент мережі і виявляє атаки шляхом "прослуховування" трафіку. Системний агент встановлюється на контрольований вузол і виявляє несанкціоновану діяльність, здійснювану на даному вузлі. Компонент RealSecure Manager відповідає за налаштування і збір інформації від RealSecure Detector. Управління компонентами системи RealSecure 6.5 можливо здійснювати як з централізованої консолі, так і за допомогою додаткового модуля, що

підключається до системи мережевого управління HP OpenView (HP OpenView Plug-In Module).

Система RealSecure є одним з кращих рішень для захисту корпоративної мережі і наступних ключових можливостей:

- велике число розпізнаваних атак;
- завдання шаблонів фільтрації трафіку;
- централізоване управління модулями стеження;
- фільтрація і аналіз великого числа мережевих протоколів, в т.ч. TCP, UDP і ICMP;
- фільтрація мережевого трафіку по протоколу, портам і IP-адресам відправника і одержувача;
- різні варіанти реагування на атаки;
- аварійне завершення з'єднання з атакуючим вузлом;
- управління міжмережевими екранами і маршрутизаторами;
- завдання сценаріїв з обробки атак;
- генерація SNMP-послідовностей, що управляють, для управління системами HP OpenView(r), IBM NetView(r) і Tivoli TME10(r);
- запис атаки для подальшого відтворення і аналізу;
- підтримка мережевих інтерфейсів Ethernet, Fast Ethernet і Token Ring;
- відсутність вимоги використання спеціального апаратного забезпечення;
- робота з різними Cryptographic Service Provider;
- встановлення захищеного з'єднання між компонентами системами, а також іншими пристроями;
- наявність всеосяжної бази даних по всіх атаках, що виявляються;
- відсутність зниження продуктивності мережі;
- робота з одним модулем стеження з декількох консолей управління;
- різні формати звітів;
- простота використання і інтуїтивно зрозумілий графічний інтерфейс;
- невисокі системні вимоги до програмного і апаратного забезпечення.

Система RealSecure дозволяє виявляти велике число атак і інших контрольованих подій. Нижче описані основні типи контрольованих подій:

"Відмова в обслуговуванні". Будь-яка дія або послідовність дій, яка приводить будь-яку частину системи, що атакується, до виходу з ладу, при якому та перестає виконувати свої функції. Причиною може бути несанкціонований доступ, затримка в обслуговуванні і так далі Прикладом можуть служити атаки SYN Flood, Ping Flood, Windows Out-of-Band (WinNuke) і тому подібне

"Неавторизований доступ". Будь-яка дія або послідовність дій, яка приводить до спроби читання файлів або виконання команд в обхід встановленої політики безпеки. Також включає спроби зловмисника отримати привілеї, більші, ніж встановлені адміністратором системи. Прикладом можуть служити атаки FTP Root, E-mail WIZ і тому подібне

"Попередні дії перед атакою". Будь-яка дія або послідовність дій з отримання інформації З або Об мережі (наприклад, імена і паролі користувачів), використовувані надалі для здійснення неавторизованого доступу. Прикладом може служити сканування портів (Port scan), сканування за допомогою програми SATAN (SATAN scan) і тому подібне

"Підозріла активність". Мережевий трафік, що виходить за рамки визначення "стандартного" трафіку. Може указувати на підозрілі дії, здійснювані в мережі. Прикладом можуть служити події Duplicate IP Address, IP Unknown Protocol і тому подібне

"Аналіз протоколу". Мережева активність, яка може бути використана для здійснення однієї з атак вищеназваних типів. Може указувати на підозрілі дії, здійснювані в мережі. Прикладом можуть служити події FTP User decode, Portmapper Proxy decode і тому подібне

Періодичне оновлення бази даних атак дозволяє підтримувати рівень захищеності Вашої корпоративної мережі на необхідному рівні.

Для точнішого настроювання системи RealSecure на роботу в мережевому оточенні, адміністратор безпеки може використовувати або один з восьми спочатку встановлюваних шаблонів, або створювати на їх основі свої власні

шаблони, що зважають на специфіку Вашої корпоративної мережі. Всі знов створені шаблони можуть бути збережені для подальшого використання. Шаблони представлені нижчим.

"Максимум можливостей". Даний шаблон дозволяє використовувати абсолютно всі можливості модуля стеження системи RealSecure™, включаючи виявлення атак, аналіз протоколів, запис сесій і тому подібне

"Детектор атак". Даний шаблон дозволяє тільки виявляти атаки. Цей шаблон може бути використаний для виявлення і віддзеркалення атак на ресурси особливо критичних ділянок або вузлів мережі.

"Аналізатор протоколів". Даний шаблон є протилежним "детектору атак", тобто всі можливості по виявленню атак відключені і доступні тільки функції контролю мережевих протоколів. Вказаний шаблон може використовуватися адміністраторами для розуміння всіх процесів, що відбуваються в корпоративній мережі.

"Web-сторож". Даний шаблон дозволяє контролювати тільки HTTP-траффик мережі. Вказаний шаблон може використовуватися адміністраторами для визначення HTTP-траффика Вашої корпоративної мережі або для контролю цього трафіку в сегментах, в яких встановлені тільки Web-сервера. При використанні даного шаблону виявляються тільки атаки, засновані на використанні протоколу HTTP.

"Windows-сети". Даний шаблон дозволяє контролювати трафік, специфічний для Windows мереж. Вказаний шаблон можна використовувати, наприклад, в тих мережах, які побудовані на базі операційної системи Windows NT. При використанні даного шаблону виявляються тільки атаки, специфічні для мереж, побудованих на основі сімейства операційних систем Windows.

"Запис сесій". Даний шаблон дозволяє записувати сесії по протоколах Telnet, FTP, SMTP (електронна пошта) і NNTP (мережеві новини).

"Модуль стеження в DMZ". Даний шаблон орієнтований на функціонування модуля стеження в демілітаризованій зоні (DMZ).

"Модуль стеження до міжмережевого екрану". Даний шаблон орієнтований на функціонування модуля стеження за міжмережевим екраном.

Централізоване управління.

Можливість установки модулів стеження на найбільш критичні ділянки Вашої мережі і можливість централізованого управління ними з єдиного робочого місця робить систему RealSecure незамінним помічником фахівців відділів технічного захисту інформації будь-якої організації. Також можливий доступ до одного модуля стеження одночасно з декількох консолей управління. Це дає можливість управляти модулем стеження декільком адміністраторам, що можливо знаходяться в різних підрозділах (наприклад, у відділі захисту інформації і управлінні автоматизації).

Система RealSecure має можливість за завданням різних варіантів реагування на виявлені атаки:

- запис факту атаки в реєстраційному журналі;
- повідомлення про атаку адміністратора через консоль управління;
- повідомлення про атаку адміністратора по електронній пошті;
- аварійне завершення з'єднання з атакуючим вузлом;
- запис атаки для подальшого відтворення і атаки;
- реконфігурація міжмережевих екранів або маршрутизаторів;
- посилка SNMP-послідовності, що управляють;
- завдання власних обробників атак.

Модуль стеження системи RealSecure™ може автоматично завершувати з'єднання з атакуючим вузлом. Дана можливість доступна тільки для з'єднань по протоколу TCP і полягає в посилці IP-пакета зі встановленим прапором RST. Вказаний вид реакції на атаки дозволяє запобігти багато загроз, здійснюваних багатьма типами атак.

Система RealSecure має можливість генерації послідовностей, що управляють, по протоколу SNMPv1 або передачу певних даних як можлива у відповідь дія на виявлену атаку або яку-небудь контрольовану системою

несанкціоновану дію. Послана послідовність містить дані про час і тип виявленої атаки або несанкціонованої дії.

Дана можливість може використовуватися для додаткової обробки виявленої атаки засобами управління мережею типу HP OpenView, IBM NetView, Tivoli TME10 або будь-яких інших, що дозволяють обробляти вхідні послідовності, що управляють, по протоколу SNMP.

Запис атаки для подальшого аналізу. Дана можливість дозволяє проглядади заздалегідь записані дії, що виконуються зловмисником при атаці

Це дозволить не тільки зрозуміти і проаналізувати дії порушника, але і наочно продемонструвати керівництву організації потенційні загрози. Відтворення атаки для аналізу може бути здійснене як в реальному часі, так і з будь-якою заданою швидкістю.

Для завдання специфічних реакцій на атаки, в системі RealSecure існує можливість визначення своїх власних обробників (наприклад, повідомлення адміністратора про атаку по пейджеру). Обробник атаки має бути будь-яким виконуваним файлом, який може запускатися з командного рядка.

Система RealSecure володіє дуже могутньою підсистемою генерації звітів, що дозволяє легко створювати різні форми звітів. Можливість деталізації даних полегшує читання підготовлених документів як керівниками організації, так і технічним фахівцями.

Створювані звіти можуть містити як докладну текстову інформацію про виявлені атаки, відсортовану по різних ознаках, так і графічну інформацію, що дозволяє наочно продемонструвати рівень захищеності вузлів Вашої корпоративної мережі.

Вся інформація в створюваних звітах може бути відсортована по різних ознаках:

- по пріоритету (ступені риски) атаки;
- по IP-адресу відправника;
- по IP-адресу одержувача;
- по іменах контрольованих подій.

Вся інформація про виявлені атаки зберігається в базі даних. Це дозволяє ефективно організувати всю інформацію і забезпечити швидкий доступ до даних при створенні різних звітів. За допомогою підсистеми налаштування можливе підключення будь-якої бази даних, що має ODBC-драйвер. Ця можливість дозволить використовувати саме ту систему управління базами даних, яка застосовується у Вашій організації (наприклад, Microsoft SQL Server, Microsoft Access і тому подібне). Крім того, дана можливість дозволяє Вам використовувати всю інформацію про мережевий трафік у Ваших власних системах.

Крім того, система RealSecure додатково дозволяє:

- зберігати звіти на жорсткому диску;
- зберігати звіти в базі даних Lotus Notes;
- зберігати звіти в теці Microsoft Exchange;
- пересилати звіти за допомогою механізму Microsoft Mail (MAPI).

Інтуїтивно зрозумілий графічний інтерфейс і простота використання системи допоможе швидко і легко набудувати її з урахуванням вимог, що пред'являються у Вашій організації. Принципи функціонування системи не вимагають реконфігурації інших систем. Це вигідно відрізняє систему RealSecure™, наприклад, від міжмережевих екранів або засобів контролю "активного" коду (Java, ACTIVEX і тому подібне).

При використанні системи RealSecure зниження продуктивності мережі незначне (не більше 3-5%). Проблеми можуть виникнути при функціонуванні модуля стеження на комп'ютері з мінімально необхідними системними вимогами і великій інтенсивності мережевого трафіку. В цьому випадку частина пакетів може бути пропущена без відповідної обробки.

2.14 Організаційні заходи щодо забезпечення інформаційної безпеки мережі

2.14.1 Інструкція використання ЛОМ ТОВ «Євро полюс»

1) Мета

Цілі програми захисту інформації ТОВ «Євро полюс» полягають в тому, щоб гарантувати цілісність, доступність і конфіденційність даних, які мають бути достатньо повними, точними, і своєчасними, щоб задовольняти виробничі потреби співробітників, не жертвуючи при цьому основними принципами, описаними в цій політиці. Визначаються наступні цілі:

- Гарантувати, що в середовищі ЛОМ ТОВ «Євро полюс» забезпечується відповідна безпека, відповідна критичності інформації;
- Гарантувати, що безпека є рентабельною і заснована на співвідношенні вартості і риски, або необхідно задовольняє відповідним керівним вимогам;
- Гарантувати індивідуальну підзвітність для даних, інформації, і інших комп'ютерних ресурсів, до яких здійснюється доступ;
- Гарантувати перевірку середовища ЛОМ компанії «Євро полюс»;
- Гарантувати, що службовці будуть забезпечені достатньо повним керівництвом по розподілу обов'язків щодо підтримки безпеки при роботі в автоматизованій інформаційній системі;
- Гарантувати, що для всіх критичних функцій компанії «Євро плюс» ЛОМ є відповідні плани забезпечення безперервної роботи, або плани відновлення при стихійних лихах.

2) Зона дії.

Дія політики безпеки ЛОМ компанії розповсюджується на всіх користувачів, як WAT им відповідно до службових обов'язків використовують ЛОМ компанії.

З даним документом повинні ознайомитися співробітники, яким необхідне використання автоматизованого робочого місця і ЛОМ компанії по своїх службових обов'язках. Співробітники надають письмове підтвердження того, що ознайомилися з політикою безпеки ЛОМ директорові.

3) Затвердження політики.

Даний документ затверджений директором компанії.

4) Відповідальність.

Наступні групи співробітників несуть відповідальність за впровадження і досягнення цілей безпеки, сформульованих в цій політиці. Детальні обов'язки представлені в Обов'язках по Забезпеченню Захисту ЛОМ ТОВ «Євро полюс».

Функціональне керівництво – директор, який несе відповідальність згідно своїм функціональним обов'язкам (не в області комп'ютерної безпеки) усередині ТОВ «Євро полюс». Функціональне Керівництво відповідає за інформування співробітників щодо цієї політики, гарантію того, що кожен співробітник має її копію, і взаємодію зі всіма службовцями по проблемах безпеки.

Адміністратор ЛОМ – адміністратор безпеки, який бере участь в щоденному управлінні і підтримці працездатності ЛОМ компанії. Він відповідає за забезпечення безперервного функціонування ЛОМ. Адміністратор ЛОМ відповідає за здійснення відповідних заходів захисту в ЛОМ відповідно до політики безпеки ЛОМ компанії.

Користувачі – є будь-якими службовцями, які мають доступ до ЛОМ компанії. Вони відповідають за використання ЛОМ відповідно до політики безпеки ЛОМ. Всі користувачі даних відповідають за дотримання специфічних політик безпеки, встановлених тими особами, хто несе основну відповідальністю за захист тих або інших даних, і за доповідь керівництву про будь-яку підозру на порушення захисту.

Відмова дотримувати цю політику може піддати інформацію, циркулюючу в компанії, неприпустимому ризику втрати конфіденційності, цілісності або доступності при її зберіганні, обробці. Порушення стандартів, процедур або керівництва, що підтримують цю політику, можуть привести до дисциплінарної відповідальності аж до звільнення з роботи.

5) Загальні правила розмежування доступу в ЛОМ

5.1) Кожен персональний комп'ютер повинен мати "власника" або "системного адміністратора", який є відповідальним за працездатність і безпеку комп'ютера, і за дотримання всіх політик і процедур, зв'язаних з використанням даного комп'ютера. Цей користувач має бути навчений і забезпечений

відповідним керівництвом так, щоб він міг коректно дотримувати всі політики і процедури.

5.2) Щоб запобігти неавторизованому доступу до даних ЛОМ, програмному забезпеченню, і іншим ресурсам, що знаходяться на сервері ЛОМ, всі механізми захисту сервера ЛОМ повинні знаходитися під монопольним управлінням адміністратора ЛОМ.

5.3) Щоб запобігти розповсюдженню зловмисного програмного забезпечення і допомогти виконанню ліцензійних угод про програми, користувачі повинні гарантувати, що їх програмне забезпечення належним чином ліцензіює і є безпечним.

5.4) За всі зміни(заміни) програмного забезпечення і створення резервних копій даних на сервері відповідає адміністратор ЛОМ.

5.5) Кожному користувачеві має бути призначений унікальний ідентифікатор користувача і початковий пароль (або інша інформація для ідентифікації і аутентифікації), тільки після того, як закінчено оформлення належної документації. Користувачі не повинні спільно використовувати призначені ним ідентифікатори користувачів.

5.6) Користувачі винні аутентифіцироватися в ЛОМ перед зверненням до ресурсів ЛОМ.

5.7) Ідентифікатор користувача повинен віддалятися після тривалого періоду не використання.

5.8) Використання апаратних засобів ЛОМ типу моніторів / реєстраторів трафіку і маршрутизаторів повинно бути авторизовано і проводитися під контролем адміністратора ЛОМ.

5.9) Звіти про безпеку повинні готуватися і розглядатися щомісячно.

6) Особливі обов'язки для забезпечення безпеки ЛОМ компанії

6.1) Користувачі

Допускається, що користувачі добре обізнані щодо політики безпеки компанії, і інших застосовних законів, політик, указів і процедур і твердо їх

дотримуються. Користувачі повністю відповідають за їх власну поведінку. Зокрема, користувачі відповідають за наступне:

– Відповідають за використання доступних механізмів безпеки для захисту конфіденційності і цілісності їх власної інформації, коли це потрібно.

– Слідують місцевим процедурами захисту критичних даних, а також процедурам безпеки самої ЛОМ ТОВ «Євро полюс». Використовують механізми захисту файлів для підтримки відповідного управління доступом до файлів.

– Вибирає і використовує хороші паролі. Не записує паролів, і не розкриває їх іншим. Не використовує спільно ідентифікатори користувачів.

– Відповідає за повідомлення адміністратора безпеки про порушення захисту або виявлену відмову.

– Відповідають за не використання слабких місць АС.

– Не здійснюють навмисної зміни, знищення, читання, або передачі інформації неавторизованим способом: не заважають спеціально дістати іншим користувачам авторизований доступ до ресурсів ЛОМ і інформації в ній.

– Надають правильну інформацію для ідентифікації і аутентифікації, коли це потрібно, і не намагаються вгадати подібну інформацію для інших користувачів.

– Відповідають за гарантію виконання резервного копіювання даних і програмного забезпечення що знаходиться на жорсткому диску їх власного автоматизованого робочого місця.

– Відповідають за розуміння принципів роботи шкідливого програмного забезпечення, методів, за допомогою яких воно вноситься і розповсюджується, і вразливих місць, які використовуються шкідливим програмним забезпеченням і неавторизованими користувачами.

– Відповідають за знання і використання відповідних політик і процедур для запобігання, виявлення, і видалення шкідливого програмного забезпечення.

– Відповідають за знання того, на що потрібно звертати увагу при роботі в певних системах і конкретних програмах, щоб виявити ознаки їх незвичайної

роботи, і що потрібно зробити або з ким зв'язатися для отримання додаткової інформації.

– Відповідає за використання програмно-апаратних засобів захисту, які доступні для захисту системи від шкідливого програмного забезпечення.

– Відповідає за знання і використання процедур по забезпеченню безперервної роботи для заборони і відновлення при потенційних інцидентах.

6.2) Функціональне керівництво.

Директор відповідає за розробку і виконання ефективних політик безпеки, які відображають специфічні цілі ЛОМ компанії. Він повністю несе відповідальність за забезпечення того, що захист інформації і ліній зв'язку є і залишається важливою і критичною метою в повсякденній діяльності. Зокрема директор відповідає за наступне:

– Відповідає за проведення ефективного управління ризиком для того, щоб забезпечити основу для формулювання розумної політики. Управління ризиком вимагає ідентифікації цінностей, які потрібно захистити, визначення вразливих місць, аналізу риски їх використання і реалізації рентабельних засобів захисту.

– Відповідає за гарантію того, щоб кожен користувач отримав, як мінімум, копію політики безпеки до внесення його до списків користувачів АС.

– Відповідає за здійснення програми навчання основам безпеки для користувачів, щоб можна було гарантувати знання ними політики безпеки і правил роботи на комп'ютері.

– Відповідає за інформування адміністратора ЛОМ про зміни в статусі будь-якого службовця, який використовує ЛОМ компанії. Це зміна статусу може включати перехід з організації в організацію в одному відомстві, перехід з відділу у відділ, або закінчення роботи в компанії.

– Відповідає за гарантію того, що користувачі розуміють природу шкідливого програмного забезпечення, розуміють, як воно взагалі розповсюджується, і які програмно-апаратні засоби захисту повинні використовуватися проти нього.

6.3) Адміністратор безпеки

Передбачається, що адміністратор безпеки здійснює місцеві політики безпеки, які зв'язані із застосуванням програмно-апаратних засобів захисту, архівацією критичних програм і даних, управлінням доступом і захистом устаткування ЛОМ. Зокрема, адміністратор безпеки відповідає за наступне:

– Відповідає за коректне застосування доступних механізмів захисту для здійснення місцевих політик безпеки.

– Відповідає за повідомлення керівництва про працездатність тих, що існують політик і будь-яких технічних міркуваннях, які могли б поліпшити їх ефективність.

– Відповідає за захищеність середовища ЛОМ усередині організації і інтерфейсів з глобальними мережами.

– Відповідає за оперативне і ефективне залагоджування подій з комп'ютерною безпекою.

– Повідомляє директора про проникнення зловмисника в ЛОМ

– Відповідає за використання надійних і доступних засобів аудиту для виявлення порушень безпеки.

– Відповідає за проведення своєчасних перевірок системних журналів серверів ЛОМ.

– Відповідає за відстежування інформації про політиків безпеки і прийоми забезпечення безпеки в інших організаціях і, коли це необхідно, інформує користувачів і повідомляє керівництво про зміни або нові розробки.

– Відповідає за розробку відповідних процедур і видання інструкцій по запобіганню, виявленню, і видаленню шкідливого програмного забезпечення.

– Відповідає за своєчасне створення резервних копій всіх даних і програмного забезпечення на серверах ЛОМ.

– Відповідає за виявлення і рекомендацію пакетів програм для виявлення і видалення шкідливого програмного забезпечення.

– Відповідає за розробку процедур, що дозволяють користувачам повідомляти про комп'ютерні віруси і інші інциденти.

– Відповідає за проведення періодичного аналізу для того, щоб гарантувати, що дотримуються належні процедури безпеки, включаючи ті, які призначені для захисту від шкідливого програмного забезпечення.

7) Порядок і періодичність перегляду політики

Політика безпеки ЛОМ може переглядатися не частіше, ніж один раз в рік. Внесення змін або доповнень відбувається на підставі заяви адміністратора безпеці про необхідність перегляду політики. У перегляді політики безпеки беруть участь адміністратор безпеки і юрист компанії.

2.15 Висновки

В даному розділі був виконаний аналіз існуючої архітектури мережі ТОВ «Євро полюс», проаналізовані інформаційні потоки мережі, а також існуюча система розмежування доступу. На основі проведеного аналізу були виявлені недоліки функціонування існуючої системи інформаційної безпеки мережі підприємства. Також були розглянуті та проаналізовані вимоги до системи інформаційної безпеки мережі і проведені дослідження можливих моделей моніторингу даних, циркулюючих у мережі. Після цього був здійснений порівняльний аналіз розглянутих моделей. Базуючись на виконаних дослідженнях, були розроблені рекомендації щодо удосконалення існуючої системи інформаційної безпеки мережі підприємства, а також рекомендації та інструкції по безпосередній роботі з системою.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Розробка комплексної системи захисту інформації комп'ютерної мережі потребує обґрунтування економічної її доцільності, виходячи з аналізу витрат на розробку та впровадження. Тому метою економічного розділу є здійснення відповідних розрахунків, які дозволять встановити економічного ефекту від впровадження та налагодження комплексів засобів захисту інформації комп'ютерної мережі.

3.1 Розрахунок (фіксованих) капітальних витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

До капітальних витрат належать витрати на розробку політики безпеки інформації, які визначаються виходячи з трудомісткості розробки політики безпеки інформації.

Визначення трудомісткості розробки політики безпеки інформації

Трудомісткість розробки політики безпеки інформації визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного спеціаліста з інформаційної безпеки):

$$t = tmз + tв + ta + tвз + tозб + tовр + tд, \text{ годин,}$$

де $tmз$ – тривалість складання технічного завдання на розробку політики безпеки інформації;

$tв$ – тривалість розробки концепції безпеки інформації у організації;

ta – тривалість процесу аналізу ризиків;

$tвз$ – тривалість визначення вимог до заходів, методів та засобів захисту;

$t_{озб}$ – тривалість вибору основних рішень з забезпечення безпеки інформації;

$t_{овр}$ – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації;

$t_{д}$ – тривалість документального оформлення політики безпеки.

Визначено, що відповідно до етапів розробки політики безпеки інформації, тривалість операцій склала наступні величини:

$t_{тз}$=15 годин, $t_{в}$=30 годин, $t_{тз}$=18 годин, $t_{вз}$=15 годин, $t_{озб}$=8 годин, $t_{овр}$=6 годин, $t_{д}$=6 годин.

Отже, t=15+30+18+15+8+6+6= 98 годин,

Розрахунок витрат на створення політики безпеки інформації

Витрати на розробку політики безпеки інформації Крп складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки Ззп і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації Змч.

$$К_{рп} = З_{зп} + З_{мч} .$$

$$К_{рп} = З_{зп} + З_{мч} = 92880 + 585,06 = 93465,06 \text{ грн.}$$

$$З_{зп} = t\ З_{пр} = 98*260 = 25480 \text{ грн.}$$

де t – загальна тривалість розробки політики безпеки, годин;

Зіб – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

$$З_{мч} = t*С_{мч}=98*5,97=585,06 \text{ грн.}$$

де $t_{д}$ – трудомісткість підготовки документації на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = 0,9 \cdot 3 \cdot 1,64 + \frac{3800 \cdot 0,4}{1920} + \frac{7200 \cdot 0,2}{1920} = 5,97 \text{ грн.}$$

Відповідно до розроблених рекомендації щодо удосконалення існуючої системи інформаційної безпеки мережі ТОВ «Євро полюс», а також рекомендацій та інструкції по безпосередній роботі з системою планується використання антивірусу NOD32, який вже встановлений на комп'ютерах підприємства та потребує лише подовження ліцензії.

Серед апаратних засобів, які відповідно до розроблених рекомендації, необхідно придбати, належить міжмережевий екран Cisco PIX-535, який буде встановлений для захисту інформації, циркулюючої в комп'ютерній мережі ТОВ «Євро полюс», з боку Internet. Вартість міжмережевого екрану Cisco PIX-535 складає 30250 грн.

Також планується придбання система виявлення атак RealSecure, вартість якої складає 2100 грн.

Витрати на встановлення обладнання та налагодження системи інформаційної безпеки складають 20% відсотків від первісної вартості програмного забезпечення, тобто 6470 грн.

Таким чином, капітальні (фіксовані) витрати на створення політики інформаційної безпеки підприємства складають:

$$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} =$$
$$= 93465,06 + 30250 + 2100 + 6470 = 132285,1 \text{ грн.}$$

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн;

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу,

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки.

3.1.1 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_{в} + С_{к} + С_{ак}, \quad грн.$$

де $С_{в}$ - вартість відновлення й модернізації системи ($С_{в} = 0$);

$С_{к}$ - витрати на керування системою в цілому;

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак} = 0$ грн.).

Витрати на керування системою інформаційної безпеки ($С_{к}$) складають:

$$С_{к} = С_{н} + С_{а} + С_{з} + С_{ел} + С_{о} + С_{тос}, \text{ грн.}$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються ($С_{н} = 5000$ грн.).

Річні амортизаційні відрахування міжмережевого екрану Cisco PIX-535 вартістю 30250 грн із корисним строком використання 2 роки, за прямолінійним методом нарахування амортизації складуть:

$$С_а = 30250 / 2 = 15125 \text{ грн.}$$

Вартість подовження ліцензії антивірусу NOD32, який вже встановлений на 10 комп'ютерах підприємства, складає 335 грн.

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн.}$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 14000 грн. Додаткова заробітна плата – 10% від основної заробітної плати. Отже,

$$С_з = 14000*12 + 14000*12*0,1= 184800 \text{ грн.}$$

Ставка ЄСВ для всіх категорій платників з 01.01.2019 р. складає 22%.

$$С_{єв} = 237600*0,22 = 40656 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.,}$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=1,2 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,64 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$$С_{ел} = 1,2*1920*1,64 = 3778,56 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат - 1% (Стос = 132285,1*0,01=1322,85 грн).

Витрати на керування системою інформаційної безпеки ($С_к$) визначаються:

$$С_к = 5000+15125+335+184800+40656+3778,56+1322,85= 52478,7 \text{ грн.}$$

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають 52478,7 грн.

3.2 Оцінка можливого збитку від атаки на вузол або сегмент мережі

3.2.1 Оцінка величини збитку

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки для умовного підприємства.

Необхідні вихідні дані для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 4 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 2 години;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 6 годин;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 7000 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 9000 грн./міс.;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 1 особи;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 9 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 400 тис. грн. у рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин, грн;

I – число атакованих сегментів корпоративної мережі, 1;

N – середнє число атак на рік, 40.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V,$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_П = \frac{\sum Зс}{F} \cdot t_n = \frac{7000 \cdot 9}{176} \cdot 4 = 1431{,}82 \quad \text{грн},$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч},$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн.;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви} = \frac{\sum Зс}{F} \cdot t_{ви} = \frac{7000 \cdot 9}{176} \cdot 6 = 2147{,}73 \text{ грн.}$$

Витрати на відновлення сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum Зо}{F} \cdot t_в = \frac{9000 \cdot 1}{176} \cdot 2 = 102{,}27 \text{ грн.}$$

$$П_в = 2147{,}73 + 102{,}27 = 2250 \text{ грн.}$$

Втрати від зниження очікуваного обсягу прибутків за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи

із средньогодинного обсягу прибутку і сумарного часу простою сегмента корпоративної мережі:

$$V = \frac{O}{Fг} \cdot (t_П + t_В + t_{ВИ})$$

$$V = \frac{400000}{2080} \cdot (4 + 2 + 6) = 2307{,}69 \text{ грн.}$$

де $F_г$ – річний фонд часу роботи філії (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 год.

$$U = 1431{,}82 + 2250 + 2307{,}69 = 5989{,}51 \text{ грн.}$$

Таким чином, загальний збиток від атаки на сегмент корпоративної мережі організації складе:

$$B = \sum_i \sum_n U = \sum_1 \sum_{40} 5989{,}51 = 239580{,}4 \text{ грн.}$$

3.2.2 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної:

$$E = B \cdot R - C \text{ грн.},$$

де B – загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці (35%);

С – щорічні витрати на експлуатацію системи інформаційної безпеки.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки:

E = 239580,4*0,35 – 52478,7 = 31374,44 грн.

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,}$$

де E – загальний ефект від впровадження системи інформаційної безпеки грн.;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{31374,44}{132285,1} = 0,24, \quad \text{частки одиниці,}$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$ROSI > (N_{деп} - N_{інф})/100),$$

де $N_{деп}$ – річна депозитна ставка, (18 %);

$N_{інф}$ – річний рівень інфляції, (11%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$0,24 > (18 - 11)/100 = 0,24 > 0,07.$$

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{0,24} = 4,17, \quad \text{років.}$$

3.4 Висновок

Розробка комплексної системи захисту інформації комп'ютерної мережі ТОВ «Євро полюс» є економічно доцільним, оскільки капітальні та експлуатаційні витрати будуть меншими за можливий відвернений збиток. Капітальні витрати складають 132285,10 грн., експлуатаційні – 52478,70 грн. Величина річного економічного ефекту складає 31374,44 грн. Коефіцієнт повернення інвестицій ROSI складає 0,24 грн./грн.

ВИСНОВКИ

У ході виконання роботи виконано аналіз існуючих мережевих систем моніторингу даних. Було проведено дослідження можливих варіантів використання засобів захисту інформації у комп'ютерній мережі ТОВ «Євро полюс». На підставі проведеного дослідження визначені найбільш ефективні засобі захисту, механізм їх роботи.

Практична цінність роботи полягає в підвищенні рівня інформаційної безпеки мережі ТОВ «Євро полюс» шляхом впровадження засобів захисту інформації циркулюючої у мережі, а також удосконалення існуючої системи інформаційної безпеки мережі.

У економічному розділі був здійснений розрахунок економічного ефекту від впровадження та налагодження розроблених засобів захисту інформації, які зменшать збитки від атак на мережу. На підставі отриманих результатів було доведено, що впровадження в систему захисту пропонованої моделі є економічно ефективним рішенням.

ПЕРЕЛІК ПОСИЛАНЬ

1 Мультисервисные сети Ethernet масштаба города (Електрон. ресурс) / Спосіб доступу: URL: http://www.pole-s.ru/index.php?option=com_content&task=view&id=12 – Загол. з екрана.

2 Metro Ethernet. Архитектура и технологии (Електрон. ресурс) / Спосіб доступу: URL: http://www.nag.ru/2005/0227/0227.shtml. – Загол. з екрана.

3 Digital subscriber line (Електрон. ресурс) / Спосіб доступу: URL: http://ru.wikipedia.org/wiki/Digital_subscriber_line. – Загол. з екрана.

4 Транспортные технологии уровня магистрали (Електрон. ресурс) / Спосіб доступу: URL: http://www.pbxlib.com.ua/network/article_5.html. – Загол. з екрана.

5 Алексеев И. Введение в архитектуру MPLS (Електрон. ресурс) / Спосіб доступу: URL: http://athena.vvsu.ru/docs/tcpip/mpls/. – Загол. з екрана.

6 Инструменты мониторинга и анализа сети (Електрон. ресурс) / Спосіб доступу: URL: http://www.citforum.ru/nets/optimize/locnop_07.shtml#31. – Загол. з екрана.

7 Возможности биллинговых систем для операторов фиксированной связи (Електрон. ресурс) / Спосіб доступу: URL: http://revolution.allbest.ru/radio/00009846_0.html. – Загол. з екрана.

8 Использование сканеров безопасности в процессе тестирование сети на устойчивости к взлому (Електрон. ресурс) / Спосіб доступу: URL: http://www.securitylab.ru/analytics/243179.php. – Загол. з екрана.

9 Сердюк В.А. Защита информационных систем от потенциальной угрозы «пятой колонны» (Електрон. ресурс) / Спосіб доступу: URL: http://www.antivir.ru/main.phtml?/press_about_us/secure_atack&print=1. – Загол. з екрана.

10 Сердюк В.А. Технологии сбора исходных данных системами обнаружения атак (Електрон. ресурс) / Спосіб доступу: URL:

http://www.antivir.ru/main.phtml?/press-center/technology&print=1. – Загол. з екрана.

11 НД ТЗІ 1.1-003-99 „Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу".

12 Закон України № 48 – ВР "Про інформацію"// Баланс. – 1992. – 17с.

13 Средства информационной безопасности в коммутаторах (Електрон. ресурс) / Спосіб доступу: URL: http://www.dreamcatcher.ru/cisco/001_switches.html. – Загол. з екрана.

14 Welcome to the Home of OSSEC (Електрон. ресурс) / Спосіб доступу: URL: http://www.ossec.net/. – Загол. з екрана.

15 Snort IDS (Електрон. ресурс) / Спосіб доступу: URL: http://www.snort.org/. – Загол. з екрана.

16 Prelude Technologies (Електрон. ресурс) / Спосіб доступу: URL: http://www.prelude-ids.com/en/welcome/index.html. – Загол. з екрана.

17 Positive Technologies (Електрон. ресурс) / Спосіб доступу: URL: http://www.ptsecurity.ru/xs7.asp. – Загол. з екрана.

18 Internet Scanner (Електрон. ресурс) / Спосіб доступу: URL: http://www.iss.net/products_services/enterprise_protection/vulnerability_assessment/scanner_internet.php. – Загол. з екрана.

19 Tenable Network Security (Електрон. ресурс) / Спосіб доступу: URL: http://www.nessus.org. – Загол. з екрана.

20 Retina Network Security Scanner (Електрон. ресурс) / Спосіб доступу: URL: http://www.eeye.com/html/products/retina/index.html. – Загол. з екрана.

21 Network Security Scanner and Vulnerability Management Solution (Електрон. ресурс) / Спосіб доступу: URL: http://www.gfi.com/lannetscan/. – Загол. з екрана.

22 Закон України № 31 – ВР "Про захист інформації в інформаційно-телекомунікаційних системах" // Баланс. – 1994. – 5с.

23 НД ТЗІ 1.4-001-2000 „Типове положення про службу захисту інформації в автоматизованій системі".

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	1 Розділ	22	
6	А4	2 Розділ	39	
7	А4	3 Розділ	11	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	
14	А4	Додаток Д	1	
15	А4	Додаток Е	1	

ДОДАТОК Б

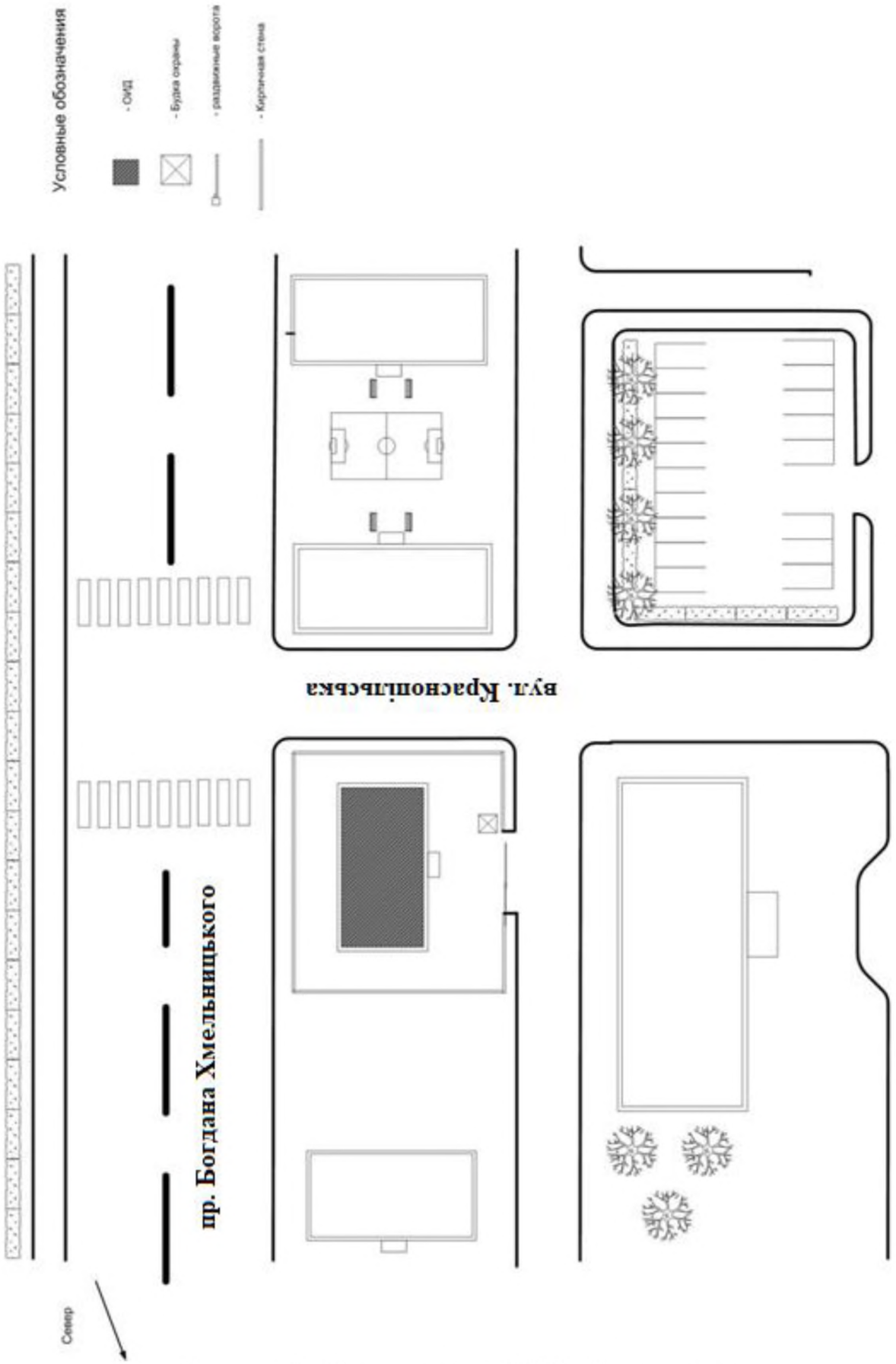

Рисунок 1 – Розташування ТОВ «Євро полюс»

ДОДАТОК В

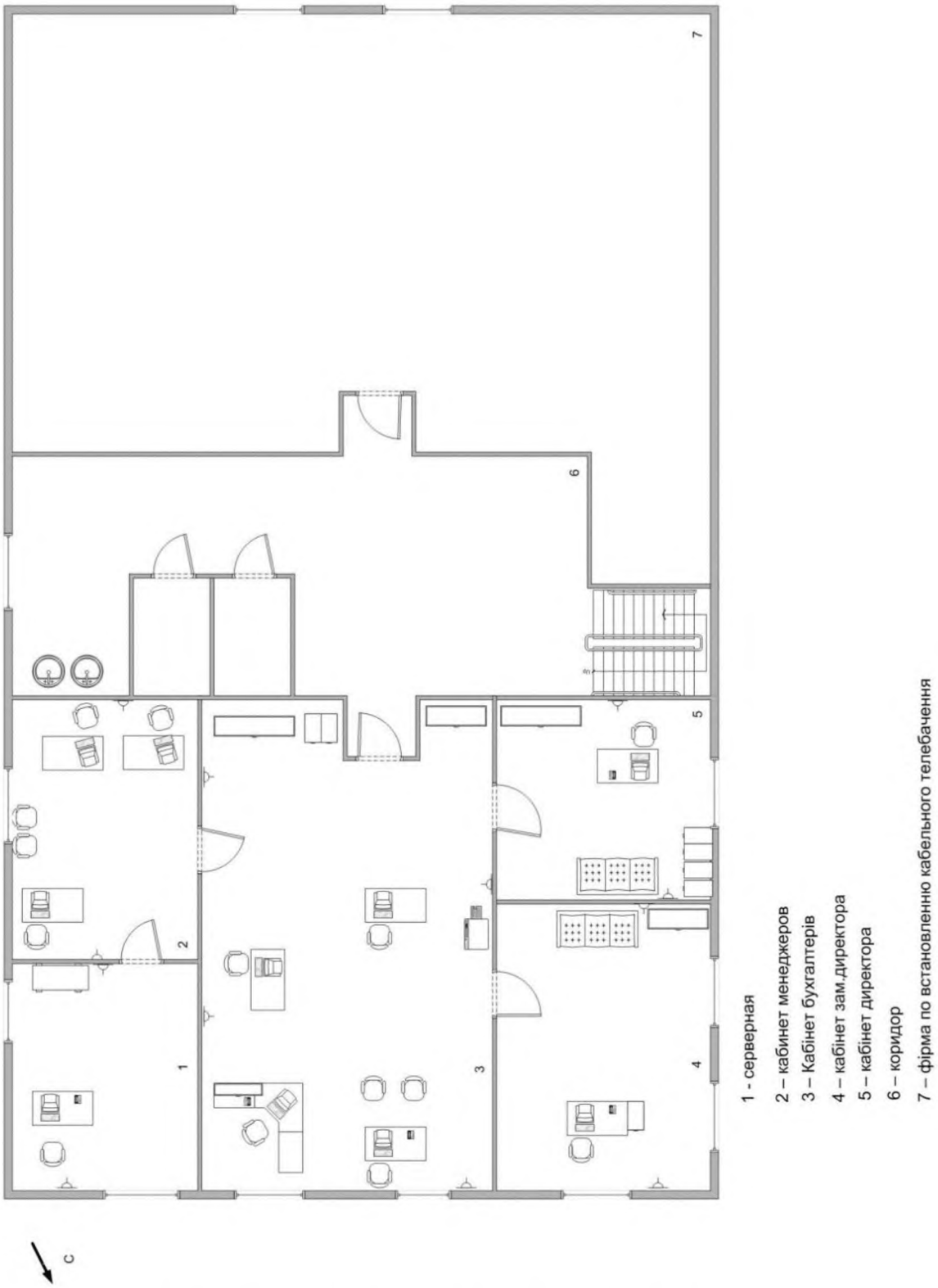

Рисунок 1 – План офісу ТОВ «Євро полюс»

ДОДАТОК Г. Перелік документів на оптичному носії

1 Титульна сторінка.pdf

2 Завдання.pdf

3 Реферат.pdf

4 Список умовних скорочень.pdf

5 Зміст.pdf

6 Вступ.pdf

7 Розділ 1.pdf

8 Розділ 2.pdf

9 Розділ 3.pdf

10 Висновки.pdf

11 Перелік посилань.pdf

12 Додаток А.pdf

13 Додаток Б.pdf

14 Додаток В.pdf

15 Додаток Г.pdf

16 Додаток Д.pdf

17 Додаток Е.pdf

Презентація.pptx

ДОДАТОК Д. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Е. ВІДГУК
на кваліфікаційну роботу бакалавра на тему:
Обґрунтування засобів захисту інформації комп'ютерної мережі
ТОВ «Євро полюс»
Стратія Гліба Івановича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на __ сторінках та містить __ рисунків, __ таблиць, __ джерел та __ додатків.

Мета роботи: за допомогою програмних, апаратних і організаційних заходів поліпшити захищеність інформації в комп'ютерній мережі ТОВ «Євро полюс» від несанкціонованого доступу.

У розділі Стан питання. Постановка задачі описані найпоширеніші загрози безпеки та основні положення захисту інформації від них.

У спеціальному розділі описана кратка характеристика об'єкту інформаційної діяльності ТОВ «Євро полюс», розроблені й описані методи підвищення захисту інформації від несанкціонованого доступу.

В економічному розділі наведені розрахунки й обґрунтовані всі заходи щодо вдосконалення системи захисту інформації в комп'ютерній мережі ТОВ "Евро полюс".

Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому робота задовольняє усім вимогам і може бути допущена до захисту, а його автор заслуговує на оцінку «_____».

Керівник