Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політех
ніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Масалова Ігора Сергійовича*

академічної групи *125—17—2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо—професійною програмою *Кібербезпека*

на тему *Розробка засобів захисту інформаційно—телекомунікаційної системи товариства з обмеженою відповідальністю «SpeedNet»*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.т.н. проф. Корнієнко В.І.			
розділів:				
спеціальний	ст. викл. Мєшков В.І.			
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 ***Масалову Ігору Сергійовичу*** **академічної групи** ***125—17—2***
(прізвище ім'я по—батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Розробка засобів захисту інформаційно—телекомунікаційної системи товариства з обмеженою відповідальністю «SpeedNet»***

затверджену наказом ректора НТУ «Дніпровська політехніка» від _07.06.2021_____№_317-С___

Розділ	Зміст	Термін виконання
Розділ 1	Обстеження ОІД, аналіз інформаційної системи підприємства, модель загроз, модель порушника	29.03.2021
Розділ 2	цінка існуючого стану захисту, проектні рішення, реалізація проектних рішень, аналіз загроз після впровадження комплексу заходів.	24.05.2021
Розділ 3	Розрахунок економічної доцільності впровадження комплексу заходів.	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: 73 с., 7 рис.,14табл., 4 додатка,14 джерел.

Об'єкт дослідження: система безпеки інформаційно-телекомунікаційної системи (ІТС)

Мета роботи: проаналізувати середовище функціонування інформаційно-телекомунікаційної системи, розробити акт, обстеження оцінити загрози, скласти модель порушника.

У спеціальній частині виконано : розроблені організаційні та програмні рекомендації щодо поліпшення системи захисту від витоку іноформації на підприємстві «SpeedNet», запропоновано стандартний профіль захищеності, проведена оцінка ризиків після впровадження запропонованих програмних та організаційних рішень.

В економічному розділі проведено розрахунок щодо доцільності впровадження запропонованих організаційних та програмних рішень.

Практичне значення роботи складається у тому, щоб поліпшити систему безпеки інформації підприємства «SpeedNet».

Результати роботи що здійснені у роботі можуть бути використані для поліпшеняня системи безпеки підприємства «SpeedNet».

ЗАГРОЗИ ВЛАСТИВОСТЕЙ ІНФОРМАЦІЇ, РІВНІ РІЗИКІВ ТА ЗБИТКІВ, КОНФЕДЕНЦІЙНІСТЬ ІНФОРМАЦІЇ.

РЕФЕРАТ

Пояснительная записка: 73 с., 7 рис., 14табл., 4 приложения, 14 источников.

Объект исследования:система безопасности информационно-телекоммуникационной системы (ИТС)

Цель работы: проанализировать среду функционирования информационно-телекоммуникационной системы, разработать акт, обследования оценить угрозы, составить модель нарушителя.

В специальной части выполнены: разработаны организационные и программные рекомендации по улучшению системы защиты от утечки иноформации на предприятии «SpeddNet», предложено стандартный профиль защищенности, проведена оценка рисков после внедрения предложенных програмных и организационных решений.

В экономическом разделе проведен расчет о целесообразности внедрения предложенных организационных и программных решений.

Практическое значение работы состоит в том, чтобы улучшить систему безопасности информации предприятия «SpeedNet».

Результаты работы осуществленные в работе могут быть использованы для улучшения системы безопасности предприятия «SpeedNet».

УГРОЗЫ СВОЙСТВ ИНФОРМАЦИИ, УРОВНИ РИЗИКОВ И УБЫТКОВ КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ.

ABSTRACT

The note is explained: 73 p., 7 figures, 14 tables, 4 supplements, 14 sources.

Object of study: security of information and telecommunication systems (ICS)

The goal of the work: analyze the middle of the function of the information—telecomunication system, develop the act, evaluate the contamination, and lay the porcelain model.

In the special part it is executed: the organization of the organization and the program recommendations for updating the system and the return of information to the "SpeddNet" enterprise, the standard profile of the abduction was carried out, the assessment was carried out

In the economic distribution, a survey was carried out for the provision of advanced organizational and program solutions.

It is practically important to have a robot in order to polish the SpeedNet safety information system of the enterprise.

The results of the work carried out in the work can be used for the polishing of the system and safety of the enterprise "SpeedNet".

THREAT TO AUTHORITIES INFORMATSIS, LEVELS OF RISKS AND LOSSES, CONFEDENTSIYNIST INFORMATSIS

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

БД – бази даних;

ІБ – інформаційна безпек

ІТС – інформаційна-телекомунікаційна система;

КЗ – контрольована зона;

КПП – контрольно пропускний пункт;

КСЗІ – комплексна система захисту інформації;

НД ТЗІ – нормативний документ технічного захисту інформації;

ОІД – об’єкт інформаційної діяльності;

ОТЗ – основні технічні засоби;

ПК – Персональний коп’ютер;

ТОВ – товариство з обмеженною відповідальністю;

ЗМІСТ

ВСТУП

Інформація в усі часи була неоцінимим ресурсом, для кожної компанії інформація є бізнес активом, котрий потрібно захищати. Розвиток інформаційних технологій та повсюдна цифровізація підприємств, відкриває простір для дій зловмисників. Тому дотримання вимог, які указані у внутрішніх документах підприємства, котрі регламентують доступ, розголошення та використання конфідеційної інформації є обов'язковим для кожного співробітники підприємства.

Не можливо уявити собі надійний захист інформації, котра циркулює на ОІД, без аналізу підприємства та його обладнання на потенціальні загрози та вразливості. Також без впровадження нових, більш досконалих, чи модернізації вже існуючих, засобів захисту, котрі забезпечують захист в АС. Для реалізації захисту інформації на підприємстві впроваджують КСЗІ.

КСЗІ— сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС.

Актульність даної кваліфікаційної роботи визначається наступними факторами :

—Глобальний процес інформатизації ;

—Зростання як технічних так і інформаційних загроз;

—Зростання ріння інформаційної злочинності.

Мета даної роботи: проаналізувати систему безпеки підприємства, обґрунтувати вибір профілю захисту інформації, яка циркулює на ТОВ «SpeeddNet» .

Для поліпшення інформаційної безпеки підприємства в роботі повинна бути розроблена політика безпеки ІТС, для цього потрібно :

—провести обстеження фізичного середовища підприємства;

—провести обстеження інформаціного середовища ;

—провести обстеження середовища користувачів;

—провести класифікацію джерел загроз та вразливостей;

—скласти модель загроз та порушника;

—Впровадити рішення по поліпшенню системи інформаційної безпеки підприємства та економічно обґрунтувати доцільність впроваджень.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1.Загальна інформація про компанію «SpeedNet».

Юридична назва: ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСЮ «SpeedNET». Компанія надає консультативні послуги у сфері надання послуг провайдингу.

Розглянемо організаційну структуру вищезазначеного підприємства, котра складається з:

—Директор

—Менеджера проекту

—IT відділ

—Бухгалтерія

—Керівник відділу дзвінків та чатів онлайн

—Супервізери

—Робітників колл центру та чатів—онлайн

—HR менеджери

—Тренери

Нижче розглянемо робочі обов'язки кожного з вище перелічених структур підприємства. Менеджер проекту — організаційні питання та умови договору з замовниками. Бухгалтерія — ведення бухгалтерського обліку,складання фінансової звітності, нарахування заробітньої плати. Керівник відділу – підготовка звітів по людино—годинах за місяць, контроль робочого процесу, обробка скарг та критичних ситуацій . Супервізери – слідкування в реальному часі за роботою агентів та допомога у вирішенні форс-мажорних ситуацій, при великій навантаженості також приймає дзвінки. Робітники колл центру– вирішення проблем та звернень клієнтів через телефонні дзвінки. Робітники чатів—онлайн— вирішення проблем та звернень клієнтів через переписку. Робітники IT—відділу – підтримка обладнання, роботи сайту та внутрішніх робочих додатків, веб додатків та

забезпечення безпеки інформації. HR—менеджери – підбір персоналу, внесення інформації про співробітників до БД. Тренер – навчання нових робітників колл центру.

Протягом робочого дня в офісі знаходяться наступні працівники :

— Керівник відділу (10:00-18:00);

— Супервізер (10:00-18:00);

— Робітники колл центру 15 чол.(10:00-18:00);

— Робітники чатів—онлайн 5 чол.(10:00-18:00);

— Робітники бухгалтерії 3 чол.(10:00-18:00

— Робітники IT відділу 9 чол.(10:00-18:00);

Також на території офісу знаходиться прибиральниця з 9:00 до 10:00 від офісного центру в якому працює компанія.

1.2. Обґрунтування потреби створення КСЗІ.

На підприємстві ТОВ «SpeedNET» циркулює інформація наступного типу : відкрита (інформація що до тарифів компанію, загальна інформація про компанію і т.д.), інформація з обмеженим доступом (персональні дані користувачів, та компанії).

Закон України «Про захист інформації» свідчить про те що, інформація з обмеженим доступом та інформація, що містить персональні дані громадян підлягає обов'язковому захисту. Тобто підставою для створення КСЗІ на підприємстві ТОВ «SpeedNET» є норми та вимоги чинного законодавства, які встановлюють обов'язковість обмеження доступу до певних видів інформації або забезпечення її цілісності чи доступності, або прийняте власником інформації рішення щодо цього, якщо нормативно-правові акти надають йому право діяти на власний розсуд.

У НД ТЗІ 3.7-003 -2005 сказано, що необхідність створення КСЗІ у загальному випадку одержується за наступними результатами:

— аналізу нормативно-правових актів (державних, відомчих та таких, що діють в межах установи, організації, підприємства), на підставі яких може встановлюватися обмеження доступу до певних видів інформації чи заборона такого обмеження, або визначатися необхідність забезпечення захисту інформації згідно з іншими критеріями;

— визначення наявності у складі інформації, яка підлягає автоматизованій обробці, таких її видів, що потребують обмеження доступу до неї або забезпечення цілісності чи доступності відповідно до вимог нормативноправових актів;

— оцінки можливих переваг (фінансово-економічних, соціальних і т.п.) експлуатації ІТС у разі створення КСЗІ.

1.3. Обстеження ОІД.

1.3.1. Ситуаційний план ОІД.

Об’єкт знаходиться за адресою узвіз. Крутогірний 1, м. Дніпро, Дніпропетровська обл., 49000; в семиповерховій офісного центру на третьому поверсі.

Контрольована зона (КЗ) обмежується лиши стінами, підлогою та стелею офісного приміщення. Додаткові міри охорони обеспечує охорона офісного центру, паркан з пропускними пунктами, камерами відеоспостереження та системою сигналізації яка підключена до КПП, доступ на територію комплексу забеспеується по магнітоконтактним карткам . Також чергові КПП мають тривожну кнопку, для виклику поліції. Уся територія будівлі офісу охороняється засобами охоронної сигналізації, яка встановлена на всіх дверях та вікнах. Усі дані з детекторів охоронної сигналізації в автоматичному режимі відправляються на пульт охорони, який знаходиться на КПП.

Схема заземлення зображена на Ситуаційному план (Рис 1). Заземлення використовується захисне. Блискавкозахист призначена для відводу розряду блискавки від об'єкта. Розряд блискавки, що йде по шляху найменшого опору потрапляє в металевий блискавкоприймач над об'єктом, потім по металевим громовідводам, розташованим зовні об'єкта, спускається до грунту, де і розходиться в ньому. Також присутній захист від імпульсної перенапруги за допомогою газового розрядника. Один з електродів цього розрядника заземлюється, а інший підключається до проводів лінії . Та коли накомичений розряд досягає установленого максимума, накопичений заряда скидається в грунт.

Інформація про навколишні будинки та споруди приведена у Таблиці №1.2.

Таблиця №1.2.— Характеристика будівель та споруд.

№	Найменування	К—ть поверхів	Адреса	Відстань до ОІД
1	Бібліотека житловий	2	Вул. Сергія Єфремова 9	30м
2	Будинок житловий	3	Вул. Сергія Єфремова 7	15м
3	Будинок житловий	1	Вул. Сергія Єфремова 5	20м
4	Гуртожиток	5	Вул. Володимира Вернадського 8А	20м
5	Будинок житловий	3	Узвіз. Крутогірний 3	15м
6	Адміністративна будівля	2	Узвіз. Крутогірний 1	30м

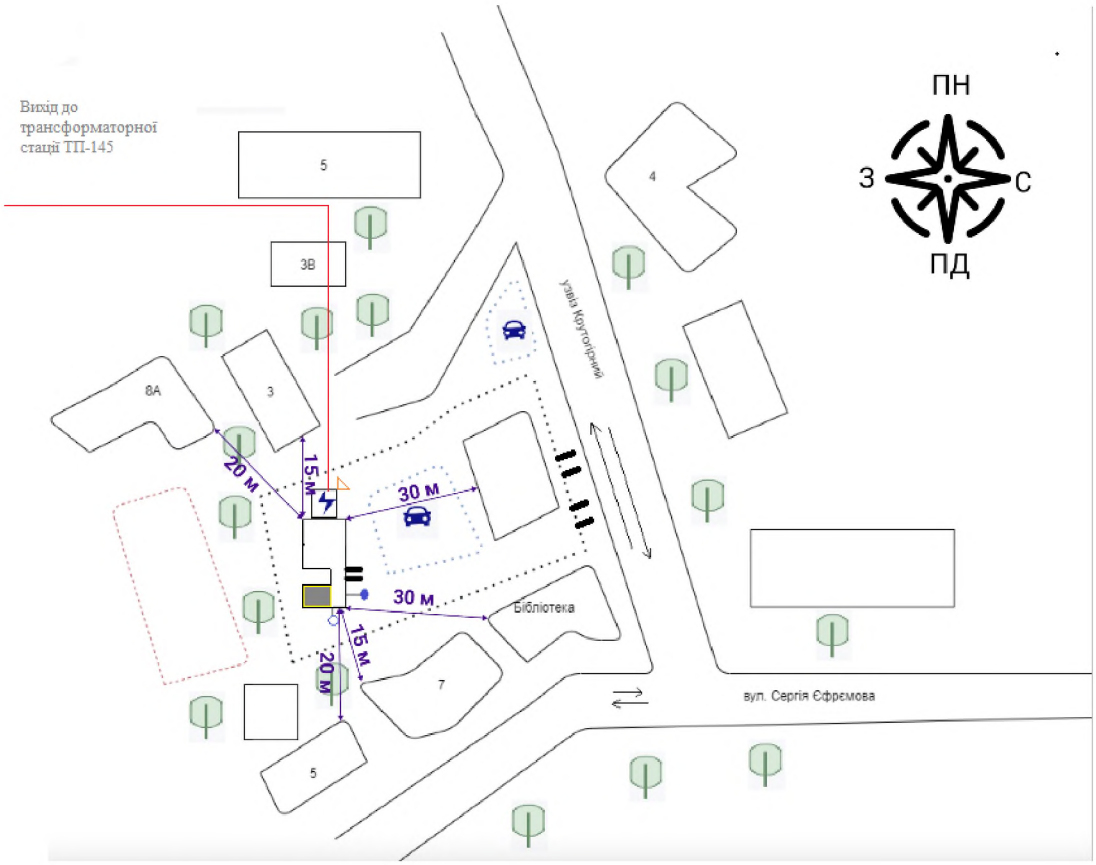


Рис 1.1— Ситуаційний план

Таблиця 1.1 — Умовні позначення.

	Зелені засадження
	Напрям руху
	Паркан
	Розподільний щит
	Стадіон

Продовження таблиці 1.1

	Будівля
	Місця паркування
	Межа кз
	Люк та лінія систем каналізації
	Люк талінія систам водопостачання
	Вихід до трансформаторної підстанції ТП—145
	Заземлення
	Область ОІД
	Вхід

1.3.2. Генеральний план.

Стіни зроблені з газо-бетонних блоків (500х200х610 мм). Фундамент стовпчастий, дах — покритий руберойдом, територія навколо будівлі покрита асфальтом, будівля має пластикові вікна. Зовнішні стіни офісу — газо-бетонні. Товщина зовнішніх стін — 500 мм. Внутрішні несучі стіни газо-бетонні, товщина — 200 мм. Перегородки зведені за допомогою металоконструкцій та гіпсокартону, загальною товщиною — 85 мм. Вхідні двері металеві 2,5м та шириною 2 м. Вхідні двері до ОІД металеві — висотою 2 м та шириною 1,5 м та оснащені мережевою системою обліку часу, вікна будівлі пластикові. Підлога – плитка(на кухні та туалеті), паркет .

Комунікації що підведені до офісного центру:

—Системи каналізації та водопостачання підключені до міської системи каналізації.

—Система електропостачання забезпечується за допомогою трансформаторнопідстанції, яка знаходиться за межами КЗ та обслуговує інших користувачів

—Інтернет проведено за допомогою оптоволоконного кабелю від провайдеру Фрегат.

—Система опалення автономна та забезпечується за допомогою електричних приладів.

Інофромація про системи комунікацій та життєзабезпечення наведена у таблиці 1.4.

Схема генерального плану ОІД, схеми підведених комунікацій до ОІД зображено на Рис 1.2.—1.4.

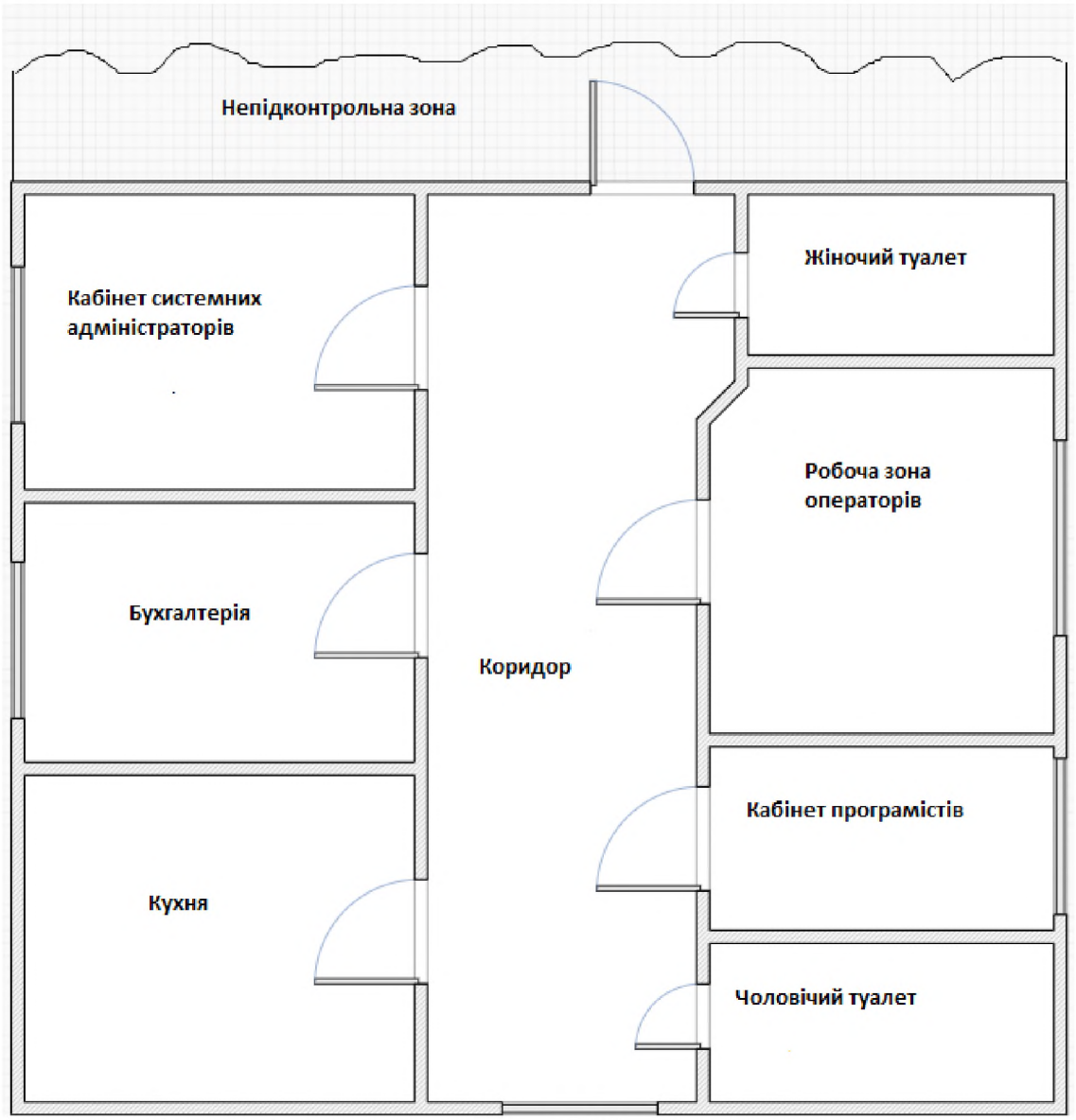


Рис 1.2.—Схема генерального плану ОІД

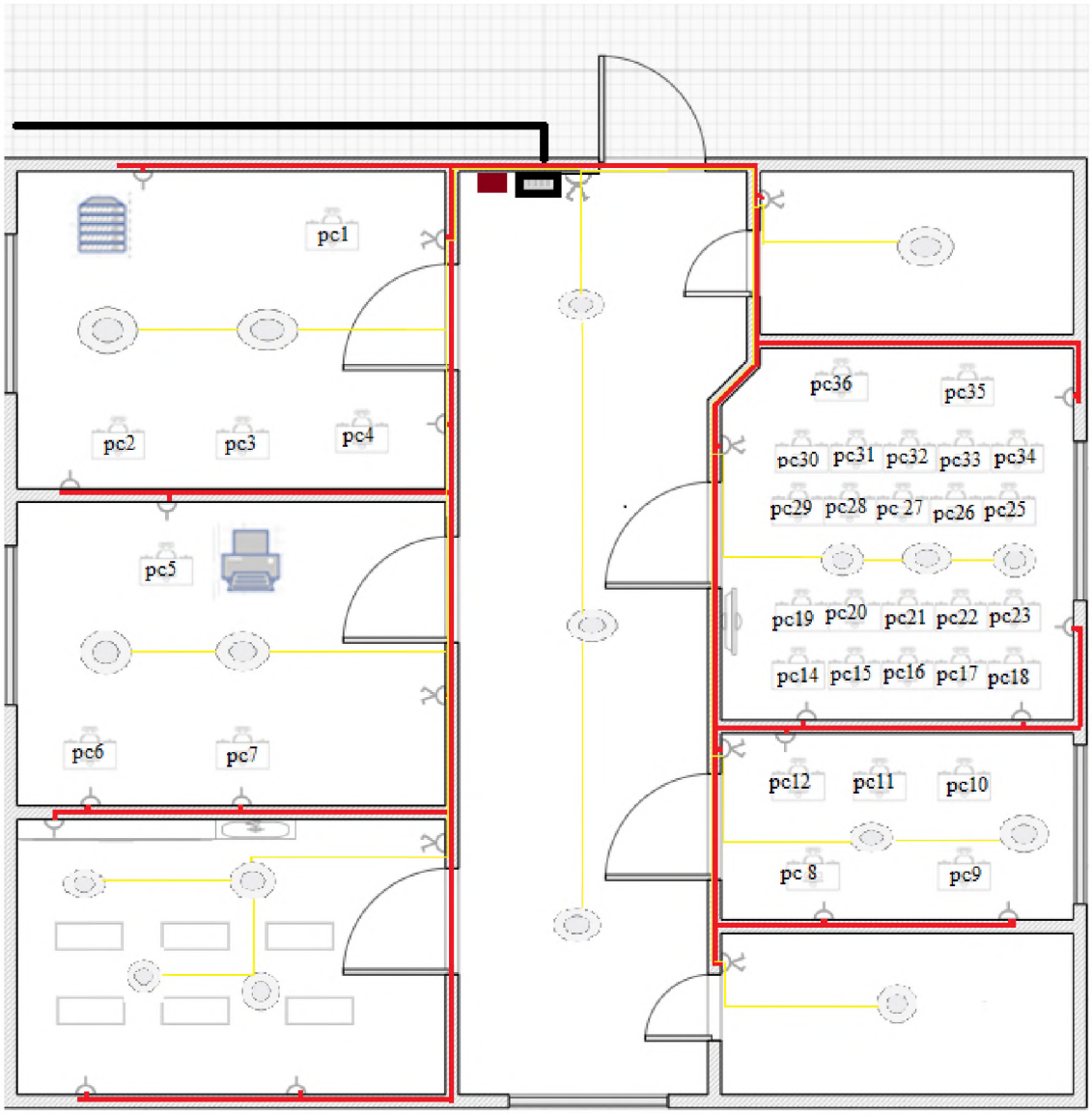


Рис 1.3— Система електропостачання та постачання світл

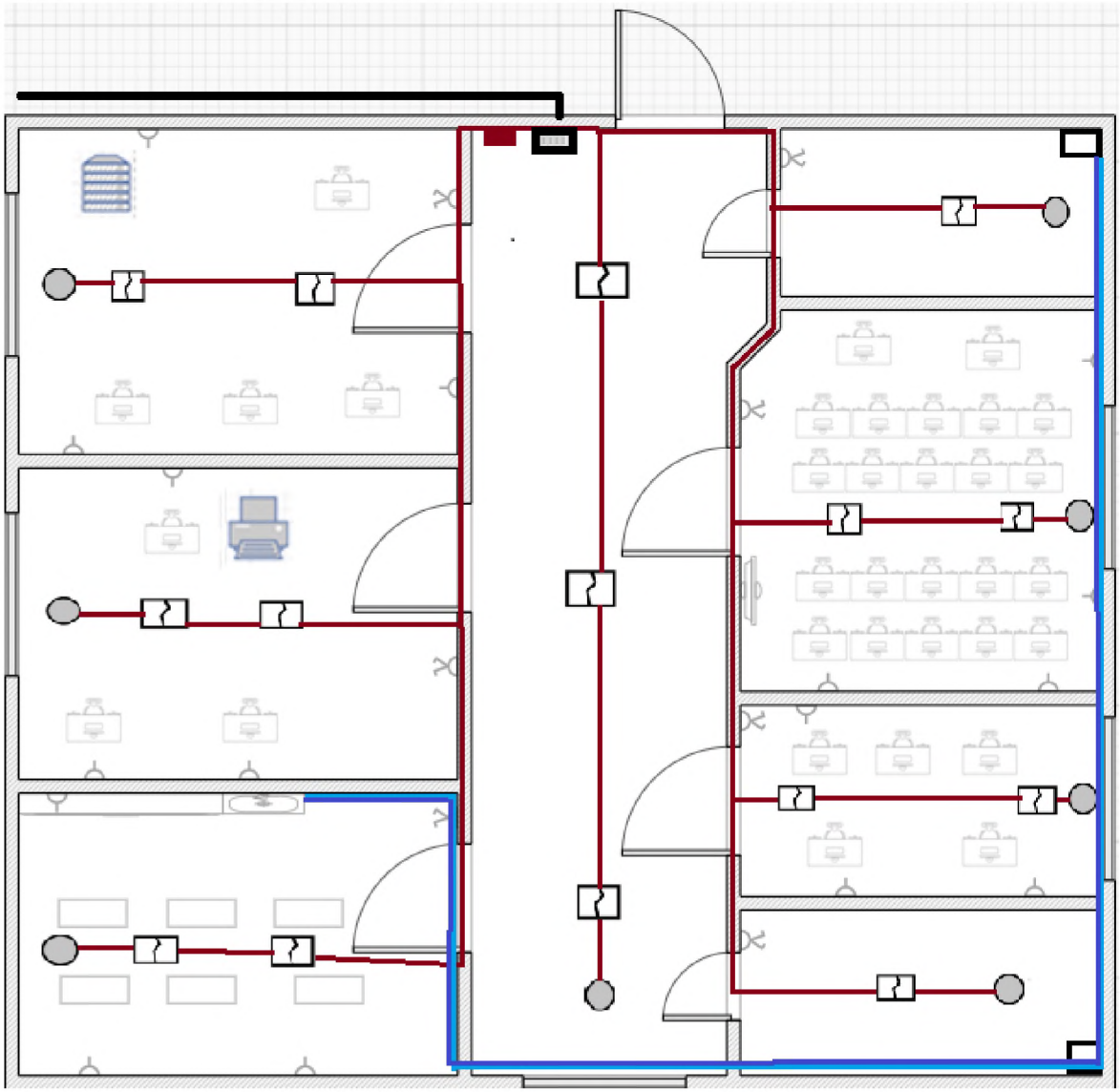
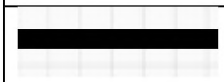


Рис 1.4— Системи каналізації, водопостачання та поженої сигналізації

Таблиця 1.3 – Умовні позначення .

	лінія електропостачання
	лінія каналізаційного відводу
	лінія водопостачання
	лінія пожежної сигналізації
	лінія світлопостачання
	шафа кухонна
	датчик пожежної безпеки
	лампа
	телевізор
	щитова
	раковина
	стіл

Продовження таблиці 1.2 —Умовні позначення

	розетка
	сервер
	пульт керування пожежної сигналізації
	вихід до розподільного щита
	робоче місце
	кінцевий елемент
	двухклавишний вимикач

Таблиця 1.4 —Системи комунікацій та життєзабезпечення.

Система комунікацій	Спосіб підключення
Системи каналізації та водопостачання	Підключено до міських комунікаціям
Електроживлення	Підключено до трансформатору який знаходиться за межами КЗ
Система опалення	Система опалення автономна та запезпечується завдяки еклектроних приладів

Продовженя таблиці 1.4

Система комунікацій	Спосіб підключення
Заземлення	Всі прилади на території КЗ зазелені на спільний контур котрий є замкненим і виходить за межі КЗ
Кабелі комп'ютерної мережі	Підключення іде за межами КЗ

ІТС ОІД являється мережа типу «пасивна зірка», побудована дана мереже з використанням одного маршрутизатору та чотирьох комутаторів. Мережа являється багатомашинним та багатокористувацьким комплексом об'єднаним в спільну мережу та має вихід до мережі Інтеренет також обробляє як інформацію з відкритим доступом, так інформацію з обмеженим доступом. Тобто дана ІТС відноситься до третього класу.

Обчислювальна система представлена у складі :

—Мережеве обладнання :

— Коммутатори (MikroTik CRS326-24G-2S на 24 порти, три UNV NSW2010-10T-POE-IN на 8 портів.);

— Маршрутизатор (Cisco RV340W Wireless-AC Dual WAN Gigabit VPN Router);

— Тридцять шість ПК з ОС Microsoft Windows 10 Pro;

— Прикладне та спеціалізоване програмне забезпечення (інформація про ПЗ ОІД наведено у таблиці 1.6.).

Загальна структура обчислювальної системи зображена на Рис.1.4.

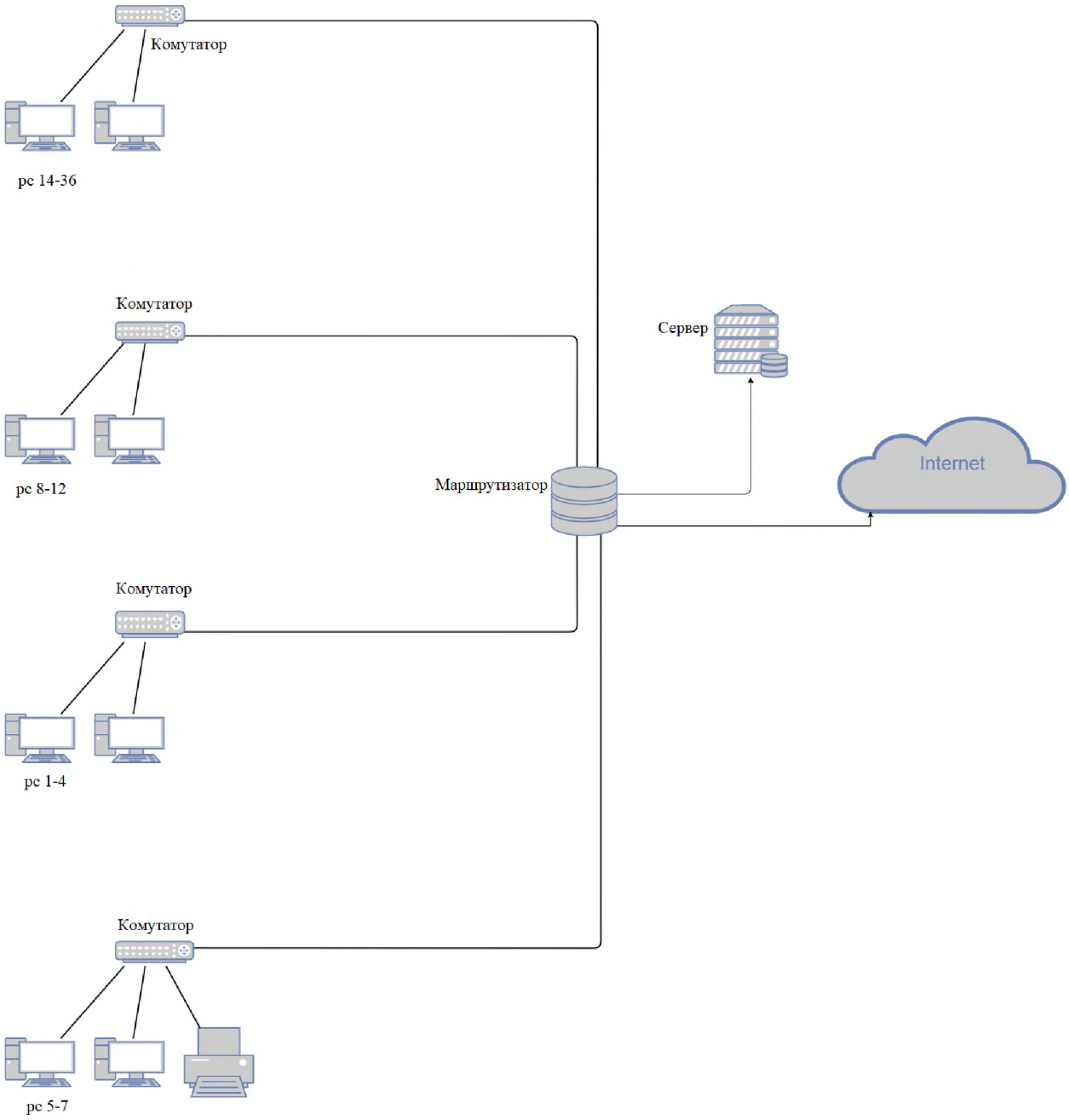


Рис. 1.5 — загальна структура ІТС

Інформація про ОТЗ підприємства та ДТЗ наведено у таблиці 1.5. та 1.7.

Таблиця 1.5. – Основні технічні засоби підприємства.

Тип	Серійний та інвентаризаційний номер	Розташування	Відстань до ДТЗС	Кількість шт.
Ноутбук	HP 15s—eq1024ua 5523486101 203— 239	Робочий стіл	2 м	36
Комп'ютерна миша	Logitech B100 5523486101 239—275	Робочий стіл	2 м	36
Принтер	5523486101276	Робочий стіл	2 м	1
Гарнітура	Sven AP—010MV 5523486101277—312	Робочий стіл	2 м	36

Характеристики персональних комп'ютерів :

—Ім'я в системі — CC 1-36
—Процесор— AMD Athlon Silver 3050U
—RAM— 8Гб DDR4 - 2400 МГц
—SSD 256 ГБ PCIe NVMe M.2, 256 Гбайт

Таблиця 1.6. – Програмне забезпечення на ПК.

Тип	Найменування	Описання	Ліцензія	Термін дії	ПК на котрих встановлено
Системне	Microsoft Windows 10 Pro	Операційна систем(Білд 1809)	Проприєтарна	—	ПК 1-36

Продовження таблиця 1.6. — Програмне забезпечення на ПК.

Тип	Найменування	Описання	Ліцензія	Термін дії	ПК на котрих встановлено
Прикладне	Google Chrome	Веб— браузер	GNU GPL, GNU LGPL	—	ПК 1-36
Прикладне	Libre Office	Пакет офісних програм	GPL	—	ПК 1-36
Прикладе	VirusScan Enterprise for Storage	Антивірус	Щорічна підписка	1 рік	ПК 1-36
Прикладне	Sender	Менсенджер	Щорічна підписка	1 рік	ПК 14-36
Спеціалізоване	Eyebeam 1.5	Клієнтське ПЗ для можливості робити дзвінки	Пропріє— тарна	—	ПК 14-36
Спеціалізоване	MS Visual Studio	Середовище розробника	Щорічна підписка	1 рік	ПК 8-12

Таблиця 1.7. – Допоміжні технічні засоби.

Тип	Розташування	Кількість
Датчик диму (Артон СПД-3.4)	Стеля	15 шт
Светильник світодіодний (LED-36R/20W NW led)	Стеля	18 шт
Мережевий комплекс обліку часу (CoVi Security Access-4)	Вхідні двері	1шт
Кондиціонер (KENTATSU KSVR70HFAN1)	Стеля	6 шт

1.4 Аналіз загрози інформації, що циркулює на ОІД.

1.4.1Інформація на підприємстві ТОВ «SpeedNET» зберігається як на цифрових так і на паперових носіях.

Детальна інформація про місце зберігання, види інформації на підприємстві та рівні конфіденційності інформації що циркулює на ОІД вказані в таблиці 1.8. та 1.9.

Таблиця 1.9. — Інформація циркулююча на ОІД.

Інформація	Режим доступу	Правовий режим	Працівники, що мають доступ	Місце зберігання
Інформація про компанію та тарифні плани, акції.	Відсутній	Відкрита	Всі працівники	Сайт компанії

Продовження таблиці 1.8.— Інформація циркулююча на ОІД.

Інформація	Режим доступу	Правовий режим	Працівники, що мають доступ	Місце зберігання
Особиста інформація клієнтів	З обмеженим доступом	Конфіденційна інформація	Системні адміністратори, працівники кол центру та чатів онлайн, супервізери, керівник відділу дзвінків та чатів онлайн	Сервер
Інформація про працівників	З обмеженим доступом	Конфіденційна інформація	Директор, менеджер проекту, бухгалтерія, керівник відділу дзвінків та чатів онлайн, системний адміністратор	Сервер
Бухгалтерська звітність	З обмеженим доступом	Конфіденційна інформація	Директор, менеджер проекту, головний бухгалтер, системний адміністратор	Паперові носії, компьютер директора, компьютер говного бухгалтера
Записи дзвінків	З обмеженим доступом	Конфіденційна інформація	Системний адміністратор, керівник відділу дзвінків та чатів онлайн, супервізер.	Сервер

Продовження таблиці 1.8. — Інформація циркулююча на ОІД.

Інформація	Режим доступу	Правовий режим	Працівники, що мають доступ	Місце зберігання
Внутрішня документація компанії	З обмеженим доступом	Конфіденційна інформація	Менеджер проекту, бухгалтери, системний адміністратор, керівник відділу дзвінків та чатів онлайн, програміст	Сервер

Використаємо наступні рівні властивостей інформації щоб класифікувати інформацію :

–К1 – рівень конфіденційності інформації, при розкриті інформації на цьому рівні, компанія не зазнає матеріальних збитків;

–К2 – при розкриті інформації на цьому рівні конфіденційності якому компанія зазнає незначних матеріальних збитків;

–К3 –при розкриті інформації на цьому рівні конфіденційності компанія зазнає відчутних матеріальних збитків;

–К4 – рівень конфіденційності інформації, при розкриті інформації на цьому рівні конфіденційності компанія зазнає значних матеріальних збитків;

–К5 –при розкриті інформації на цьому рівні конфіденційності якому компанія зазнає критичних збитків, котрі приведуть до її банкрутсва.

–Ц1–при втраті цілісності на даному рівні, компанія не зазнає матеріальних збитків.

–Ц2 – при втраті цілісності на даному рівні, компанія зазнає не значних матеріальних збитків;

–Ц3 – при втраті цілісності на даному рівні, компанія зазнає відчутних матеріальних збитків;

–Ц4 – при втраті цілісності на даному рівні, компанія зазнає значних матеріальних збитків;

–Ц5 – при втраті цілісності на даному рівні, компанія зазнає краху.

–Д1 при втраті доступності на даному рівні, компанія не зазнає матеріальних збитків ;

–Д2 – при втраті доступності на даному рівні, компанія зазнає не значних матеріальних збитків;

–Д3 – при втраті доступності на даному рівні, компанія зазнає відчутних матеріальних збитків ;

–Д4 – при втраті доступності на даному рівні, компанія зазнає значних матеріальних збитків;

–Д5 –у разі втрати доступності інформації на даному рівні компанія зазнає краху.

Таблиця 1.9. — Класифікація інформації ОІД за порушення її властивостей.

Інформація	Рівень конфіденційності	Рівень цілісності	Рівень доступності
Інформація про компанію та тарифні плани, акції.	К1	Ц2	Д2
Особиста інформація клієнтів	К4	Ц3	Д4
Інформація про працівників	К3	Ц2	Д2
Бухгалтерська звітність	К4	Ц5	Д4
Записи дзвінків	К4	Ц2	Д3
Внутрішня документація компанії	К2	Ц3	Д3

Інформація що до можливостей взаємодії з інформацією користувачів системи наведено у таблиці 1.10. де :

R – читання;

W – запис;

M – модифікація;

D – видалення;

Таблиця 1.10. – Розмежування доступу до інформації, користувачів системи.

Інформація	Інформація про компанію та тарифні плани, акції.	Особиста інформація клієнтів	Інформація про працівників	Бухгалтерська звітність	Записи дзвінків	Внутрішня документація компанії
Користувачі						
Менеджер проекту	R	—	R	R	—	R,W, M, D
Системний адмін.	R, D	R, M,D	R, D	R, D	R, D	R, W,M,D
Робітник КЦ та чатів	R	R, W, M	—	—	—	R
Супервізер	R	R, W, M,D	—	—	R	R
Бухгалтер	R	—	R	R, W, M,D	—	—
Програміст	R, W, M, D.	—	—	—	—	R,W,M,D
Керівник відділу	R	R,D	R	—	R	R
HR— менеджери	R	—	R, W,M,D	—	—	R

1.4.2. Побудова моделі порушника.

Для надійного захисту інформації компанії потрібно не тільки оцінити усі можливі загрози, але й побудувати модель порушника. З гідно з НД ТЗІ

1.1-003-99 модель порушника — абстрактний формалізований або неформалізований опис порушника. Для розробки моделі порушника були використані данні надані службою безпеки, статистичні данні, а також данні отримані від аналітичних груп про можливі способи перехвату та сбору інформації на різних етапах її передачі. Модель порушника може корегуватись від появи нових даних про порушення які вже трапились чи ті котрих вдалося уникнути.

При розробці моделі порушника бралися до уваги наступні критерії :

—Категорії осіб, до яких може належати порушник;

—Мотиви та цілі, для дій порушника ;

—Рівень обізнаності про ІТС компанії

—Можливості подолати систему захисту компанії;

—Можливості за часом дії;

—Можливості за місцем дії;

Для оцінки порушника за вище названими критеріями використовується наступна система оцінювання :

—М1 — безвідповідальність (рівень загрози 1);

—М2 — самоствердження (рівень загрози 2);

—М3 — корисливий інтерес (рівень загрози 3);

—К1 — низький рівень знань ІТС компанії, але вміє працювати з технічними засобами ІТС (рівень загрози 1);

—К2 — середній рівень знань ІТС компанії та має практичні навички роботи з технічними засобами ІТС та їх обслуговування (рівень загрози 2);

—К3 – знає структуру, функції й механізми дії засобів захисту інформації в ІТС, їх недоліки та можливості(рівень загрози 3);

—З1 — може лише підслуховувати розмови у приміщеннях та підглядати у документи на робочих місцях(рівень загрози 1);

—З2 — використовує лише штатні засоби та недоліки системи захисту для її подолання, а також компактні машинні носії інформації(рівень загрози 2);

—З3 — використовує технічні, або програмні засоби активного впливу, з метою модифікації інформації та компонентів ІТС, дезорганізації систем обробки інформації(рівень загрози 3);

—Ч1 — під час повної бездіяльності ІТС з метою відновлення та ремонту(рівень загрози 1);

—Ч2 — під час призупинки компонентів ІТС з метою технічного обслуговування та модернізації(рівень загрози 2);

—Ч3 — під час функціонування ІТС (або компонентів системи) (рівень загрози 3);

—Ч4 — як у процесі функціонування ІТС, так і під час призупинки компонентів системи(рівень загрози 4);

—Д1 — усередині приміщень, але без доступу до технічних засобів ІТС(рівень загрози 1);

—Д2 — з робочих місць користувачів ІТС(рівень загрози 2);

—Д3 – дистанційно(рівень загрози 3);

—Д4 — з доступом у зону керування засобами забезпечення безпеки ІТС(рівень загрози 4);

Таблиця 1.11. – Модель порушника.

Посада	Мотив порушень	Рівень обізнаності про ІТС компанії	Можливості за часом дії	Можливості за місцем дії	Можливості щодо подолання системи захисту компанії	Сума загроз
Менеджер проекту	М1	К3	Ч3	Д2	З2	11
Робітники ІТ	М3	К3	Ч4	Д4	З2	16
Робітник КЦ та чатів	М3	К2	Ч3	Д2	З2	12
Супервізер	М2	К2	Ч3	Д2	З2	11
Бухгалтер	М1	К1	Ч3	Д2	З2	9
Керівник відділу	М2	К3	Ч3	Д2	З2	12
HR—менеджери	М1	К1	Ч3	Д2	З2	9
Охорона комплексу	М2	К1	Ч1	Д3	З2	9
Прибиральниця	М1	К1	Ч3	Д1	З1	7
Хакери	М3	К2	Ч4	Д3	З3	15

Беручи до уваги дані з таблиці 1.11. можливо зробити висновки, що найбільший рівень загрози становлять робітники ІТ, а саме системний адміністратор, через те що має майбільші можливості доступу до інформації яка циркулює на ОІД. Також небезпеку можуть складати робітники чатів, кол—центру та супервізери, які мають доступ до особистих даних клієнтів. Також об’єкт представляє інтерес для хакерів то що, має персональні данні користувачів підприємства.

1.4.3. Виявлення актуальних загроз

Спираючись на НД ТЗІ 1.1-003-99 загроза – це будь—які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків АС. Перелік загроз та наслідки для ІТС після їх реалізації наведено у таблиці 1.12.

Таблиця 1.12 – загрози з впливом порушень на ІТС компанії.

№	Загрози	Властивості		
		К	Ц	Д
1	Загрози природні			
1.1	Стихійні лиха та аварії(пожежа, повінь і т.д.)	—	—	+
1.2	Втрата електроживлення	—	+	+
1.4	Втрата / пошкодження комунікаційних каналів	—	—	+
2	Загрози штучні			
2.1	Перенавантаження системи	—	—	+
2.2	Пошкодження проводу чи проблеми з доступом до мережі Інтернет	—	—	+
2.3	Помилки при експлуатації технічних засобів	—	+	+
2.4	Безвідповідальне зберігання документів, носіїв інформацції	+	2.4	Безвідповідальне зберігання документів, носіїв інформацції
2.5	Розголошення інформації про ІТС персоналом	+	—	—
2.6	Хакерські атаки	+	+	+
2.7	Втарата або розголошення інформації з носіїв інформації	+	+	+

Таблиця 1.13 – Визначення рівня збитків та загроз.

№	Механізм реалізації	Рівень		Сумма загроз
		Ризики	Збитки	
1	Загрози конфіденційності			
1.1	Збір інформації про клієнтів	3	3	6
1.2	Копіювання ІОД на зовнішні носії з метою несанкціонованого ознайомлення сторонніх осіб	2	3	5
1.3	Перегляд інформації на екранах моніторів, робочих місцях; підслуховування	2	1	3
2	Загрози цілосності			
2.1	Використання продуктів компанії в своїх цілях	3	1	4
2.2	Модифікація інформації персоналом ІТС на носіях інформації	2	2	4
2.3	Помилки користувачів ІТС, які призвели до модифікації або спотворення інформації на жорсткому диску або зовнішніх носія	2	2	4
3	Загрози доступності			
3.1	Помилки користувачів ІТС, які призвели до знищення інформаціїабо втрати доступу до неї	2	3	5
3.2	Втрата інтернет з’єднання	2	2	4
3.3	Втрата електропостачання	1	2	3

Для оцінювання ризиків була використана наступна система де :

—1 бал – реалізація загрози, призведе до незначних збитків;

—2 бали – реалізація загрози, призведе до середнього рівня збитків;

—3 бали – реалізація загрози, призведе до високого рівня збитків;

Модель загроз за сумою балів :

—Загрози конфіденційності – 14 ;

—Загрози доступності – 12;

—Загрози цілосності – 11;

Найбільшу небезпеку представляє загроза конфіденційності . Через те що на робочих місцях ніяк не обмежений доступ до інтернету та відсутній автоматизований контроль запитів користувачів системи.

В першому розділі кваліфікаційної роботи був зроблений детальний аналіз підприємства ТОВ «SpeedNET», в ході якого було зроблено :

—Детальний аналіз споруди та розроблений ситуаційний план, генеральний плани.

—Проаналізоване програмне та технічне забезпечення;

—Класифікація інформації, яка циркулює на ОІД;

—Аналіз вразливостей та загроз ;

—Розроблена модель порушника.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Оцінка стану захисту підприємства.

Згідно з таблицею 1.13. можливо зробити висновки, що найбільші ризики складають наступні загрози :

—Збір інформації про клієнтів;

—Копіювання ІОД на зовнішні носії з метою несанкціонованого ознайомлення сторонніх осіб;

—Модифікація чи спотворення інформації на носіях компанії;

—Збір інформації про клієнтів компанії може відбуватися завдяки, тому що робітники кол—центру мають безконтрольний доступ до облікових записів клієнтів, де зберігається їх особиста інформація.

Для входу працівників у програмні комплекси використовується логін та пароль, який у кожного працівника свій. Політика паролів представляє собою:

—Мінімальна довжина паролю – 6 символів;

—Пароль може використовувати лише латинську абетку, цифри та спец символи;

—Пароль обов’язково має складатись з мінімум одного символу верхнього регістру, включати в себе цифри, та може включати в себе спец символи (@, #, _,!,% тощо);

—Пароль не має складати асоціації та включати в себе інформацію про користувача;

—Пароль не може складатись з послідовного використання букв, цифр та спец символів (garw1234$!@);

—При зміні, відновлені паролю, новий пароль має відрізнятися від попереднього.

На підприємстві відсутні джерела безперебійного живлення.

На підприємстві ТОВ «SpeedNet» використовується антивірусний захист компанії McAfee версія VirusScan Enterprise for Storage, який сканує всі ПК в автоматичному режимі та який може відслідковувати приховані шпигунські програми, має можливість забезпечити безпеку великої кількості пристроїв та операційних систем, захищає від вірусів, коду що може задати шкоди системі, а також від скритих загроз в стиснутих файлах. Має централізована систему управління системою безпеки, та формування звітів завдяки консолі.

Для входу на територію об’єкту використовується мережевий комплекс обліку часу CoVi Security Access—4. Кожному працівнику видається карта доступа EM—Marine у якої є особистий номер, для ідентифікації користувача у системі, при тимчасовому виході з ладу сервера обліку робочого часу, або обриві лінії зв'язку, контролер зберігає в пам'яті до 47000 останніх подій, які, надалі, передає на сервер. Зв'язок з комп'ютером здійснюється через мережу Ethernet. Зчитувач зчитує дані з ідентифікатора і передає їх контролеру. Функціонує тільки при підключенні до контролера. Придатний для роботи при негативних температурах. Має світлозвукову індикацію. Безпосередньо вхід до кабінетів, на територію ОІД, обмежується механічними замками.

Підприємство використовує стандартні профілі захищеності КС, які входять до третього класу АС, головною вимогою якого є забезпечення конфіденційності, цілісності та доступності оброблюваної інформації. А саме : 3.КЦД.1 = { КД-2, КО-1,КВ-1, ЦД-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }.

Згідно з НД ТЗІ 2.-500-599 та НД ТЗІ 2.-500-499:

КД-2 – це базова довірча конфіденційність, ця послуга застосовується для розмежування доступу користувачів до захищених об'єктів і дозволяє користувачу керувати потоками інформації в АС від захищених об'єктів, що належать його домену, до інших користувачів. Політика довірчої

конфіденційності, що реалізується КЗЗ, стосується слабо та сильно зв'язаних об’єктів, які створюються користувачем у процесі виконання ним функціональних обов’язків. Користувач, який створив об’єкт, має право визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від цього об'єкта.

КО-1 – це повторне використання об'єктів, дана послуга дозволяє забезпечити коректність повторного використання розділюваних об’єктів, якщо розділюваний об'єкт виділяється новому користувачу або процесу, він не містить інформації, яка залишилась від використання його попереднім користувачем або процесом. Дана політика стосується тільки об’єктів АС, котрі містять службову інформацію і ресурси які поділяються між користувачами АС та прикладними процесами які виконуються в АС.

КВ-1 – мінімальна конфіденційність при обміні забезпечує захист від несанкціонованого ознайомлення за рахунок пасивного спостереження за лініями зв'язку або розкрадання носіїв інформації. Прикладом реалізації може служити програмне шифрування файлів перед їх передачею каналами зв'язку або прозоре шифрування файлів перед їх записуванням на диск. Послуга конфіденційність при обміні дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що в них міститься, під час їх експорту/імпорту через незахищене середовище. Найчастіше дана послуга реалізується з використанням криптографічних перетворень. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування. Під повнотою захисту в даному випадку розуміють множину типів загроз, від яких забезпечується захист. Під ступенем захищеності об'єктів, що експортуються, як правило, розуміють криптостійкість використовуваних алгоритмів шифрування.

ЦД-1 – мінімальна довірча цілісність послуга застосовується для захисту оброблюваної інформації від несанкціонованої модифікації і дозволяє користувачу будь—якої категорії керувати потоками інформації в АС від інших користувачів до захищених об'єктів, що належать його домену.

Політика довірчої цілісності, що реалізується КЗЗ, поширюється на слабо— та сильнозв'язані об'єкти, які створюються користувачем у процесі виконання ним функціональних обов'язків. Користувач, який створив об'єкт, має право визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати цей об'єкт. КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта. Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта. Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації .

ЦО-1 – це відкат, послуга надає можливість відмінити останню операції чи їх послідовність та повернути захищений об'єкт, з яким проводив маніпуляції користувач, до попереднього заздалегідь визначеного стану. Політика обмеженого відкату поширюється на: користувачів усіх категорій; сильно— та слабозв'язані об'єкти, які містять службову інформацію і в процесі обробки яких передбачається можливість їхньої модифікації користувачем, а також технологічну інформацію КСЗІ — і забезпечує взаємодію зазначених об'єктів.

Компоненти КЗЗ повинні мати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити певну множину операцій, що вже виконані над захищеним об'єктом за певний проміжок часу.

ЦВ-1 – це мінімальна цілісність при обміні, дана послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище.

ДР-1 – квоти, послуга дозволяє користувачам керувати використанням послуг і ресурсів. Політика використання ресурсів, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.,а використання ресурсів повинна визначати обмеження, які можна накладати,

на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу.

ДВ-1 – ручне відновлення, послуга надає можливість повернути КС до відомого захищеного стану після відмови чи переривання обслуговування.

Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов КС і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція КС.

Після відмови чи переривання КС КЗЗ повинен перевести КС до стану системи з якого повернути її до нормальної роботи може лише адміністратор або користувачі які володіють відповідними повноваженнями.

НР-2 – це захищений журнал послуга реєстрації рівня дозволяє контролювати небезпечні для АС дії зі сторони користувачів будь—яких категорій відносно процесів і об'єктів, що існують в АС і стосуються захищених об’єктів.

Політика реєстрації поширюється на: користувачів усіх категорій; сильно— та слабо зв'язані об'єкти, що містять службову інформацію; системне та функціональне програмне забезпечення, призначене для оброблення цих об'єктів; використання периферійного обладнання, задіяного для оброблення службової інформації; використання обчислювальних ресурсів АС, а також створену в процесі обробки сильно— та слабо зв'язаних об'єктів технологічну інформацію КСЗІ та технологічну інформацію щодо управління АС, — і забезпечує взаємодію зазначених об’єктів.

НИ-2 – це одиночна ідентифікація та автентифікація дана політика повинна визначати атрибути для кожного користувача та послуги для яких потрібне використання цих атрибутів. Кожний користувач повинен бути автентифікованим КЗЗ з використанням захищеного механізму, перш ніж користувач зможе виконувати будь—які дії контрольовані КЗЗ.

НК-1 – це однонаправлений достовірний канал послуга дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ.

Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ. Достовірний канал використовується для початкової ідентифікації і автентифікації зв’язок з даним каналом ініціюється тільки користувачем.

НО-2 – розподіл обов'язків адміністраторів, послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції.

НЦ-2 – це комплекси засобів захисту з гарантованою цілісністю послуга визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

Політика реалізації послуги повинна гарантувати, що усі послуги безпеки доступні тільки через інтерфейс КЗЗ й усі запити в АС на доступ до захищених об'єктів контролюються КЗЗ. Якщо існують якісь обмеження, недотримання яких може призвести до надання послуг в обхід інтерфейсу КЗЗ і порушення політики безпеки, то такі обмеження повинні бути описані і задокументовані. Порядок дотримання користувачами цих обмежень визначається і контролюється адміністратором безпеки або уповноваженим співробітником СЗІ. З метою захисту від зовнішніх впливів КЗЗ повинен визначати й підтримувати власний домен виконання, який є відмінним від доменів виконання усіх інших процесів, а також повинен мати механізми, що використовуються для реалізації розмежування доменів.

НТ-2 – це самотестування при старті дана послуга дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ та

має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження, при ініціалізації КЗЗ.

НВ-1 – це автентифікація вузла послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ та перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму. Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації.

2.2 Проектні рішення

2.2.1 Впровадження системи запобігання витоку даних

Система запобігання витоку даних – технологія яка допомагає запобігти витоку конфіденційної інформації з інформаційної системи підприємства.

Для ефективної роботи система запобігання витоку даних повинна вміти розрізняти конфіденційну інформацію від неконфіденційної. Функціональність даної системи будується навколо ядра системи – це програмний алгоритм який відповідає за категорізацію та пошуку інформації яку потрібно захистити.

Ядро багатьох систем витоку даних базуються на технологіях лінгвістичного аналізу та статистичних методах.

Лінгвістичний метод аналізу працює з вмістом файлу чи докумет на пряму. Такий метод дозволяє не звертати уваги на такі параметри як: на то має файл чи документ гриф, на ім’я файлу чи на те хто і коли створив цей файл чи документ. Дана технологія вкючає у себе:

—Морфологічний аналіз – це пошук інформації за усіми словоформами які тільки можуть бути;

—Семантичний аналіз – це пошук ключової інформації в вмісті файлу, вплив входжень на якісні характеристики файлу, оцінка контексту використання.

Лінгвістичний аналіз показує високу якість роботи з великим об'ємом інформації. Для об'ємного тексту система з алгоритмом лінгвістичного аналізу більш точно обере коректний клас, віднесе до потрібної категорії і запустить налаштоване правило. Для документів невеликого обсягу краще використовувати методику стоп—слів, яка ефективно зарекомендувала себе в боротьбі зі спамом.

Хоч у більш ранніх версіях систем запобігання витоку даних були проблеми з здатність до навчання систем з лінгвістичним методом, але у нових версіях систем здатність до навчання реалізована на самому вищому рівні. Завдяки новим алгоритмам самонавчання таких як :

—Виявлення ознак категорій;

—Можливість самостійно формувати та редагувати правила реагування;

До недоліків лінгвістичного методу аналізу можливо віднести той факт що систему яка використовує англійське ядро для аналізу інформації неможливо використовувати для російськомовних на українськомовних потоків інформації.

Інший недолік пов'язаний зі складністю чіткої категоризації з використанням імовірнісного підходу, що утримує точність спрацьовування в межах 95%, тоді як для компанії критичною може виявитися витік будь-якого обсягу конфіденційної інформації.

Статистичний метод аналізу інформації використовує аналіз хешу файлів, документів. На першому етапі документ розділяється на частини приблизно однакової величини та з цих фрагментів знімається хеш. Знятий хеш система порівнює з хешем який був взятий еталоним раніше. Якщо система знаходить збіг, то помічає цей документ як конфіденційний та діє згідно з політиками безпеки.

Переваги цього рішення складаються у то що результати статистичного аналізу не залежать від мови на якій написан документ та від наявності в цьому документі нетекстової інформації.

Недолік статистичного методу в тому, що алгоритм не здатний самостійно навчатися, формувати категорії і типізувати. Як наслідок — залежність від компетенцій фахівця і ймовірність завдання хешу такого розміру, при якому аналіз буде давати надмірну кількість помилкових спрацьовувань. Усунути недолік нескладно, якщо дотримуватися рекомендацій розробника з налаштування системи.

З формуванням хешів пов'язаний і інший недолік. У розвинених IT— системах, які генерують великі обсяги даних, база відбитків може досягати такого розміру, що перевірка трафіку на збіги з еталоном серйозно уповільнити роботу всієї інформаційної системи.

Також рівні контролю на яких працює система контролю витоку інформації має велике значення. Сучасні системи використовують поєднання рівнів контролю таких як :

—Мережевий рівень – це рівень мережі, який контролює мережевий трафік в інформаційній системі підприємства;

—Рівень контролю на хостовому рівні – це рівень хоста, коли інформація контролюється на всіх робочих станціях компанії;

Саме тому сучасні системи запобігання витоку інформації використовуються використовують методи для запобігання витоку інформації які компенсують один одного.

Причиною витоку інформацію досить часто буває халатність, неуважність чи корисливий намір персоналу. Саме тому сучасні компанії мають потребу у системах захисту витоку інформації, які мають наступні функції:

—Контроль веб—трафику;

—Контроль почтового трафіку;

—Контроль переписки в месенджерах;

—Контроль інформаційного обміну на робочих станціях співробітника компанії через комунікаційні порти (COM, LPT, USB, IrDA—порти і т.д.), пристрої введення—виведення (CD, знімні накопичувачі і т.д.), засоби бездротового доступу (Bluetooth, Wi-Fi і т.д.), друк на локальних і мережевих принтерах;

—Контроль дії співробітників на робочих місцях таких як : контроль буферу обміну, моніторинг відвіданих сайтів, контроль використання додатків, контроль за діями на робочому місці (скріншоти екрану, запис екрану, відео і т.д.);

—Контроль пошукових запитів;

—Контроль зберігання інформації на робочих комп'ютерах;

—Копіювання перехвачених файлів;

—Зберігання усіх перехвачених файлів в єдиному сховищі;

—Надання аналітики перехвачених даних.

Щоб мінімізувати ризики витоку інформації компанії ТОВ «SpeedNet» була обрана система запобігання витоку інформації від компанії McAfee. Так як компанія вже користується продуктами від компанії McAfee, а саме антивірусний захист, то було прийнято рішення в сторону системи запобігання витоку інформації від цієї компанії.

Дана система запобігання витоку інформації складається з наступних модулів, які доповнюють один одного :

—Єдина консоль керування завдяки якої можливо керувати антивірусним захистом, файрволом, різними додатками. Усі політики захисту налаштовуються з єдиної консолі керування та можливо слідкувати за всіма системами які знаходяться у компанії і швидко розгортати на них оновлення чи програмне забезпечення по захисту. Можливість переглядати всі інциденти які трапилися у компанії та швидко створити звіти за цими інцидентами;

—Агент McAfee – це посередник між центральним керуючим органом та кінцевою точкою. Агент встановлюється на кінцеві точки для налаштування зв'язку з сервером після чого можливо встановлювати на кінцевих точках системи запобігання витоку інформації, антивірусний захист і т.д.

—Контроль за кінцевими точками який захищає кінцеві точки від витоку інформації;

—Модуль для захисту почтового та веб шлюзу який у режимі реального часу сканує та приймає міри по захисту від витоку інформації через ці шлюзи;

—Модуль виявлення та захисту конфіденційних даних – це модуль в який задається критерії конфіденційної інформації, та котрий сканує сервер, знаходить цю інформацію та захищає її від витоку;

—Модуль моніторингу – це модуль пасивного моніторингу трафіку, який дозволяє побачити які витоки інформації сталися щоб потім можливо було налаштувати систему з урахуванням цих витоків;

—Модуль контролю кінцевих точок – це модуль який контролює всі дії з інформацією на кінцевих точка;

—Модуль контролю зовнішніх пристроїв контролює дані, які копіюються на зовнішні носії, підключення нових носіїв, забезпечує контроль Bluetooth. Схема розташування модулів системи захисту інформації зображена на *Рис2.1*.

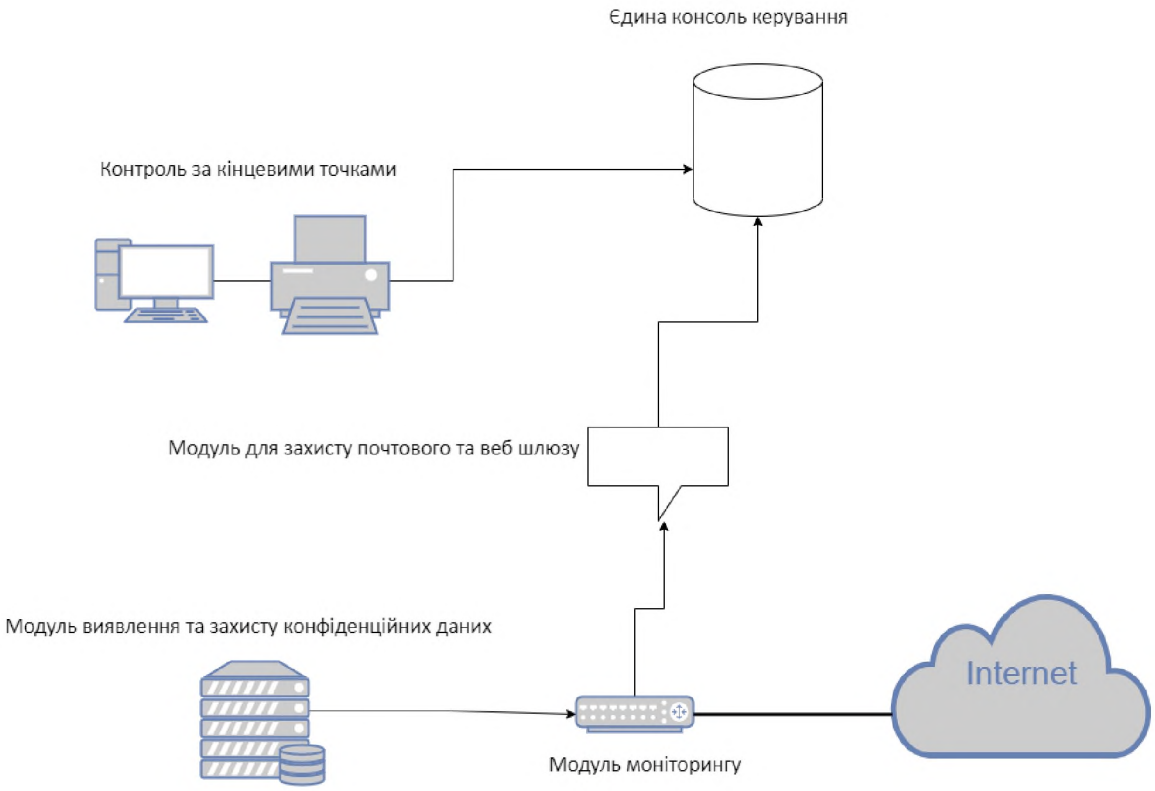


Рис. 2.1— Схема розташування модулів системи захисту інформації

Методи класифікації даних в системі захисту витоку інформації від McAfee:

— Ключові слова (може виступати будь-яке слово у файлі чи документі яке буде показувати що даний файл треба захистити).Наприклад: конфіденційно, з обмеженими доступом тощо;

— Словники (набір термінів чи професійних термінів які будуть виступати маркером) Можливо робити свої словники та завантажувати їх.

— Розширені шаблони – це регулярні вирази які трудно класифікувати. Наприклад: IP адреси, номера телефонів і т.д.;

— За типами файлів (Excel, Word і т.д.);

— Мітки та метадані. Ві

Процес забезпечення захисту інформації завдяки системі запобігання витоку інформації зображено на *Рис2.2.*

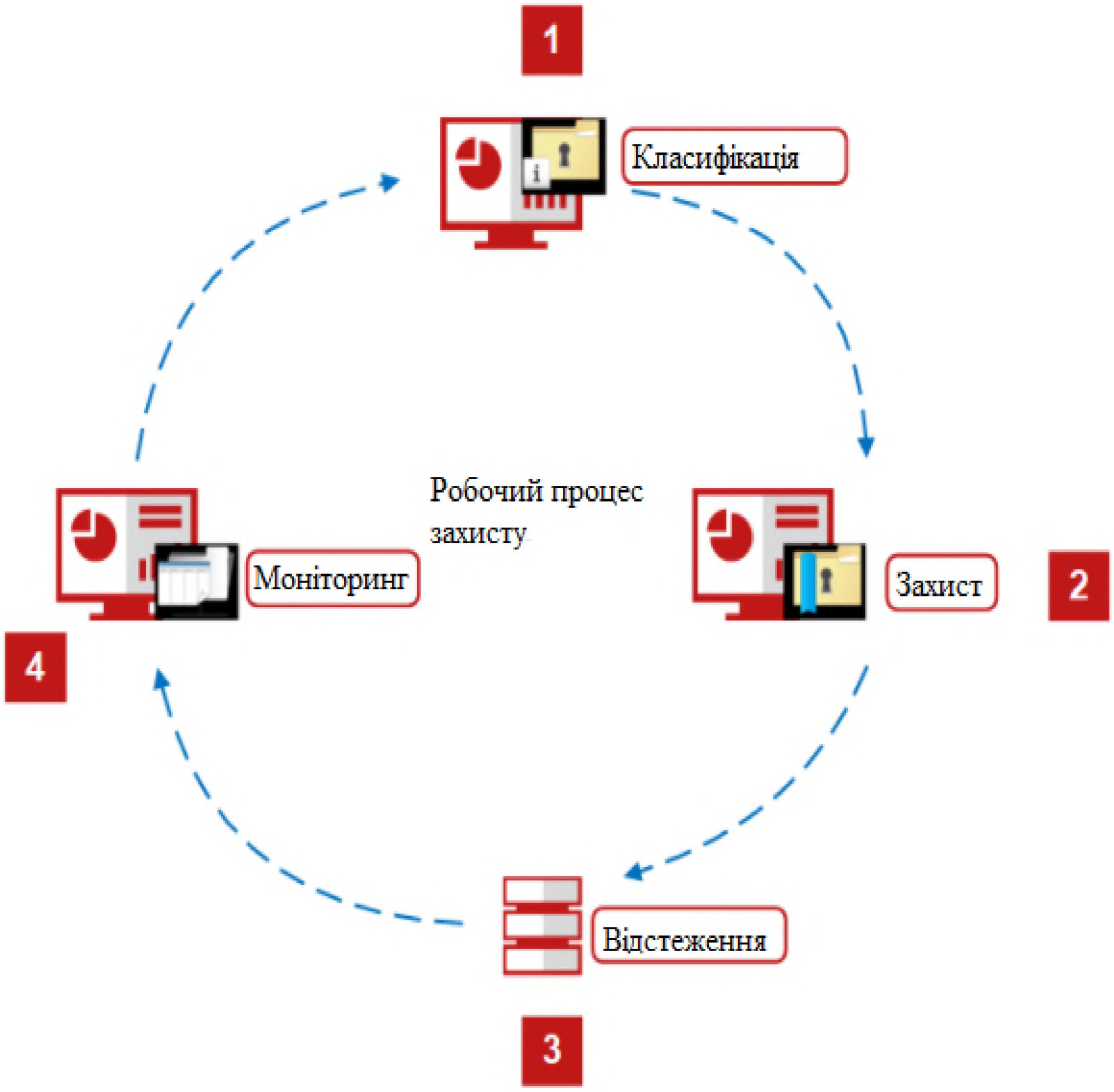


Рис2.2 — Процес забезпечення захисту інформації завдяки системі запобігання витоку інформації

1. Створення класифікацій завдяки єдиній консолі керування;
2. Захист конфіденційних даних завдяки диспечеру політик;
3. Відстеження використання конфіденційних файлів;
4. Відстеження результату завдяки диспечеру інцидентів та інструментом управління проблемами та операціями, створення звітів завдяки панелі моніторингу.

2.2.2 Рекомендації по налаштування комплексу

Через те що першою ціллю ворожих програм являється відключення програмного забезпечення системи безпеки потрібно правильно налаштувати самозахист служб та файлів для цього потрібно :

—Виберіть Меню → Політика → Каталог політик, потім зі списку Продукти на лівій панелі виберіть Загальні параметри захист кінцевих точок;

—У списку Категорія на правій панелі виберіть Параметри;

—Натисніть на ім'я редагованої політики;

—У розділі Самозахист переконайтеся, що Самозахист увімкнен;

—Вкажіть дію для кожного з наступних ресурсів:

Файли і папки — запобігає зміні баз даних, довічних файлів, файлів безпечного пошуку і файлів конфігурації McAfee;

Реєстр — запобігає зміні гілки реєстру, COM—компонентів і видалення McAfee за допомогою параметра реєстру;

Процеси — запобігає зупинці процесів McAfee;

—Натисніть зберегти.

Налаштування журналу активності користувачів :

—Виберіть Меню → Політика → Каталог політик, потім зі списку Продукти на лівій панелі виберіть Загальні параметри захист кінцевих точок:

—У списку Категорія на правій панелі виберіть Параметри;

—Натисніть посилання Змінити для змінною політики;

—Натисніть показати додаткові параметри та виберіть наступні значення:

Ведення журналу активності та оберіть включити ведення журналу активностей

—Натисніть кнопку зберегти.

Налаштування обмежень

—Виберіть Меню → Політика → Каталог політик, потім зі списку Продукти на лівій панелі виберіть Система адаптивної захисту від загроз на кінцевих точках:

—У списку Категорія на правій панелі виберіть Динамічне обмеження додатків;

—Клацніть посилання Змінити для змінною політики;

—У розділі Правила обмеження виберіть Заблокувати, Звіт або обидві дії для правила:

Щоб вибрати або скасувати вибір всіх правил для дій Заблокувати або Звіт, клацніть Блокувати всі або Звіт по всьому;

Щоб відключити правило, скасуйте вибір параметрів Заблокувати і Звіт;

—У розділі Винятки налаштуйте виконувані файли, які слід виключити з динамічного обмеження додатків;

—Процеси в списку Винятки виконуються звичайним чином (без обмежень);

—Натисніть кнопку Зберегти.

2.2.3 Розробка вимог до інформаційної безпеки

На підприємстві ТОВ «SpeedNet» потрібно ввести наступні вимоги до інформаційної безпеки, які будуть встановлювати наступні правила під час роботи:

—Забороняється підключати до робочого комп'ютеру, зовнішні носії інформації (флеш накопичувачі, телефони і т.д.) без письмового погодження з директором компанії;

—Користуватися мобільним телефоном/смартфоном на робочому місці;

—Користуватися особистою гарнітурою (навушниками, клавіатурою, коп'терною мишкою тощо) ;

—Вживати будь-які продукти що можуть нашкодити робочими коп'ютерам;

—Виносити робочі комп'ютери з місця їх розташування без дозволу письмового дозволу керівника відділу, системного адміністратора;

—Фотографувати, знімати відео на території ОІД;

—Самостійно ремонтувати коп'ютери чи інші електронні пристрої на робочому місці;

—Залишати увімкненим коп'ютер після кінця робочого дня;

—Обов'язково виходити з усіх програмних комплексів та облікових записів після кінця робочого ;

—При виході на обід чи при любому іншому відлучені з робочого місця блокувати комп'ютер;

—Приносити та підключати на робочому місці, локальної мережі чи до допоміжних електронних пристроїв будь-яке стороннє обладнання, без письмового ухвалення директора;

—Розкривати свої облікові дані від програмних комплексів компанії іншим співробітникам;

—Вживати дії які можуть завдати шкоди АС компанії чи дії для отримання несанкціонованого доступу до мережевого, серверного обладнання чи робочих місці інших співробітників;

—Використовувати Інтернет для обміну особистою інформацією у месенджерах, чатах тощо;

—Використовувати робочу телефонію у власних цілях;

—Завантажувати та/ або зберігати з Інтернету будь-яке програмне забезпечення, фото, відео і т.д. ;

—Переходити по будь-яким посилання які відправляють вам клієнти у чатах чи стороні особи;

—Використовувати корпоративну пошту поширення інформації яка не відноситься до робочої. Переходити по рекламним чи підозрілим посиланням;

—Створи створити посаду адміністратора безпеки;

—Надати повноваження адміністратора безпеки старшому системному адміністратору який буде тільки функції адміністратора безпеки;

2.3 Аналіз ризиків після впровадження комплексу захисту

Розглянемо таблицю 2.1, де показано як змінилися показники після впровадження запропонованих технологій та вимог.

Таблиця 2.1 – Модель загроз з визначенням рівня ризиків та збитків після впровадження рекомендацій

№	Механізм реалізації	Рівень		Сумма загроз
		Ризики	Збитки	
1	Загрози конфіденційності			
1.1	Збір інформації про клієнтів	1	3	4
1.2	Копіювання ІОД на зовнішні носії з метою несанкціонованого ознайомлення сторонніх осіб	1	3	4

Продовження таблиці –2.1

№	Механізм реалізації	Рівень		Сумма загроз
		Ризики	Збитки	
1.3	Перегляд інформації на екранах моніторів, робочих місцях; підслуховування	2	1	3
2	Загрози цілосності			
2.1	Використання продуктів компанії в своїх цілях	1	1	2
2.2	Модифікація інформації персоналом ІТС на носіях інформації	1	2	3
2.3	Помилки користувачів ІТС, які призвели до модифікації або спотворення інформації на жорсткому диску або зовнішніх носія	1	2	3
3	Загрози доступності			
3.1	Помилки користувачів ІТС, які призвели до знищення інформаціїабо втрати доступу до неї	1	3	4
3.2	Втрата інтернет з'єднання	2	2	4
3.3	Втрата електропостачання	1	2	3

Звернувшись до таблиці 2.2 можна побачити, що рівень ризику загроз зменшився відносно того який був раніше, до впровадження рекомендацій. Після прийняття рекомендацій рівень загроз став наступний :

— Загрози конфіденційності складають 11 балів до впровадження складали 14 балів;

— Загрози цілісності складають 8 балів до впровадження складали 11 балів;

— Загрози доступності складають 11 до впровадження складали 12 балів.

Впровадження технології запобігання витоку даних та впровадження вимог до інформаційної безпеки вплинуло на зменшення рівня загроз за наступними пунктами :

—Помилки користувачів ІТС, які призвели до знищення інформаціїабо втрати доступу до неї;

—Модифікація інформації персоналом ІТС на носіях інформації;

—Помилки користувачів ІТС, які призвели до модифікації або спотворення інформації на жорсткому диску або зовнішніх носія;

—Збір інформації про клієнтів;

—Копіювання ІОД на зовнішні носії з метою несанкціонованого ознайомлення сторонніх осіб;

В спеціальній частині кваліфікаційної роботи було наведено оцінку існуючого захисту підприємства ТОВ « SpeedNet», а також розроблені вимоги з інформаційної безпеки та впроваджена система система запобігання витоку інформації.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Річні прибутки підприємства ТОВ «SpeedNet » складають — 3 500 000 млн. грн. Підприємство розпочало свою діяльність у 2008 році, чисельність працівників складає 105 чоловік.

Прийняті нововведення для захисту конфіденційної інформації на підприємстві ТОВ «SpeedNet » потребують економічних обґрунтувань, які покажуть доцільність прийнятих рішень. Саме тому у економічному розділі розділі будуть проведені розрахунки, які допоможуть зробити висновки про економічну доцільність прийнятих комплексів захисту інформації та їх налагодження.

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 вимог до інформаційної безпеки та на впровадження системи запобігання витоку інформації, які визначаються виходячи з трудомісткості вимог до інформаційної безпеки та на впровадження системи запобігання витоку інформації.

Визначення трудомісткості розробки вимог до інформаційної безпеки впровадження системи запобігання витоку інформації

Трудомісткість розробки вимог до інформаційної безпеки та впровадження системи запобігання витоку інформації визначається тривалістю кожної робочої операції, починаючи з обстеження середовища і закінчуючи оформленням документації (за умови роботи одного спеціаліста з інформаційної безпеки):

$$t = t_{об} + t_{в} + t_{м} + t_{вб} + t_{звб} + t_{тнс}, \text{ годиу} \qquad (3.1)$$

де $t_{об}$ – тривалість обстеження об'єкту інформаційної діяльності;

$t_{в}$ – тривалість процесу аналізу загроз і оцінки ризиків ;

$t_{м}$ – тривалість процесу розробки моделі порушника ;

$t_{вб}$ – тривалість розробки вимог до інформаційної безпеки;

$t_{звб}$ – тривалість впровадження системи запобігання витоку інформації ;

$t_{тнс}$ – тривалість тестування і налагодження системи.

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

$t_{об}$=24 годин, $t_{в}$=16 годин, $t_{м}$=16 годин, $t_{вб}$=8 годин, $t_{звб}$=40 годин, $t_{тнс}$=24 годин.

Отже, t=24+16+16+8+40+24= 128 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 вимог до інформаційної безпеки та впровадження системи запобігання витоку інформації Змч.

$$К_{рп} = З_{зп} + З_{мч} . \quad (3.2)$$

$$К_{рп} = З_{зп} + З_{мч} = 25600 + 18\ 365{,}6 = 43\ 965{,}6 \text{грн.}$$

$$З_{зп} = t\ Зіб = 128 \cdot 200 = 25600 \text{ грн.}$$

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:

$$З_{мч} = t_{роб} \cdot С_{мч} = 104 \cdot 176{,}5 = 18\ 365{,}6 \text{грн.}$$

де $t_{роб}$ – трудомісткість роботи на ПК, годин(104 год);

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

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = Р \cdot t \cdot С_е + \frac{Фзал \cdot На}{Fp} + \frac{Клпз \cdot Напз}{Fp} = 0,8 \cdot 128 \cdot 1,68 + \frac{15500 \cdot 0,5}{1994} + \frac{5600 \cdot 0,24}{1994}$$

176,5грн/год

де Р – встановлена потужність персонального комп'ютера, кВт;

Се – тариф на електричну енергію, грн/кВт·година;

Фзал– залишкова вартість персонального комп'ютера на кінець року, грн.;

На – річна норма амортизації на персональному комп'ютері, частки одиниці;

Напз – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

Клпз – вартість ліцензійного програмного забезпечення, грн.;

Fp – річний фонд робочого часу (за 40 – годинного робочого тижня Fp= 1994 год)

Також витри на придбання щорічної підписки на систему запобігання витоку інформації від компанії McAfee складае 60526 грн. Витрати на налагодження системи складають 20 % відсотків від вартості ПЗ, тобто 12105,2 грн.

Таким чином, капітальні (фіксовані) витрати на створення та впровадження вимог до політики інформаційної безпеки та впровадження системы запобігання витоку інформації підприємства складають:

$$К = 43\ 965,6 + 60526 + 12105,2 = 116\ 596,83 грн.$$

3.3.1Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_в + С_к + С_{ак}\text{ , грн.} \qquad (3.3)$$

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:

$$С_к = С_н + С_а + С_з + С_{ел} + С_о + С_{тос}, \text{ грн.} \quad (3.4)$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються ($С_н = 4000$ грн.).

Вартість подовження ліцензії системи запобігання витоку інформації , який вже встановлений на всіх комп'ютерах підприємства, складає 60526грн,

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

$$С_з = З_{осн} + З_{дод}, \text{ грн.} \quad (3.5)$$

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 10000 грн. Додаткова заробітна плата – 10% від основної заробітної плати. Отже,

$$С_з = 10000 \cdot 12 + 10000 \cdot 12 \cdot 0,1 = 132000 \text{ грн.}$$

Ставка ЄСВ для всіх категорій платників з 01.01.2021 р. складає 22%.

$$С_{єв} = 132000 \cdot 0,22 = 29040 \text{ грн.}$$

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

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.}, \quad (3.6)$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=2,5 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1994 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,68 грн./кВт за годину).

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

$$С_{ел} = 2,5 \cdot 1994 \cdot 1,68 = 8\ 374,8\text{грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат — 1% (Стос = 116 596,83· 0,01=1 165,96грн).

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

$$С_к = 4000 + 60526 + 161040 + 8\ 374,8 + 29040 + 1\ 165,96 = 264\ 146,76\text{грн.}$$

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають 264 146,76грн.

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, 6 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, 8 годин;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 20000 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 15000 грн./міс.;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 5 особи;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 27 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 3 500 000 млн. 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, 27.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V, \qquad (3.7)$$

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:

$$П_п = \frac{\sum Зо}{F} \cdot t_п = \frac{15000 \cdot 27}{160} \cdot 6 = 15\ 187{,}5 грн,$$

де F – місячний фонд робочого часу (при 40—а годинному робочому тижні становить 160 ч).

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

$$П_в = П_{ви} + П_{пв}, \qquad (3.8)$$

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

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, 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 $t_{ви}$:

$$П_{ви} = \frac{\sum Зс}{F} \cdot t_{ви} = \frac{20000 \cdot 5}{160} \cdot 8 = 5000 грн.$$

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

$$П_{пв} = \frac{\sum Зо}{F} \cdot t_в = \frac{20000 \cdot 5}{160} \cdot 2 = 1\ 250 грн.$$

$$П_в = 5000 + 1\ 250 = 6\ 250 грн.$$

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:

$$V = \frac{O}{Fг} \cdot (t_п + t_в + t_{ви}) \quad (3.9)$$

$$V = \frac{3500000}{2080} \cdot (5 + 2 + 7) = 23\ 557{,}69 грн.$$

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.

$$U = 23\ 557{,}69 + 15\ 187{,}5 + 6\ 250 = 44\ 995{,}19 грн.$$

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

$$B = \sum 1 \sum 27\ 44\ 995{,}19 = 1\ 214\ 870{,}19 грн.$$

3.2.2 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = В \cdot R - C \text{ грн.}, \quad (3.10)$$

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

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці (30%);

С – щорічні витрати на експлуатацію системи інформаційної безпеки.

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

$$E = 1\ 214\ 870{,}19 \cdot 0{,}3 - 264\ 146{,}76 = 100\ 314{,}29 \text{грн.}$$

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:

$$\text{ROSI} = \frac{E}{K}, \text{ частки одиниці,} \qquad (3.11)$$

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

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

Коефіцієнт повернення інвестицій ROSI:

$$\text{ROSI} = \frac{100\ 314{,}29}{116\ 596{,}83} = 0{,}86 \text{ частки одиниці,}$$

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

$$\text{ROSI} > (N_{\text{деп}} - N_{\text{інф}})/100), \qquad (3.12)$$

де $N_{\text{деп}}$ – річна депозитна ставка, (7,5 %);

$N_{\text{інф}}$ – річний рівень інфляції, (5%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$0{,}86 > (7{,}5 - 5)/100 = 0{,}86 > 0{,}025.$$

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

$$T_o = \frac{К}{Е} = \frac{1}{ROSI} = \frac{1}{0{,}83} = 1{,}1, \text{ років.}$$

ВИСНОВКИ

Розробка комплексної системи захисту інформації комп'ютерної мережі ТОВ «SpeedNet» є економічно доцільним, оскільки капітальні та експлуатаційні витрати будуть меншими за можливий відвернений збиток. Капітальні витрати складають 116 596,83грн., експлуатаційні – 264 146,76грн грн. Величина річного економічного ефекту складає 100 314,29грн грн. Коефіцієнт повернення інвестицій ROSI складає 0,86грн./грн. Та термін окупності становить 1,16роки.

У кваліфікаційній роботі розв'язано завдання щодо створення КСЗІ на підприємстві та удосконалення існуючих систем інформаційної безпеки. Було виконано:

—Аналіз будівль та створений ситуаційний та генеральний плани;

—Проаналізованне програмне забеспечення котрим користується компанія;

—Класифікована інформація, що циркулює на ОІД;

—Проаналізовані загрози та вразливості;

—Розлоблено модель порушника;

—Оцінка існуючого захису ОІД;

—Запропоновані впровадження що до поліпшеня інформаційного захисту підприємства;

—Прораховано доцілініть запропонованих впроваджень.

ПЕРЕЛІК ПОСИЛАНЬ

1. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу НД ТЗІ 2.5-004-99 [Електронний ресурс]. – 1999р. — Режим доступу до ресурсу: https://tzi.com.ua/downloads/2.5—004—99.pdf.
2. Порядок проведення робіт по створенню комплексної системи захисту інформації в інформаційно—телекомунікаційній системі НД ТЗІ 3.7—003 —2005 [Електронний ресурс]. - 2005. — Режим доступу до ресурсу: https://tzi.com.ua/downloads/3.7—003—2005.pdf.
3. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. НД ТЗІ 2.5-005-1999 – Київ 1999 р.
4. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу НД ТЗІ 2.5-005 -99 [Електронний ресурс]. — 1999. — Режим доступу до ресурсу: https://tzi.ua/assets/files/%D0%9D%D0%94—%D0%A2%D0%97%D0%86-2.5-005-99. pdf.
5. Налаштування захисту кінцевих точок [Электронный ресурс] — Режим доступу к ресурсу: https://docs.mcafee.com/ru—RU/bundle/endpoint—security—10.7.x—common—product—guide—windows/page/GUID—E3F80434—FD29—4D5C—A150—7BD6DC88BC21.html.
6. Закон України про інформацію: [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text
7. Закон України про телекомунікації: [Електронний ресурс] – Режим до—ступу: https://zakon.rada.gov.ua/laws/show/1280-15#Text
8. Вибір DLP системи [Електронний ресурс] — Режим доступу до ресурсу: https://q.center/kak—vybrat—dlp—i—ne—oshibitsya—funktsionalnost—stoimost—vladeniya—i—doverie—k—vendoru/.

9. Компьютерные сити [Электронный ресурс]. — 2012. — Режим доступа к ресурсу: https://www.litmir.me/br/?b=639789.
10. Вимоги до системи захисту інформації [Електронний ресурс] – Режим доступу до ресурсу: https://studfiles.net/preview/6012701/page:6
11. Конспект лекций по курсу «Безопасность», «Программное обеспечение систем» информационных систем »[Электронный ресурс] — Режим доступа к ресурсу: https://blanki—ua.com.ua/zayava/18966/index.html?page=7
12. 1. ВПЛИВ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ НА ЕКОНОМІЧНУ БЕЗПЕКУ ПІДПРИЄМСТВА [Електронний ресурс] — Режим доступу до ресурсу: https://www.researchgate.net/publication/321981170_VPLIV_SUCASNIH_INFORMACIJNIH_TEHNOLOGIJ_NA_EKONOMICNU_BEZPEKU_PIDPRIEMSTVA.
13. Принципы организации ЗАЩИТЫ ИНФОРМАЦИИ В Современных информационно—коммуникационных СИСТЕМАХ И СЕТЯХ [Электронный ресурс] — Режим доступа к ресурсу: http://www.rusnauka.com/16_ADEN_2010/Informatica/68642.doc.htm.
14. Документація по налаштуванню DLP McAfee [Електронний ресурс] — Режим доступу до ресурсу: https://docs.mcafee.com/ru—RU/bundle/data—loss—prevention—11.2.x—product—guide/page/GUID—E62A2640 —56B4—4D07—8446—FA29D72D44C3.html.

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	25	
6	А4	2 Розділ	16	
7	А4	3 Розділ	14	
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	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____
(підпис) (ініціали, прізвище

ДОДАТОК Г. ВІДГУК

на кваліфікаційну роботу студента групи 125-17-2
Гуні Владислава Олеговича
на тему: «Комплексна система захисту інформації інформаційно-телекомунікаційної системи відділу бухгалтерії дитячо-юнацької спортивної школи»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на _57___ сторінках.

Метою кваліфікаційної роботи є розробка комплексної системи захисту інформації інформаційно-телекомунікаційної системи компанії «SpeedNet».

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: аналіз нормативно-правової бази у сфері забезпечення кібербезпеки; аналіз інформаційного середовища підприємства; аналіз моделі порушника та загроз.

На основі моделі загроз було розроблено елементи комплексної системи захисту інформації. Практичне значення результатів кваліфікаційної роботи полягає у підвищенні ефективності забезпечення безпеки інформації, за рахунок розробки політики безпеки інформації та обрання програмних засобів забезпечення захисту інформації.

За час дипломування Масалов І.С. проявив себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації бакалавра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека».

Рівень запозичень у кваліфікаційній роботі не перевищує вимог "Положення про систему виявлення та запобігання плагіату".

Кваліфікаційна робота заслуговує оцінки ____.

Керівник