Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ПОЯСНЮВАЛЬНА ЗАПИСКА

Дипломної роботи

магістра

(назва освітньо-кваліфікаційного рівня)

галузь знань *12 Інформацімайні технології*
(шифр і назва галузі знань)

спеціальність *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*
(назва освітньої програми)

освітньо-наукова програма *кібербезпека*

на тему: «Оцінка та удосконалення засобів та методів захисту інформації на підприємст

Виконавець: студент ІІ курсу, групи КБм-21

(підпис) **Рекуненко Денис Вадимович** (прізвище ім'я по-батькові)

	Прізвище, ініціали	**Оцінка**	**Підпис**
Науковий керівник	Лукова-Чуйко Н.В		
Рецензент			
Нормоконтроль	Даков С.Ю.		

Київ 2022

Міністерство освіти і науки України
«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри кібербезпеки
та захисту інформації
_____ Н.В. Лукова-Чуйко
«__» _____ 2021 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

студенту КБм-21 (група) Рекуненку Денису Вадимовичу (прізвище ім'я по-батькові)

Тема дипломної роботи Оцінка та удосконалення засобів та методів захисту інформації на підприємстві

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 5 від 29.10.2021

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень Процес захисту інформації на підтприємстві

Предмет досліджень Методи захисту інформації на підтприємстві

Мета Удосконалення засобів та методів захисту інформації на підприємстві.

Вихідні дані для проведення роботи Засоби та методи захисту інформації на підпрємстві.

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна Удосконалено метод захисту інформації на підприємстві за рахунок поєднання методів та засобів сучасних технологій та застосунків захисту інформації також демонстрування економічної вигідності

Практична цінність

Покращення системи захисту даних на підприємстві

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота виконана у повному обсязі відповідно до теми.

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Розробка плану для досягнення мети роботи	29.10.2021 – 23.01.2022
Аналіз літературних джерел	24.01.2022 – 14.02.2022
Розробка методу захисту від витоку даних платіжних карток через інтернет-браузер	15.02.2022 – 24.04.2022
Оформлення і друк пояснювальної записки	25.04.2022 – 19.05.2022

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект Зниження збитків через викрадення даних

Соціальний ефект Покращення технологій забезпечення захисту інформації як особисто так і на підприємствах.

7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ _____
(підпис) (прізвище, ініціали)

Завдання прийняв до виконання _____ _____
(підпис) (прізвище, ініціали)

Дата видачі завдання: _____
Термін подання дипломної роботи до ЕК _____

ЗМІСТ

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Оцінка та удосконалення методів та засобів захисту інформації на підприємстві»: 68 сторінок, 11 рисунків, 14 таблиць. 20 літературних джерел.

Об’єкт дослідження – процес захисту корпоративної мережі від атак.

Мета роботи – Аналіз та удосконалення засобів захисту інформації на підприємстві.

Методи дослідження – аналіз існуючих методів та засобів захисту інформації на підприємстві

У роботі досліджено сучасні засоби та методи захисту інформації на підриємстві . Проведено аналіз ринку рішень, захисту інформації . Надано список рекомендацій по удосконаленю захисту інформації на підприємстві .

Наукова новизна: удосконалено метод захисту інформації на підприємстві за рахунок поєднання методів та засобів сучасних технологій та застосунків захисту інформації також демонстрування економічної вигідності використання даних методів захисту на 15%.

Актуальність теми: втрата даних є серйозною загрозою безпеки інфраструктур практично кожної організації. Традиційний набір засобів захисту інформації не здатний протистояти невідомим загрозам. Удосконалення системи зменшує втрати або унеможливлює витоку інформації. Тому представлення методу, у якому захист реалізований за допомогою комбінацій сучасних застосунків є актуальною темою.

Ключові слова: підприємство ,методи захисту, засоби захисту , комплекс захисту , система захисту інформації, корпоративна мережа.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ІБ – Інформаційна система;

СЗІ – Система захисту інформації;

ПЗ – Програмне забезпечення

АСУ – Автоматизована система управління

ПК – Персональний комп’ютер

КС – компютерна система

ІТ – Information Technology

ІКТ – Інформаційно-комунікаційні технології

ПЗ – Програмне забезпечення

ЦОД – Центр обробки даних

ВСТУП

Організація є одним із найефективніших чинників розвитку громади. Зазвичай вони взаємодіють зі своїм внутрішнім і зовнішнім середовищем. Завдяки цій взаємодії вони можуть створити не тільки послугу або продукт, бажаний цільовою групою, але й безперервне джерело інформації та інформації, особливо в електронному середовищі. У зв'язку з цим можна сказати, що управління знаннями є ключовим моментом у розвитку організацій, інтегрованих з новими технологіями. Крім того, управління знаннями забезпечує управління інформацією, створеною для організаційних цілей, організаційної роздефективності та продуктивності, а також конкурентних переваг.

Розвиток Інтернету та мережевих технологій відкрив нові перспективи щодо конкурентних переваг та зміни методів, а також підвищив важливість управління знаннями для організацій. Особливо в 1990-х роках, з використанням інформаційних систем у сучасному розумінні, питання управління знаннями та безпека стали важливими факторами розвитку та конкурентних переваг глобальних організацій. Численні стандарти, політики, правила та інформаційна безпека були розроблені для методів оцінки організації та інструментів оцінки. У зв’язку з цим організації можуть впровадити підхід до інформаційної безпеки, заснований на стандартах, і переглянути свій підхід до інформаційної безпеки на основі інструментів оцінки та реагувати на виявлені ризики.

Актуальність роботи обумовлена наступними причинами:

- різко зросла обчислювальна потужність сучасних комп'ютерів, при цьому спростилася їх робота;

- високі темпи зростання парків ПК, що працюють у різних сферах діяльності;

- різке збільшення кількості інформації, що накопичується, зберігається на електронних носіях (у вигляді електронних документів) та обробляється комп'ютерами;

- інформація, централізована та централізована в єдиній базі даних (БД) різного призначення та різної належності;

- динамічний розвиток програмного забезпечення, яке не відповідає навіть мінімальним вимогам безпеки;

- коло користувачів з прямим доступом до обчислювальних ресурсів і наборів даних різко розширилося;

- демократизація доступу до інформації за рахунок розвитку локальних і глобальних комп'ютерних мереж;

- розвиток електронної пошти та розвиток електронного документообігу в комп'ютерних мережах;

- впровадження електронних технологій у різноманітну професійну діяльність на фінансових та товарних ринках (електронна комерція, інтернет-банкінг та фінансові послуги);

– розвиток глобальної мережі Інтернет фактично не запобігає порушенням безпеки в глобальній системі обробки інформації.

З цих причин існує різке протиріччя між розширенням можливостей IT-методів та інструментів і можливостями методів. та засоби захисту інформаційних ресурсів.

РОЗДІЛ 1

ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Створення публічних інформаційних просторів та майже широке використання персональних комп'ютерів та впровадження комп'ютерних систем вимагали вирішення складних питань інформаційної безпеки.

Під захистом інформації в КС розуміється регулярне використання засобів і методів, заходів і заходів для систематичного забезпечення необхідної достовірності інформації, що зберігається та обробляється за допомогою КС.

Об'єктом захисту є інформація, засоби масової інформації чи інформаційні процеси, які мають бути захищені відповідно до мети захисту інформації. Захист комп'ютерної інформації включає запобігання та відстеження несанкціонованого доступу (UDI) з боку неавторизованих осіб, зловживання, пошкодження, знищення, спотворення, копіювання, блокування, пов'язані з комп'ютерними засобами та методами зберігання, обробки, передачі та доступу. Форми та заходи інформації в засобах масової інформації Для забезпечення безпеки інформації в КС необхідно захистити: - масиви інформації, представленої на різних машинних носіях, технічні засоби обробки та передачі даних, реалізацію відповідних методів, алгоритмів і прийомів обробки інформації програмним забезпеченням, користувача.

Під інформаційною безпекою розуміють захист інформації від незаконного розпізнавання, перетворення та знищення, а також захист інформаційних ресурсів від впливів, покликаних підірвати їх працездатність.

Інформаційна безпека досягається шляхом забезпечення конфіденційності, цілісності та надійності оброблених даних та доступності та цілісності інформаційних компонентів і ресурсів КС. Конфіденційність — це властивість, яка свідчить про необхідність встановлення обмежень на доступ до цієї інформації певних груп осіб.

Іншими словами, це гарантія того, що тільки законні користувачі дізнаються про дані, що передаються. Цілісність — це властивість інформації зберігати свою

структуру та/або зміст у неспотвореній формі щодо деякого фіксованого стану під час передачі та зберігання.

Інформацію може створювати, змінювати або знищувати лише уповноважений персонал (законні користувачі з правами доступу). Достовірність — це ознака інформації, яка проявляється як сувора приналежність між суб'єктом джерела інформації або суб'єктом, який отримує інформацію. Доступність — це властивість інформації, що характеризує можливість надавати користувачам своєчасний і безперешкодний доступ до необхідної інформації.

Інформаційна безпека досягається шляхом управління відповідним рівнем політики інформаційної безпеки. Основним документом для реалізації політики інформаційної безпеки є план інформаційної безпеки. Цей документ розроблено як офіційний керівний документ для вищих керівних органів держави, відомства та організації. У документі визначено цілі політики інформаційної безпеки та основні напрями вирішення мандата Конституційного Суду щодо захисту інформації. План інформаційної безпеки також містить загальні вимоги та принципи побудови системи захисту інформації в КС.

1.1 Загрози інформаційної безпеки

Щоб забезпечити ефективний захист інформації, необхідно в першу чергу розглянути і проаналізувати всі фактори, що становлять загрозу інформаційній безпеці.

Під загрозою інформаційної безпеки КС зазвичай розуміють потенційно можливу подію, дію, процес чи явище, що може мати небажаний вплив на систему та інформацію, яка в ній зберігається та обробляється. Такі загрози, впливаючи на інформацію через компоненти КС, можуть призвести до знищення, спотворення, копіювання, несанкціонованого поширення інформації, обмеження або блокування доступу до неї. Нині відомий досить великий перелік загроз, який класифікують за кількома ознаками.

За природою виникнення розрізняють:

- природні загрози, спричинені впливами на КС об'єктивних фізичних процесів чи стихійних природних явищ;

- штучні загрози безпеці, викликані діяльністю людини.

За рівнем навмисності прояви розрізняють випадкові та навмисні загрози безпеці.

По безпосередньому джерелу загроз. Джерелами загроз можуть бути:

- природне середовище, наприклад, стихійні лиха;

- людина, наприклад, розголошення конфіденційних даних;

- санкціоновані програмно-апаратні засоби, наприклад, відмова у роботі операційної системи;

- несанкціоновані програмно-апаратні засоби, наприклад, зараження комп'ютера вірусами.

За станом джерела загроз. Джерело загроз може бути розташоване:

- поза контрольованою зоною КС, наприклад, перехоплення даних, що передаються каналами зв'язку;

- у межах контрольованої зони КС, наприклад, розкрадання роздруківок, носіїв інформації;

- безпосередньо в КС, наприклад, некоректне використання ресурсів.

За ступенем на КС розрізняють:

- пасивні загрози, які при реалізації нічого не змінюють у структурі та змісті КС (загроза копіювання даних);

- активні загрози, які при впливі вносять зміни до структури та змісту КС (впровадження апаратних та програмних спецвкладень).

За етапами доступу користувачів або програм до ресурсів КС:

- погрози, які можуть виявлятися на етапі доступу до ресурсів КС;

- погрози, що виявляються після дозволу доступу (несанкціоноване використання ресурсів).

За поточним місцем розташування інформації в КС:

- загроза доступу до інформації на зовнішніх пристроях (ЗУ), наприклад, копіювання даних з жорсткого диска;

- загроза доступу до інформації в оперативній пам'яті (несанкціоноване звернення до пам'яті);

- погроза доступу до інформації, що циркулює в лініях зв'язку (шляхом незаконного підключення).

За способом доступу до ресурсів КС:

- загрози, що використовують прямий стандартний шлях доступу до ресурсів за допомогою незаконно отриманих паролів або шляхом несанкціонованого використання терміналів законних користувачів;

- загрози, що використовують прихований нестандартний шлях доступу до ресурсів КС в обхід наявних засобів захисту.

За рівнем залежності від активності КС розрізняють:

- погрози, що виявляються незалежно від активності КС (розкрадання носіїв інформації);

- загрози, що виявляються лише у процесі обробки даних (поширення вірусів).

1.2 Види загроз інформаційної безпеки

Вся безліч потенційних загроз безпеки інформації в КС може бути поділено на 2 основні класи

Загрози, які пов'язані з навмисними діями зловмисників і реалізуються у випадкові моменти часу, називають випадковими чи ненавмисними. Механізм реалізації випадкових загроз загалом досить добре вивчений, накопичено значний досвід протидії цим загрозам.

Стихійні лиха та аварії загрожують найбільш руйнівними наслідками для КС, оскільки останні зазнають фізичного руйнування, інформація втрачається або доступ до неї стає неможливим. Збої та відмови складних систем неминучі. В результаті збоїв та відмов порушується працездатність технічних засобів, знищуються та спотворюються дані та програми, порушується алгоритм роботи пристроїв.

Помилки при розробці КС, алгоритмічні та програмні помилки призводять до наслідків, аналогічних наслідків збоїв та відмов технічних засобів.

Рисунок 1.1 Загрози безпеки інформації у КС

Крім того, такі помилки можуть бути використані зловмисниками для на ресурси КС.

Внаслідок помилок користувачів та обслуговуючого персоналу порушення безпеки відбувається у 65% випадків . Некомпетентне, недбале чи неуважне виконання функціональних обов'язків співробітниками призводить до знищення, порушення цілісності та конфіденційності інформації.

Умисні загрози пов'язані з цілеспрямованими діями порушника. Цей клас загроз вивчений недостатньо, дуже динамічний і постійно поповнюється новими загрозами.

Методи та засоби шпигунства та диверсій найчастіше використовуються для отримання відомостей про систему захисту з метою проникнення в КС, а також для розкрадання та знищення інформаційних ресурсів. До таких методів відносять підслуховування, візуальне спостереження, розкрадання документів та машинних

носіїв інформації, розкрадання програм та атрибутів системи захисту, збирання та аналіз відходів машинних носіїв інформації, підпали.

Несанкціонований доступ до інформації (НСД) зазвичай відбувається з використанням штатних апаратних та програмних засобів КС, внаслідок чого порушуються встановлені правила розмежування доступу користувачів або процесів до інформаційних ресурсів. Під правилами розмежування доступу розуміється сукупність положень, що регламентують права доступу осіб або процесів до одиниць інформації. Найбільш поширеними порушеннями є:

- перехоплення паролів – здійснюється спеціально розробленими програмами;
- "маскарад" - виконання будь-яких дій одним користувачем від імені іншого;
- Незаконне використання привілеїв - захоплення привілеїв законних користувачів порушником.

Процес обробки та передачі інформації технічними засобами КС супроводжується електромагнітними випромінюваннями в навколишній простір та наведенням електричних сигналів у лініях зв'язку. Вони отримали назви побічних електромагнітних випромінювань та наведень (ПЕМІН). За допомогою спеціального обладнання сигнали приймаються, виділяються, посилюються і можуть або переглядатися, або записуватися в пристроях, що запам'ятовуються (ЗУ). Електромагнітні випромінювання використовуються зловмисниками як для отримання інформації, а й у її знищення.

Велику загрозу безпеці інформації в КС є несанкціонована модифікація алгоритмічної, програмної та технічної структур системи, яка отримала назву “закладка”. Як правило, “закладки” впроваджуються у спеціалізовані системи та використовуються або для безпосереднього шкідницького на КС, або для забезпечення неконтрольованого входу в систему.

Одним з основних джерел загроз є використання спеціальних програм, що отримали загальну назву “шкідницькі програми”. До таких програм належать:

- комп'ютерні віруси - невеликі програми, які після впровадження в ЕОМ самостійно поширюються шляхом створення своїх копій, а при виконанні певних умов негативно впливають на КС

- хробаки – програми, які виконуються щоразу при завантаженні системи, що мають здатність переміщатися в КС або мережі та самовідтворювати копії. Лавиноподібне розмноження програм призводить до перевантаження каналів зв'язку, пам'яті, а потім блокування системи;

- троянські коні - програми, які мають вигляд корисної програми, а насправді виконують шкідливі функції (руйнування програмного забезпечення, копіювання та пересилання зловмиснику файлів з конфіденційною інформацією тощо).

Окрім зазначених вище загроз безпеки, існує також загроза витоку інформації, яка з кожним роком стає дедалі значущою проблемою безпеки. Щоб ефективно справлятися з витоками, необхідно знати як вони відбуваються .

На чотири основних типи витоків припадає переважна більшість (84%) інцидентів, причому половина цієї частки (40%) посідає найпопулярнішу загрозу – крадіжку носіїв. 15% складає інсайд. До цієї категорії належать інциденти, причиною яких стали дії працівників, які мали легальний доступ до інформації. Наприклад, співробітник не мав права доступу до інформації, але зміг обійти системи безпеки. Або інсайдер мав доступ до інформації та виніс її за межі організації. На хакерську атаку також припадає 15% загроз. У цю велику групу інцидентів потрапляють усі витоки, що сталися внаслідок зовнішнього вторгнення. Не дуже висока частка хакерських вторгнень пояснюється тим, що самі вторгнення стали непомітнішими. 14% склав веб-витік.

До цієї категорії потрапляють усі витоки, пов'язані з публікацією конфіденційних відомостей у загальнодоступних місцях, наприклад, у Глобальних мережах. 9% - це паперовий витік. За визначенням паперовим витоком є будь-який витік, який стався в результаті друку конфіденційних відомостей на паперових носіях. 7% становлять інші можливі небезпеки. До цієї категорії потрапляють інциденти, точну причину яких встановити не вдалося, а також витоку, про який

стало відомо постфактум, після використання персональних відомостей у незаконних цілях.

Крім того, нині активно розвивається фішинг – технологія Інтернет-шахрайства, яка полягає у крадіжці особистих конфіденційних даних, таких як паролі доступу, номери кредитних карток, банківських рахунків та іншої персональної інформації. Фішинг (від анг. Fishing - риболовля) розшифровується як вивужування пароля та використовує не технічні недоліки КС, а легковірність користувачів Інтернету. Зловмисник закидає в Інтернет приманку та "виловлює всіх рибок" - користувачів, які на це клюнуть

Незалежно від специфіки конкретних видів загроз, інформаційна безпека має зберігати цілісність, конфіденційність, доступність. Загрози порушення цілісності, конфіденційності та доступності є первинними. Порушення цілісності включає будь-яке навмисне зміна інформації, що зберігається в КС або передається з однієї системи в іншу. Порушення конфіденційності може призвести до ситуації, коли інформація стає відомою тому, хто не має повноважень доступу до неї. Загроза недоступності інформації виникає щоразу, коли внаслідок навмисних дій інших користувачів чи зловмисників блокується доступ до деякого ресурсу КС.

Ще одним видом загроз інформаційній безпеці є загроза розкриття параметрів КС. В результаті її реалізації не завдається жодної шкоди інформації, що обробляється в КС, але при цьому істотно посилюються можливості прояву первинних загроз.

1.3 Методи та засоби захисту інформації

Загальна характеристика засобів та методів захисту

Протидія численним загрозам інформаційної безпеки передбачає комплексне використання різних способів та заходів організаційного, правового, інженерно-технічного, програмно-апаратного, криптографічного характеру тощо.

Організаційні заходи щодо захисту включають сукупність дій з підбору та перевірки персоналу, що бере участь у підготовці та експлуатації програм та інформації, суворе регламентування процесу розробки та функціонування КС .

До правових заходів та засобів захисту відносяться чинні в країні закони, нормативні акти, що регламентують правила поводження з інформацією та відповідальність за їх порушення.

Інженерно-технічні засоби захисту досить різноманітні і включають фізико-технічні, апаратні, технологічні, програмні, криптографічні та інші засоби. Дані засоби забезпечують такі рубежі захисту: контрольована територія, будівля, приміщення, окремі пристрої разом із носіями інформації.

Програмно-апаратні засоби захисту безпосередньо застосовуються в комп'ютерах і комп'ютерних мережах, містять різні електронні, електромеханічні пристрої, що вбудовуються в КС. Спеціальні пакети програм або окремі програми реалізують такі функції захисту, як розмежування та контроль доступу до ресурсів, реєстрація та аналіз протікаючих процесів, подій, користувачів, запобігання можливим руйнівним впливам на ресурси та інші .

Суть криптографічного захисту полягає у приведенні (перетворенні) інформації до неявного виду за допомогою спеціальних алгоритмів або апаратних засобів та відповідних кодових ключів.

Захист інформації від випадкових загроз

Для блокування (парування) випадкових загроз безпеки в КС має бути вирішено комплекс завдань (рис.1.2)

Дублювання інформації є одним із найефективніших способів забезпечення цілісності інформації. Воно забезпечує захист інформації, як від випадкових загроз, і від навмисних впливів. Для дублювання інформації можуть застосовуватися не тільки незнімні носії інформації або спеціально розроблені для цього пристрою, а й звичайні пристрої зі знімними носіями. Поширеними методами дублювання даних у КС є використання виділених областей пам'яті на робочому диску та дзеркальних дисків (жорсткий диск з інформацією, ідентичною як на робочому диску).

Рисунок 1.2 Завдання захисту інформації у КС від випадкових загроз

Під надійністю розуміється властивість системи виконувати покладені на неї функції за певних умов обслуговування та експлуатації.

Надійність КС досягається на етапах розробки, виробництва, експлуатації. Важливим напрямом у забезпеченні надійності КС є своєчасне виявлення та локалізація можливих несправностей у роботі її технічних засобів. Значно скоротити можливості внесення суб'єктивних помилок розробників дозволяють сучасні технології програмування.

Відмовостійкість - це властивість КС зберігати працездатність при відмови окремих пристроїв, блоків, схем. Відомі три основних підходи до створення відмовостійких систем: просте резервування (використання пристроїв, блоків, вузлів, схем, лише як резервні); завадостійке кодування інформації (робоча інформація доповнюється спеціальною контрольною інформацією-кодом, яка дозволяє визначати помилки та виправляти їх); створення адаптивних систем, які передбачають збереження працездатного стану КС за деякого зниження ефективності функціонування у разі відмов елементів.

Блокування помилкових операцій. Помилкові операції в роботі КС можуть бути викликані не лише випадковими відмовами технічних та програмних засобів, а й помилками користувачів та обслуговуючого персоналу. Для блокування помилкових дій використовуються технічні та апаратно-програмні засоби, такі як

блокувальні тумблери, запобіжники, засоби блокування запису на магнітні диски та інші.

Оптимізація. Одним з основних напрямків захисту є скорочення кількості помилок користувачів і персоналу, а також мінімізація наслідків цих помилок. Для досягнення цих цілей необхідні: наукова організація праці, виховання та навчання користувачів та персоналу, аналіз та вдосконалення процесів взаємодії людини та КС.

Мінімізація збитків. Запобігти стихійним лихам людина поки що не в змозі, але зменшити наслідки таких явищ у багатьох випадках вдається. Мінімізація наслідків аварій та стихійних лих для об'єктів КС може бути досягнута шляхом: правильного вибору місця розташування об'єкта (подалі від місць, де можливі стихійні лиха); обліку можливих аварій та стихійних лих при розробці та експлуатації КС; організації своєчасного оповіщення про можливі аварії; навчання персоналу боротьби зі стихійними лихами та аваріями, методами ліквідації їх наслідків.

1.4 Захист КС від несанкціонованого втручання

Основним способом захисту від зловмисників вважається використання про засобів ААА, чи 3А (аутентифікація, авторизація, адміністрування).

Авторизація (санкціонування, дозвіл) – процедура, за якою користувач при вході в систему опізнається та отримує права доступу, дозволені системним адміністратором, до обчислювальних ресурсів (комп'ютерів, дисків, папок, периферійних пристроїв).

Авторизація виконується програмою і включає ідентифікацію та аутентифікацію.

Ідентифікація – надання ідентифікатора, яким може бути несекретне ім'я, слово, число, реєстрації користувача в КС. Суб'єкт вказує ім'я користувача, що пред'явлений ідентифікатор порівнюється з переліком ідентифікаторів. Користувач, у якого ідентифікатор зареєстровано у системі, розцінюється як правомочний

(легальний). Синонімом ідентифікатора є логін – набір літер та цифр, унікальний для даної системи.

Аутентифікація – автентифікація, тобто те, що пред'явлений ідентифікатор дійсно належить суб'єкту доступу. Виконується на основі зіставлення імені користувача та пароля. Після автентифікації суб'єкту дозволяється доступом до ресурсів системи з урахуванням дозволених йому повноважень.

Найчастіше застосовуваними методами авторизації є методи, засновані на використанні паролів (секретних послідовностей символів). Пароль можна встановити на запуск програми, окремі дії на комп'ютері або мережі. Крім паролів для підтвердження справжності можуть використовуватись пластикові картки та смарт-картки.

Адміністрація – це реєстрація дій користувача в мережі, включаючи спроби доступу до ресурсів. Для своєчасного припинення несанкціонованих дій, для контролю за дотриманням встановлених правил доступу необхідно забезпечити регулярний збір, фіксацію та видачу за запитами відомостей про всі звернення до комп'ютерних ресурсів, що захищаються. Основною формою реєстрації є програмне ведення спеціальних реєстраційних журналів, що є файлами на зовнішніх носіях інформації.

Найчастіше виток інформації відбувається шляхом несанкціонованого копіювання інформації. Ця загроза блокується:

- методами, що ускладнюють зчитування скопійованої інформації. Засновані на створенні в процесі запису інформації на відповідні накопичувачі таких особливостей (нестандартна розмітка, форматування, носія інформації, встановлення електронного ключа), які не дозволяють зчитувати отриману копію на інших накопичувачах, що не входять до складу КС, що захищається. Іншими словами, ці методи спрямовані на забезпечення сумісності накопичувачів лише усередині цієї КС .

- методами, що перешкоджають використанню інформації. Ускладнюють використання отриманих копіюванням програм та даних. Найбільш ефективним у цьому відношенні засобом захисту є зберігання інформації у перетвореному

криптографічними методами вигляді. Іншим методом протидії несанкціонованого виконання скопійованих програм є використання блоку контролю середовища розміщення програми. Він створюється при інсталяції програми та включає характеристики середовища, в якому розміщується програма, а також засоби порівняння цих характеристик. Як характеристики використовуються характеристики ЕОМ чи носія інформації.

Для захисту КС від різноманітних шкідницьких програм (вірусів) розробляють спеціальні антивірусні засоби.

Антивірусна програма – частина програмного забезпечення, яка встановлюється на комп'ютер, щоб шукати на дисках та у вхідних файлах комп'ютерні віруси та видаляти їх при виявленні .

Програма виявляє віруси, пропонуючи вилікувати файли, а за неможливості видалити. Існує кілька різновидів антивірусних програм:

- сканери або програми-фаги – це програми пошуку у файлах, пам'яті, завантажувальних секторах дисків сигнатур вірусів (унікального програмного коду саме цього вірусу), перевіряють та лікують файли;

- монітори (різновид сканерів) – перевіряють оперативну пам'ять при завантаженні операційної системи, автоматично перевіряють усі файли в момент їх відкриття та закриття, щоб не допустити відкриття та запис файлу, зараженого вірусом; блокує віруси;

- імунізатори - запобігають зараженню файлів, виявляють підозрілі дії при роботі комп'ютера, характерні для вірусу на ранній стадії (до розмноження) і надсилають користувачеві відповідне повідомлення;

- ревізори – запам'ятовують вихідний стан програм, каталогів до зараження та періодично (або за бажанням користувача) порівнюють поточний стан з вихідним;

- лікарі – як знаходять заражені вірусами файли, а й “лікують” їх, тобто видаляють з файлу тіло програми-вірусу, повертаючи файли у вихідний стан;

- блокувальники – відстежують події та перехоплюють підозрілі дії (вироблені шкідливою програмою), забороняють дію або вимагають дозволу користувача.

1.5 Криптографічні методи захисту інформації та міжмережеві екрани

Ефективним засобом протидії різним загрозам інформаційної безпеки є закриття інформації методами криптографічного (від грец. Kryptos – таємний) перетворення. У результаті такого перетворення інформація, що захищається, стає недоступною для ознайомлення та безпосереднього використання особами, які не мають на це повноважень. По виду на вихідну інформацію криптографічні методи поділені на такі види.

Шифрування – процес маскування повідомлень або даних з метою приховування їхнього змісту, обмеження доступу до змісту інших осіб. Полягає у проведенні оборотних математичних, логічних, комбінаторних та інших перетворень вихідної інформації, у яких зашифрована інформація є хаотичний набір букв, цифр, інших символів і двійкових кодів. Для шифрування використовуються алгоритм перетворення та ключ.

Стеганографія – метод захисту комп'ютерних даних, що передаються каналами телекомунікацій, шляхом приховування повідомлення серед відкритого тексту, зображення або звуку у файлі-контейнері. Дозволяє приховати не тільки зміст інформації, що зберігається або передається, але і сам факт зберігання або передачі закритої інформації. Прихований файл можна зашифрувати. Якщо хтось випадково виявить прихований файл, то зашифрована інформація буде сприйнята як збій у роботі системи.

Кодування – заміна змістових конструкцій вихідної інформації (слів, речень) кодами. Як коди можуть використовуватися поєднання букв, цифр. При кодуванні та зворотному перетворенні використовуються спеціальні таблиці або словники, що зберігаються в секреті. Кодування широко використовується для захисту від спотворень в каналах зв'язку.

Метою стиснення інформації є скорочення обсягів інформації. У той же час, стиснена інформація не може бути прочитана або використана без зворотного перетворення. Враховуючи доступність засобів стиснення та зворотного

перетворення, ці методи не можна розглядати як надійні засоби криптографічного перетворення інформації. Тому стислі файли піддаються шифруванню.

Розсічення-рознесення полягає в тому, що масив даних, що захищаються, ділиться (розсікається) на такі елементи, кожен з яких окремо не дозволяє розкрити зміст інформації, що захищається. Виділені таким чином елементи даних розносяться різними зонами ЗУ або розташовуються на різних носіях.

Електронний цифровий підпис (ЕЦП) являє собою рядок даних, який залежить від деякого секретного параметра (ключа), відомого тільки особі, що підписує, і від змісту підписуваного повідомлення, представленого в цифровому вигляді. Використовується для підтвердження цілісності та авторства даних, не можна змінити документ без порушення цілісності підпису.

Для блокування загроз, що виходять із загальнодоступної системи, використовується спеціальний програмний чи апаратно-програмний засіб, який отримав назву міжмережевий екран (МЕ) або fire wall. МЕ дозволяє розділити загальну мережу на дві або більше частини і реалізувати набір правил, що визначають умови проходження пакетів з даними через кордон з однієї частини загальної мережі в іншу. Іноді мережевий захист повністю блокує трафік зовні, але дозволяє внутрішнім користувачам вільно зв'язуватися із зовнішнім світом. Зазвичай МЕ захищають внутрішню мережу підприємства від вторгнень із глобальної мережі Інтернет. Міжмережевий екран виконує чотири основні функції:

- Фільтрування даних на різних рівнях;

- використання екрануючих агентів (proxy-сервери), які є програмами-посередниками та забезпечують з'єднання між суб'єктом та об'єктом доступу, а потім пересилають інформацію, здійснюючи контроль та реєстрацію;

- трансляція адрес – призначена приховування від зовнішніх абонентів справжніх внутрішніх адрес;

- реєстрація подій у спеціальних журналах. Аналіз записів дозволяє зафіксувати спроби порушення встановлених правил обміну інформацією в мережі та виявити зловмисника.

Висновок до першого розділу

Інформаційна безпека досягається шляхом управління відповідним рівнем політики інформаційної безпеки. Основним документом для реалізації політики інформаційної безпеки є план інформаційної безпеки. Цей документ розроблено як офіційний керівний документ для вищих керівних органів держави, відомства та організації. У документі визначено цілі політики інформаційної безпеки та основні напрями вирішення мандата Конституційного Суду щодо захисту інформації. План інформаційної безпеки також містить загальні вимоги та принципи побудови системи захисту інформації в КС.

В першому розділі було розглянуто поняття інформаційної безпеки. Також було описано основні загрози безпеці та їх повний опис . проведено аналіз методів захисту інформації.

РОЗДІЛ 2
АНАЛІЗ ПІДПРИЄМСТВА ТА ЗАСОБІВ РЕАЛІЗАЦІЇ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Місія системи захисту полягає в тому, щоб забезпечити збереження та передачу даних компанії, що зберігаються на персональному робочому комп'ютері співробітника, захищено від втрати або пошкодження через відключення електроенергії, крадіжки, а також зміцнити існуючі системи безпеки від несанкціонованого проникнення, крадіжки або пошкодження. інформації. В рамках даної роботи не буде розглядатися вдосконалення системи безпеки мережі ТОВ «РДВ», оскільки ІТ-відділ компанії регулярно перевіряє лінії зв'язку, мережеве та серверне обладнання, а також підтримує програмне забезпечення, що захищає основний сервер компанії від зовнішніх вторгнень, крім що Поза роботою ІТ-відділу також будуть розглянуті заходи щодо підвищення рівня безпеки даних, що зберігаються на персональних комп'ютерах співробітників.

2.1 Організаційно- функціональний устрій компанії

У цьому розділі розглядається ієрархічна організація та функціональна структура компанії (рисунок 1), яка є деревоподібною структурою з різними ієрархіями.

Сферу діяльності компанії представляють відповідні підрозділи:

• Системна інтеграція - Розробка та реалізація унікальних проектів від етапу проектування до урочистого відкриття:

1. Конференц-зал.
2. Кімната для переговорів.
3. Диспетчерсько-ситуаційний центр.
4. Спортивні споруди та концертні зали.
5. Кімната 3D модуляції.

6. Керівник робочого місця.

• Оренда обладнання для презентацій, конференцій, виставок та заходів, створення інтерактивних презентацій, що демонструють орендоване обладнання.

• Авторизовані центри ремонту та гарантійного обслуговування надають технічну підтримку та післяпродажне обслуговування.

• Розповсюджуйте продукцію від провідних виробників аудіотехнічного обладнання, щоб забезпечити своєчасну доставку.

• IT-відділ займається установкою програмного забезпечення, встановленням та моніторингом комп'ютерних технологій, виявленням та усуненням збоїв у системі інформаційної безпеки компанії

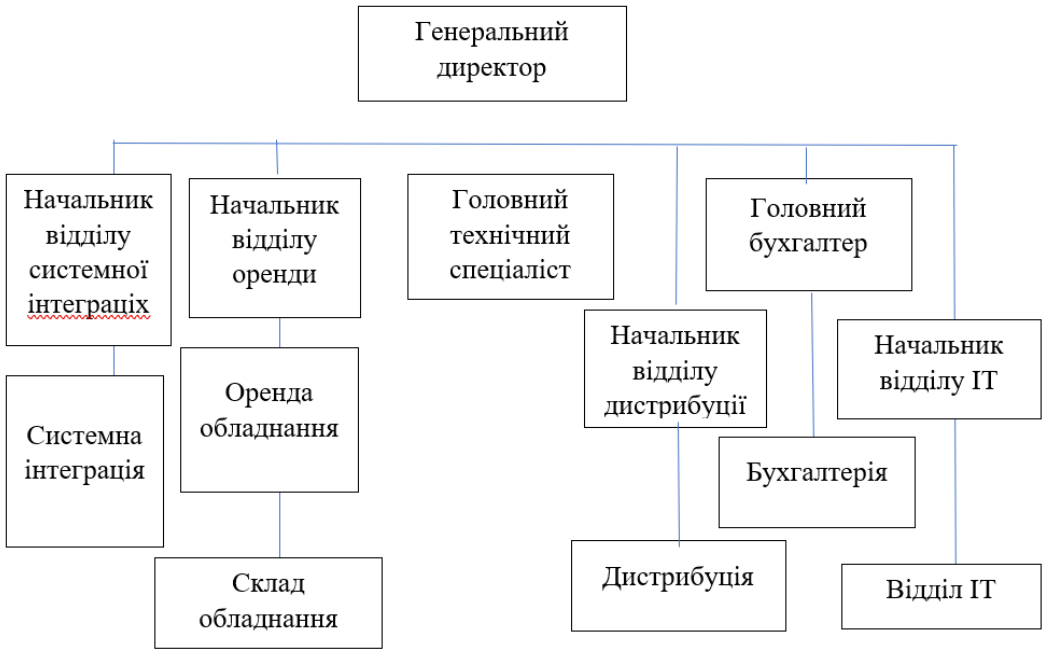

Рисунок 3 Організаційно-функціональна структура

2.2 Аналіз ризиків інформаційної безпеки

Відповідно до наказу генерального директора від 12 жовтня 1998 року, компанія проводить аналіз ризиків інформаційної безпеки один раз на місяць. Начальник відділу інформаційних технологій приймає рішення щодо аналізу ризиків. Кожен відділ готує звіт про всі випадки порушення інформаційної безпеки, щоб IT-відділ міг додатково розслідувати та вжити заходів, щоб запобігти

повторенню інциденту. Щокварталу профілактичні огляди ліній зв’язку на предмет прослуховування, обривів та перешкод. Щокварталу профілактичні огляди засобів захисту на предмет порушення. Основні аспекти інформаційної безпеки в ТОВ «РДВ»:

• Відділ IT-безпеки визначає прогалини безпеки та інші проблеми під час обробки інформації. Відділ IT-безпеки приймає рішення щодо усунення несправностей за результатами профілактичних перевірок і службових записок, а команда управління системою несе безпосередню відповідальність за їх вирішення.

• Необхідні витрати визначаються працівниками відділу, розподіл достатніх витрат на інформаційну безпеку здійснюється за погодженням з генеральним директором, у разі його відсутності - за погодженням з технічним директором.

• Вибір конкретних заходів, методів, інструментів і систем безпеки залежить від працівників IT-безпеки за консультацією з командою управління системою.

2.3 Ідентифікація та оцінка інформаційних активів

Інформаційні активи є компонентами або частинами загальної системи, в яку організація безпосередньо інвестує і тому вимагає від організації захисту. Причини вибору активу:

• Конфіденційна інформація (документи компанії, електронні листи) – цей актив містить документи, що містять конфіденційну інформацію про фінансову діяльність WFD, співробітників, контракти та іншу діяльність компанії, яку не повинні отримувати треті сторони. Електронний зв’язок працівника має бути захищений, оскільки він може містити зв’язок із клієнтами та додаткові документи.

• Зберігання файлів на спільних мережевих дисках. Спільні мережеві диски використовуються для швидкого обміну великими обсягами інформації між співробітниками компанії, яка може містити проміжні версії вмісту, підготовленого для клієнтів на додаток до документів. Ця інформація є суворо конфіденційною і не повинна бути розголошена ні за яких обставин

Таблиця 1

Оцінка інформаційних активів компанії

Вид діяльності	Найменуванн активу	Форма уявлення	Власник	Критерій визначення вартості	Розмірність оцінки	
					Кількість. (тис.грн)	Якісна
Конфіденційна інформація (документи компанії, електронні повідомлення)	Документ	Електронний Матеріальни об'єкт	Творець, Керівництво	Довіра клієнтів, репутація	-	Висока
Сховище файлів на спільному мережному диску	Документ, Програмне забезпечення	Електронна	Творець, Керівництво	Довіра клієнтів, репутація	-	Висока
Захист персональних комп'ютерів працівників від вірусних атак та збоїв, пов'язаних із неполадками в електромережі	Програмне Забезпечення обладнання	Електронна, Матеріальни об'єкт	Група системного адміністрування	Ціна ліцензійного забезпечення, обслуговування	420	Висока
Захист від незаконного проникнення	Охоронне устаткування	Матеріальни об'єкт	Керівництво, підрозділ охорони	Початкова вартість, обслуговування	315,6	Висока

.

• Захист комп'ютерів співробітників від вірусних атак і збоїв в мережі. Через високу початкову вартість і так само важливе для збереження інформації компанії необхідно забезпечити захист програмного та апаратного забезпечення.

• Запобігання вторгненню. Забезпечення обладнання для запобігання вторгненню в приміщення компанії є першою лінією захисту у захисті та попередженні зловмисників про потенційні вторгнення в конфіденційні справи компанії. Несправність обладнання безпеки може призвести до серйозних фінансових втрат, включаючи ремонт і відновлення, а також втрату конфіденційної інформації. Конфіденційна інформація:

• Бухгалтерські документи – відомості про заробітну плату працівників, податкові декларації, доходи та витрати підприємства.

• Персональна інформація - Інформація про співробітників, які працюють у компанії.

• Інформація про контракт – дані про поточні та виконані контракти, інформація про суму контракту, послуги, що надаються компаніями та клієнтами.

• Інформація про склад – обладнання, доступне компанії. Наявність інвентаризації та отримані та видані звіти.

• Інформація про архітектуру системи компанії та її впровадження для запобігання вірусним атакам і несанкціонованим вторгненням.

• Вимоги щодо забезпечення професійної конфіденційності працівників компанії. Для загальної оцінки активів зазвичай використовується метод ранжування, і кожному активу присвоюється певна оцінка (номер) із зазначенням його вартості відносно інших активів. Чим вище ранг, тим важливіший актив. У таблиці 3 наведено оцінку активів за експертною оцінкою начальника відділу інформаційних технологій:

Таблиця 2

Результати оцінки активів

Найменування активу	**Цінність активу (ранг)**
Престиж компанії	1
Інформація	1
Активне обладнання	2
Мережеве і северне обладнання	2
Програмне забезпечення	3

Активами, що мають найбільшу цінність, є - конфіденційна інформація та престиж компанії.

2.4 Оцінка вразливості активів

У цьому розділі визначаються вразливі місця в предметних областях (Таблиця 3), які потенційно можуть бути використані як джерело загроз для компрометації активів і ділової діяльності компанії через їх використання. Відкриті бази даних в Інтернеті використовуються як джерела інформації для оцінки вразливості активів.

Опис уразливості предметної області:

• Уразливості в системах безпеки – які можуть призвести до крадіжки та пошкодження обладнання, викрадення та використання конфіденційної інформації

компанії, а також заміни чи знищення конфіденційної інформації. • Нестабільна робота живлення (коливання напруги або повне відключення електроенергії) – якщо персональний робочий комп’ютер працівника вимкнено або перезавантажено в аварійній ситуації, а також у разі пошкодження апаратного забезпечення, незбережена інформація може бути втрачена.

Таблиця 3

Ідентифікація уразливостей предметної області

Група вразливостей / Зміст вразливості	Престиж компанії	інформація	Мережеве обладнання	Серверне обладнання	Програмне забезпечення
1. Середовище та інфраструктура					
Вразливість у системі охорони	висока	висока	висока	висока	висока
Нестабільна робота електромережі (коливання напруги або повне відключення електроенергії)	низкая	висока	висока	висока	середня
2. Апаратне забезпечення					
Вразливості у мікропрограмному забезпеченні	середня	висока	середня	середня	середня
3. Програмне забезпечення					
Критичні вразливості засобів антивірусного захисту та контролю доступу	висока	висока	низька	низька	висока
4. Комунікації					
Проведення атаки на відмову в обслуговуванні	середня	середня	висока	висока	середня
5. Документи (документообіг)					
Розкрадання документів	висока	висока	низька	низька	середня
6. Персонал					
Використання методів соціальної інженерії	середня	середня	низька	низька	середня
7. Загальні вразливі місця					
Не визначено					

• Уразливість мікропрограми - можна використовувати для відключення корпоративних пристроїв.

• Критичні антивірусні уразливості та вразливості контролю доступу – можуть використовуватися для крадіжки, заміни, знищення конфіденційної інформації та втручання в локальну мережу компанії.

• Атаки відмови в обслуговуванні – можуть призвести до збою в локальній мережі компанії та обмежити можливість співробітників обмінюватися інформацією.

• Крадіжка документів – може призвести до вимагання з боку керівництва компанії або окремих співробітників, заманити співробітників в іншу компанію та використовувати інформацію про замовлення для перехоплення товарів клієнтів.

• Використання методів соціальної інженерії – може призвести до розшифровки даних аутентифікації співробітників, бізнес-інформації, інформації про контракт, архітектури системи безпеки (розташування камери, датчиків руху).

2.5 Оцінка загроз активам

Загроза є основною причиною події, яка може завдати шкоди системі чи організації, тоді як інцидент (інцидент інформаційної безпеки) — це будь-яка непередбачена або несприятлива подія, яка може порушити діяльність організації або інформаційну безпеку. Основою для оцінки загроз активів є необхідність їх опису в цій статті. У IT-відділі інформації про такі оцінки немає.

Джерелом загрози може бути:

• Недбалість або неправильна поведінка співробітників, що може призвести до пошкодження обладнання, яке зберігає та обробляє конфіденційну інформацію, ненавмисне спотворення інформації (наприклад, при заміні старих файлів на нові) або її видалення.

Раптовість таких загроз може завдати значної шкоди бізнесу. Неповідомлення співробітників-порушників про інцидент і невжиття заходів щодо усунення загрози може призвести до значної фінансової шкоди компанії. Через відсутність інформації

щодо оцінки загроз активам важко визначити частоту таких загроз, проте ця загроза, безсумнівно, є однією з найпоширеніших.

• Природні, техногенні та природні катаклізми - надзвичайні ситуації, не пов'язані або опосередковано з діяльністю людини, такі як пожежа, повінь, землетрус, саморуйнування будівель, що зберігають обладнання та обробляють інформацію, через порушення техніки будівництва або інших факторів у населених пунктах. наслідки аварії Під час процесу або під час евакуації персоналу він може бути пошкоджений або знищений, а порушники можуть проникнути в будівлю на ім’я пожежників, рятувальників тощо. Поруч з будівлею компанії будуються чотири нові офісні будівлі, тому ризик нещасних випадків з людьми зростає.

• Погрози з боку третіх осіб або умисні дії осіб, такі як захоплення будівель зловмисниками, вандалізм, страйки, терористичні акти, місцеві заворушення, що супроводжуються нападами на будівлі компанії тощо. Поведінка, створена зловмисниками для проникнення в будівлі та отримання секретної інформації та обладнання.

На основі оцінки загроз для активів підготовлено таблицю 2.5 для опису та якісної оцінки можливих загроз для активів.

Таблиця 4

Результати оцінки загроз активам

Категорія загроз	**загрози**	**Актив**	
		Інформація	**Престиж компанії**
Недбалість персоналу або їх помилкові дії	Ненавмисне псування обладнання	Середня	Середня
	Ненавмисне розголошення інформації	Висока	Висока
	Ненавмисне псування або втрата інформації, включаючи носії інформації	Висока	Висока
Стихійні та природні катаклізми	Пожар	Висока	Висока
	Обвалення будівлі внаслідок порушення технології будівництва	Висока	Висока
Загрози з боку третіх осіб або навмисні дії персоналу	Умисне псування або виведення з ладу обладнання	Середня	Средняя
	Несанкціоноване отримання конфіденційної інформації	Висока	Висока
	Викрадення носіїв інформації	Висока	Висока

2.6 Оцінка існуючих та запланованих заходів

Відділ інформаційних технологій компанії відповідає за інформаційну безпеку. Серед запобіжників від проникнення в будівлю є два безпечних місця з турнікетом, який можна відкрити за допомогою смарт-картки або чергування охоронцями 24/7.

Доступ до службового входу обмежений дверима з електронними замками та відеотелефонами.

Доступ до вантажного входу доступний лише за домовленістю та заздалегідь запланованим часом, але він не захищений, оскільки двері вантажного входу відкриваються лише зсередини і лише тоді, коли ліфт знаходиться на першому поверсі.

Двері кожного офісу зачиняються на магнітні замки, які відкриваються на персональні смарт-картки (пропуски) співробітників компанії. Вночі в кожній кімнаті горить будильник. Будильник для певних приміщень можна вибірково вмикати та вимикати, наприклад, для ночівлі співробітників. Проте перепустки звільненого працівника не розшифровуються, а залишаються у відповідному відділі технолога; якщо зловмисник отримує місце для зберігання цих пропусків, він може не тільки увійти в офіс, а й безперешкодно пройти через вхід в будівлю Турнікет форпосту. Схема системи безпеки показана на рисунках 1 і 2

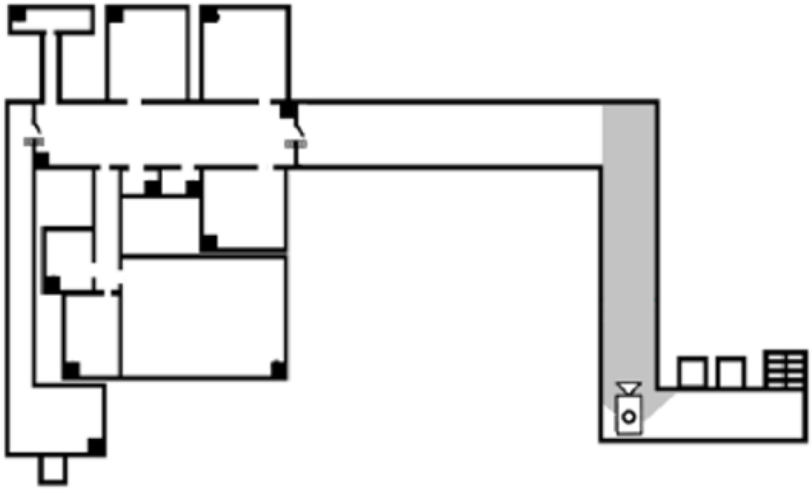

Рисунок 4 Реалізація системи відеозахисту

На кожному поверсі громадського коридору є камера відеоспостереження, але громадський коридор має L-подібну форму, тому охорона не може стежити за кутовими кімнатами.

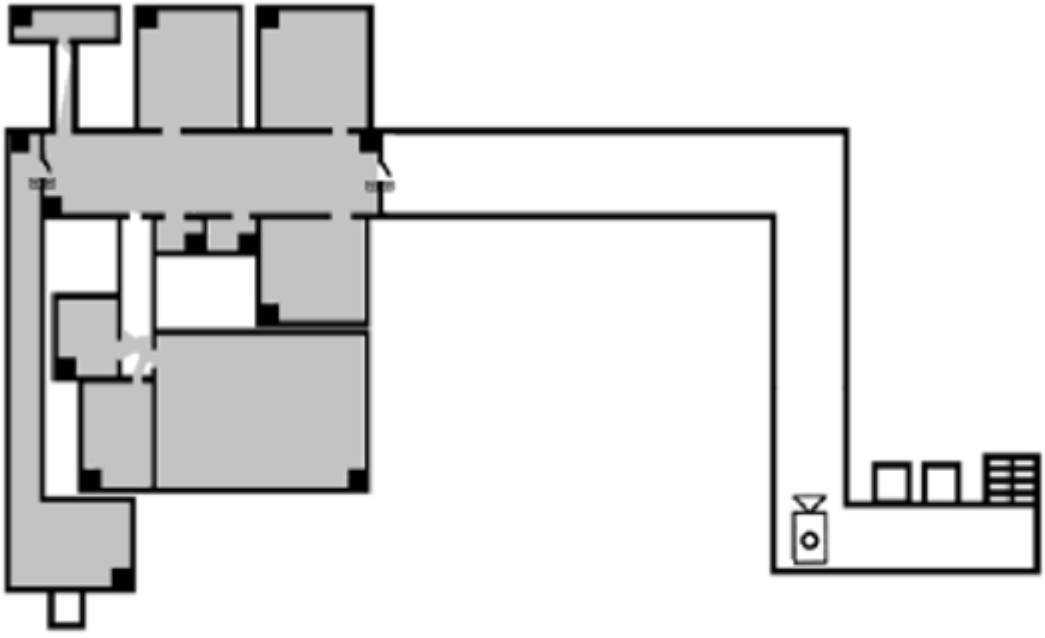

Рисунок 5 Інфрачервоні датчики руху

Відеоспостереження здійснюється купольними камерами SAMSUNG SCC-B5366B з такими технічними характеристиками:

• Тип камери – купольна аналогова.

• Кольоровість – кольорова.

• Матриця – 1/3» Super HAD IT.

• Об'єктив – варифокальний діапазон фокусних відстаней 2,5 – 6 мм.

• Роздільна здатність – 600 ТБ ліній.

• Чутливість – 0,12 лк (15 IRE) у кольоровому режимі та 0,012 лк (15 IRE) у чорно-білому.

• Співвідношення сигнал/шум – більше 52 дБ при вимкненому АРУ.

• День/ніч – кольоровий/монохромний/автоматичний.

• Баланс білого – більше 52 дБ при вимкненому АРУ.

• Електронний затвор (швидкість) – 1/50 – 1/10000.

• Автодіафрагма – керована сигналом постійного струму DC або фіксована.

• BLC (компенсація зустрічного засвічення).

• Екранне меню російською мовою.

• Детектор руху.

• Інтерфейс RS-485 та CCVC.

• Живлення – 12 В DC та 24 В AC.

• Діапазон робочих температур – 10 – +50 градусів за Цельсієм.

• Габарити – 128x78 мм.

• Вага – 330 г.

Рисунок 6 Камера SAMSUNG SCC-B5366B

В офісі є інфрачервоні датчики руху. Однак вони є єдиним засобом оповіщення охоронців, тому при спрацьовуванні охоронних датчиків не буде даних ні про проникнення зловмисників, ні про їхню кількість.

Системи антивірусного захисту на більшості комп’ютерів або відсутні, або не діють через особисту ворожість більшості співробітників до того, що системи антивірусного захисту уповільнюють роботу персональних робочих комп’ютерів. Заходи безпеки інформації не вживаються.

Доступ до комп’ютера кожного співробітника обмежено персональним паролем. Доступ до спільних мережевих дисків також обмежений паролем, але на більшості комп’ютерів цей пароль вводиться автоматично, щоб прискорити процес підключення. Персональні робочі комп'ютери всіх співробітників підключені до локальної мережі компанії та мають доступ до Інтернету. Технічна структура компанії показана на рисунку 4

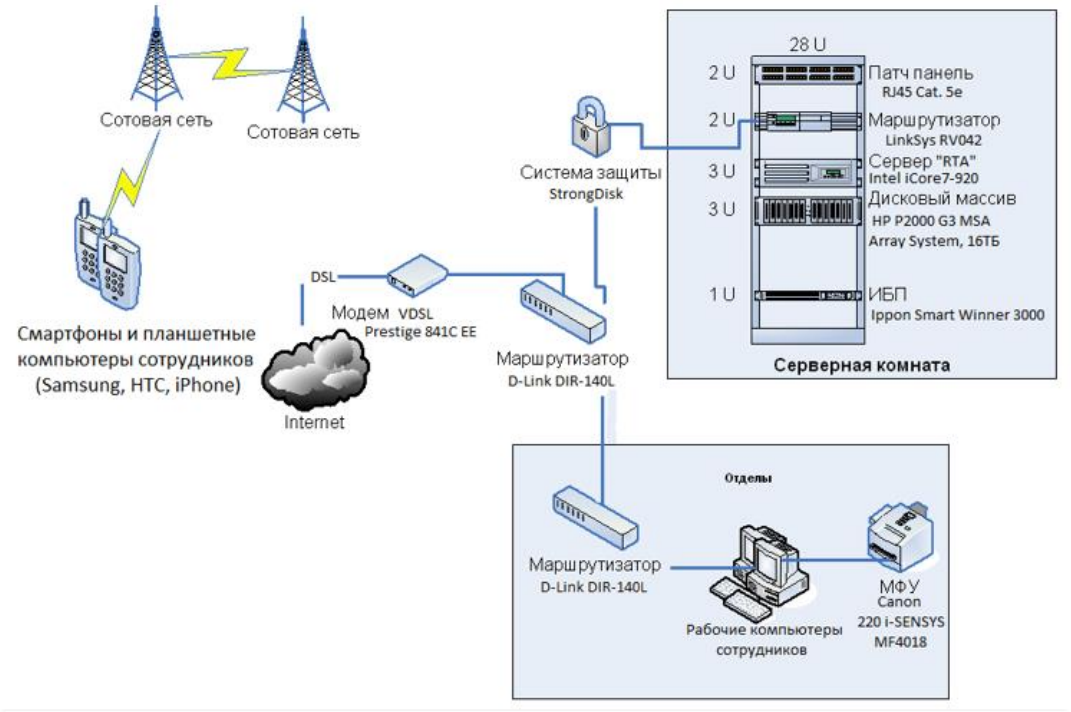

Рисунок 7 Технічна архітектура компанії

Для підключення до Інтернету використовується модем Prestige 841C EE, а для підключення комп’ютера до локальної мережі – маршрутизатор D-Link DIR-140L.

Основний сервер — це серверна шафа з процесором Intel iCore7 з дисковим масивом HP P2000 G3 MSA Array System ємністю 16 ТБ, маршрутизатором LynkSys RV042 і патч-панеллю RJ45 Cat. 5e та джерело безперебійного живлення Ippon Smart Winner 3000.

Комп’ютери співробітників збираються з компонентів всередині компанії, і їх конфігурації сильно відрізняються. Кожен відділ має МФУ Canon 220 i-SENSYS MF 4018.

Персональний робочий комп’ютер співробітника – Windows7 Ultimate або Windows XP Professional і Microsoft Office 2003, 2007 або 2010, а також Windows Server 2012 і Oracle Database Administration.

Більш детального опису технічних характеристик Міністерство інформаційних технологій не надало. У цій статті розглядається розвиток захисту від крадіжки інформації, тому є лише один актив, який слід розглянути: конфіденційна корпоративна інформація, в тому числі:

• Дані аутентифікації користувачів – паролі співробітників, знаючи які паролі, зловмисники мають доступ до їхніх жорстких дисків і вмісту спільних мережевих дисків.

• Дані про поточні контракти компанії - замовлення оренди обладнання, написання програмного забезпечення або інші види діяльності. За результатами аналізу існуючих відновлювальних заходів підготовлено таблицю рівня безпеки активів.

Таблиця 5

Ступінь забезпечення безпеки активів

Актив	**Оцінюється критерій**	**Результат аналізу**	**Вплив на безпеку**
Дані аутентифікації	Зберігання	У пам'яті співробітників, або у паперовому вигляді	Високе

користувачів	Доступність	Індивідуальна для кожного працівника	Високе
Дані про поточні договори компанії	Зберігання	У цифровому вигляді на жорстких дисках особистих ноутбуків керівників проектів, або у паперовому вигляді у особистих сейфах керівників проектів, або тимчасове зберігання на загальному мережевому диску	Середнє
	Доступність	Індивідуальна для керівників проектів або практично у всіх співробітників компанії	Середнє

Для зниження рівня загрози для активів було проведено аналіз, у результаті якого було складено перелік запланованих заходів щодо захисту активів:

• Звести до мінімуму зберігання інформації в паперовій формі та перетворити її в цифрову форму.

• Інформація, що зберігається на папері після відтворення в цифровому вигляді, знищується.

• Примусово вимкнути автоматичний введення пароля під час підключення до мережевого диска.

• Забезпечити встановлення антивірусних засобів на комп'ютерах співробітників.

• Скасування звільнень для звільнених працівників, щоб запобігти їх використанню для несанкціонованого доступу до офісів компанії.

• Обладнати коридори загального користування додатковими камерами відеоспостереження.

• Оснащений камерами відеоспостереження на додаток до ІЧ-датчиків руху для перетворення приміщення.

2.7 Оцінка ризиків

Ризик характерний для ситуації, коли результат невизначений, і повинні бути несприятливі наслідки, такі як пошкодження або втрата. Ризик має такі властивості:

• Невизначеність. Ризик існує тоді і тільки тоді, коли можливий більш ніж один розвиток.

• Втрата. Ризик існує, коли результат може мати негативний вплив.

• Наявність аналітики. Ризик існує лише тоді, коли формується «передбачувана» суб'єктивна думка про ситуацію та проводиться якісна чи кількісна оцінка негативних подій у майбутньому періоді.

• Значення. Ризик існує, коли подія має практичне значення та зачіпає інтереси хоча б одного суб'єкта. Характеристики ризику:

• Захисний – показує, що ризик є нормальним станом речей для суб'єктів господарювання, тому слід виховувати раціональне ставлення до невдач.

• Аналіз – існування ризику вимагає вибору одного з можливих варіантів прийняття правильного рішення.

• Інновації – проявляються у стимулюванні дослідження нетрадиційних рішень проблем.

• Регулювання – суперечливого характеру, що має дві форми: конструктивну та деструктивну. Щоб оцінити ризик, потрібно розуміти такі засоби контролю:

• Цінності – інформація, яку потрібно захищати.

• Загрози – шкідливі елементи, інформація щодо яких захищена.

• Наслідки – проблеми, які можуть виникнути після успішної реалізації загрози.

• Заходи захисту – комплекс заходів для запобігання загрозам. Оскільки компанія не проводила окремої оцінки ризиків інформаційної безпеки, її оцінювали виключно для цієї роботи.

Результати оцінки наведені в таблиці 6 і умовно впорядковані від 1 (найвищий) до 5 (найнижчий) відповідно до ступеня ризику.

Таблиця 6

Результати оцінки ризиків інформаційним активам компанії

Ризик	Актив	Ранг ризика
Збій або злом систем антивірусного захисту та засобів контролю доступу	Престиж компанії, конфіденційна інформація, дані аутентифікації працівників	1
Розкрадання документів	Престиж компанії, конфіденційна інформація, дані аутентифікації працівників (залежить від рівня підготовки зловмисника)	2
Відмова системи охорони проти несанкціонованого проникнення	Престиж компанії, конфіденційна інформація, дані аутентифікації працівників (залежить від рівня підготовки зловмисника)	3
Збій апаратного забезпечення	Конфіденційна інформація, активне обладнання	4
Збій систем комунікацій та недбалість персоналу у сфері збереження інформації	Престиж компанії, конфіденційна інформація	5

Тож виходить, що найбільший ризик – це репутація компанії та конфіденційна інформація, а також дані аутентифікації співробітників.

2.8 Вибір комплексів завдань із захисту інформації та захисту інформації

Завдання, що виконуються підприємствами та наявні ризики, характеристики існуючих засобів захисту інформації Спектр завдань із забезпечення безпеки та захисту інформації включає:

• Звести до мінімуму зберігання інформації в паперовій формі та оцифрувати її, передбачивши резервне копіювання для відновлення в разі збою

Рисунок 8 Комплекс завдань із забезпечення захисту інформації

• Інформація, що зберігається на папері після відтворення в цифровому вигляді, знищується.

• Примусово вимкнути автоматичний введення пароля під час підключення до мережевого диска.

• Запровадити антивірусний захист на комп'ютерах співробітників та встановити автоматичне оновлення антивірусних баз та операційних систем на робочих комп'ютерах працівників

• Розшифруйте звільнення звільнених працівників, щоб уникнути несанкціонованого доступу до офісів компанії.

• Обладнати коридори загального користування додатковими камерами відеоспостереження.

• Оснащений камерами відеоспостереження на додаток до ІЧ-датчиків руху для перетворення приміщення.

На наступному рисунку показано схематичне розташування набору завдань інформаційної безпеки. Завдання, що вирішуються в рамках цієї роботи,виділені темнішим фоном.

2.9 Визначення позиції очікуваного набору завдань у наборі завдань підприємства та уточните завдання інформаційної безпеки та захисту інформації

Місцем для виконання комплексу завдань, описаних у попередньому розділі, є офісні приміщення ТОВ «РДВ». Завдання обмежується розробкою систем запобігання крадіжок інформації в товаристві з обмеженою відповідальністю «РДВ», що включає в себе вдосконалення існуючих систем захисту безпеки та опис заходів, призначених для більш безпечного зберігання інформації на комп'ютерах співробітників і спільних мережах під час водіння.

2.10 Вибір заходів захисту

2.10.1 Вибір організаційних заходів

Як організаційні заходи рекомендується провести такі заходи:

Таблиця 7

Вибір організаційних заходів

Подія	**Організаційний захід**
Провести повідомлення співробітників компанії про нерозголошення їхніх паролів, заборонити вимикати систему антивірусного захисту з поясненням можливих наслідків недотримання цих запобіжних заходів	Випуск наказу та доведення його до відома начальників кожного підрозділу, що бере участь в обігу конфіденційної інформації компанії
Провести повідомлення керівників проектів про нерозголошення та надійне зберігання документів, що містять дані про поточні проекти компанії	Організація зборів із керівниками проектів

2.10.2 Вибір інженерних заходів

Як інженерний захід, поточні системи безпеки будуть оновлені для підвищення безпеки та моніторингу, а також буде встановлено додаткове обладнання для підвищення стабільності комп’ютерів, які обробляють та зберігають конфіденційну інформацію:

• Встановити додаткові камери відеоспостереження в громадських коридорах для підвищення рівня безпеки.

• Крім інфрачервоних датчиків руху, офіси оснащуються камерами відеоспостереження або замінюють датчики руху камерами з вбудованими датчиками руху для посиленого моніторингу безпеки.

• Оснащений системами відеоспостереження та інфрачервоними датчиками руху для вантажних входів у корпоративні будівлі для посиленого моніторингу безпеки.

• Закупівля та встановлення джерел безперебійного живлення для того, щоб співробітники вчасно зберігали поточні файли, щоб уникнути втрати даних під час відключень електроенергії та підвищити надійність зберігання інформації.

• Розшифруйте смарт-картки звільнених працівників для додаткової безпеки.

Висновок до другого розділу

Місія системи захисту полягає в тому, щоб забезпечити збереження та передачу даних компанії, що зберігаються на персональному робочому комп’ютері співробітника, захищено від втрати або пошкодження через відключення електроенергії, крадіжки, а також зміцнити існуючі системи безпеки від несанкціонованого проникнення, крадіжки або пошкодження. інформації. В рамках даної роботи не буде розглядатися вдосконалення системи безпеки мережі ТОВ «РДВ».

В другому розділі описано організаційний устрій . Оцінено можливі ризики для інформаційної безпеки та виріб методів захисту для їх зменшення . Реалізація цих заходів підвищить рівень безпеки компанії та рівень безпеки інформації, що зберігається на комп’ютерах співробітників. Складений первинний список обладнання та технологій для забезпечення належного рівня безпеки.

РОЗДІЛ 3
ПРОЕКТНА ЧАСТИНА

3.1 Набір розроблених інструментів нагляду за інформаційною безпекою та організаційного управління

3.1.1 Вітчизняна та зарубіжна нормативна база інформаційної безпеки

У цій статті розглядається процес розробки, впровадження та вдосконалення інструментів інформаційної безпеки на основі національних та міжнародних законів і нормативних актів.

До міжнародних нормативно-правових актів відносяться:

• BS 7799–1:2005 – Британський стандарт BS 7799 – перша частина. BS 7799 Part 1 – Code of Practice for Information Security Management (Практичні правила управління інформаційною безпекою) описує 127 механізмів контролю, необхідних для побудови системи управління інформаційною безпекою (СУІБ) організації, визначених на основі найкращих прикладів світового досвіду (best practices) у цій галузі . Цей документ є практичним посібником зі створення СУІБ

• BS 7799–2:2005 – Британський стандарт BS 7799 – друга частина стандарту. BS 7799 Part 2 – Information Security management – specification for information security management systems (Специфікація системи управління інформаційною безпекою) визначає специфікацію СУІБ. Друга частина стандарту використовується як критерії при проведенні офіційної процедури сертифікації СУІБ організації.

• BS 7799–3:2006 – Британський стандарт BS 7799 – третина стандарту. Новий стандарт у галузі управління ризиками інформаційної безпеки

• ISO/IEC 17799:2005 – «Інформаційні технології – Безпекові технології – Практичні правила менеджменту інформаційної безпеки». Міжнародний стандарт, що базується на BS 7799-1:2005.

• ISO/IEC 27000 – Словник та визначення.

• ISO/IEC 27001:2005 – «Інформаційні технології – Методи забезпечення безпеки – Системи управління інформаційною безпекою – Вимоги». Міжнародний стандарт, що базується на BS 7799-2:2005.

• ISO/IEC 27002 – Зараз: ISO/IEC 17799:2005. "Інформаційні технології - Технології безпеки - Практичні правила менеджменту інформаційної безпеки". Дата виходу – 2007 рік.

• ISO/IEC 27005 – Зараз: BS 7799–3:2006 – Посібник з управління ризиками ІБ.

German Information Security Agency. IT Baseline Protection Manual – Standard security safeguards (Посібник з базового рівня захисту інформаційних технологій).

Створити організаційно-управлінську основу системи інформаційної безпеки та захисту інформації підприємства Організаційно-технічний захист інформації забезпечується такими заходами:

• Обмежте доступ сторонніх осіб до будівель компанії та офісних приміщень, оскільки біля входу в будівлі охороняються магнітні замки на дверях та турнікетах. • Комп'ютер менеджера проекту оснащений операційною системою Mac OS, що зменшує можливість втрати даних через вірусні атаки.

• Рівень доступу співробітників до інформації поділяється на рівень конфіденційності. Відповідно до наказу Генерального директора «Про заходи щодо захисту комерційної таємниці» сформовано такі документи:

• Інструкції та обов'язки співробітників у сфері захисту комерційної таємниці, підписані кожним працівником компанії.

• «Інструкції для системних адміністраторів щодо забезпечення інформаційної безпеки та запобігання витоку інформації через технічні канали зв’язку».

3.2 Набір програмно-технічних засобів, призначених для забезпечення інформаційної безпеки підприємства та захисту інформації

3.2.1 Структура програмно-апаратного комплексу інформаційної безпеки підприємства та захисту інформації

Система відеоспостереження

Системи відеоспостереження (Closed Cable Television Systems, CCTV) - Апаратно-програмні системи, призначені для відеоспостереження. Локальна система - система, сфера і застосування якої географічно обмежені будівлями, підприємствами, організаціями тощо. Системи відеоспостереження централізовані та децентралізовані:

• Централізована система має центр і кілька камер.

•Децентралізована система — це сукупність централізованих, логічно інтегрованих у структуру, але фізично відокремлених і здатних функціонувати незалежно. Характеристики та одиниці вимірювання, що використовуються в системах відеоспостереження: Чутливість камери характеризується найменшою діафрагмою (максимальне число F), що дає відеосигнал 1 В на випробувальному стенді, з освітленістю 2000 люкс і колірною температурою 3200°К.

Чутливість камери, яка добре визначена в мовному телебаченні, часто неправильно розуміється в охоронному телебаченні, і її часто плутають з мінімальним освітленням.

Мінімальна освітленість - (у властивостях камери цей параметр зазвичай виражається як чутливість) - це мінімальна освітленість об'єкта, коли камера випромінює розпізнаваний сигнал, знайдений в комплекті на об'єкт. Деякі виробники використовують цей термін для ідентифікації сигналу в широкому сенсі і не вказують рівень сигналу на виході камери. Цей рівень може досягати 10%, що здається набагато вищим, якщо включити AGC.

Типові рівні освітлення:

• Хмарна і безмісячна ніч - 0,0001 лк

• Ясна безмісячна ніч - 0,001 лк

• Повний місяць - 0,01-0,1 лк

• Вуличне освітлення - 1-10 люкс

• Освітлення офісу - 100-1000 Люкс

• Сонячний день - до 100 000 лк

Динамічний діапазон ПЗС камери визначається як максимальний сигнал відносно середньоквадратичного значення експонованого фону, тобто співвідношення темних і яскравих об'єктів в одній сцені. Що це за взаємозв’язок, темніші елементи видно на світлому загальному фоні кадру.

Роздільна здатність камери – це максимальна кількість рядків (телевізійних – телевізійних рядків), що міститься в одному кадрі дисплея.

Зазвичай вказується роздільна здатність по горизонталі, а роздільна здатність по вертикалі становить 3/4 від горизонтальної.

Роздільна здатність пристроїв обробки відео та відображення зазвичай вимірюється в пікселях. Це здатність пристрою відповідно спостерігати, захоплювати та/або відображати сусідні точки графічного зображення об’єкта. Він вимірюється кількістю точок, які відображаються окремо на дюйм площі рамки. Перша цифра - кількість точок по горизонталі, друга - по вертикалі.

Іноді вимірюється в CIF. Відношення сигнал/шум – це значення, при якому рівень сигналу перевищує рівень шуму при найнижчому освітленні, вимірюється в дБ, залежно від якості ПЗС відеокамери.

На екрані зображення з шумом виглядають як зерно або сніг, а кольорові зображення виглядають у вигляді коротких кольорових смуг або спалахів.

Формула напруги S / N = 20lg (Uc / Ush) Формула потужності сигналу S / N = 10lg (Pc / Psh) Швидкість запису (відтворення або відтворення) –

Частота кадрів - Кількість кадрів в секунду, записаних (відтворених або переданих) відеосистемою. У кадрах в секунду (fps). Іноді виробники використовують pps - кількість напівполів, які відеосистема відображає за секунду. 1 кадр/с = 2 кадр/с. Режим запису:

• Безперервний запис – це безперервний цілодобовий запис відео.

• Запис за розкладом — запис у певний час.

• Реєстрація нагадування - починає реєстрацію, коли надходить певний сигнал.

• Запис на детекторі руху – запис виконується лише при зміні зображення.

• Екстренний запис або запис вручну - запис починається за командою оператора (натисненням кнопки).

Купольні камери відеоспостереження є одними з найбільш універсальних типів камер, які в даний час використовуються в організаційних системах Відеоспостереження будь-якої складності. Багато моделей купольних камер відеоспостереження оснащені 3D кріпленнями, які дозволяють кріпити купол на стелі та стіни, не спотворюючи зображення з камери.

Сучасні куполи відеоспостереження мають широкий спектр опцій, від найпростішої роздільної здатності телевізора 420 і матриці CMOS або SHARP до найповніших комплектів, включаючи DNR (цифрове зниження шуму) і WDR (розширений діапазон). Деякі купольні камери відеоспостереження мають вбудовану інфрачервону підсвітку та зум-об’єктиви.

IP-камера - IP-камера - це цифрова камера, яка характеризується передачею відеопотоків у цифровому форматі через Ethernet за допомогою протоколу IP. Як мережевий пристрій, кожна IP-камера в мережі має власну IP-адресу.

На відміну від аналогових камер, при використанні IP-камер, після отримання відеокадрів з ПЗС-матриці (зарядний пристрій) або CMOS (комплементарна логіка на транзисторах метал-оксид-напівпровідник), матриця зображення залишається оцифрованою, поки не відобразиться на моніторі. Як правило, перед передачею зображення, отримані з матриці, стискаються за допомогою методів покадрового (MJPG) або потокового (MPEG-4, H.264). Існують спеціалізовані IP-камери, які передають відео в стисненому вигляді. Транспортні протоколи IP мережі, такі як TCP і UDP, можуть використовуватися як протоколи транспортного рівня в IP-камерах. Можливість живлення IP-камер через PoE дуже поширена. Оскільки IP-камери не потребують передачі аналогових сигналів у форматі PAL або NTSC, можна використовувати IP-камери

Велика роздільна здатність, включаючи мегапікселі. Типова роздільна здатність для веб-камери: 640x480 пікселів. Камери з мегапіксельною роздільною

здатністю: 1280x1024, 1600x1200 і вище. Відмовляючись від використання стандартів аналогового телебачення PAL і NTSC, IP-камери можуть передавати відео на бажаній частоті. Існують IP-камери зі швидкістю передачі, що перевищує 60 кадрів в секунду. AGC - автоматична система контролю посилення сигналу.

Використовується лише для стабілізації вихідного сигналу на рівні 1В, оскільки ПЗС-матриця камери спостереження завжди видає сигнал достатньої амплітуди, тому наявність внутрішнього автоматичного регулювання посилення дозволяє вивести вихідний сигнал до рівня. Однак слід пам’ятати, що підсилюючи відеосигнал, АРУ однаково посилює шум, зберігаючи співвідношення сигнал/шум однаковим.

У деяких відеокамерах система AGC може бути вимкнена, а в деяких випадках необхідно переконатися, що співвідношення сигнал/шум не погіршується. Глибина АРУ в різних камерах може бути від 12 до 30 дБ. У компанії є централізована система відеоспостереження, яка зберігає дані на відеосерверах у безперервному записі. Відеоспостереження здійснюється купольною камерою SAMSUNG SCC-B5366B, яка має такі технічні характеристики: • Тип камери - аналогова купольна.

• Chroma - Колір.

• Матриця - 1/3 »супер мало. є

• Об'єктив - діапазон фокусної відстані збільшення 2,5 - 6 мм.

• Роздільна здатність - 600 ТБ рядків.

• Чутливість - 0,12 люкс (15 IRE) у кольоровому режимі, 0,012 люкс (15 IRE) у чорно-білому режимі.

• Співвідношення сигнал/шум - понад 52 дБ з вимкненим АРУ. • День/Ніч - кольоровий/монохромний/автоматичний.

• Баланс білого - більше 52 дБ при вимкненому АРУ.

• Електронний затвор (швидкість) - 1/50 - 1/10000. • Апертура - керується або фіксується сигналом постійного струму.

• BLC (Компенсація підсвічування).

• Російське екранне меню.

• Детектор руху.

• Інтерфейси RS-485 і CCVC.

• Джерело живлення - 12 В постійного струму та 24 В змінного струму.

• Діапазон робочих температур - 10 - +50 градусів Цельсія.

• Розміри - 128x78 мм.

• Вага - 330 грам.

Система контролю пропускної здатності.

Турнікет - пристрій, призначений для обмеження проходу людей на випадок, якщо вам потрібно перевірити вхід і вихід усіх, хто проходить. Основним завданням турнікета є створення фізичного бар'єру перед людиною, його авторизація може бути здійснена за допомогою механізмів чи електронних пристроїв, або за рішенням працівника, відповідального за вхід на територію.

Ворота належать до класу систем контролю та управління доступом. Основні види турнікетів:

Штатив - це найпростіша конструкція для поворотних дверей.

Перешкоди – це планки, встановлені на барабані під кутом до його осі обертання, причому в початковому положенні одна з планок паралельна землі і перекриває прохід, а дві інші розташовані в нижньому проході поза барабаном. Один проходить через турнікет, штовхає штангу, і в результаті барабан обертається, шток виходить з проходу, а його місце займає інша людина, перекриваючи прохід наступній людині. Переваги штативів:

• Простий дизайн.

• Малий розмір.

• Конструкція таких турнікетів часто передбачає функцію «антипаніки» – перила можна зняти або опустити, щоб забезпечити безперешкодний рух у разі надзвичайних ситуацій. Мінусом штатива є те, що турнікети легко обійти: перешкода — це всього лише брусок, і під нього легко залізти, а то й переїхати. Тому штатив слід встановлювати лише в тому випадку, якщо правопорушника можна швидко затримати.

Система контролю пропускної здатності. Турнікет - пристрій, призначений для обмеження проходу людей на випадок, якщо вам потрібно перевірити вхід і

вихід всіх перехожих. Основним завданням турнікетів є створення фізичного бар’єру перед людьми, авторизація якого може здійснюватися за допомогою механізмів чи електронних пристроїв, або на розсуд працівника, відповідального за вхід на територію. Ворота належать до системи контролю та управління доступом. Основні типи каретних дверей: Штативи є найпростішою конструкцією каретних дверей. Перешкоди являють собою планки, встановлені на барабані під кутом до його осі обертання, у вихідному положенні одна з планок паралельна землі і закриває канал, а дві інші розташовані в нижньому каналі поза барабаном. Одна людина проходить через турнікет, штовхає шток, барабан обертається, шток виходить з проходу і його замінює інша людина, перекриваючи прохід наступній людині. Переваги штативів: • Проста конструкція.

• найменший розмір.

• Конструкція таких воріт часто передбачає функцію «захищеності від паніки» перила можна зняти або опустити, щоб забезпечити безперешкодний доступ у аварійній ситуації. Недоліком штативів є те, що турнікет можна легко обійти: перешкода – це всього лише стовп, під який легко залізти і навіть пересунутися. Тому штатив слід встановлювати лише в тому випадку, якщо злочинця можна швидко затримати.

Робить автентифікацію комп’ютера за допомогою смарт-карт більш зручною.

Безконтактна смарт-карта (BSC). Це смарт-карти, де карта спілкується із зчитувачем за допомогою технології RFID (радіочастотної ідентифікації). Щоб виконати потрібну дію, карту потрібно піднести близько до пристрою зчитування карт. Зазвичай вони використовуються в місцях, де потрібно швидко працювати, наприклад, у громадському транспорті. Стандартом для безконтактних смарт-карт є ISO/IEC 14443 і рідше ISO/IEC 15693.

Технологія RFID використовується для безконтактних смарт-карт. Як і контактні смарт-картки, безконтактні смарт-картки не мають батарейок. Вони мають вбудований індуктор для накопичення енергії початкового РЧ-імпульсу, який потім випрямляється і використовується робочою картою. Приклади широко використовуваних безконтактних смарт-карт: метро та автомобільний транспорт,

електронні («біометричні») паспорти, деякі види карток в системах контролю доступу.

Карта пам'яті- Такі карти містять деякі дані та фіксований механізм обмеження доступу до них. Як правило, це мікроплатіжні картки, які використовуються для транспортування, телефонії, парків відпочинку, картки лояльності клієнтів тощо. За механізмом обмеження доступу можуть бути дуже простими (одноразовий запис, пароль, унікальний номер) або більш складними (взаємна аутентифікація за допомогою стандартних алгоритмів симетричного шифрування AES, DES). Наприклад: метро та наземний транспорт, телефонні картки загального користування.

Смарт-карта- вони містять мікропроцесор і можливість завантажувати алгоритми для його запуску. До можливих дій таких карток належать складні дії аутентифікації, складні протоколи обміну, реєстрація фактів доступу тощо. На додаток до симетричного шифрування (AES, DES), також відомого як асиметричне (RSA), алгоритм інфраструктури відкритих ключів (PKI) має апаратний генератор випадкових чисел і покращує захист від фізичних атак. Зазвичай вони працюють під керуванням операційної системи (наприклад, JCOP або MULTOS) і надають відповідний пакет сертифікатів.

Приклади: електронні («біометричні») паспорти та візи, мобільні SIM-карти. Контроль і контроль доступу підприємства здійснюється за допомогою двох турнікетних штативів ARGO TRT 11-02G, які відкриваються з панелі безпеки та особистої безконтактної смарт-картки співробітника для відповідного доступу на стіні біля турнікета. пристрій для зчитування.

Джерело безперебійного живлення. Джерело безперебійного живлення (ДБЖ) - вторинний джерело живлення, автоматичний пристрій, метою якого є забезпечення безперебійної подачі електроенергії в межах нормального діапазону до підключеного електричного обладнання. ГОСТ 13109-97 (замінює ГОСТ 13109-87) визначає такі критерії в мережах електропостачання:

напруга 220 ± 5% (граничне значення ± 10%);

частота 50 Гц ± 0,2 Гц (граничне значення ± 0,4 Гц);

форма напруги. коефіцієнт нелінійної деформації менше 8% (довгострокове) і менше 12% (короткострокове).

Проблемами з живленням вважаються:

• Збій напруги мережі (напруга живлення повністю зникає).

Слід також зазначити, що використання брандмауера збільшує час відповіді та зменшує пропускну здатність, оскільки фільтрація не є миттєвою. Брандмауер сам по собі не є панацеєю від усіх кіберзагроз. Зокрема, він:

• Вузли мережі не можуть бути захищені від «люків» або програмних уразливостей.

• Не забезпечує захист від багатьох внутрішніх загроз, особливо від злому даних.

• Не захищає користувачів від завантаження шкідливого програмного забезпечення, включаючи віруси. Для вирішення двох останніх проблем потрібні відповідні додаткові інструменти, зокрема антивірусне програмне забезпечення. Зазвичай вони підключаються до брандмауера і передають відповідні частини мережевого трафіку, діють як прозорі проксі до інших вузлів мережі або отримують копії всіх переданих даних від брандмауера. Однак такий аналіз вимагає значних апаратних ресурсів і тому зазвичай виконується незалежно на кожному вузлі мережі.

Антивірусна програма (антивірус) - будь-яка програма, яка виявляє комп'ютерні віруси і взагалі небажані (вважаються шкідливими) програми і використовує такі програми для відновлення заражених (модифікованих) файлів, а також для запобігання - запобігання зараженню (модифікованих) файлів програм або операційної системи. На даний момент антивірусне програмне забезпечення в основному розробляється для сімейства Microsoft Windows, що викликано великою кількістю шкідливих програм під платформою (знову ж таки, через популярність операційної системи та розробку великої кількості інструментів, у тому числі безкоштовних і навіть «інструкції щодо написання вірусів».»). Тепер доступні продукти для інших настільних платформ, таких як Linux і Mac OS X. Це пов’язано з тим, що шкідливі програми почали поширюватися на цих платформах, хоча UNIX-

подібні системи завжди були відомі своєю надійністю. Виявлення на основі сигнатур (реактивна технологія) — це метод антивірусних систем і систем виявлення вторгнень, при якому програма переглядає файл або пакет і посилається на словник відомих вірусів, зібраний автором програми. Якщо будь-яка частина переглянутого програмного коду збігається з відомим кодом (сигнатурою) вірусу в словнику, антивірусна програма може виконати одну з наступних дій:

• Видалити заражені файли.

• Помістіть файли на карантин, навіть якщо вони недоступні, щоб запобігти подальшому поширенню вірусу.

• Спробуйте відновити файл, видаливши вірус із тіла файлу.

Технологія активного антивірусного захисту — це сукупність технологій і методів, які використовуються в антивірусному програмному забезпеченні, основне призначення якої відрізняється від реактивної (сигнатурної) технології, головне призначення — запобігти зараженню системи користувача, не виявити в системі відомі шкідливі програми.

Антивірусні продукти можна класифікувати за кількома ознаками, наприклад: Використана технологія антивірусного захисту, особливості продукту, цільові платформи.

За технологією антивірусного захисту:

• Класичні антивірусні продукти (продукти, які використовують лише методи виявлення сигнатур).

• Продукти активного антивірусного захисту (продукти, які використовують лише технологію активного антивірусного захисту).

Комбіновані продукти (продукти, які використовують як класичні, фірмові та активні методи захисту). За функціями продукту:

• Антивірусні продукти (продукти, які забезпечують лише антивірусний захист).

• Комбіновані продукти (продукти, які забезпечують не лише захист від шкідливого програмного забезпечення, але й такі функції, як фільтрація спаму, шифрування та резервне копіювання даних).

За цільовою платформою:

• Антивірусні продукти для Windows.

• Антивірусні продукти для сімейства операційних систем *NIX (до сімейства входять BSD, Linux, Mac OS X тощо).

• Антивірусні продукти для мобільних платформ (Windows Mobile, Symbian, iOS, BlackBerry, Android, Windows Phone 7 тощо).

Антивірусні продукти для корпоративних користувачів також можна класифікувати за об’єктами захисту:

• Антивірусні засоби захисту робочих станцій.

• Антивірусні продукти для захисту файлів і термінальних серверів.

• Антивірусні продукти для захисту електронної пошти та Інтернет-шлюзів.

• Антивірусні продукти для захисту серверів віртуалізації.

Програмне забезпечення безпеки компанії включає брандмауер Windows і один тип антивірусу, що працює на кожному комп’ютері: Avira, Dr. Web, Kaspersky (встановити антивірус на вибір співробітника).

Об'єктом модернізації є охоронні системи підприємства, тобто охоронні, технічні та програмні системи безпеки.

Модернізація систем відеоспостереження.

Щоб підвищити захист від витоку інформації з камер через аналогові канали зв’язку, а також збільшити швидкість оновлення інформації безпеки, аналогові камери слід замінити IP-камерами, оскільки вони мають багато переваг перед аналоговими камерами:

• Швидкість зйомки не обмежена аналоговими системами кодування PAL і NTSC.

• Сигнал з камери не перекодується в аналоговий сигнал, а потім перекодується, що покращує швидкість обробки та передачі відео та зменшує ризик перехоплення сигналу аналоговим каналом зв'язку.

• Роздільна здатність відеопотоку IP-камер перевищує роздільну здатність аналогових камер.

• IP-камери можуть надсилати бездротові сигнали.

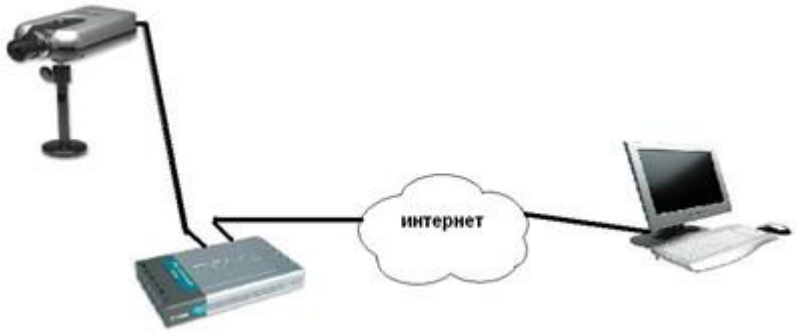

Рисунок 9 Принцип роботи IP камери

Для заміни камер було обрано модель Evidence Apix-MiniDome/M2 Lite 40

Рисунок 10 IP-Камера Evidence Apix-MiniDome/M2 Lite 40

Камера Evidence Apix-MiniDome / M2 Lite 40 виготовлена в купольному корпусі, призначеному для використання всередині приміщень.

Матриця з роздільною здатністю 2 МП і прогресивною розгорткою дозволяє отримати чітке зображення високої чіткості з роздільною здатністю Full HD 1080p.

Крім того, пристрій має кілька функцій для покращення деталей зображення: AWB (автоматичний баланс білого), BLC (компенсація підсвічування), AGC (автоматичний рівень посилення), WDR (розширення динамічного діапазону). Для стиснення відеосигналу використовуються загальні кодеки H.264, MJPEG і MPEG4, а також підтримується подвійне потокове передавання, що дозволяє ефективно використовувати локальний мережевий трафік. Оскільки встановлений мікрофон, є можливість записувати звук з об’єкта. Ваш пристрій має кілька рівнів доступу до

локальної мережі. Висока якість зображення, компактний розмір і оптимальний набір функцій роблять Evidence Apix - MiniDome / M2 Lite 40 відмінним вибором для сучасних цифрових систем відеоспостереження з особливими вимогами до якості відео. Особливості камер Evidence Apix - MiniDome / M2 Lite 40, які впливають на вибір:

• Денний і нічний режим - знімайте в будь-який час.

• Формати стиснення - Motion JPEG, MPEG-4, H.264 - один з найпоширеніших і найкращих форматів мовлення.

• Колір - Колір - Отримайте більш детальну інформацію про своїх відвідувачів, якщо вам потрібно точно описати характеристики: колір одягу, колір волосся тощо.

• Швидкість передачі (кадрів в секунду) - до 25 - для найшвидшого оновлення інформації.

• Роздільна здатність (точки на дюйм) - 1920x1080 - максимальна доступна роздільна здатність для більшості відеопроцесорів

• Чутливість, LUX - 0,1 LC - підходить для зйомки в умовах слабкого освітлення.

• Розміри, мм - 110x47.

• Працює через Ethernet.

• Компенсація підсвічування - камеру не можна заблокувати.

• Вага - 0,18 кг.

• Споживана потужність - 6 Вт.

• Екранні меню. Оптова ціна камери Evidence Apix-MiniDome/M2 Lite 40 становить 7697 гривень, що на 353 гривні дешевше за SAMSUNG SCC-B5366B. Встановіть джерело безперебійного живлення.

У зв’язку з будівництвом новобудов поблизу підприємства, часто виходить з ладу електромережа та можливі відключення електроенергії, рекомендую придбати та встановити джерело безперебійного живлення IPPON Back Verso 800 з наступними характеристиками:

• Вихідна потужність, ВА - 800.

• Вихідна потужність Вт - 480.

• Номінальна вхідна напруга 220В.

• Вихідна частота (рівень мережі) - 50 Гц (авторозпізнавання)

• Форма сигналу вихідної напруги - приблизно синусоїда.

• Діапазон вхідної напруги - 170-260В.

• Номінальна вихідна напруга - 220 В +/- 10%.

• Вихідна частота - 50 Гц +/- 1 Гц.

Вихідна напруга має форму поетапної синусоїди.

• Час перемикання батареї, мс - 2-6

• Постійний захист від бризок/шуму.

• Захист від короткого замикання.

• Захист від перевантаження – якщо навантаження досягає 110% від допустимого протягом 60 секунд, ДБЖ автоматично вимкнеться. і 130% за 3 секунди.

• Deep Battery Saver - Автоматично вимикається через 30 хвилин автономної роботи, незалежно від навантаження.

• Захист вхідного ланцюга - автоматичний вимикач повернувся в вихідне положення.

• Захист комп'ютерної мережі або телефонної лінії - порти RJ-45 / RJ-11

• Кількість і тип акумуляторних батарей, В/В*шт. - 12V9Ah x 1

• Найдовший нормальний час зарядки - 12 годин після повного розряду до 90%

• Час роботи від батареї при навантаженні ПК + 15" монітор (100 Вт типово) - ~ 27-30 хвилин.

• Світлодіодні індикації: мережа (зелене світло), акумулятор працює (жовтий), несправність (червоне світло).

• Розміри, мм - 252x130x209.

• Вихідні роз'єми - 6 Schuko CEE 7 (2 з фільтром, 4 з акумулятором). • Рівень шуму <40 дБ (1 м від поверхні).

• Підтримувані стандарти ISO9002, CE, cUL, PCT. • Нето/Брутто, кг - 7,0. Пристрій з ціною 2870 гривень за одиницю отримав дуже позитивні відгуки в інтернет-магазині.

Рисунок 11. Джерело безперебійного живлення IPPON Back Verso 800

Модернізація систем захисту програмного забезпечення.

Як єдиний антивірус, який встановлюється на всіх комп'ютерах співробітників, я рекомендую встановити корпоративну версію Kaspersky Antivirus, яка не тільки відмінно справляється з антивірусним захистом (він знищує руткіт-вірус, який замінює систему), команди для відправки Інтернет-пакетів, тим самим передаючи копію всього трафіку безсилим зловмисникам і Dr.Web і Avira), а також надає можливість фільтрувати інтернет-трафік як брандмауер. Крім стандартного диспетчера завдань Windows, я рекомендую встановити безкоштовний AnVir Task Manager, який, на відміну від стандартного taskmgr.exe, пригнічує процеси запуску, відображає дерево запуску для подальшого завантаження з нього непотрібних програм, зберігає всі журнали, пов'язані з програмами Події (час запуску, повний шлях до файлу, відкриті/закриті вікна, батьківський процес тощо), дозволяють перейти до виконуваного файлу запущеної програми або процесу, дають змогу надсилати цікавлять виконувані файли для сканування через 40 антивірусів і має чудовий налаштування та оптимізований запуск Windows.

Здебільшого AnVir Task Manager використовує стандартні інструменти Windows, але всі ці інструменти об'єднані в одну програму та зручно розділені на

розділи, які допомагають у процесі налаштування та керування комп’ютером. Диспетчер завдань також надає користувачам безліч зручностей, таких як:

• Можливість розташовувати будь-яке вікно поверх інших вікон і згортати вікна в третій, щоб не займати місце на панелі завдань.

• Створіть піктограму, щоб згорнути програму на робочий стіл замість панелі завдань.

• Вивести інформацію про кількість інформації, що зберігається на системному диску, під значком диска (дуже актуально, особливо для Windows XP).

Оскільки всі ліцензовані версії Windows встановлені на всіх комп’ютерах вашої компанії, доцільно перевірити стан автоматичних оновлень операційної системи.

У рамках цієї дипломної роботи необхідна система автоматичного оновлення для забезпечення цілісності системних програм і процесів, які можуть бути пошкоджені вірусами, яких немає в антивірусній базі.

Завдяки цій системі було відновлено системний процес, що відповідає за доступ до Інтернету та аудіопристроїв, заражених новим вірусом, який не був виявлений жодним із перерахованих вище антивірусних програм.

Висновок до третього розділу

В третьому розділі описано список використаної вітчизняна та зарубіжна нормативна база інформаційної безпеки У цій статті розглядається процес розробки, впровадження та вдосконалення інструментів інформаційної безпеки на основі національних та міжнародних законів і нормативних актів

У проектній частині розділу розглядаються всі методи, які використовуються при модернізації систем захисту баз даних. Після розгляду технології описуються цілі модернізації. В основному розроблено модернізацію систем захисту баз даних підприємства.

РОЗДІЛ 4
ДЕМОНСТРАЦІЯ ЕКОНОМІЧНОЇ ВИГОДИ ПРОЕКТУ

4.1 Вибір і демонстрація методів розрахунку економічної ефективності

Як метод розрахунку економічної ефективності використовуються розрахункові методи, які описують ресурси, що використовуються для модернізації, і розкривають залежність розміру збитків в організації. Такий підхід є найкращим приводом надати керівництву детальну інформацію для прийняття рішень в рамках модернізації системи захисту від крадіжки інформації корпорації «РДВ».

Таблиця 8

Величини втрат для критичних інформаційних ресурсів до модернізації системи захисту проти розкрадання інформації

Актив	Загроза	Величина втрат (тис. грн.)
Престиж компанії	Крадіжка інтелектуальної власності компанії	500
Інформація	Порушення цілісності інформації	50
Інформація	Знищення даних	50
Інформація	Несанкціонований доступ до інформації	400
Інформація	Ненавмисна втрата носіїв інформації	70
Інформація	Перехоплення даних, що передаються каналами зв'язку	60
Інформація	Розголошення, передача або втрата ідентифікаційних даних	73
Персонал	Витік фахівців	150
Персонал	Вербування персоналу	200
Сумарна величина втрат		1553

Тому для визначення економічної ефективності систем інформаційної безпеки необхідні наступні дані

• Витрати (виділені ресурси) на створення/модернізацію системи та підтримання її в роботі.

• Загроза інформаційним активам після впровадження/модернізації систем захисту інформації.

У таблиці нижче наведено результати експертної оцінки «РДВ» обсягу втрат критичних інформаційних ресурсів до модернізації БЛВС.

З результатів розрахунків видно, що більшість загроз є загрозами інформаційній безпеці підприємства. Під час модернізації головним завданням є усунення цих загроз для зменшення втрат

4.2 Розрахунок індексу економічної вигоди від проекту

У рамках цієї дипломної програми до цієї роботи залучаються лише співробітники компанії. У таблиці нижче представлений показник співробітників компанії, всю інформацію надають працівники бухгалтерії компанії.

Таблиця 10

Показники середньогодинної зарплати спеціалістів

Посада	**Середньогодинна заробітня плата (грн.)**
Начальник відділу технічної підтримки	375
Старший інженер відділу технічної підтримки	325
Системний адміністратор	320
Співробітник служби охорони	265

Всі подальші розрахунки, пов’язані з витратами на оплату праці, будуть проводитися відповідно до таблиці вище. Далі в наведеній нижче таблиці ми розглядаємо дані про вміст і обсяги одноразових ресурсів, що виділяються на модернізацію систем безпеки баз даних підприємства.

Як видно з таблиці, сума одноразових ресурсів складає всього 74 970 грн . В основі витонченості лежать цінності експертів, які вирішують конкретні проблеми.

Далі ми розглянемо обсяг постійних ресурсів, виділених для забезпечення ефективності та належного рівня захисту безпеки. Усі витрати на оплату праці, зазначені в Розмірі, розраховуються за рік роботи системи.

Виходячи з необхідності забезпечення постійної підтримки продуктивності корпоративних баз даних і серверів, які беруть участь у процесі аутентифікації користувачів, необхідно виділити ресурси для постійної підтримки. На додаток до інженерних заходів щоквартально слід перевіряти системи інформаційної безпеки та рівні безпеки для виявлення нових вразливостей. У наступній таблиці розраховується кількість фіксованих ресурсів.

Таблиця 11

Обсяг разового ресурсу, що виділяється на захист інформації

Організаційні заходи				
№ п\п	**Дія, що виконуються**	**Середнього динна зарплата спеціаліста (грн.)**	**Трудомісткість операції (чол. година)**	**Вартість, всього (тис. грн.)**
1	Проведення оцінки активів	375	40	15
2	Розробка та внесення змін до політики інформаційної безпеки компанії	375	30	11,25
3	Випуск озпорядження для працівників на тему захисту конфіденційної інформації	375	8	3
Вартість проведення організаційних заходів, всього		**29,25**		
Заходи інженерно-технічного захисту інформації				
№ п\п	**Дія, що виконуються**	**Середнього динна зарплата спеціаліста (грн.)**	**Трудомісткість операції (чол. година)**	**Вартість, всього (тис. грн.)**
1	Проектування модернізації системи захисту від розкрадання інформації	325	70	22,75
2	Закупівля та монтаж нових камер відеоспостереження та джерел безперебійного живлення	325	50	16,25
3	Встановлення антивірусного ПЗ, додаткового диспетчера задач та	320	21	6,72

	перевірка стану системи автоматичного оновлення			
Вартість проведення інженерно-технічних заходів, всього		**45,72**		
Обсяг разового ресурсу, що виділяється на захист інформації		**74,97**		

Таблиця 12

Кількість витрат на організаційні заходи

Організаційні заходи				
№ п\п	**Дія, що виконуються**	**Середньогодинна зарплата спеціаліста (грн.)**	**Трудомісткість операції (чол. година)**	**Вартість, всього (тис. грн.)**
1	Проведення аудиту захисту інформації та ступеня захищеності	325	28	9,1
Стоимость проведения организационных мероприятий, всего				9,1
Мероприятия инженерно-технической защиты				
№ п\п	**Дія, що виконуються**	**Середньогодинна зарплата спеціаліста (грн.)**	**Трудомісткість операції (чол. година)**	**Вартість, всього (тис. грн.)**
1	Підтримка працездатності системи захисту інформації підприємства	325	112	36,4
2	Обслуговування охоронного обладнання та джерел безперебійного живлення	320	112	35,84
Вартість проведення інженерно-технічних заходів, всього				**72,24**
Обсяг постійного ресурсу, що виділяється на захист інформації				**81,34**

Організаційні заходи здійснюватиме начальник відділу технічного забезпечення.

Графік роботи – щоквартально. Інженерно-технічні роботи виконуватимуть системні адміністратори (підтримка технічного обслуговування) та старші інженери відділу технічної підтримки. Відведений робочий час - 2 години на тиждень для кожного виду роботи. Після того як ви отримаєте вартість одноразових і постійних ресурсів, виділених для модернізації та захисту бази даних, ви можете відобразити загальну вартість цього ресурсу.

Загальна вартість ресурсу розраховується за такою формулою:

$$R\sum = Rp + Rп \quad (1)$$

Звідси

$R\sum = 74,97 + 81,34 = 156,31$ тис. грн.

Для проведення розрахунку необхідно шляхом експертної оцінки отримано прогнозовані дані про величину втрат (ризиків) для критичних інформаційних ресурсів після модернізації системи захисту інформації.

Таблиця 13

Прогнозовані дані про величину втрат

Актив	Загроза	Величина втрат (тис. грн.)
Престиж компанії	Крадіжка інтелектуальної власності компанії	500
Інформація	Порушення цілісності інформації	0
Інформація	Знищення даних	50
Інформація	Несанкціонований доступ до інформації	0
Інформація	Ненавмисна втрата носіїв інформації	70
Інформація	Перехоплення даних, що передаються каналами зв'язку	60
Інформація	Розголошення, передача або втрата ідентифікаційних даних	0
Персонал	Витік фахівців	150
Персонал	Вербування персоналу	200
Сумарна величина втрат		1030

Як видно з таблиці вище, загальна кількість можливих проблем значно зменшилася після модернізації системи безпеки баз даних. Будь ласка, зверніть увагу на таку інформацію: • Загальна вартість ресурсів ($R\sum$), виділених на захист інформації, становить 156 310 гривень; • Середньорічні збитки (Rsr) компанії через інциденти інформаційної безпеки склали 1,553 млн. грн.; • Очікуваний річний збиток (Rprogn) становить 1 030 000 грн. На основі отриманої інформації необхідно оцінити динаміку розмірів збитків за річний період.

Після застосування обов’язкових припущень щодо незмінності частоти загроз та постійного рівня надійності створеної системи інформаційної безпеки необхідно

визначити термін окупності (поточний) системи. Це робиться аналітично за формулою посібника

Таблиця 14

Прогнозоване зниження втрат після впровадження покращеної системи

	кв.	**кв.**	**кв.**	**год**
До впровадження СЗІ	23,25	46,5	69,75	293
Після впровадження СЗІ	57,5	15	72,5	030
Зниження витрат	5,75	31,5	97,25	63

$$T_{ок} = R_{\sum} / (R_{ср} – R_{прогн}). \quad (2)$$

Отже, TOk = 156,31 / (1293–1030) ≈ 0,5943346, що становить приблизно 7 місяців і 1 тиждень. Впровадження розглянутих у цій дипломній програмі систем захисту дозволить знизити витрати на ліквідацію інцидентів інформаційної безпеки та забезпечити високий рівень безпеки. Як видно з наданих розрахунків, проект було реалізовано за низькою ціною (156 310 гривень) при забезпеченні необхідного рівня захисту. За рахунок зменшення кількості ризиків можна істотно знизити річний коефіцієнт збитковості компанії. До модернізації він сягнув 1,293 млн грн. 1,03 млн грн на рік після модернізації. один рік. Варто відзначити, що термін окупності даної системи складає всього 7 місяців і 1 тиждень, що є значною перевагою перед іншими рішеннями.

Висновок до четвертого розділу

В четвертому розділі зроблені розрахунки економічної ефективності використовуються розрахункові методи, які описують ресурси, що використовуються для модернізації, і розкривають залежність розміру збитків в організації. Такий підхід є найкращим приводом надати керівництву детальну

інформацію для прийняття рішень в рамках модернізації системи захисту від крадіжки інформації корпорації «РДВ».

Тому для визначення економічної ефективності систем інформаційної безпеки необхідні наступні дані

• Витрати (виділені ресурси) на створення/модернізацію системи та підтримання її в роботі.

• Загроза інформаційним активам після впровадження/модернізації систем захисту інформації.

ВИСНОВОК

У запропонованій дипломній програмі в ТОВ «РДВ» розроблено та впроваджено систему запобігання крадіжок інформації Під час дипломного проектування була проведена наступна робота. Розділ аналізу описує загальні характеристики підприємства, його організаційну та функціональну структуру в межах предметної області, ідентифікацію та оцінку активів, а також оцінку вразливостей та загроз для активів.

Оцінено існуючі системи безпеки в базі даних та рівень безпеки всієї системи. Вибирайте заходи захисту на основі отриманих даних.

У проектній частині диплома розглядаються всі методи, які використовуються при модернізації систем захисту баз даних. Після розгляду технології описуються цілі модернізації. В основному розроблено модернізацію систем захисту баз даних підприємства. Третя частина демонструє економічні переваги програми на основі структурованого матеріалу дипломної програми. У рамках демонстрації економічної вигоди проекту здійснюється вибір методів розрахунку та розрахунок показників. У розрахунку відображаються рівні заробітної плати працівників, які беруть участь у процесі модернізації, обсяги одноразових і постійних ресурсів, що виділяються на захист інформації.

На основі отриманих даних оцінено динаміку збитків в організації за рік експлуатації системи. Після цього розраховується термін окупності проекту. Наприкінці третьої частини економічні вигоди від проекту підсумовуються на основі попередніх розрахунків.

До основних переваг розробленої системи можна віднести високий рівень захисту інформації від крадіжки та пошкодження, низькі витрати на впровадження та досить високу віддачу.

Поставлені цілі досягнуто.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Методичні вказівки з дипломного проектування за спеціальністю «Інформаційні системи та технології», спеціалізація «Безпека інформаційних систем». МФПУ. 2012

2. Комплексна автоматизація управління підприємством: Інформаційні технології – теорія та практика. / Петров Ю.А.М.: Фінанси та статистика, 2008

3. Голдовський І.М. Банківські мікропроцесорні картки. - М.: "Альпіна Паблішер", 2010. - 694 с. – (Бібліотека Центру досліджень платіжних систем та розрахунків). – ISBN 978–5–9614–1233–8

4. Девід В. Чепмен, мл., Енді Фокс Брандмауери Cisco Secure PIX = Cisco® Secure PIX® Firewalls. - М.: "Вільямс", 2003. - С. 384. - ISBN 1-58705-035-8

5.Стаття «Антивірусна програма» – http://ua.wikipedia.org/wiki/Антивірусна_програма

6. Стаття "Смарт-карта" - http://ua.wikipedia.org/wiki/Смарт-карта

7.Стаття «Міжмережевий екран» – http://ua.wikipedia.org/wiki/Міжмережевий_екран

8. Стаття «Проактивний захист» – http://ua.wikipedia.org/wiki/Проактивний_захист

9. Стаття «Виявлення, що ґрунтується на сигнатурах» – http://ua.wikipedia.org/wiki/Виявлення,_засноване_на_сигнатурах

10. Стаття "IP-камера" - http://ua.wikipedia.org/wiki/IP-камера

11. Стаття «Турнікет» – http://ua.wikipedia.org/wiki/Турнікет

12. Стаття «ПЗЗ-матриця» – http://ua.wikipedia.org/wiki/ПЗЗ-матриця

13. Willard S. Boyle Nobel Lecture: CCD-An extension of man's view (англ.) // Rev. Mod. Phys. - 2010. - В. 3. - Т. 82. - С. 2305-2306.

14. George E. Smith Nobel Lecture: The invention and early history of the CCD (англ.) // Rev. Mod. Phys. - 2010. - В. 3. - Т. 82. - С. 2307-2312.

15. Arif Mohamed. A history of cloud computing [Електронний ресурс]. – Режим доступу: http://www.computerweekly.com/feature/A-history-of-cloud-computing

16. SoCC 10: Proceedings of the 1st ACM symposium on Cloud computing, Hellerstein, Joseph M. - N. Y.: ACM, 2010. - ISBN 978-1-4503-0036-0.

17. Gillam, Lee. Cloud Computing: Principles, Systems and Applications / Nick Antonopoulos, Lee Gillam. — L.: Springer, 2010. — p. 379.

18. Баранов А.П. Чи можна захистити в «хмарі» конфіденційну інформацію? А. Баранов // Системи високої доступності. — 2012. — Т. 8. — № 2. — С. 12-15.

19. Бабаш А.В., Гольєв Ю.І., Ларін Д.А., Шанкін Г.П. Про розвиток криптографії в XIX столітті // Захист інформації. Конфидент. — 2003. — №5 — с. 90-96.

20. Безпека життєдіяльності. Безпека технологічних процесів і виробництв (Охорона праці): Навч. посібник для вузів // П.П. Кукін, Е.А. Підгорний та ін. - М .: Висш.шк., 1999. — с. 318.