

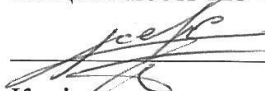
Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему:

«Проект комплексної системи захисту інформації торговельного
підприємства»

Виконав студент 4-го курсу, групи КБ-1
спеціальності 125 «Кібербезпека»

 Патлай С.В.
Керівник, доцент кафедри КІ та КБ, кандидат
технічних наук

 Пірог О.В.
Рецензент, доцент кафедри КІ та КБ,
кандидат технічних наук

_____ Лобанчикова Н.М.

Житомир 2021

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 125 «КІБЕРБЕЗПЕКА»

ЗАТВЕРДЖУЮ

Завідувач кафедри
комп'ютерної інженерії
та кібербезпеки

 Ефіменко А. А.

«12» квітня 2021 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу

Студента **Патлая Сергія Васильовича**

Тема роботи: **Проект комплексної системи захисту інформації торговельного підприємства**

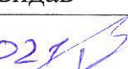
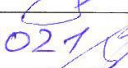
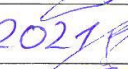
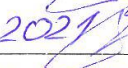
затверджена Наказом по університету від « » **Квітня 2021 р. №**

Термін здачі студентом закінченої роботи – «**29**» **Червня 2021р.**

Вихідні дані для роботи:

1. Організаційна структура ТОВ «Механіка Трейд»
2. Існуюча автоматизована інформаційна система документообігу
3. Положення про комерційну таємницю ТОВ «Механіка Трейд»
4. Графічний симулятор мереж Cisco Packet Tracer
5. Інструмент для моделювання загроз OWASP Threat Dragon

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

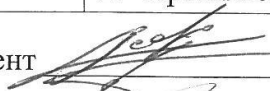
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Пірог О.В.	12.04.2021 	12.04.2021 
2	Пірог О.В.	20.04.2021 	20.04.2021 
3	Пірог О.В.	28.04.2021 	28.04.2021 
4	Пірог О.В.	12.05.2021 	12.05.2021 
5	Пірог О.В.	20.05.2021 	20.05. 

Керівник

 Пірог О.В.

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	6 квітня 2021 – 7 квітня 2021	Виконано
2	Пошук, огляд та аналіз літературних джерел щодо організації КСЗІ	8 квітня 2021 – 11 квітня 2021	Виконано
3	Аналіз правового забезпечення захисту інформації	12 квітня 2021 – 16 квітня 2021	Виконано
4	Дослідження існуючої системи захисту інформації	17 квітня 2021 – 24 квітня 2021	Виконано
5	Розрахунок ризиків	25 травня 2021 – 4 травня 2021	Виконано
6	Розробка організаційних заходів	5 травня 2021 – 9 травня 2021	Виконано
7	Розробка інженерно-технічних заходів	10 травня 2021 – 13 травня 2021	Виконано
8	Моделювання загроз в OWASP Threat Dragon	14 травня 2021 – 18 травня 2021	Виконано
9	Моделювання роботи мережі в Cisco Packet Tracer	19 травня 2021 – 22 травня 2021	Виконано
10	Аналіз результатів тестування	23 травня 2021 – 24 травня 2021	Виконано
11	Написання пояснювальної записки	25 травня 2021 – 29 травня 2021	Виконано
12	Підготовка презентації та виступу	30 травня 2021 – 31 травня 2021	Виконано
13	Отримання відгуку керівника та рецензії на кваліфікаційну роботу	4 червня 2021 – 8 червня 2021	Виконано
14	Захист	29 червня 2021	Виконано

Студент  Патлай С.В.

Керівник  Пірог О.В.

РЕФЕРАТ

Кваліфікаційна робота містить розробку комплексної системи захисту інформації.

Основний зміст пояснювальної записки роботи викладено на 68 сторінках тексту, записка містить 14 таблиць, 2 ілюстрації. Список використаних літературних джерел налічує 54 найменування.

Метою роботи є розробка заходів із підвищення рівня захищеності інформаційної системи підприємства ТОВ «Механіка Трейд».

Для виконання поставленої задачі необхідно провести аналіз можливих загроз, та дослідити існуючу інформаційну систему та виявити в ній слабкі місця з точки зору безпеки.

Необхідно розробити комплекс заходів, що підвищать рівень захищеності інформаційних ресурсів підприємства.

Дипломна робота складатиметься із п'яти розділів, які міститимуть аналіз поточного стану інформаційної безпеки на підприємстві, розрахунки ризиків та збитків від загроз різного характеру та запропоновані заходи із підвищення рівня захищеності інформаційних ресурсів ТОВ «Механіка Трейд».

КЛЮЧОВІ СЛОВА: ЗАХИСТ, КОМП'ЮТЕРНА МЕРЕЖА, ІНФОРМАЦІЙНА СИСТЕМА, СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, CISCO.

					КБ.КВ.Б – 125 -14 -ПЗ				
Зм.	Арк.	№ докум.	Підпис	Дата	Проект комплексної системи захисту інформації торговельного підприємства	Літ.	Арк.	Аркуші	
Розроб.		Патлай С.В.		29.06.21					
Керівник		Пірог О.В.А.		29.06.21			4	86	
Рецензент.		Лобанчикова Н.М.				Державний університет «Житомирська політехніка», група КБ-1			
Зав. каф.		Єфіменко А. А.		29.06.21					

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра

на тему:

«Проект комплексної системи захисту інформації торговельного підприємства»

Виконав студент 4-го курсу, групи КБ-1
спеціальності 125 «Кібербезпека»

_____ Патлай С.В.

Керівник, доцент кафедри КІ та КБ,
кандидат технічних наук

_____ Пірог О.В.

Рецензент, доцент кафедри КІ та КБ,
кандидат технічних наук

_____ Лобанчикова Н.М.

Житомир 2021

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 125 «КІБЕРБЕЗПЕКА»

ЗАТВЕРДЖУЮ

Завідувач кафедри
комп'ютерної інженерії
та кібербезпеки

_____ Єфіменко А. А.

«12» квітня 2021 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу

Студента **Патлая Сергія Васильовича**

Тема роботи: **Проект комплексної системи захисту інформації торговельного підприємства**

затверджена Наказом по університету від « » **Квітня 2021 р. №**

Термін здачі студентом закінченої роботи – **«29» Червня 2021р.**

Вихідні дані для роботи:

1. Організаційна структура ТОВ «Механіка Трейд»
2. Існуюча автоматизована інформаційна система документообігу
3. Положення про комерційну таємницю ТОВ «Механіка Трейд»
4. Графічний симулятор мереж Cisco Packet Tracer
5. Інструмент для моделювання загроз OWASP Threat Dragon

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Пірог О.В.		
2	Пірог О.В.		
3	Пірог О.В.		
4	Пірог О.В.		
5	Пірог О.В.		

Керівник _____ Пірог О.В.

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	6 квітня 2021 – 7 квітня 2021	Виконано
2	Пошук, огляд та аналіз літературних джерел щодо організації КСЗІ	8 квітня 2021 – 11 квітня 2021	Виконано
3	Аналіз правового забезпечення захисту інформації	12 квітня 2021 – 16 квітня 2021	Виконано
4	Дослідження існуючої системи захисту інформації	17 квітня 2021 – 24 квітня 2021	Виконано
5	Розрахунок ризиків	25 травня 2021 – 4 травня 2021	Виконано
6	Розробка організаційних заходів	5 травня 2021 – 9 травня 2021	Виконано
7	Розробка інженерно-технічних заходів	10 травня 2021 – 13 травня 2021	Виконано
8	Моделювання загроз в OWASP Threat Dragon	14 травня 2021 – 18 травня 2021	Виконано
9	Моделювання роботи мережі в Cisco Packet Tracer	19 травня 2021 – 22 травня 2021	Виконано
10	Аналіз результатів тестування	23 травня 2021 – 24 травня 2021	Виконано
11	Написання пояснювальної записки	25 травня 2021 – 29 травня 2021	Виконано
12	Підготовка презентації та виступу	30 травня 2021 – 31 травня 2021	Виконано
13	Отримання відгуку керівника та рецензії на кваліфікаційну роботу	4 червня 2021 – 8 червня 2021	Виконано
14	Захист	29 червня 2021	Виконано

Студент _____ Патлай С.В.

Керівник _____ Пірог О.В.

РЕФЕРАТ

Кваліфікаційна робота містить розробку комплексної системи захисту інформації.

Основний зміст пояснювальної записки роботи викладено на 68 сторінках тексту, записка містить 14 таблиць, 2 ілюстрації. Список використаних літературних джерел налічує 54 найменування.

Метою роботи є розробка заходів із підвищення рівня захищеності інформаційної системи підприємства ТОВ «Механіка Трейд».

Для виконання поставленої задачі необхідно провести аналіз можливих загроз, та дослідити існуючу інформаційну систему та виявити в ній слабкі місця з точки зору безпеки.

Необхідно розробити комплекс заходів, що підвищать рівень захищеності інформаційних ресурсів підприємства.

Дипломна робота складатиметься із п'яти розділів, які міститимуть аналіз поточного стану інформаційної безпеки на підприємстві, розрахунки ризиків та збитків від загроз різного характеру та запропоновані заходи із підвищення рівня захищеності інформаційних ресурсів ТОВ «Механіка Трейд».

КЛЮЧОВІ СЛОВА: ЗАХИСТ, КОМП'ЮТЕРНА МЕРЕЖА, ІНФОРМАЦІЙНА СИСТЕМА, СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, CISCO.

					КБ.КВ.Б – 125 -14 -ПЗ			
Зм.	Арк.	№ докум.	Підпис	Дата	Проект комплексної системи захисту інформації торговельного підприємства	Літ.	Арк.	Аркушів
Розроб.		Патлай С.В.						
Керівник		Пірог О.В.А.					4	86
Рецензент.		Лобанчикова Н.М.				Державний університет «Житомирська політехніка», група КБ-1		
Зав. каф.		Єфіменко А. А.						

ABSTRACT

The work is devoted to the development of a comprehensive information security system at the company "Mechanics Trade". The work consists of five sections. The first section is devoted to the analysis of possible threats to information security, ways to reduce the risk of their occurrence and the principles of building a comprehensive information security system. The second section contains research on the current state of the document management system and its protection. The third section contains the calculation of enterprise risks and assessment of losses from them. The fourth section is devoted to the development of a comprehensive information security system. The fifth section contains modeling of information security risks of the enterprise and modeling of the local network.

KEY WORDS: SECURITY, COMPUTER NETWORK, INFORMATION SYSTEM, INFORMATION PROTECTION SYSTEM, CISCO.

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						9
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

Вступ	9
1 АНАЛІЗ ПОБУДОВИ КСЗІ	12
1.1 Організація КСЗІ	12
1.2 Загальні принципи побудови системи комплексного захисту інформації	16
2 АНАЛІЗ ДІЯЛЬНОСТІ ТОВ «МЕХАНІК ТРЕЙД»	21
2.1 Аналіз правового забезпечення захисту інформації	27
2.2 Дослідження існуючої системи захисту інформації	30
3 РОЗРАХУНОК РИЗИКІВ	42
4 РОЗРОБКА КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ	55
4.1 Організаційні заходи	55
4.2 Розробка інженерно-технічних заходів	59
5 МОДЕЛЮВАННЯ КСЗІ ТОВ «МЕХАНІК ТРЕЙД»	71
5.1 Моделювання загроз в OWASP Threat Dragon	71
5.2 Моделювання роботи мережі в Cisco Packet Tracer	75
Висновки	78
Перелік літературних джерел	81

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АМДЗ – апаратний модуль довіреного завантаження

АСОІ – автоматизована система обробки інформації

АПК – апаратно-програмний комплекс

АРМ – автоматизоване робоче місце

АС – автоматизована система

АСОД – автоматизована система обробки даних

БД – база даних

ДБЖ – джерело безперебійного живлення

КК – криптографічний комплекс

КПЗ – комплекс програмних засобів

КСЗІ – комплексна система захисту інформації

ЛОМ – локальна обчислювальна мережа

ММЕ – міжмережевий екран

НДМ – недокументовані можливості

ОІ – об'єкт інформатизації

ОС – операційна система

ПЗ – програмне забезпечення

ПЕОМ – персональна електронно-обчислювальна машина

ПЕМВН – побічні електромагнітні випромінювання та наведення

СЗІ – система захисту інформації

СКЗІ – система криптографічного захисту інформації

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						11
Змн.	Арк.	№ докум.	Підпис	Дата		

СКБД – система керування базами даних

ТПР – типове проектне рішення

ТЗ – технічні засоби

ПКЗД – пристрій криптографічного захисту даних

ЦККК – центр керування криптографічними ключами

ЕМП – електромагнітне поле

ЕЦП – електронно-цифровий підпис

EFS - Encrypting File System, шифруюча файлова система

IDS – Intrusion Detection Systems, система виявлення вторгнення

VPN – Virtual Private Network, віртуальні приватні мережі

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						12
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми: З кожним роком збільшується кількість інформації та зростає її цінність, в зв'язку з цим зростають вимоги щодо її захисту. Так само швидкими темпами удосконалюються комп'ютерні технології та збільшуються галузі їх застосування. Через щорічне поновлення комп'ютерних технологій виникають нові загрози для інформації. Отже, зросте необхідність захисту від них.

Забезпечення інформаційної безпеки останнім часом входить в число найбільш найкритичніших питань життєдіяльності підприємств та організації. Від грамотного підходу до реалізації захисту, в подальшому буде залежати фінансове благополуччя підприємства. І навпаки халатне ставлення до цього питання, може призвести до економічних втрат, пов'язаних з витоком інформації і навіть втратою довіри з боку зовнішнього оточення (покупців, компаньйонів).

Витік будь-якої інформації може негативно вплинути на діяльність підприємства. Особливу роль відіграє конфіденційна інформація, втрата якої може спричинити великі зміни в самій організації і матеріальні втрати.

Для забезпечення повноцінного захисту конфіденційної інформації необхідно проводити комплексний аналіз каналів витоку, каналів і методів несанкціонованого впливу на інформацію.

Для зниження ймовірності витоку інформації, яка циркулює в автоматизованій системі(АС), крім організаційно-правових та технічних засобів захисту використовуються програмно-апаратні засоби. Вони покликані захистити інформацію що зберігається в ЕОМ.

Необхідність забезпечення захисту цінної і критичною важливої інформації ставить перед підприємством завдання проектування системи

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						13
Змн.	Арк.	№ докум.	Підпис	Дата		

комплексного захисту інформації, невід'ємним аспектом якої є захист за допомогою програмно-апаратних засобів.

Метою кваліфікаційної роботи є розробка проекту комплексної системи захисту інформації в ТОВ «Механік Трейд».

Поставлена мета вимагає вирішення наступних задач:

- Визначити нормативно-правові аспекти захисту інформації на підприємстві ТОВ «Механіка Трейд»;
- Провести загальний аналіз існуючої системи захисту інформації ТОВ «Механіка Трейд».
- Запропонувати технічні та організаційні заходи для поліпшення системи захисту інформації;
- Розробити модель загроз інформаційній безпеці ТОВ «Механіка Трейд»
- Провести тестування та діагностику на вразливості.
- Розробити комплексну систему захисту інформації в ТОВ «Механік Трейд». Спроектowana система повинна забезпечувати захист інформації від несанкціонованого доступу до персональних ЕОМ, серверів баз даних і поштових серверів, , а також захист інформації при її передачі по каналах зв'язку.
- Розглянути захищені Інтернет технології, міжмережеві екрани, забезпечити облік і моніторинг ІР-трафіку, виявлення і попередження атак. Необхідно провести аналіз сучасної ситуації на ринку постачальників послуг і розробників засобів інформаційної безпеки і на його основі зробити вибір програмно-апаратних засобів забезпечення інформаційної безпеки. Повинен бути розроблений комплекс організаційних заходів щодо захисту інформації.
- Система повинна безперервно забезпечувати збереження цілісності, доступності та конфіденційності інформації, що зберігається, обробляється і передається.
- Захист інформації в системі повинна бути комплексним (повинні бути

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						14
Змн.	Арк.	№ докум.	Підпис	Дата		

захищені всі компоненти системи) і безперервним (захист інформації повинен бути забезпечена на всіх етапах її існування).

Об’єкт дослідження – система захисту інформації торговельного підприємства ТОВ «Механік Трейд».

Предмет дослідження – комплексна система захисту інформації.

Методи дослідження:

- емпіричні: аналіз, синтез, спостереження, розрахунок.
- експериментальні: комп’ютерне моделювання.

Інформаційну базу дослідження складають матеріали органів державної влади України, офіційні статистичні дані, технічна документація торговельного підприємства ТОВ «Механіка Трейд», а саме його накази по підприємству с приводу захисту інформації, функціональні обов’язки служби безпека, положення про комерційну таємницю та про документообіг на підприємстві, технічна документація на приміщення, апаратні та програмні засоби.

Практичне значення роботи полягає у розробці:

- політики безпеки документообігу на підприємстві ТОВ «Механіка Трейд» в паперовій та електронній формі;
- наданні рекомендацій щодо побудови програмного комплексу системи захисту інформації.

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						15
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1

АНАЛІЗ ПОБУДОВИ КСЗІ

1.1. Організація КСЗІ

Інформація є одним з найцінніших ресурсів будь-якого підприємства, тому забезпечення захисту інформації є однією з найважливіших і пріоритетних завдань.

Безпека інформаційної системи - це властивість, яка полягає в здатності системи забезпечити її нормальне функціонування, тобто забезпечити цілісність і секретність інформації. Для забезпечення цілісності та конфіденційності інформації необхідно забезпечити захист інформації від випадкового знищення або несанкціонованого доступу до неї[1].

Під цілісністю розуміється неможливість несанкціонованого або випадкового знищення, а також модифікації інформації. Під конфіденційністю інформації - неможливість витоку і несанкціонованого заволодіння під час зберігання, передачі чи приймання.

Відомі такі джерела загроз безпеці інформаційних систем[2]:

- антропогенні джерела, викликані випадковими або навмисними діями суб'єктів;
- техногенні джерела, що призводять до відмов технічних і програмних засобів через застарілість програмних і апаратних засобів або помилок в програмному забезпеченні;
- стихійні джерела, викликані природними катаклізмами або форс-мажорними обставинами.

У свою чергу антропогенні джерела загроз діляться:

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						16
Змн.	Арк.	№ докум.	Підпис	Дата		

- на внутрішні (дії з боку співробітників компанії) і зовнішні (несанкціоноване втручання сторонніх осіб із зовнішніх мереж загального призначення) джерела;
- на ненавмисні (випадкові) і навмисні дії суб'єктів.

Існує досить багато можливих напрямків витоку інформації і шляхів несанкціонованого доступу до неї в системах і мережах:

- перехоплення інформації;
- модифікація інформації (вихідне повідомлення або документ змінюється або підміняється іншим і відсилається адресату);
- підміна авторства інформації;
- використання недоліків операційних систем і прикладних програмних засобів;
- копіювання носіїв інформації і файлів з подоланням заходів захисту;
- незаконне підключення до апаратури та ліній зв'язку;
- маскування під зареєстрованого користувача і присвоєння його повноважень;
- введення нових користувачів;
- впровадження комп'ютерних вірусів.

Для забезпечення безпеки інформаційних систем застосовують системи захисту інформації, які являють собою комплекс організаційно - технологічних заходів, програмно - технічних засобів і правових норм, спрямованих на протидію джерел загроз безпеці інформації.

При комплексному підході методи протидії загрозам інтегруються, створюючи архітектуру безпеки систем. Необхідно відзначити, що будь-яка система захисту інформації не є повністю безпечною. Завжди доводиться вибирати між рівнем захисту і ефективністю роботи інформаційних систем.

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						17
Змн.	Арк.	№ докум.	Підпис	Дата		

До засобів захисту інформації інформаційних систем від дій суб'єктів відносяться:

- засоби захисту інформації від несанкціонованого доступу;
- захист інформації в комп'ютерних мережах;
- криптографічний захист інформації;
- електронний цифровий підпис;
- захист інформації від комп'ютерних вірусів.

1.1.1. Засоби захисту інформації від несанкціонованого доступу

Отримання доступу до ресурсів інформаційної системи передбачає виконання відразу трьох процедур: ідентифікація, аутентифікація і авторизація.

Ідентифікація - присвоєння користувачу (об'єкту або суб'єкту ресурсів) унікальних імен та кодів (ідентифікаторів) [3].

Аутентифікація - встановлення автентичності користувача, який представив ідентифікатор або перевірка того, що особа або пристрій, яка повідомила ідентифікатор є дійсно тим, за кого вона себе видає. Найбільш поширеним способом аутентифікації є привласнення користувачеві пароля і зберігання його в комп'ютері [4].

Авторизація - перевірка повноважень або перевірка права користувача на доступ до конкретних ресурсів і виконання певних операцій над ними. Авторизація проводиться з метою розмежування прав доступу до мережевих і комп'ютерних ресурсів [5].

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						18
Змн.	Арк.	№ докум.	Підпис	Дата		

1.1.2. Захист інформації в комп'ютерних мережах

Локальні мережі підприємств дуже часто підключаються до мережі Інтернет. Для захисту локальних мереж компаній, як правило, застосовуються міжмережеві екрани - брандмауери (firewalls). Екран (firewall) - це засіб розмежування доступу, який дозволяє розділити мережу на дві частини (межа проходить між локальною мережею і мережею Інтернет) і сформувати набір правил, що визначають умови проходження пакетів з однієї частини в іншу. Екрани можуть бути реалізовані як апаратними засобами, так і програмними[6].

1.1.3. Криптографічний захист інформації

Для забезпечення секретності інформації застосовується її шифрування або криптографія. Для шифрування використовується алгоритм або пристрій, який реалізує певний алгоритм. Управління шифруванням здійснюється за допомогою коду ключа, що змінюється.

Витягти зашифровану інформацію можна тільки за допомогою ключа. Криптографія - це дуже ефективний метод, який підвищує безпеку передачі даних в комп'ютерних мережах і при обміні інформацією між віддаленими комп'ютерами [8].

1.1.4. Електронний цифровий підпис

Для виключення можливості модифікації вихідного повідомлення або підміни цього повідомлення іншим необхідно передавати повідомлення разом з електронним підписом.

Електронний цифровий підпис - це послідовність символів, отримана в результаті криптографічного перетворення вихідного повідомлення з використанням закритого ключа і дозволяє визначати цілісність

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						19
Змн.	Арк.	№ докум.	Підпис	Дата		

повідомлення та належність його автору за допомогою відкритого ключа [21].

Іншими словами повідомлення, зашифроване за допомогою закритого ключа, називається електронним цифровим підписом. Відправник передає незашифроване повідомлення в початковому вигляді разом з цифровим підписом. Одержувач за допомогою відкритого ключа розшифровує набір символів повідомлення з цифрового підпису і порівнює їх з набором символів незашифрованого повідомлення.

При повному збігу символів можна стверджувати, що отримане сполучення не модифіковано і належить його автору.

1.1.5. Захист інформації від комп'ютерних вірусів

Комп'ютерний вірус - це невелика шкідлива програма, яка самостійно може створювати свої копії та впроваджувати їх в програми (виконувані файли), документи, завантажувальні сектори носіїв даних і поширюватися по каналах зв'язку [20].

Залежно від місця існування основними типами комп'ютерних вірусів є:

- Програмні (вражають файли з розширенням COM і EXE) віруси
- завантажувальні віруси
- Макровіруси
- Мережеві віруси

1.2. Загальні принципи побудови системи комплексного захисту інформації

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						20
Змн.	Арк.	№ докум.	Підпис	Дата		

При побудові будь-якої системи необхідно визначити принципи, відповідно до яких вона буде побудована. КСЗІ - складна система, яка функціонує, як правило, в умовах невизначеності, що вимагає значних матеріальних витрат. Тому визначення основних принципів КСЗІ дозволить визначити основні підходи до її побудови[3].

Принцип законності полягає у відповідності вжитих заходів із законодавством України про захист інформації, а в разі відсутності відповідних законів - іншим державним нормативним документам щодо захисту.

Відповідно до принципу повноти інформації, що захищається, захисту підлягає не тільки інформація, яка становить державну, комерційну або службову таємницю, а й та частина несекретної інформації, втрата якої може завдати шкоди її власнику. Реалізація цього принципу дозволяє забезпечити і охорону інтелектуальної власності.

Принцип обґрунтованості захисту інформації полягає у встановленні шляхом експертної оцінки доцільності засекречування та захисту тієї чи іншої інформації, ймовірних економічних та інших наслідків такого захисту виходячи з балансу життєво важливих інтересів держави, суспільства і громадян. Це, в свою чергу, дозволяє витратити кошти на захист тільки тієї інформації, втрата або витік якої може завдати дійсної шкоди її власнику.

Принцип створення спеціалізованих підрозділів по захисту інформації полягає в тому, що такі підрозділи є неодмінною умовою організації комплексного захисту, оскільки тільки спеціалізовані служби здатні належним чином розробляти і впроваджувати захисні заходи і здійснювати контроль за їх виконанням.

Принцип участі в захисті інформації всіх дотичних з нею осіб виходить з того, що захист інформації є службовим обов'язком кожної особи, що має за

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						21
Змн.	Арк.	№ докум.	Підпис	Дата		

родом роботи, що виконується, відношення до інформації, що захищається, і така участь дає можливість підвищити якість захисту.

Принцип персональної відповідальності за захист інформації вимагає, щоб кожна особа персонально відповідало за збереження і нерозголошення довіреної йому інформації, що захищається, а за втрату або поширення такої інформації вона несе кримінальну, адміністративну або іншу відповідальність.

Принцип наявності і використання всіх необхідних сил і засобів для захисту полягає в тому, що КСЗІ вимагає, з одного боку, участі в ній керівництва підприємства і спеціальної служби захисту інформації та всіх виконавців, які працюють із інформацією, що захищається, з іншого боку, використання різних організаційних форм і методів захисту, з третього боку, наявність необхідних матеріально-технічних ресурсів, включаючи технічні засоби захисту.

Принцип превентивності вжитих заходів щодо захисту інформації передбачає апріорне випереджаюче завчасне вжиття заходів щодо захисту до початку розробки або отримання інформації. З цього принципу випливає, зокрема, необхідність розробки захищених інформаційних технологій.

Серед розглянутих принципів навряд чи можна виділити більш-менш важливі. А при побудові КСЗІ важливо використовувати їх в сукупності.

Оскільки комплексна система захисту інформації призначена забезпечувати безпеку всієї інформації, що захищається, до неї ставляться такі вимоги:

- вона повинна бути прив'язана до цілей і завдань захисту інформації на конкретному підприємстві;
- вона повинна бути цілісною: містити всі її складові, мати структурні зв'язки між компонентами, що забезпечують її узгоджене функціонування;

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						22
Змн.	Арк.	№ докум.	Підпис	Дата		

- вона повинна бути всеохоплюючою, що враховує всі об'єкти і складові їх компоненти захисту, всі обставини і фактори, що впливають на безпеку інформації, і всі види, методи і засоби захисту;
- вона повинна бути достатньою для вирішення поставлених завдань і надійної в усіх елементах захисту, тобто базуватися на принципі гарантованого результату;
- вона повинна бути «вмонтованою» в технологічні схеми збору, зберігання, обробки, передачі і використання інформації;
- вона повинна бути компонентно, логічно, технологічно і економічно обґрунтованою;
- вона повинна бути придатною до реалізації та забезпеченою всіма необхідними ресурсами;
- вона повинна бути простою і зручною в експлуатації і управлінні, а також у використанні законними споживачами;
- вона повинна бути безперервною;
- вона повинна бути досить гнучкою, здатною до цілеспрямованого пристосуванню при зміні компонентів її складових частин, технології обробки інформації, умов захисту.

Таким чином, забезпечення безпеки інформації - безперервний процес, який полягає в контролі захищеності, виявленні вузьких місць в системі захисту, обґрунтуванні і реалізації найбільш раціональних шляхів вдосконалення та розвитку системи захисту:

- безпеку інформації в системі обробки даних може бути забезпечена лише при комплексному використанні всього арсеналу наявних засобів захисту;
- ніяка система захисту не забезпечить безпеки інформації без належної підготовки користувачів і дотримання ними всіх правил захисту;

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						23
Змн.	Арк.	№ докум.	Підпис	Дата		

- ніяку систему захисту не можна вважати абсолютно надійною, оскільки завжди може знайтися зловмисник, який знайде лазівку для доступу до інформації.

Висновки

В розділі приведено огляд основних загроз інформаційним системам, засобів захисту від них, та показано основні принципи побудови КСЗІ та вимоги до них.

Показано, що не існує універсальних рішень, які підійдуть для всіх випадків і реалізація комплексної системи захисту інформації залежить від особливостей підприємства, на якому вона запроваджується. Тому для реалізації комплексної системи захисту інформації першочерговою задачею є аналіз структури підприємства та особливостей його роботи.

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						24
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2

АНАЛІЗ ДІЯЛЬНОСТІ ТОВ «МЕХАНІК ТРЕЙД»

Товариство із обмеженою відповідальністю «Механік Трейд» є комерційним підприємством, який зареєстровано за адресою: м. Житомир, вул. Кафедральна, 5. ТОВ «Механік Трейд» діє на основі законодавства України та її конституції.

Основною метою діяльності є отримання прибутку та задоволення потреб промислових підприємств та приватних осіб в запасних частинах до промислового обладнання та автомобільної техніки

Місії компанії: організовувати для клієнтів безперебійні поставки запасних частин до автомобільної техніки та промислового обладнання. Стати взірцем високої якості обслуговування і швидкості роботи. Давати співробітникам компанії можливість реалізовувати свої устремління. Запровадження комплексної системи захисту інформації в свою чергу збільшить вірогідність досягнення цілей за рахунок зменшення ризиків витоку інформації і відповідно покращить роботу підприємства як за рахунок стабільної роботи автоматизованих систем (вчасне на в повному обсязі виконання замовлень), так і за рахунок переваг в конкурентній боротьбі за покупців, що досягається збереженням відомостей, які становлять комерційну таємницю конфіденційними.

Цінності компанії:

- професіоналізм,
- націленість на результат,
- порядність,
- чесність,

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						25
Змн.	Арк.	№ докум.	Підпис	Дата		

- командність,
- відповідальність,
- ініціативність,

Дані цінності це збірка принципів, на підставі яких керівники будуть ставити цілі, і визначати, чи досягнуті вони. Ці цінності лежать в основі взаємин між співробітниками.

Наявність формалізованих правил корпоративної культури відіграють важливу роль в побудові КСЗІ. Оголошення формалізованих правил дозволяє ставити цілі та планувати заходи по їх досягненню, тобто надає напрямок руху в процесі вдосконалення механізмів захисту інформаційних ресурсів компанії.

Асортимент продукції складає запасні частини до агротехніки, автомобільної техніки, оливи та мастильні матеріали, розхідники та запасні частини до промислового обладнання.

Торгівля проводиться як гуртовим клієнтам, так і роздрібним.

Така специфіка роботи обумовлює наступну структуру підприємства: роздрібний магазин, склад та офіс.

Підприємство також запровадило можливість покупок через мережу інтернет. Для реалізації цієї можливості запроваджено інтернет магазин.

Чисельність персоналу підприємства: директор, заступник директора з загальних питань, бухгалтерія (5 осіб), фахівець з найму і навчання персоналу, спеціаліст із закупівель, прибиральниця, ІТ-відділ (2), транспортний відділ (4), в комерційному відділі працюють 9 чоловік, на складах – 7, відділ охорони – 5 чоловік, роздрібний магазин – 8 чоловік. В цілому в організації числиться 45 чоловік.

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						26
Змн.	Арк.	№ докум.	Підпис	Дата		

Обов'язки між працівниками чітко поділені і кожному із них виділений конкретний напрямок, за який від відповідає:

Бухгалтерія:

- головний бухгалтер - відповідає в цілому за роботу підрозділу та консолідує інформацію, що формується кожний із підлеглих;
- бухгалтер із зарплати – нарахування зарплат, бонусів та премій, податкові питання в галузі заробітної плати;
- бухгалтер із первинного обліку(2) – проведення вхідних та вихідних документів;
- бухгалтер по обліку товарно-матеріальних цінностей

ІТ відділ:

- інженер-електронник – відповідає за апаратну частину обладнання
- системний адміністратор – відповідає за безпеку мережі та адміністрування мережі.

Транспортний відділ:

- керівник – організовує роботу по переміщенню товару.
- водії 3 чоловіки - відповідають за переміщення товарів, завантаження та розвантаження автомобілів(водій навантажувача).

Комерційний відділ:

- керівник – організовує роботу відділу;
- менеджер із постачання – організовує закупку товару;
- менеджер із продажів – організовує продаж товарів;
- консультанти 6 чоловік – надають консультації по характеристикам товарів за телефоном та он-лайн. Оформляють замовлення. Робота в 2 зміни.

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						27
Змн.	Арк.	№ докум.	Підпис	Дата		

Складський відділ:

- керівник відділу – організовує роботу відділу;
- приймальник – матеріально відповідальна особа відповідає за видачу та приймання товарів;
- вантажники – 5 чоловік – відповідають за формування посилок, переміщення товарів всередині складу.

Охорона:

- начальник охорони – організовує роботу відділу;
- спеціаліст із відео нагляду;
- охоронець – 3 чоловіки – здійснюють фізичну охорону підприємства;

Роздрібний магазин:

- керівник – організовує роботу магазину;
- вантажник – здійснює переміщення товарів із підсобних приміщень в торговельну залу;
- продавець – 5 чоловік – надання консультацій, допомога у виборі товарів.
- касир – робота із готівковою оплатою та банківський терміналом.

Кожен із зазначених працівників має доступ лише до тієї частини загальної інформації, що необхідна для його роботи.

На даний момент організація зіткнулася з проблемою - плинністю кадрів в комерційному відділі. Така ситуація негативно впливає на функціонування системи захисту інформації. це обумовлено тим, що по статистиці найбільш уразливою ланкою в системі захисту інформації є персонал та його дії. В даній ситуації негативним фактором є те, що нові працівники роблять багато ненавмисних помилок при роботі в процесі адаптації. Ці помилки в роботі можуть наражати на небезпеку

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						28
Змн.	Арк.	№ докум.	Підпис	Дата		

автоматизовану інформаційну систему, а також стають можливі факти ненавмисного витоку конфіденційної інформації.

Також не можливо не враховувати той факт, що із звільненням працівників відбувається витікання інформації разом із її носіями – працівниками до конкуруючих підприємств. Це відбувається внаслідок того, що працівники влаштовуючись на підприємства подібного профілю використовують вже відомі напрацювання в своїй роботі.

Основні причини плинності кадрів:

- Погана адаптація або її відсутність у співробітників на випробувальному терміні. Через відділ продажів щодня проходить величезний потік інформації, більшість рішень необхідно приймати оперативно і по можливості точно, кожна помилка менеджера коштує грошей для компанії. Новоприбулі працівники не встигають справлятися з обсягами інформації і не проходять випробувальний термін.
- Перспектива отримання вищої зарплати. Співробітник, який пропрацював на підприємстві рік і більше та отримав значний досвід в сфері продажів, може розраховувати на отримання посади в іншому підприємстві на кращих умовах.
- Відсутність кар'єрного росту. У комерційному відділі існують посади: помічник менеджера, менеджер і начальник відділу продажів. Проміжних посад між двома останніми не існує, працівник, який прийшов на місце менеджера, залишиться на цій посаді на весь час роботи в компанії.

Організаційна структура ТОВ «Механік Трейд» є дивізійною. Дивізійний підхід до організаційної структури характеризується тим, що вищий рівень в організації (директор) централізує планування та розподіл основних ресурсів, приймає стратегічні рішення, в той час, як підрозділи приймають оперативні рішення і відповідальні за отримання прибутку.

Така система дозволяє провести розмежування повноважень та

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						29
Змн.	Арк.	№ докум.	Підпис	Дата		

провести ранжування доступу до різного рівня інформації відповідно до займаної посади та покладеним на працівника обов'язкам.

В цілому, дивізійна схема в побудові організації дозволяє останній продовжувати своє зростання і ефективно здійснювати управління різними видами діяльності і на різних ринках [12].

Проаналізувавши діяльність ТОВ «Механік Трейд» були виявлені слабкі і сильні сторони організації.

Сильні сторони:

- Хороші ринкові позиції, що виражаються у високій ринковій частці при постійному зростанні продажів, вдале розташування офісу та складу, високий рівень знання бренду при збереженні рекламно-маркетингової активності і в цілому позитивний імідж компанії в очах цільової аудиторії.
- Надійність, обумовлена успішною діяльністю компанії протягом більше десяти років, кредитною історією і стійкими фінансовими показниками.
- Професіоналізм команди менеджерів при регулярному підвищенні кваліфікації співробітників.
- Диверсифікація і розвиток додаткових напрямків бізнесу.

Сильні сторони, що приведені вище показують, що підприємство є стабільно працюючим та здатне інвестувати кошти в систему охорони інформації та персонал. Крім того, робота досить розгалуженої та складної системи обліку товарно-матеріальних ресурсів призводить до високої чутливості підприємства до питань інформаційної безпеки.

Слабкі сторони:

- Дублювання функцій на різних рівнях управління в підрозділах (продуктових і територіальних), що призводить до повторного виконання робіт і зростання загально організаційних і накладних витрат, поганій взаємодії при вирішенні питань, тяганині.
- Відсутність (недостатність) проактивної поведінки, стратегічного мислення.
- Недостатньо швидка реакція на запити ринку.

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						30
Змн.	Арк.	№ докум.	Підпис	Дата		

– Можливість витоку інформації, що становить комерційну таємницю, відсутність оперативного управлінського обліку.

В області документарного та інформаційного забезпечення існують такі проблеми функціонування:

– Розрізненість місць зберігання та відсутність резервного копіювання файлів. Підрозділи ведуть документацію по операціях самостійно і раз на місяць передають всі документи, що накопичилися, в бухгалтерію.

Часто відбувається втрата документів, або через неоперативність відповіді бухгалтерії проблеми з оформлення документів так і залишаються невирішеними.

– У зв'язку з віддаленістю доступу і якістю Internet-з'єднання на території підрозділів відбуваються збої в роботі автоматизованої програми, що призводить до збою нумерації документів або і зовсім зупиняє роботу по виписці документів.

– Відсутність єдиного електронного сховища документів призводить до втрати і тривалого пошуку документів.

– Неповне та (або) ненадійне документування своєї діяльності підрозділами.

2.1. Аналіз правового забезпечення захисту інформації

Нормативно-методична база діловодства - це сукупність законів, нормативних правових актів та методичних документів, що регламентують технологію створення, обробки, зберігання і використання документів в поточній діяльності установи, а також регламентують роботу служби діловодства - її структуру, функції, штати, технічне забезпечення і деякі інші аспекти [9].

В даний час регламентація документування, достовірності і захисту документарного забезпечення управління ведеться в декількох напрямках:

- законодавче регулювання,
- стандартизація,
- розробка нормативних і нормативно-методичних документів

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						31
Змн.	Арк.	№ докум.	Підпис	Дата		

загальнодержавної дії.

У своїй діяльності ТОВ «Механік Трейд» керується Конституцією України, законами та іншими нормативними правовими актами. Закон України 80/94-ВР «Про захист інформації в інформаційно-телекомунікаційних системах» встановив ряд термінів, врегулював відносини, що виникають при створенні та використанні інформаційних технологій [7].

Принципи управління документами в рівній мірі можуть бути застосовані до документів на різних носіях, незалежно від способу доставки документів. Це особливо важливо, тому що спостерігається перехід від традиційного паперового документообігу іде не до електронного, а до змішаного документообігу. Законом встановлено право власності на окремі документи і масиви документації, категорії інформації за рівнями доступу до неї [7].

Вся інформація в компанії ТОВ «Механік Трейд» захищена відповідно до ступеня її важливості та конфіденційності. Ніколи і ні за яких умов співробітники не повинні використовувати в своїх цілях або в цілях третіх осіб закриту інформацію, отриману під час роботи в Компанії згідно Положення про комерційну таємницю[22]. До організаційних заходів щодо захисту інформації відноситься розмежування прав доступу в приміщення і до інформації. Це серія заходів, оснований на різних документах.

У «Механік Трейд» застосовуються регламенти, порядок доступу в приміщення і до ресурсів, посадові інструкції тощо. Головне правило у всіх цих документах одне - кожен співробітник повинен мати доступ тільки до тієї інформації, яка йому необхідна для виконання своїх службових обов'язків.

Відповідно до цього розмежовується доступ в приміщення, до комп'ютерних і мережових ресурсів, програмного забезпечення. Частина інформації, до якої мають доступ співробітники компанії, є конфіденційною.

Компанія чітко регламентує в Положенні про комерційну таємницю[22] те, яка саме інформація є конфіденційною, і доводить це до

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						32
Змн.	Арк.	№ докум.	Підпис	Дата		

відома співробітників. Поступаючи на роботу, співробітники приймають на себе зобов'язання не розголошувати інформацію, що є комерційною таємницею. Дана умова має юридичну силу після підписання співробітниками «Угоди про нерозголошення комерційної таємниці», складеного юристами компанії. Ця Угода набуває чинності з моменту його підписання і діє протягом 3 (Трьох) років з моменту припинення трудового договору з працівником.

Під комерційною таємницею в цій Угоді розуміється режим конфіденційності інформації, що дозволяє її власникові при існуючих або можливих обставин збільшити доходи, уникнути невиправданих витрат, зберегти положення на ринку товарів, робіт, послуг або отримати іншу комерційну вигоду.

Інформація, що відноситься до комерційної таємниці, визначена у Положенні про комерційну таємницю[22].

До конфіденційної інформації ТОВ «Механік Трейд» згідно з цим переліком відносяться відомості:

1) Управління - відомості про організаційну та функціональну структури управління підприємством.

2) Плани - відомості про плани інвестицій, закупівель і продажів.

3) Наради - відомості про цілі, розглянуті питання, результати, факти проведення нарад на підприємстві.

4) Ринок - відомості про результати вивчення ринку, про ринкової стратегії підприємства, відомості про ефективність комерційної діяльності підприємства.

5) Переговори - відомості, про пропозиції, які отримані і опрацьовуються, відомості про терміни, місце, предмет переговорів, рівень пропонуваніх цін.

6) Контракти - умови комерційних контрактів з іншими підприємствами.

7) Ціни - відомості про методи розрахунків, структури, рівні цін на

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						33
Змн.	Арк.	№ докум.	Підпис	Дата		

продукцію і розміри знижок.

8) Програмні продукти - відомості про оригінальні програмні продукти, що застосовуються підприємством.

9) Безпека - відомості про порядок і стан організації охорони, пропускний режим, системи сигналізації та відео спостереження; відомості, що становлять комерційну таємницю підприємств.

10) Оплата праці - відомості про систему оплати, структуру, розмірах, терміни та способи отримання заробітної плати окремих співробітників.

При співпраці з клієнтами, постачальниками та іншими зовнішніми компаніями співробітники повинні виступати від імені компанії і тільки в її цілях (а не особистих).

У співробітників, так і у їхніх найближчих родичів не повинно бути особистих фінансових інтересів в будь-якій організації, що співпрацює або конкурує з компанією «Механік Трейд», якщо ці фінансові інтереси приведуть до якогось конфлікту інтересів, або створять конфлікт інтересів з компанією .

Якщо співробітник поєднує трудову діяльність в Компанії з роботою в іншій організації, то його додаткова трудова діяльність:

- Не може здійснюватися в компанії, яка є конкурентом «Механік Трейд».
- Може здійснюватися тільки у вільний від виконання основних службових обов'язків час.
- не повинна негативно впливати на виконання його основних обов'язків.
- не повинна завдавати шкоди репутації або матеріальним інтересам компанії.
- не суперечить положенням Угоди про нерозголошення комерційної таємниці.
- Повинна бути відома безпосередньому керівнику.

2.2. Дослідження існуючої системи захисту інформації

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						34
Змн.	Арк.	№ докум.	Підпис	Дата		

Документообіг на підприємстві здійснюється у вигляді потоків документів, що циркулюють між пунктами обробки інформації (керівники, фахівці, службовці) і пунктами технічної обробки (бухгалтерія). Існують три основні потоки документів: вхідний, вихідний, внутрішній.

В організації прийом вхідних документів здійснює помічник менеджера (по суті виконує функції секретаря), розглядає кореспонденцію, що поступила, і сортує документи по відділах, попередньо вносить відомості про документ в журнал вхідної кореспонденції і привласнює вхідний номер. У відділах документи розподіляються між виконавцями.

Вхідні документи в день надходження поділяють на документообіг, що направляються керівникам, в структурні підрозділи і окремим виконавцям.

Вихідні документи формуються в підрозділах. Проект документа складається виконавцем і узгоджується із зацікавленими посадовими особами або структурними підрозділами. Виконавець перевіряє його зміст, додатки до документа. Співробітники бухгалтерії перевіряють правильність оформлення, наявність необхідних реквізитів.

Контроль виконання документів в установі здійснює керівник підрозділу. У контроль виконання документів входить:

- постановка документа на контроль,
- перевірка своєчасного доведення документів до виконавців,
- попередня перевірка і регулювання ходу виконання,
- облік і узагальнення результатів контролю, виконання документів,
- інформування керівника за результатами виконання особливо важливих документів.

Терміни виконання встановлюються керівником підрозділу.

Кожен документ в організації реєструється в день надходження, а створювані

- у день підписання або затвердження.

У ТОВ «Механік Трейд» використовується журнальна реєстрація

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						35
Змн.	Арк.	№ докум.	Підпис	Дата		

кореспонденції. Всі журнали мають номери по номенклатурі справ. При реєстрації документ отримує свій порядковий номер, який проставляється на документі.

Найбільш поширеними внутрішніми документами є:

1. Розпорядження Директора та керівника підрозділу.

Створюються для вирішення оперативних завдань і прояснення спірних питань, підписуються всіма менеджерами при ознайомленні.

2. Службова записка, включає в себе наступні поля:

- кому, від кого, дата;
- ситуація (проблема);
- дані (факти);
- рішення (пропозиції співробітника за рішенням ситуації, проблеми, строки; відповідальна особа на період відсутності, його підпис).

Для забезпечення безпеки на території ТОВ «Механік Трейд» ведеться відео спостереження, а саме в охоронному пункті, на території бази і в комерційному відділі. На в'їзді на територію бази компанії організований контрольно-пропускний пункт, потрапити на територію можливо лише за умови пред'явлення пропуску. Наприклад, при надходженні товару на склад відбувається наступне:

1. Представнику постачальника передається копія товарної накладної, бланк здачі товару на склад (в ньому проставляється номер і дата товарної накладної) і пропуск на в'їзд на територію складу.

2. Після вивантаження товару представник постачальника повертається в офіс до підписаного комірником бланком здачі товару на склад.

3. Постачальнику передаються документи, попередньо перевірені бухгалтерією і завірені директором підрозділу.

4. На підставі отриманих документів складається акт узгодження, який включає в себе:

- номер і дату товарної накладної,
- дату фактичного прибуття товару на склад,

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						36
Змн.	Арк.	№ докум.	Підпис	Дата		

- найменування постачальника,
- умови і вартість доставки,
- розрахунково-закупівельні і продажні ціни на товар.

5. Дане узгодження складає і підписує керівник підрозділу, підкріплює бланком здачі товару на склад і передає в бухгалтерію.

6. Бухгалтерія вносить всі дані в інформаційну систему «1С: Підприємство 8»).

Приміщення, в яких обробляється, або зберігається важлива для організації інформація, мають надійні стіни, підлогу, стелю, вікна та двері. У неробочий час (ніч, вихідні, свята), дані приміщення надійно закриті і здані під охорону. Доступ стороннім особам (в тому числі і співробітникам організації) в дані приміщення і на територію бази заборонений.

Кабінети оснащені системами пожежного оповіщення. При цьому системи пожежної сигналізації виведені на пульт охорони. Приміщення, в яких зберігається або обробляється важлива для організації інформація, оснащені системами контролю доступу. Щоб потрапити з комерційного відділу в інші відділи організації, наприклад в бухгалтерію, необхідно набрати цифровий код на магнітному замку двері, який змінюється 1 раз на місяць.

До основних завдань ТОВ «Механік Трейд» відносять:

- закупівлю товару і продукції і їх реалізацію;
- збереження власних матеріальних і нематеріальних ресурсів;
- стабільність здійснення бізнес-процесів.

На підприємстві використовується система програм "1С: Підприємство 8», яка включає в себе платформу і прикладні рішення, розроблені на її основі, для автоматизації діяльності організацій і приватних осіб.

Сама платформа не є програмним продуктом для використання кінцевими користувачами, які зазвичай працюють з одним з багатьох прикладних рішень (конфігурацій), розроблених на даній платформі [23].

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						37
Змн.	Арк.	№ докум.	Підпис	Дата		

За рахунок гнучкості платформи «1С: Підприємство 8» використовується для вирішення наступного:

- автоматизація діяльності торгових підприємств;
- підтримка оперативного управління підприємством;
- автоматизація організаційної і господарської діяльності;
- ведення бухгалтерського обліку з декількома планами рахунків і довільними вимірами обліку, регламентована звітність;
- проведення управлінського обліку і формування аналітичної звітності;
- вирішення завдань планування, бюджетування і фінансового аналізу;
- розрахунок зарплати і управління персоналом.

Технологічна платформа містить наступні рішення, що дозволяють посилити інформаційну безпеку, достовірність і захист інформації:

1. Відмовостійкість.

Система забезпечує безперебійну роботу користувачів при програмних і апаратних збоїв в кластері серверів.

Такі події, як вихід з ладу робочого сервера (в тому числі і центрального сервера), аварійне (або планове) завершення робочого процесу або менеджера кластера не впливають на роботу користувачів. Користувачі продовжують працювати так, як ніби нічого не сталося.

У разі фізичного розриву з'єднання користувача з кластером (наприклад, прибиральниця висмикнула дріт) і подальшого його відновлення користувач може продовжити роботу без повторного з'єднання з інформаційною базою і без втрати своїх поточних даних.

Якщо який-небудь робочий процес завершився аварійно, кластер запускає замість нього один з неактивних резервних процесів і автоматично перерозподіляє наявне навантаження на нього. Кластер «запам'ятовує»

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						38
Змн.	Арк.	№ докум.	Підпис	Дата		

користувачів, що підключилися і стан дій, що виконуються ними, завдяки тому, що для кожного користувача створюється власний сеанс.

У разі втрати фізичного з'єднання кластер буде очікувати відновлення з'єднання з цим користувачем. У переважній більшості випадків після відновлення з'єднання користувач зможе продовжити роботу з того «місця», на якому вона була припинена. При цьому не потрібне повторне підключення до інформаційної бази, для кожного користувача створюється власний сеанс.

2. Механізм криптографії.

Механізм криптографії дозволяє прикладним рішенням використовувати криптографічні операції для обробки даних, що зберігаються в інформаційній базі.

Механізм криптографії не містить реалізації власне алгоритмів криптографії. Він забезпечує набір об'єктів, що дозволяють взаємодіяти із зовнішніми модулями криптографії сторонніх виробників - криптопровайдерами.

Для взаємодії з криптопровайдерами в операційній системі Windows використовується інтерфейс CryptoAPI. Таким чином, прикладні рішення можуть взаємодіяти з будь-якими криптопровайдерами, що підтримують цей криптографічний інтерфейс.

На даний момент дані можливості з криптографічного захисту не використовуються.

3. Система прав доступу.

Система прав доступу дозволяє описувати набори прав, що відповідають посадам користувачів або виду діяльності.

Крім цього, для об'єктів, що зберігаються в базі даних (довідники, документи, реєстри і т.д.) можуть бути визначені права доступу до окремих полів і записів. Наприклад, користувач може оперувати документами

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						39
Змн.	Арк.	№ докум.	Підпис	Дата		

(накладними, рахунками і т.д.) певних контрагентів і не мати доступу до аналогічних документів інших контрагентів.

Серед дій над об'єктами, що зберігаються в базі даних (довідниками, документами і т.д.), є дії, що відповідають за читання або зміні інформації, що зберігається в базі даних. До таких дій відносяться:

- читання - отримання записів або їх фрагментів з таблиці бази даних;
- додавання - додавання нових записів без зміни існуючих;
- зміна - зміна існуючих записів;
- видалення - видалення деяких записів без внесення змін до залишилися.

У ТОВ «Механік Трейд» права найбільш відрізняються у співробітників комерційного відділу:

- найбільші правами доступу має керівник підрозділу,
- права менеджерів і помічника менеджера включають в себе стандартний набір прав, необхідних для виконання посадових обов'язків,
- у стажистів встановлений мінімальний об'єм прав.

4. Список користувачів.

Список користувачів - це один з інструментів адміністрування.

Система дозволяє вести список користувачів, яким дозволена робота з системою. Цей список не є частиною прикладного рішення, а створюється окремо в конкретній організації, в якій використовується система.

Адміністратор інформаційної бази має можливість додавати, копіювати, видаляти користувачів, а також модифікувати дані користувача. Створення нових користувачів можливо також шляхом копіювання вже існуючих користувачів.

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						40
Змн.	Арк.	№ докум.	Підпис	Дата		

Для кожного користувача може бути задане ім'я, яке ідентифікує користувача в системі, повне ім'я, яке використовується при відображенні довідкової інформації, і порядок аутентифікації (розпізнавання) користувача системою. У разі використання аутентифікації «1С: Підприємства» користувачу можна заборонити змінювати пароль.

Список користувачів грає важливу роль в забезпеченні безпеки і підприємства, керівник підрозділу може переглянути яким співробітником і які дії здійснювалися в програмі протягом певного часового періоду. Кожен співробітник заходить в програму під своїм ім'ям, використовуючи пароль. При такому порядку доступу до програми всі операції з інформацією прозорі, інформація не може бути змінена або видалена безкарно.

5. Журнал реєстрації.

Журнал реєстрації містить інформацію про те, які події відбувалися в інформаційній базі в певний момент часу або які дії виконував той чи інший користувач. Для кожного запису журналу, що відображає зміну даних, відображається статус завершення транзакції (транзакція завершена успішно, або ж транзакція скасована). Це дозволяє зрозуміти змінені реально дані чи ні.

Сервер 1С встановлено на персональному комп'ютері, який має наступні параметри: Intel Core i3 2100 3.1GHz / 3MB / NoTurbo Макс. об'єм пам'яті: 32 ГБ. Типи пам'яті: DDR3-1066 / 1333. Кількість каналів пам'яті: 2. Макс. пропускна здатність пам'яті: 21 Гб / с.

На підприємстві не запроваджено реєстрацію носіїв інформації, крім тих, що вбудовані в обладнання інформаційних систем(накопичувачі на жорстких магнітних дисках SSD накопичувачі).

Всі відділи компанії оснащені робочими станціями з наступними параметрами: Intel Atom D525 (1.8 ГГц) / RAM 2 ГБ / HDD 1000 ГБ / nVidia ION 2, 512 МБ / DVD +/- RW Slim.

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						41
Змн.	Арк.	№ докум.	Підпис	Дата		

Для друку документів у відділах компанії встановлені принтери, з наступними параметрами: SamsungSCX-4600 + USB cable / 360 МГц / 256Мб / Технологія друку: Лазерний друк (ч / б) / Швидкість друку становить 22 стор. / хв. при роздільній здатності до 1200х600 точок на / дюйм.

Офіси компанії оснащені багатофункціональними пристроями з наступними параметрами: SamsungCLX-6220FX + USB cable / 360 МГц / 256Мб / Технологія друку: Лазерний друк (кольорова) / Вбудований факс / Мережеві інтерфейси: Ethernet / Швидкість друку становить 20 стор. / хв.

Директор компанії для роботи використовує ноутбук, який має наступні параметри: IntelAtomD525 (1.8 ГГц) / RAM 2 ГБ / HDD 250 ГБ / NVIDIA ION 2 / без ОДР / LAN / Wi-Fi / Bluetooth / веб-камера.

Всі робочі станції офісу з'єднані в локальну мережу каналами зв'язку, за допомогою технології передачі даних Ethernet з використанням маршрутизаторів великої потужності - AirLive A.Duo. Даний маршрутизатор підтримує одночасно два діапазони частот - 5 ГГц і 2,4 ГГц і забезпечує високу швидкість передачі даних до 108 Мбіт/с в режимі Turbo.

На сьогоднішній день бухгалтерський і податковий облік в компанії здійснюється бухгалтерією за допомогою програмного продукту «1С: Бухгалтерія 8.0», який забезпечує високий рівень автоматизації ведення бухгалтерського і податкового обліку і підготовки обов'язкової (регламентованої) звітності в госпрозрахункових організаціях.

Сервер 1С - це програма і комп'ютер, на якому встановлена і працює дана програма.

Сервер 1С не є однією програмою, а складається з кілька процесів :

- Агент сервера (ragent.exe) - власне і є сервером 1С. Він нічого не робить крім зберігання та ідентифікації одного або групи кластерів 1С.

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						42
Змн.	Арк.	№ докум.	Підпис	Дата		

- Кластер 1С (rmngr.exe) - група робочих процесів 1С, які здійснюють власне обробку даних. Сам по собі кластер нічого не обробляє, а здійснює менеджмент робочих процесів.

- Робочий процес 1С (rphost.exe) - програма, яка обробляє сеанс роботи користувача.

Система 1С: Бухгалтерія 8.0 забезпечує рішення всіх завдань, що стоять перед бухгалтерською службою. Підготовка внутрішньої і зовнішньої звітності менеджерами по продажах і адміністраторами, а також необхідної супровідної документації в компанії проводиться за допомогою програмних продуктів пакета прикладних програм Microsoft Office 2007:

- Microsoft Office Word дозволяє створювати і редагувати звіти та документи суворої звітності.

- Microsoft Office Excel дозволяє виконувати обчислення, а також аналізувати і візуалізувати дані в електронних таблицях.

- Microsoft Office Outlook дозволяє отримувати і відправляти пошту, працювати з розкладами, контактами і завданнями, а також вести запис своїх дій.

- Microsoft Office InfoPath дозволяє розробляти і заповнювати динамічні форми для збору і повторного використання даних в організації.

- Microsoft Office PowerPoint дозволяє готувати презентації для демонстрації, зборів та веб-сторінок.

- Веб-браузер Google Chrome використовується всіма відділами компанії для роботи в інтернеті (пошуку, робота з електронною поштою, банківських операцій і читання новин).

Таким чином дослідження роботи підприємства, показало наявність наступних каналів витоку інформації:

- несанкціонований доступ до інформації, що обробляється на ПЕОМ та на

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						43
Змн.	Арк.	№ докум.	Підпис	Дата		

сервері;

- НСД до паперових і машинних носіїв інформації;
- вихід з ладу технічних і програмних засобів, в т.ч. машинних носіїв інформації;

Порушення цілісності інформації можливо як шляхом фізичного руйнування носіїв інформації, так і шляхом спотворення її за допомогою програмних засобів:

- Аварії, стихійні лиха (пожежа, затоплення);
- Коливання в мережі електроживлення;
- Старіння магнітної поверхні носіїв інформації;
- Помилкове видалення інформації користувачем;
- Збої прикладного програмного забезпечення.

Можливі такі способи несанкціонованого доступу до ресурсів, що захищаються АС:

- фізичний доступ до носіїв інформації (до сервера) і їх резервних копій з метою їх розкрадання;
- фізичний доступ до паперових носіїв інформації, з метою їх розкрадання, розмноження, фотографування;
- безпосередній (поза рамками прикладного ПЗ) доступ до файлів сховища інформації, таблиць БД і виконуваним модулям ПЗ
- віддалено або локально з метою їх копіювання та подальшої установки, а також з метою їх знищення;
- застосування нештатних спеціальних програм, що забезпечують відновлення видалених даних з машинних носіїв інформації;
- передача файлів по каналах зв'язку між співробітниками і за межі станції з метою надання НСД особам, які не мають допуску до даної інформації в обхід штатних засобів захисту;
- доступ в рамках прикладного ПЗ локально або віддалено до баз даних і файлів з використанням недокументованих можливостей і режимів роботи цього ПЗ, розроблених і встановлених в якості модифікацій, в разі, коли

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						44
Змн.	Арк.	№ докум.	Підпис	Дата		

розробником ПЗ є стороння організація;

- будь-який доступ до ПЗ і даними з використанням технологій злому засобів захисту з метою отримання або знищення даних (в т.ч. комп'ютерні віруси);
- доступ з використанням чужого ідентифікатора, а також з чужого робочого місця під час відсутності користувача цього АРМ.

Висновки

Таким чином в розділі проведено аналіз діяльності підприємства його існуючу структуру. Приведено аналіз існуючої системи, що забезпечує безпеку. Виявлені недоліки та недоопрацювання з точки зору безпеки.

Так проведено роботи організаційного характеру та розроблено порядок обігу інформації в межах підприємства, розроблено положення про комерційну таємницю.

Однією із основних організаційних недоліків є проблема плинності кадрів, що призводить до формування можливого витоку інформації, як навмисного, так і ненавмисного.

Однак до недоліків існуючої системи слід віднести відсутність захисту інформації, що міститься на електронних носіях: таких як захист від вірусів, захист від крадіжки, відсутність криптографічного захисту інформації на носіях, використання підсанкційного програмного забезпечення.

В якості основної програмної платформи обліку товарно-матеріальних цінностей використовується 1С: Підприємство. Цей програмний продукт підпадає під санкції. Тому на території України заборонений його продаж, обслуговування та оновлення. Оновлення можливі лише через неофіційні канали із Російської федерації. Використання цього програмного продукту із сірими оновленнями та без сервісного обслуговування приводить до морального застарівання (змінюються форми документів, порядок

Змн.	Арк.	№ докум.	Підпис	Дата

нарахування податків, і т.п.) програмного забезпечення та до не документованих можливостей доступу зломисників до внутрішніх документів підприємства.

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						46
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3

РОЗРАХУНОК РИЗИКІВ

Активи, що мають цінність і які характеризуються певним ступенем уразливості, щоразу наражаються на ризик при наявності загроз. Завдання аналізу ризику полягає у визначенні та оцінці ризиків, яким піддається система інформаційної технології і її активи, з метою визначення та вибору доцільних і економічно обґрунтованих засобів забезпечення безпеки. Для оцінки ризиків обраний метод, який пропонує використання таблиці «штрафних балів» для кожної комбінації цінності активів, рівня загроз і вразливостей (табл. 3.1).

Таблиця 3.1

Таблиця «штрафних балів»

Цінність активу	Рівень загрози								
	Низький			Середній			Високий		
	Рівень вразливості			Рівень вразливості			Рівень вразливості		
	Н	С	В	Н	С	В	Н	С	В
0	0	1	2	1	2	3	2	3	4
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6
3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8
Позначення: Н - низький, С - середній, В - високий.									

Цінності активів, а також рівні загроз і вразливості, відповідні кожному типу впливу вводять в матрицю для визначення кожного поєднання

відповідних заходів ризику за шкалою від 1 до 8. Значення величин розміщують в матриці в структурованій формі відповідно до таблиці 3.1.

Для кожного активу розглядають вразливі місця і відповідні їм загрози. Якщо є вразливі місця без відповідної загрози або загрози без відповідного уразливого місця, то вважають, що в даний час ризик відсутній. Потім ідентифікують відповідний ряд матриці по цінності активу, а відповідну колонку - за ступенем загрози і вразливості. Цінність даного методу полягає в ранжируванні відповідних ризиків (табл. 3.2).

Таблиця 3.2

Результати оцінки ризиків інформаційним активам підприємства

Ризик	Актив	Ранг ризику
Втрата доступності	Ціни на товари і матеріали	64
Втрата доступності	Інформаційні послуги	59
Втрата конфіденційності	Внутрішня переписка	56
Втрата конфіденційності	Приходні накладні	53
Втрата конфіденційності	Розхідні накладні	48
Втрата конфіденційності	Інвентаризаційна відомість	35
Втрата конфіденційності	Закази клієнтів	27
Втрата доступності	Знижки клієнтів	22
Порушення цілості	Програмне забезпечення	22
Втрата доступності	Наряд на виконання робіт	21
Втрата доступності	Бухгалтерська та податкова звітність	6

Дана таблиця містить ризики найбільш цінним інформаційним активам, ранжирування в порядку спадання. Результати оцінки ризиків є підставою для вибору і формулювання завдань щодо забезпечення інформаційної безпеки підприємства, і вибору захисних заходів.

Ще одним методом оцінки загроз інформаційної безпеки є оцінка захищеності окремих об'єктів захисту. До них на підприємстві належать:

- АРМ співробітників;
- сервер локальної мережі;
- конфіденційна інформація (документи);
- кабельні лінії;
- кабінети з конфіденційною документацією;
- бази даних підприємства.

Для кожного об'єкта необхідно розрахувати інформаційні ризики. При розрахунках використовуються такі поняття.

Критичність ресурсу (D) - ступінь значущості ресурсу. Показує вплив реалізації загрози на роботу інформаційної системи. Визначається на основі експертних оцінок фахівців підприємства.

Критичність реалізації загрози (ER) - ступінь впливу реалізації загрози на ресурс, задається в %. Визначається на основі статистичних даних, доступних на порталах фірм - інтеграторів.

Імовірність реалізації загрози через дану уразливість протягом року (P (v)) - ступінь можливості реалізації загрози через дану уразливість в тих чи інших умовах, вказується в %.

1. Об'єкт захисту - автоматизоване робоче місце (АРМ) співробітника. В організації є 43 автоматизованих робочих місць співробітників. Доступ до приміщення стороннім особам заборонений, на кожному комп'ютері є свій пароль, однак користувачі можуть залишити свій комп'ютер включеним, якщо їм необхідно відійти від робочого місця, і інформація буде доступна іншим співробітникам. Паролі практично ніколи не змінюються, трапляються ситуації, що користувачі записують їх на листочках і залишають біля

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						49
Змн.	Арк.	№ докум.	Підпис	Дата		

комп'ютера. Антивірус встановлений тільки на сервері, тому що вся інформація проходить через нього, проте usb-порти не відключені, і у користувачів є можливість підключати флеш-пристрої. Крім того, у користувачів є вихід в Інтернет. Заборонено вихід на сайти соціальних мереж, однак інші шляхи майже не контролюються і розмір трафіку не обмежується, що є причиною зараження вірусами.

Відправлення та отримання електронної пошти проводиться через сервер, де відслідковуються всі вхідні і вихідні листи, тому відправка листів з особистих питань або на недозволені адреси неможлива. Всі бланки документів зберігаються на сервері, а самі документи - на робочих комп'ютерах користувача.

Шляхом експертної оцінки, що враховує збиток від витоку інформації конкурентам, який полягає в можливому зменшенні товарообігу із покупцями критерій критичності (D) визначено на рівні 48 337 гривень.

Проведемо аналіз основних загроз, характерних для обраного об'єкта і вразливостей, через які ці загрози можуть бути реалізовані (табл. 3.3).

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						50
Змн.	Арк.	№ докум.	Підпис	Дата		

Таблиця загроз та вразливостей

Загроза	Вразливість
1.Фізичний доступ порушника до АРМ	1. Відсутність системи контролю доступу працівників до чужих АРМ (користувачі можуть залишити свій комп'ютер без нагляду з введенням паролем).
	2.Відсутність системи відеоспостереження в кабінетах.
	3.Відсутність політики паролів
2.Збої в роботі АРМ	1. Відсутність антивірусного ПЗ на самих АРМ
	2. Людський фактор
3.Руйнування конф. інформації за допомогою спеціальних програм та вірусів	1. Відсутність антивірусного ПЗ на самих АРМ
	2.Відсутність обмеження доступу користувачів до зовнішньої мережі.

Таблиця(3.4) містить ймовірності реалізації даної загрози через уразливість протягом року (P (V)) і критичності реалізації загрози (ER).

Таблиця ймовірності реалізації загрози

Загроза/вразливість	P(V), %	ER,%
1/1	10	50
½	10	50
1/3	20	90
2/1	40	80
2/2	10	20
3/1	50	80
3/2	20	60

Таблиця(3.5) рівня загрози з певної уразливості (Th) і за рівнем загроз по всім вразливостям (CTh), які розраховуються за формулами:

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						51
Змн.	Арк.	№ докум.	Підпис	Дата		

$$Th = \frac{P(v)}{100 \cdot \frac{ER}{100}} \quad (3.1)$$

та

$$CTh = 1 - \prod(1 - Th) \quad (3.2)$$

Таблиця 3.5

Таблиця рівня загрози

Загроза/вразливість	Th	CTh
1/1	0,05	0,260
1/2	0,05	
1/3	0,18	
2/1	0,32	0,334
2/2	0,02	
3/1	0,4	0,472
3/2	0,12	

Проведемо розрахунок загального рівня загрози по ресурсу:

$$CThR = 1 - \prod(1 - Th) = 0,74$$

Проведемо розрахунок ризику по ресурсу:

$$R = CThR \cdot D = 0,74 \cdot 48337 = 35750.36 \text{ грн.}$$

З одного автоматизованого робочого місця.

Оскільки кожне робоче місце містить унікальні документи та мають особливості в складі та налаштуванні програмного забезпечення, то відновлення автоматизованих робочих місць потребує індивідуального налаштування. Крім того, під час робіт із налаштування робочих місць робота підприємства буде паралізована, тобто підприємство буде витратити кошти на поточну діяльність і при цьому не буде отримувати доходів. Причому збитки пропорційні кількості робочих місць, що не працюють, тому загальний ризик усіх 43 робочих місць складе:

$$R\Sigma == 43 \cdot 35750.36 = 1537265,48 \text{ грн.}$$

Результати розрахунків показують, що рівень ризику, який виникає із використанням автоматизованих робочих місць складає 74% і втрати в грошовому виміру складають 1537265,48 грн.

Причому основними проблемами є:

- відсутність антивіруса на локальних комп'ютерах
- відсутність політики паролів
- недбалість користувачів

2. Об'єкт захисту - сервер локальної мережі.

Критерій критичності (D) визначено шляхом проведення експертної оцінки і включає в себе вартість робіт по відновленню роботи сервера, та збитки, що виникли в результаті неможливості роботи підприємства визначено 515 400 грн.

Виділений сервер знаходиться в спеціальному приміщенні, доступ до якого заборонений стороннім особам. На сервері зберігаються загальні

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						53
Змн.	Арк.	№ докум.	Підпис	Дата		

ресурси, які доступні працівникам з їх робочих місць. Це різні бланки документів, які періодично оновлюються, щоб всі користувачі працювали з затвердженими формами документів. Доступ організований так, що всі документи доступні всім користувачам мережі. Це і визначає наявність таких загроз, як загрози розголошення та зміни конфіденційної інформації, однак імовірність виникнення таких загроз досить мала, тому що всі співробітники зацікавлені в нормальному функціонуванні підприємства. У своїй більшості, це ненавмисні загрози (через неухважність або незнання). Також виникають збої в роботі сервера, але досить рідко.

На сервері встановлено сервер електронної пошти, який здійснює прийом і відправку всіх поштових повідомлень, що дозволяє відстежувати адресатів і відправників повідомлень. Також встановлено проксі-сервер, який контролює вихід в Інтернет. Політика роботи в Інтернеті така - заборонений вихід на певні сайти, однак розмір трафіку практично не контролюється, що викликає іноді перевантаження мережі і вихід сервера з ладу.

Крім того, для деяких категорій працівників є віддалений доступ до документів, що дає можливість витоку і пошкодження інформації на сервері.

Проведемо аналіз основних загроз, характерних для обраного об'єкта і вразливостей, через які ці загрози можуть бути реалізовані (табл. 3.6).

Таблиця 3.6

Таблиця загроз та вразливостей

Загроза	Вразливості
1. Розголошення, знищення або розголошення конфіденційної інформації, що зберігається на сервері	1. Доступ до інформації з АРМ
	2. Наявність віддаленого доступу
2. Вихід сервера із ладу	1. Велика кількість підключень
	2. Збої в подачі електроенергії

Йймовірності реалізації даної загрози через уразливість протягом року (P (V) і критичності реалізації загрози (ER) зведено в табл. 3.7.

Таблиця 3.7

Таблиця ймовірності реалізації загрози

Загроза/Вразливість	P(V), %	ER,%
1/1	10	60
½	10	20
2/1	20	20
2/2	10	40

Таблиця 3.8 містить зведену інформацію про рівні загрози з певної вразливості (Th) і за рівнем загроз по всьм вразливостям (CTh).

Таблиця 3.8

Таблиця рівня загрози по певній вразливості

Загроза/вразливість	Th	CTh
1/1	0,06	0,079
½	0,02	
2/1	0,04	0,078
2/2	0,04	

Розрахуємо загальний рівень загроз по ресурсу:

$$CThR = 1 - \prod (1 - Th) = 0,151$$

Проведемо розрахунок ризику по ресурсу:

$$R = CThR \cdot D = 0,151 \cdot 515400 = 77825,4 \text{ грн.}$$

Можливо зробити висновок, що ризик по цьому ресурсу досить невеликий в порівнянні з АРМ - всього 15,1% і втрати – 77825,4 грн. Однак слід звернути увагу на такі загрози, як наявність віддаленого доступу, відсутність розмежувань дій користувача та надійність електроживлення.

3. Об'єкт захисту - Конфіденційна документація.

Конфіденційна документація зберігається, як в електронному, так і в паперовому вигляді. Велика частина конфіденційних документів зберігається в сейфах, хоча частина інформації зберігається прямо на робочих столах комп'ютера. Через те, що співробітникам доводиться працювати з великою кількістю паперів, іноді виникають ситуації втрати окремих документів.

Самі співробітники попереджені про відповідальність за розголошення конфіденційної інформації, однак через нечітку організації конфіденційного документообігу і великого обсягу роботи, є можливість крадіжки документів іншими співробітниками.

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						56
Змн.	Арк.	№ докум.	Підпис	Дата		

Таблиця загроз та вразливостей

Загроза	Вразливість
1.Фізичний доступ порушника до документів	1.Безлад на робочому місці
	2.Відсутність відеонагляду
2.Несанкціоноване копіювання, друк і розмноження конфіденційної інформації	1. Нечітка організація конфіденційного документообігу
	2.Неконтрольований доступ співробітників до копіювальної і розмножувальної техніки

Конфіденційна інформація підприємства оцінена службою безпеки 300 000 грн., Ця сума не точна і може змінюватися в більшу і меншу сторони.

Критерій критичності (D) дорівнює 300 000 грн.

Табл. 3.10 містить ймовірності реалізації даної загрози через уразливість протягом року (P (V) і критичності реалізації загрози (ER).

Таблиця 3.10

Таблиця ймовірності реалізації загрози

Загроза/вразливість	P(V), %	ER,%
1/1	20	10
1/2	20	10
2/1	20	30
2/2	10	20

Таблиця рівня загрози з певної вразливості (Th) і за рівнем загроз по всім вразливостям (CTh).

Таблиця рівня загрози з певної вразливості

Загроза/вразливість	Th	CTh
1/1	0,04	0,050
1/2	0,01	
2/1	0,06	0,079
2/2	0,02	

Розрахуємо загальний рівень загроз по ресурсу:

$$CThR = 1 - \prod (1 - Th) = 0,124$$

Проведемо розрахунок ризику по ресурсу:

$$R = CThR \cdot D = 0,124 \cdot 300000 = 37200 \text{ грн.}$$

Ризик з цього ресурсу також невеликий - всього 12,4% і втрати - 37 200 грн. Головною проблемою є неорганізованість працівників.

4. Об'єкт захисту - кабінети з конфіденційною інформацією і кабельні системи.

Так як доступ на підприємство обмежений, то проникнути на територію підприємства, а також в офісні приміщення стороннім особам неможливо.

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						58
Змн.	Арк.	№ докум.	Підпис	Дата		

Висновки

В розділі проведений аналіз існуючої структури підприємства з метою оцінки ризиків втрати конфіденційної інформації. розрахунки показали. Що найбільший збиток та ймовірність загроз існує від автоматизованих робочих місць та сервера. Також існує загроза втрати конфіденційної інформації через халатність працівників.

Розрахунки показали, що:

- ризику, який виникає із використанням автоматизованих робочих місць складає 74% і втрати в грошовому виміру складають 1537265,48 грн.
- ризик, пов'язаний із сервером складає 15,1% і втрати – 77825,4 грн.
- ризик витоку конфіденційної інформації складає 12,4%, а можливі збитки складають - 37 200 грн.

Таким чином, виявлені недоліки та шляхи вдосконалення систем захисту інформації.

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						59
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 4

РОЗРОБКА КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

4.1. Організаційні заходи

Заходи захисні для фізичної безпеки включають в себе забезпечення міцності внутрішніх стін будівель, використання кодових замків, систем пожежогасіння і охоронних служб.

Забезпечення безпеки персоналу включає в себе перевірку осіб при прийомі на роботу (особливо осіб, які наймаються на важливі з точки зору забезпечення безпеки посади), контроль роботи персоналу і реалізацію програм знання і розуміння заходів захисту.

Однією із важливих проблем є плинність кадрів, яка напряду впливає на інформаційну безпеку. Для зменшення плинності кадрів та мінімізації впливу цього явища на інформаційну безпеку, необхідно здійснити ряд заходів:

- ввести систему преміювання за стаж роботи. При цій системі оплати праці створюються стимули для працівників, що працюють довгий термін;
- ввести контрактну форму прийому на роботу. При цьому внести пункти про комерційну таємницю з додатковим підписанням угоди про дотримання правил роботи із конфіденційною інформацією. При цьому чітко вказати відповідальність за невиконання пунктів цих документів.

Адміністративна безпека включає в себе безпечні способи ведення документації, наявність методів розробки та прийняття прикладних програм,

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						60
Змн.	Арк.	№ докум.	Підпис	Дата		

а також процедур обробки інцидентів у випадках порушення систем безпеки.

Існують три стратегії забезпечення інформаційної безпеки:

- оборонна;
- наступальна;
- упереджувальна.

В рамках даного підприємства оберемо наступальну стратегію інформаційної безпеки. Наступальна стратегія передбачає активну протидію відомим загрозам, що впливають на інформаційну безпеку системи. Наступальна стратегія може включати установку додаткових програмно-апаратних засобів аутентифікації користувачів, впровадження більш досконалих технологій розвантаження і відновлення даних, підвищення доступності системи з використанням гарячого і холодного резервування.

В основному режимі функціонування система обліку замовлень компанія повинна забезпечувати роботу користувачів в режимі «24x7» (24 години на добу, 7 днів на тиждень). До складу персоналу, необхідного для забезпечення експлуатації програми автоматизації обліку матеріальних ресурсів MASTER:Бухгалтерія в рамках відповідного підрозділу входять менеджери з продажу і завідувач складом.

Технічна підтримка та адміністрування здійснюється штатним програмістом. До кваліфікації персоналу, що експлуатує систему, що розробляється, пред'являються наступні вимоги:

- Менеджер з продажу - знання принципів роботи з клієнтами при реєстрації замовлень і підборі меблів; вивчення інструкції з експлуатації MASTER:Бухгалтерія (керівництво користувача).
- Завідувач складом - знання принципів роботи з клієнтами при прийомі

Змн.	Арк.	№ докум.	Підпис	Дата

матеріалів на склад; вивчення інструкції з експлуатації MASTER:Бухгалтерія (керівництво користувача).

– Адміністратор MASTER:Бухгалтерія - знання методології проектування сховищ даних; знання MASTER:Бухгалтерія; досвід адміністрування MASTER:Бухгалтерія; знання і навички операцій архівування та відновлення даних; знання і навички оптимізації роботи MASTER:Бухгалтерія ; знання і навички адміністрування програми; знання інструментів розробки.

Рівень надійності повинен досягатися узгодженим застосуванням організаційних, організаційно-технічних заходів і програмно-апаратних засобів.

Надійність повинна забезпечуватися за рахунок:

- застосування технічних засобів, системного і базового програмного забезпечення, що відповідають класу завдань, що вирішується;
- своєчасного виконання процесів адміністрування системи;
- дотримання правил експлуатації і технічного обслуговування програмно-апаратних засобів;
- попереднього навчання користувачів і обслуговуючого персоналу.

Для забезпечення безпеки при використанні MASTER:Бухгалтерія користувачам потрібно дотримуватися стандартних вимог по техніці безпеки при роботі з ПК.

Для забезпечення безпеки під час аварій та збоїв необхідно передбачити наступні заходи по відновленню працездатності системи:

- Створення резервних копій бази даних - операція створення резервних архівних копій повинна проводитися автоматично щодня в кінці робочого дня при завершенні роботи MASTER:Бухгалтерія, або в будь-який момент часу адміністратором системи з його ініціативи.

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						62
Змн.	Арк.	№ докум.	Підпис	Дата		

– відновлення з резервної копії - операція повинна проводитися тільки адміністратором системи. Передбачається, що єдина база даних для роботи з інформаційною системою буде знаходитися на виділеному сервері зі встановленою СКБД «MASTER:Бухгалтерія о».

Користувачі зможуть приєднуватися і працювати з системою за допомогою клієнтської програми. Для цього на сервері повинно бути встановлене наступне системне ПО:

- Операційна система Windows 2003;
- СКБД «MASTER:Бухгалтерія»;

На клієнтській машині повинні бути встановлені:

- Операційна система Windows 7;
- Офісний пакет Microsoft Office 2010;
- Поштовий клієнт;
- СКБД «MASTER:Бухгалтерія»;

Таблиця 4.1

Розмежування прав користувачів

Користувачі	Довідники	Документи	Звіти
Адміністратор	Повний доступ	Повний доступ	Повний доступ
Менеджер з продажів	Читання Добавляння Редагування	Формування Попердній огляд Друк	Формування Попердній огляд Друк
Працівник складу, продавець	Читання Добавляння Редагування	Формування Попердній огляд Друк	Формування Попердній огляд Друк

Для того щоб співробітники компанії використовували ресурси системи, що проектується, кваліфіковано, ефективно і за призначенням,

дотримуючись норм етики і дотримуючись законів, визначені дві категорії користувачів системи, опис яких представлено в табл. 4.1.

План містить докладні відомості про найважливіші функції і пріоритети, які підлягають відновленню, необхідні умови обробки інформації та способах організації, які необхідно здійснювати в разі аварії або тимчасового припинення роботи системи.

До числа планів, що розроблюються, можна віднести:

- положення про пропускний режим підприємства;
- регламент захищеного (конфіденційного) документообігу;
- порядок реагування на інциденти;
- технічне завдання на розробку інформаційної системи;
- керівництво користувача;
- керівництво адміністратора;
- керівництво програміста.

4.2. Розробка інженерно-технічних заходів

В цілому засоби забезпечення захисту інформації в частині запобігання навмисних дій в залежності від способу реалізації можна розділити на групи:

- Технічні (апаратні) засоби. Це різні за типом пристрої (механічні, електромеханічні, електронні та ін.), які апаратними засобами вирішують завдання захисту інформації. Вони або перешкоджають фізичному проникненню, або, якщо проникнення все ж відбулося, доступу до інформації, в тому числі за допомогою її маскування.

Першу частину завдання вирішують замки, решітки на вікнах, захисна сигналізація та ін.

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						64
Змн.	Арк.	№ докум.	Підпис	Дата		

Другу - генератори шуму, мережеві фільтри, скануючі радіоприймачі і інші пристрої, що «перекривають» потенційні канали витоку інформації або дозволяють їх виявити. Переваги технічних засобів пов'язані з їх надійністю, незалежністю від суб'єктивних факторів, високу стійкість до модифікації. Слабкі сторони - недостатня гнучкість, відносно великі об'єм і вага, висока вартість.

В якості технічних засобів захисту необхідно встановити реле напруги в вхідному щитку електроживлення. Це реле дозволить вимикати подачу електроживлення за умови, що напруга перевищує задані межі робочих напруг електронного обладнання, що використовується.

В якості такого реле використаємо РН-240 (263) т.

Для забезпечення стабільної роботи ПЕОМ та серверів необхідно встановити джерело безперебійного живлення. Можлива реалізація декількох варіантів: на кожне робоче місце встановити джерело безперебійного живлення на весь офіс, або на кожен із комп'ютерів та серверів окремо.

Перший варіант має більшу вартість, однак забезпечує кращий захист, оскільки дозволяє встановлювати більшу ємність батарей та, відповідно, забезпечує більш тривалий час роботи обладнання без мережевого електроживлення. В якості такого джерела використаємо наступне обладнання:

- Джерело безперебійного живлення LPY-B-PSW-7000VA+ - дозволяє працювати як від електромережі, так і від акумуляторних батарей.

Номінальна потужність пристрою становить 5 кВт, Зарядний пристрій у безперебійника даної моделі розрахований на зарядний струм до 20 А, що достатньо для зарядки акумулятора 48 В 200 А (і більше).

- Акумуляторна батарея LogicPower LPM MG-12-200 виготовлена за технологією AGM. В комплект входить 4 таких акумулятори сумарною потужністю з акумуляованої електроенергії 9 600 Вт/год.

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						65
Змн.	Арк.	№ докум.	Підпис	Дата		

При роботі із локальною мережею можуть виникати збої в результаті чого можлива тимчасова недоступність мережевих ресурсів. Для захисту внутрішньої локальної мережі необхідно встановити сервер безпеки MOXA NPort 6000, який підтримує TCP-сервер, TCP-клієнт, UDP-протокол і режим Pair-Connection, що забезпечує його сумісність зі стандартними мережевими програмами.

MOXA NPort 6000 забезпечує також підтримку Secure TCP Server, Secure TCP Client, Secure Pair-Connection і моду Secure Real COM для надійних і безпечних додатків, які використовуються в задачах, що потребують передачі конфіденційних даних по відкритих мережах.

Для стандартів DES та 3DES - термінальні сервери MOXA NPort 6000 підтримують режими ECB, CBC, CFB і OFB, ECB, CBC, CFB, OFB і CTR 128-bit, 192-bit або 256-bit ключами. Крім того, ці сервери мають спеціальний буфер пам'яті, що оберігає від втрати даних при обриві Ethernet-з'єднання. Якщо воно переривається, то всі дані записуються в буфер сервера і при відновленні з'єднання вся інформація з нього передається в тому порядку, в якому була записана. Розмір пам'яті буфера за замовчуванням становить 64 КВ для кожного з портів, але при цьому користувачі можуть збільшувати обсяг пам'яті на серверах MOXA NPort 6250/6450/6650 при установці зовнішньої пам'яті (SD-карти).

Програмні засоби включають програми для ідентифікації користувачів, контролю доступу, шифрування інформації, видалення залишкової (робочої) інформації типу тимчасових файлів, тестового контролю системи захисту та ін. Переваги програмних засобів - універсальність, гнучкість, надійність, простота установки, здатність до модифікації і розвитку. Недоліки - обмежена функціональність мережі, використання частини ресурсів файл-сервера і робочих станцій, висока чутливість до випадкових або навмисним змін, можлива залежність від типів комп'ютерів (їх апаратних засобів).

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						66
Змн.	Арк.	№ докум.	Підпис	Дата		

Для підвищення захищеності конфіденційної інформації необхідно перейти від платформи «1С:Підприємство», яке в Україні знаходиться під санкціями та внаслідок цього не доступні оновлення та сервісне обслуговування на програмну платформу «MASTER:Бухгалтерія». Ця програмна платформа має майже ту ж функціональність, що і 1С, однак має технічну підтримку, постійне оновлення та країна розробник Україна.

Для захисту інформації від несанкціонованого доступу використаємо систему ЛОЗА-1. Ця система яка являє собою комплекс програмних засобів, який забезпечує захист інформації від несанкціонованого доступу.

Система ЛОЗА-1 призначена для використання в автоматизованих системах класу “1” (згідно з класифікацією, наведеною в [8]). Система може використовуватись для захисту інформації, що становить державну таємницю. Система містить засоби, необхідні для побудови комплексної системи захисту інформації:

- засоби перевірки цілісності,
- реєстрації подій,
- аналізу журналу подій,
- керування системою та ін.

Крім того, до складу системи входять спеціалізовані засоби, які дозволяють захистити інформацію, що міститься в текстових документах та електронних таблицях. Система ЛОЗА-1 може працювати під керуванням таких операційних систем: – Microsoft Windows XP Professional (Service Pack 2 або вище); – Microsoft Windows Vista (Service Pack 2 або вище); – Microsoft Windows 7.

Систему ЛОЗА-1 необхідно встановлювати на диск із файловою системою NTFS.

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						67
Змн.	Арк.	№ докум.	Підпис	Дата		

За рахунок взаємодії з Microsoft Office система ЛОЗА-1 може забезпечити надійний захист документів Microsoft Word та Microsoft Excel. Підтримуються такі версії Microsoft Office:

- Microsoft Office XP (SP-2 або вище);
- Microsoft Office 2003;
- Microsoft Office 2007 (SP-2 або вище);
- Microsoft Office 2010.

Для роботи системи необхідно приблизно 10 МБ оперативної пам'яті і до 20 МБ на жорсткому диску.

Система ЛОЗА-1 розроблена ТОВ НДІ “Автопром”, м. Київ.

Таким чином, проводячи аналіз встановленого програмного забезпечення та технічних засобів система ЛОЗА-1 підходить для вирішення задачі захисту інформації.

Система ЛОЗА-1 на підприємстві «Механік Трейд» буде використана для вирішення наступних задач щодо захисту інформації:

- ідентифікація та автентифікація користувачів;
- захист даних на знімних носіях;
- захист даних на рівні папок жорсткого диска;
- захист текстових документів та електронних таблиць;
- контроль цілісності програмного середовища (перевіряється цілісність файлів та папок, розділів та параметрів реєстру, завантажувальних секторів, а також облікових записів Windows);
- реєстрація важливих подій та аудит журналів Windows.

Система ЛОЗА-1 підтримує:

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						68
Змн.	Арк.	№ докум.	Підпис	Дата		

- різні рівні повноважень користувачів та різні рівні конфіденційності інформації (цілком таємно, таємно, для службового користування, відкрита інформація);
- різні ролі користувачів: роль звичайного користувача та декілька адміністративних ролей (адміністратор безпеки, системний адміністратор, адміністратор документів);
- зберігання документів на жорсткому диску та на знімних носіях.

Тому використання такої системи дозволить провести ефективне розмежування доступу персоналу до інформації, що зберігається в інформаційній системі підприємства.

Конфігурації ЛОЗА-1 постачається у двох конфігураціях: „Стандартна безпека” та „Підвищена безпека”.

Конфігурація „Підвищена безпека” задовольняє більш жорстким вимогам щодо захисту інформації. Зокрема, в цій конфігурації виконуються такі вимоги:

- застосовується множинна (двох факторна) автентифікація користувачів (за паролем та ключовим диском);
- неможливо відмінити вимоги щодо мінімальної довжини, складності та неповторюваності паролів.

Система ЛОЗА-1 у конфігурації „Підвищена безпека” може використовуватись в АС класу „1” для захисту інформації, що становить державну таємницю.

Оскільки на підприємстві відсутні документи, що становлять державну таємницю, то використовуватись буде конфігурація «Стандартна безпека».

Для коректної роботи системи необхідно забезпечити виконання наступних умов:

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						69
Змн.	Арк.	№ докум.	Підпис	Дата		

- На комп'ютері, на якому використовується система ЛОЗА-1, має бути встановлена тільки одна операційна система;
- завантаження операційної системи зі знімних дисків необхідно унеможливити за допомогою утиліти CMOS SETUP UTILITY (або аналогічної).
- Папка, в яку встановлюється система ЛОЗА-1, має знаходитись на диску з файловою системою NTFS.

На підприємстві необхідно використання брандмауера, який розділяє сегменти, мережі в яких обробляється конфіденційна інформація, персональні дані співробітників, а також інформація відкритого характеру.

Брандмауер - комплекс апаратних або програмних засобів, здійснює контроль і фільтрацію мережевих пакетів, що проходять через нього, на різних рівнях моделі OSI відповідно до заданих правил. Для вирішення цього завдання підійде програмно-апаратний міжмережевий екран Cisco ASA 5505, який відповідає вимогам до 3 класу .

Міжмережевий екран Cisco Systems серії ASA (Adaptive Security Appliances) - вископродуктивні пристрої для фільтрації трафіку, захисту від вірусів, хробаків і різних видів інтернет-атак, охорони периметра корпоративних мереж, організації шифрованих каналів через інтернет для зв'язку офісу і філій, а також для віддаленого підключення співробітників і організації extranet-доступу.

Cisco ASA 5505 - багатофункціональний пристрій захисту ресурсів мережі від внутрішніх і зовнішніх атак. В інфраструктурі підприємства ASA 5505 займає місце класичного брандмауера (firewall), що дозволяє захистити мережу підприємства або окремі сегменти.

ASA 5505 об'єднує в собі технології і рішення щодо забезпечення інформаційної безпеки.

Контроль з'єднань між вузлами мережі забезпечує вбудований міжмережевий екран з механізмами інспекції пакетів з урахуванням стану

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						70
Змн.	Арк.	№ докум.	Підпис	Дата		

протоколу (stateful inspection firewall) на рівнях 2-7, який дозволяє стежити за станом всіх мережових комунікацій і допомагає запобігти несанкціонованому доступу до мережі.

Механізми аналізу протоколів на прикладному рівні дозволяють забезпечити захист від нелегального використання дозволених портів, наприклад HTTP - TCP порт 80 для ICQ і інших додатків.

ASA 5505 може функціонувати в «тихому» режимі, при цьому вона не буде видимим вузлом мережі, буде прозоро для користувача пропускати трафік, забезпечуючи необхідний рівень захисту.

ASA 5505 реалізує частину функцій сучасного маршрутизатора, такі як протоколи динамічної маршрутизації RIP і OSPF, резервування каналів доступу в мережу Інтернет, механізми забезпечення якості обслуговування (QoS).

Для забезпечення можливості відновлення всіх критично важливих даних і програм після виходу з ладу автоматизованої робочої станції, сервера або псування цифрового носія інформації, необхідно мати належні засоби резервного копіювання.

Резервне копіювання - процес створення копії даних на цифровому носії, призначеної для відновлення даних в оригінальному місці їх розташування в разі їх пошкодження або руйнування.

Для вирішення завдання резервного копіювання рекомендується використовувати програмний продукт Backup Maker, який необхідно встановити на кожну робочу станцію, на якій планується резервне копіювання даних. Для віддаленого адміністрування програми можна встановити на будь-якому з комп'ютерів, що входить до складу локальної обчислювальної мережі підприємства Paragon Remote Manager 14.0 Pro .

Для зберігання резервних копій використовується сервер в сегменті мережі з відкритою інформацією, в інші сегменти додані комп'ютери, на ці комп'ютери також пропонується встановити засоби захисту інформації він

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						71
Змн.	Арк.	№ докум.	Підпис	Дата		

несанкціонованого доступу, а також консоль віддаленого адміністрування Paragon Remote Manager 14.0 Pro .

Від комп'ютерів, призначених для зберігання резервних копій, не потрібно високої продуктивності, основна вимога - великий обсяг дискового простору. Рекомендується використовувати ПК з об'ємом дискового простору більше 1 ТБ.

Адміністратор безпеки налаштовує розклад завдань резервного копіювання для кожної машини за допомогою консолі управління, або створює розкладу завдань для окремих робочих груп. Управління контрольними точками резервування і дисковим простором, виділеним під резервні копії, відбувається автоматично.

Адміністратор безпеки повинен регулярно переглядати звіти завдань, які формуються віддаленими клієнтами, і стежити за станом резервних архівів.

В якості комплексного захисту, що забезпечує антивірусний захист і межмережеве екранування використовуємо на робочих станціях Trend Micro InterScan VirusWall.

Trend Micro InterScan VirusWall - це рішення для антивірусного захисту інтернет-шлюзів, фільтрації спаму і небажаних даних. Дана система фільтрує електронну пошту та інші наді, що поступають з Інтернету на рівні інтернет-шлюзу, не дозволяючи вірусам і спаму проникати в корпоративну мережу.

InterScan VirusWall оснащується інтуїтивно зрозумілим інтерфейсом єдиної панеллю управління. У InterScan VirusWall вбудована система боротьби зі спамом і фільтрації вмісту інтернет-ресурсів. Ретельна перевірка даних, що передаються по протоколу SMTP, забезпечує захист внутрішніх поштових серверів від вірусів і спаму. InterScan VirusWall здійснює перевірку пошти, що приймається і по протоколу POP3. InterScan VirusWall - це високопродуктивний евристичний механізм боротьби зі спамом, що має об'ємні бази зразків спаму і списками довірених адрес електронної пошти,

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						72
Змн.	Арк.	№ докум.	Підпис	Дата		

забезпечуючи високу точність розпізнавання і низьке число помилкових спрацьовувань. Ефективні функції фільтрації даних дозволяють блокувати або маркувати спам, який передається по протоколах SMTP і POP3. Trend Micro InterScan VirusWall перевіряє на наявність вірусів всі файли, що поступають з Інтернету, не дозволяючи співробітникам випадково занести в корпоративну систему вірус в процесі роботи із зовнішньою поштовою скринькою або завантаження файлів. Дане рішення також здійснює перевірку коду, що використовується на веб-сторінках (зокрема, сценаріїв і аплетів Java), а також фіксує адреси сайтів, що відвідуються, полегшуючи реалізацію корпоративної політики безпеки. Для захисту файлового сервера доцільно використовувати ServerProtect for Microsoft Windows.

ServerProtect призначений для ретельної антивірусної перевірки серверів, оперативного пошуку і видалення вірусів, що містяться в файлах і архівах, до того, як вони потраплять до кінцевого користувача.

Панель управління, реалізована у вигляді додатку для Windows, дозволяє централізовано контролювати процес боротьби з епідеміями, виконувати пошук вірусів, оновлювати файли сигнатур, розсилати повідомлення і робити віддалене встановлення додатків.

Пакет ServerProtect сумісний з серверними платформами Microsoft Windows 2003 Microsoft Windows 2000, Microsoft Windows NT і Novell NetWare. Поєднання технологій виявлення вірусів, оснований на використанні наборів правил і розпізнаванні сигнатур, дозволяє підвищити ефективність роботи ServerProtect. Розроблені Trend Micro технології видалення макровірусів і шкідливих сценаріїв забезпечують додатковий захист.

Процес пошуку вірусів та іншого шкідливого коду здійснюється ServerProtect на рівні ядра з використанням інтерфейсів прикладного програмування Microsoft і Novell, що дозволяє звести до мінімуму зниження продуктивності системи. Для підвищення швидкості сканування і мінімізації навантаження на сервер використовується багато-скануючий механізм.

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						73
Змн.	Арк.	№ докум.	Підпис	Дата		

Панель управління ServerProtect, реалізована у вигляді Windows-додатку, дозволяє централізовано керувати всіма серверами, розташованими на одному майданчику. Адміністратор може встановлювати програми та файли оновлення на всі сервери одночасно, а також в режимі реального часу відслідковувати інформацію про стан серверів.

Адміністратори також можуть використовувати панель управління Trend Micro Control Manager, доступ до якої здійснюється через Інтернет. Дане рішення Trend Micro призначене для централізованого управління антивірусними системами, що забезпечують захист розподілених мереж. ServerProtect for Microsoft Windows є одним з ключових компонентів Стратегії захисту підприємств Trend Micro (Trend Micro Enterprise Protection Strategy), що дозволяє використовувати для боротьби з гібридними вірусами служби профілактики епідемій Outbreak Prevention Services і служби усунення завданої шкоди Damage Cleanup Services.

Ефективність антивірусного сканера безпосередньо залежить від частоти оновлення його бази даних. ServerProtect можна налаштувати таким чином, щоб він автоматично завантажував нові сигнатури вірусів і поновлення скануючого механізму, а потім поширював їх за вказаними серверами. У ServerProtect використовується механізм фрагментарного поновлення (incremental update), що дозволяє завантажувати тільки сигнатури нових вірусів, додані за час, що минув з моменту останнього оновлення бази даних.

Ця функція дозволяє скоротити час завантаження оновлень і знизити створювану даною процедурою навантаження на канали передачі даних. ServerProtect забезпечує збір історії вірусної активності за всіма серверів в єдиний протокол, дані з якого потім можна експортувати в який-небудь зовнішній додаток для докладного аналізу.

ServerProtect також може повідомляти певне коло осіб про спалахи вірусів і інших подіях. Для розсилки повідомлень адміністратори можуть використовувати внутрішню і зовнішню електронну пошту, пейджери,

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						74
Змн.	Арк.	№ докум.	Підпис	Дата		

принтери, переривання SNMP або журнал подій Windows.

Висновки

В розділі проведено розробку заходів, що забезпечують інформаційну безпеку підприємства. Комплекс містить організаційні заходи, які включають в себе інструкції, що регламентують обіг документів та інженерно—технічні, які включають в себе:

- фізичний захист
- змінити систему оплати праці із врахуванням стажу роботи;
- ввести контрактну форму оформлення на роботу;
- заходи із забезпечення стабільного електроживлення шляхом встановлення
- реле напруги РН-240 (263) т;
- джерела безперебійного живлення LPY-B-PSW-7000VA+ та 4 акумуляторних батарей LogicPower LPM MG-12-200;
- Заходи із забезпечення захисту внутрішньої мережі локальної шляхом встановлення сервера безпеки MOXA NPort 6000;
- програмні заходи захисту:
- перевести ведення обліку із програмної платформи «1С:Підприємство» на програмну платформу «MASTER:Бухгалтерія»;
- встановити пакет програм захисту від несанкціонованого доступу «ЛЮЗА-1» конфігурація «Стандартна безпека»;
- встановити програмно-апаратний міжмережевий екран Cisco ASA 5505;
- встановити програму резервного копіювання Backup Maker;
- встановити програму віддаленого адміністрування Paragon Remote Manager 14.0 Pro;
- для забезпечення антивірусного захисту і межмережевого екранування на робочих станціях необхідно встановити Trend Micro InterScan VirusWall.

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						75
Змн.	Арк.	№ докум.	Підпис	Дата		

- для захисту файлового сервера необхідно встановити ServerProtect for Microsoft Windows.

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						76
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 5

МОДЕЛЮВАННЯ КСЗІ ТОВ «МЕХАНІК ТРЕЙД»

5.1. Моделювання загроз в OWASP Threat Dragon

Моделювання роботи КСЗІ та загроз, що можуть впливати на неї проведемо в пакеті прикладних програм: OWASP Threat Dragon.

Згідно із розділів 2-4, де було проаналізовано структуру підприємства, організацію його роботи, слабкі та сильні сторони, а також проведено розробку заходів по запровадженню комплексної системи захисту інформації.

На основі інформації наведеної вище, можливо створити модель кожного елемента для моделювання:

Робочі станції:

Обладнання: Intel Atom D525 (1.8 ГГц) / RAM 2 ГБ / HDD 1000 ГБ / nVidia ION 2, 512 МБ / DVD +/- RW Slim

Програмне забезпечення:

- Операційна система Windows 7;
- Офісний пакет Microsoft Office 2010;
- Поштовий клієнт;
- СКБД «MASTER:Бухгалтерія»;
- «ЛЮЗА-1» конфігурація «Стандартна безпека»;
- Backup Maker;
- Trend Micro InterScan VirusWall.

Сервер:

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						77
Змн.	Арк.	№ докум.	Підпис	Дата		

Обладнання: Intel Core i3 2100 3.1GHz / 3MB / NoTurbo Макс. об'єм пам'яті: 32 ГБ. Типи пам'яті: DDR3-1066 / 1333.

Програмне забезпечення:

- Windows 2003
- ServerProtect for Microsoft Windows.
- Paragon Remote Manager 14.0 Pro
- Backup Maker;
- СКБД «MASTER:Бухгалтерія»;
- «ЛЮЗА-1» конфігурація «Стандартна безпека»;

Локальна мережа

- Cisco ASA 5505
- MOXA NPort 6250/6450/6650

Глобальна мережа

- Cisco ASA 5505
- MOXA NPort 6250/6450/6650

Робочих станцій на підприємстві 43 шт. для зручності розділимо ці робочі станції на окремі групи:

- група робочих станцій бухгалтерії;
- група робочих станцій адміністрації;
- група робочих станцій працівників складу;
- група робочих станцій комерційного відділу;
- група робочих станцій магазину.

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						78
Змн.	Арк.	№ докум.	Підпис	Дата		

Робочі станції передають та отримують дані від сервера. Передача даних здійснюється через окремий елемент – локальна мережа.

Таким чином кожна робоча станція з'єднується із локальною мережею. Також із цією локальною мережею з'єднано сервер.

Сервер здійснює зв'язок між локальною та глобальною мережами.

До глобальної мережі під'єднано також зовнішні для організації об'єкти: Постачальники та Покупці.

Покупці отримують інформацію про товари підприємства та формулюють замовлення товарів.

Постачальники використовують глобальну мережу для передачі інформації комерційного та юридичного характеру: комерційні пропозиції, рахунки, накладні, листи.

Також глобальну мережу використовують зловмисники, серед яких найбільш важливими є :

- хакери;
- конкуренти;
- інсайдери.

Хакери намагаються отримати доступ до персональних даних клієнтів підприємства та до комерційної та фінансової інформації.

Конкуренти намагаються отримати доступ до комерційної інформації.

Інсайдери внаслідок того, що знаходяться всередині підприємства і мають доступ до його інформаційних ресурсів можуть внаслідок порушення правил роботи з інформаційними ресурсами підприємства створювати великий рівень загрози інформаційній безпеці.

Також в моделі слід врахувати техногенні явища. Найбільш суттєвим явищем є якість та стабільність електроживлення.

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						79
Змн.	Арк.	№ докум.	Підпис	Дата		

Модель загроз наведена на рис. 5.1

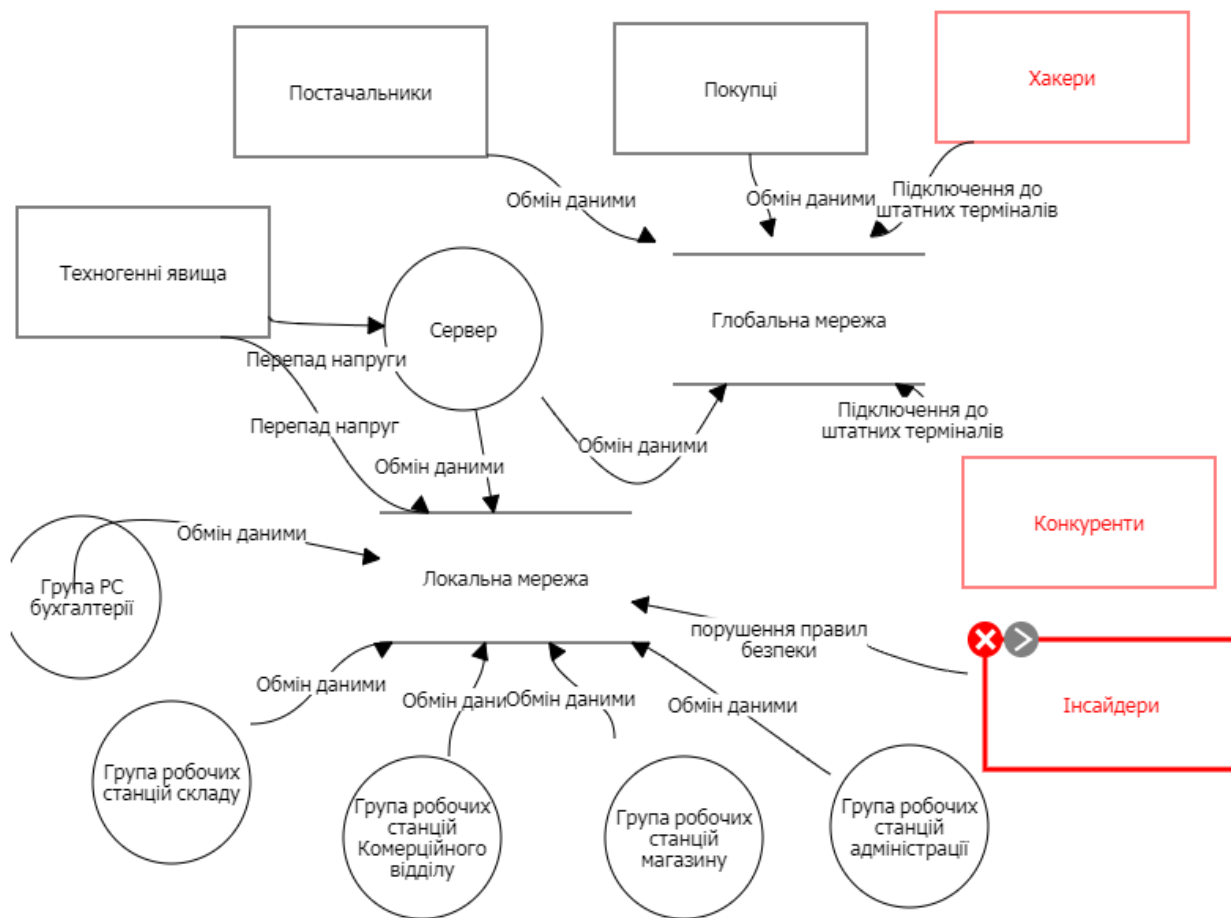


Рис. 5.1. Модель загроз ТОВ «Механіка Трейд»

Аналіз моделі, наведеної на рисунку 5.1, показує, що техногенні явища найбільше впливають на локальну мережу та сервер.

Це пояснюється тим, що робочі станції захищені джерелом безперебійного живлення.

Сервер також захищено джерелом безперебійного живлення, однак час автономної роботи джерела безперебійного живлення складає 2 годин, чого достатньо для коректного вимкнення всіх процесів на сервері, однак не достатньо для нормальної роботи підприємства у випадку відсутності електроживлення.

На локальну мережу підприємства вплив відсутності електроживлення має суттєве значення оскільки обладнання частково знаходиться в зонах, які не забезпечені безперебійним живленням.

Глобальна мережа в свою чергу несе загрози пов'язані із діями хакерів та конкурентів.

Вузьким місцем в цих загрозах є сервер, який має захищати внутрішню локальну мережу від хакерів та дій конкурентів.

Аналіз моделі показує, що основним шляхом потрапляння загрози є глобальна мережа. Перекрити цей шлях повністю не виявляється можливим, оскільки цим шляхом підприємство здійснює комунікацію із покупцями та постачальниками.

Таким чином моделювання наочно показало слабкі місця в КСЗІ та вказало напрямки, які вимагають підвищеної уваги та вдосконалення систем захисту.

5.2. Моделювання роботи мережі в Cisco Packet Tracer

Роботу локальної мережі можливо промоделювати в додатку cisco packet tracer.

Згідно аналізу підприємства, наведеного в розділі 2, локальна мережа складається із робочих станцій, маршрутизаторів, сервера та роутера.

При побудові мереж можливо використовувати динамічний або статичний розподіл адресного простору. На підприємстві ТОВ «Механіка Трейд» використовується статичний спосіб адресації.

Розподіл адрес наведено в табл. 5.1 та 5.2.

У локальній мережі буде використовуватися мережа 10.8.240.0/26. Все активне мережеве обладнання і сервери будуть займати діапазон ір-адрес від

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						81
Змн.	Арк.	№ докум.	Підпис	Дата		

10.8.241.1 до 10.8.241.62. Робочі станції будуть мати ір-адреси в діапазоні 10.8.242.129 і закінчуючи 10.8.248.255

В табл. 5.1 наведено дані про розподіл ір адрес активного обладнання мережі.

Таблиця 5.1

Розподіл ір адрес активного обладнання

Назва активного мережевого обладнання	Адреса підмережі	Діапазон адрес, що використовується	ІР адреси
	10.8.241.0	10.8.241.1-10.8.241.62	
Сервер			10.8.241.1
Маршрутизатор 1			10.8.241.2
Маршрутизатор 2			10.8.241.3

Таблиця 5.2

Розподіл адресних ресурсів мережі

Назва VLAN	Адреса підмережі	Діапазон адрес, що використовується	Назва відділу	ІР адреси відділів
KVD	10.8.242.0/26	10.8.242.1 – 10.8.242.62	Керівництво виконавчої дирекції	10.8.242.1-10.8.242.4
IT	10.8.243.0/26	10.8.243.1-10.8.243.62	ІТ	10.8.243.1-10.8.243.2
Finans	10.8.244.0/26	10.8.244.1-10.8.244.62	Бухгалтерія	10.8.244.1-10.8.244.5
CMV	10.8.245.0/26	10.8.245.1-10.8.245.62	Комерційний відділ.	10.8.245.1-10.8.245.9
SK	10.8.246.0/26	10.8.246.1-10.8.246.62	Склад	10.8.246.1-10.8.246.7
TV	10.8.247.0/26	10.8.247.1-10.8.247.62	Транспортний відділ.	10.8.247.1-10.8.247.4
MAG	10.8.248.0/26	10.8.248.1-10.8.248.62	Магазин	10.8.248.1-10.8.248.6

Модель локальної мережі наведено на рис. 5.2.

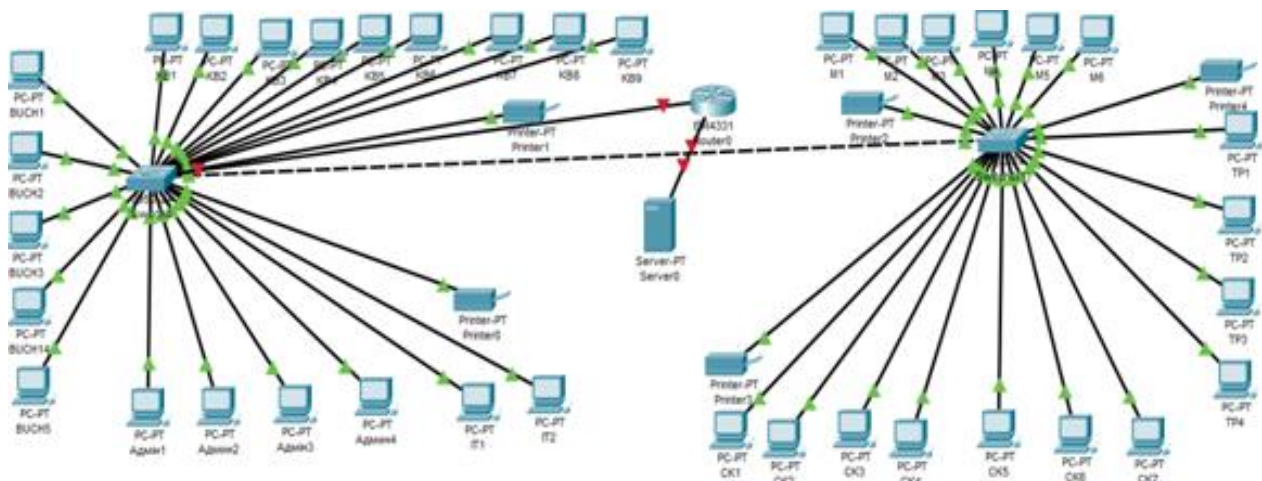


Рис. 5.2. Модель локальної мережі ТОВ «Механіка Трейд»

Для підвищення безпеки кожен відділ утворює свою віртуальну локальну мережу, як це наведено в табл. 5.2.

Моделювання показало працездатність вибраного мережевого обладнання та розподілу мережевих ресурсів.

Висновки

В розділі проведено моделювання загроз, що діють на інформаційну систему ТОВ «Механіка Трейд». Моделювання наочно показало, наявність трьох основних напрямків загроз:

- зовнішніх, які діють через глобальну мережу і включають в себе дії хакерів та конкурентів;
- внутрішніх, які діють через локальну мережу і включають в себе дії працівників підприємства;
- техногенні явища, які впливають на працездатність обладнання підприємства.

ВИСНОВКИ

При виконанні бакалаврської роботи було проведено аналітичний огляд літературних джерел з метою вивчення основних загроз інформаційним системам, засобів захисту від них, основних принципів побудови КСЗІ та вимог до них.

Аналіз літературних джерел показав, що не існує універсальних рішень, які підійдуть для всіх випадків і реалізація комплексної системи захисту інформації залежить від особливостей підприємства, на якому вона запроваджується. Тому для реалізації комплексної системи захисту інформації першочерговою задачею постав аналіз структури підприємства та особливостей його роботи.

Тому було проведено аналіз діяльності підприємства його існуючої структури. Приведено аналіз існуючої системи, що забезпечує безпеку. Виявлені недоліки та недоопрацювання з точки зору безпеки.

Так проведено роботи організаційного характеру та розроблено порядок обігу інформації в межах підприємства, розроблено положення про комерційну таємницю.

Однією із основних організаційних недоліків, який було виявлено являється проблема плинності кадрів, що призводить до формування каналу можливого витоку інформації, як навмисного, так і ненавмисного.

Також аналіз існуючої системи показав відсутність захисту інформації, що міститься на електронних носіях: таких як захист від вірусів, захист від крадіжки, відсутність криптографічного захисту інформації на носіях, використання підсанкційного програмного забезпечення.

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						84
Змн.	Арк.	№ докум.	Підпис	Дата		

В якості основної програмної платформи обліку товарно-матеріальних цінностей використовується 1С: Підприємство. Цей програмний продукт підпадає під санкції. Тому на території України заборонений його продаж, обслуговування та оновлення. Оновлення можливі лише через неофіційні канали із Російської федерації. Використання цього програмного продукту із сірими оновленнями та без сервісного обслуговування приводить до морального застарівання (змінюються форми документів, порядок нарахування податків) програмного забезпечення та до не документованих можливостей доступу зловмисників до внутрішніх документів підприємства.

Основними проблемами в системі забезпечення інформаційної безпеки було визначено:

- автоматизовані робочі місця;
- сервер;
- система захисту конфіденційної інформації.

Була проведена оцінка ризиків та можливих збитків через наявність приведених вище загроз. Згідно отриманих даних оцінки, отримали наступні результати:

- ризик, який виникає із використанням автоматизованих робочих місць складає 74% і втрати в грошовому виміру складають 1537265,48 грн.
- ризик, пов'язаний із сервером складає 15,1% і втрати – 77825,4 грн.
- ризик витоку конфіденційної інформації складає 12,4%, а можливі збитки складають - 37 200 грн.

При виконанні роботи було проведено розробку заходів, що забезпечують інформаційну безпеку підприємства. Комплекс містить організаційні заходи, які включають в себе інструкції, що регламентують обіг документів та інженерно—технічні, які включають в себе:

- фізичний захист
- запровадити контрактну форму влаштування на роботу;

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						85
Змн.	Арк.	№ докум.	Підпис	Дата		

- запровадити стимулюючу систему преміювання, яка залежить від стажу роботи;
- заходи із забезпечення стабільного електроживлення шляхом встановлення
- реле напруги РН-240 (263) т;
- джерело безперебійного живлення LPY-B-PSW-7000VA+ та 4 акумуляторних батарей LogicPower LPM MG-12-200;
- Заходи із забезпечення захисту внутрішньої мережі локальної шляхом встановлення сервера безпеки MOXA NPort 6000;
- програмні заходи захисту:
- перевести ведення обліку із програмної платформи «1С:Підприємство» на програмну платформу «MASTER:Бухгалтерія»;
- встановити пакет програм захисту від несанкціонованого доступу «ЛЮЗА-1» конфігурація «Стандартна безпека»;
- встановити програмно-апаратний міжмережевий екран Cisco ASA 5505;
- встановити програму резервного копіювання Backup Maker;
- встановити програму віддаленого адміністрування Paragon Remote Manager 14.0 Pro;
- для забезпечення антивірусного захисту і межмережевого екранування на робочих станціях необхідно встановити Trend Micro InterScan VirusWall.
- для захисту файлового сервера необхідно встановити ServerProtect for Microsoft Windows.

Також було проведено моделювання загроз інформаційній безпеці в додатку OWASP Threat Dragon.

Моделювання наочно показало, наявність трьох основних напрямків загроз:

- зовнішніх, які діють через глобальну мережу і включають в себе дії хакерів та конкурентів;
- внутрішніх, які діють через локальну мережу і включають в себе дії працівників підприємства;
- техногенні явища, які впливають на працездатність обладнання підприємств

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						86
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. Искусство управления информационными рисками. [Электронный ресурс] – Режим доступа: <http://анализ-риска.рф/>
1. Анализ рисков в управлении информационной безопасностью. [Электронный ресурс] – Режим доступа: <http://www.iso27000.ru/>
2. Симонов С. Технологии и инструментарий для управления рисками // Jet Info. – 2003. – № 2 (117). – С. 3–32.
3. Информационная безопасность (2-я книга социально-политического проекта "Актуальные проблемы безопасности социума"). М.: "Оружие и технологии", 2009.
4. Домарев В. В. Безопасность информационных технологий. Системный подход - К.: ООО ТИД Диа Софт, 2004. - 992 с.
5. Ильюшенко В.Н. Информационная безопасность общества. Учебное пособие. - Томск, 1998.
6. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. [Електронний ресурс] – Режим доступу:– URL: <https://zakon.rada.gov.ua/laws/show/80/94-vr>
7. НД ТЗІ 2.5–005–99 “Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу”.
8. Кустов Г.А. Управление информационными рисками организации на основе логико-вероятностного метода: автореф. дис. канд. тех. наук. – Уфа, 2008. – 18 с.
9. Словарь терминов по безопасности и криптографии. Европейский институт стандартов по электросвязи
10. Бачило И.Л. Информационное право: основы практической информатики. Учебное пособие. М.: 2001.
11. Безопасность: теория, парадигма, концепция, культура. Словарь-

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						87
Змн.	Арк.	№ докум.	Підпис	Дата		

справочник / Автор-сост. профессор В. Ф. Пилипенко. 2-е изд., доп. и перераб. - М.: ПЕР СЭ-Пресс, 2005.

12. Кулаков В.Г. Региональная система информационной безопасности: угрозы, управление, обеспечение. - Автореф. дисс. ... д-ра техн. наук. - Воронеж, 2005.

13. Лапина М. А., Ревин А. Г., Лапин В. И. Информационное право. М.: ЮНИТИ-ДАНА, Закон и право, 2004.

14. Уткин А.И. Глобализация: процесс осмысления. М.: "Логос", 2001.

20. Норткат, С. Обнаружение нарушений безопасности в сетях, 3-е издание / С. Норткат, Д. Новак; пер. с англ. В.С. Иващенко. – М.: Вильямс, 2003. – 448 с.

21. Козиол, Дж. Искусство взлома и защиты систем / Дж. Козиол, Д. Личфилд, Д. Эйтел, К. Энли и др.; пер. с англ. Е. Матвеева. – СПб.: Питер, 2006. – 416 с

22. Положення про комерційну таємницю ТОВ «Механіка Трейд».

23. Функции Сервера 1С. [Электронный ресурс] – Режим доступа: <http://howknow1c.ru/nastroika-1c/1s-server.html>.

24. Система «Ареал CRM». [Электронный ресурс] – Режим доступа: <http://www.arealcrm.ru/features#part1>

25. Система «CRM клиенты и продажи». [Электронный ресурс] – Режим доступа: <http://www.megaplan.ru/products/crm.html>

26. 1С: Предприятие 8. Управление торговлей и взаимоотношениями с клиентами (CRM). [Электронный ресурс] – Режим доступа: <http://www.1service.com.ua/price/sale.php>

27. Система «Backup Maker». [Электронный ресурс] – Режим доступа: <https://www.ascompsoftware.com/en>

28. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу [Електронний ресурс] – Режим доступу: https://tzi.ua/assets/files/1.1_003_99.pdf

29. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						88
Змн.	Арк.	№ докум.	Підпис	Дата		

комп'ютерних системах від несанкціонованого доступу [Електроний ресурс]
– Режим доступу:

<https://tzi.ua/assets/files/%D0%9D%D0%94%20%D0%A2%D0%97%D0%98%201.1-002-99.pdf>

30. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу [Електроний ресурс]

– Режим доступу:

<https://tzi.ua/assets/files/%D0%9D%D0%94%20%D0%A2%D0%97%D0%98%201.1-002-99.pdf>

31. НД ТЗІ 2.5-008-2002 Вимоги із захисту службової інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2 [Електроний ресурс] – Режим доступу:

<https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-008-2002.pdf>

32. НД ТЗІ 2.5-005 -99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу [Електроний ресурс] – Режим доступу:]

<https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-005--99.pdf>

33. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу [Електроний ресурс]

– Режим доступу: <https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-004-99.pdf>

34. НД ТЗІ 2.6-001-11 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах [Електроний ресурс] – Режим доступу:

<https://tzi.com.ua/downloads/2.6-001-11.pdf>

35. НД ТЗІ 2.7-010-09 Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						89
Змн.	Арк.	№ докум.	Підпис	Дата		

інформації від несанкціонованого доступу [Електроний ресурс] – Режим доступу: <https://tzi.com.ua/downloads/2.7-010-09.pdf>

36. НД ТЗІ 3.1-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи [Електроний ресурс] – Режим доступу: <https://www.youtube.com/watch?v=0gpN7iTTaRU>

37. НД ТЗІ 3.3-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації [Електроний ресурс] – Режим доступу: <https://tzi.ua/assets/files/3.3-001-07.pdf>

38. НД ТЗІ 3.7-003 -2005 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі [Електроний ресурс] – Режим доступу: <https://tzi.com.ua/downloads/3.7-003-2005.pdf>

39. ГОСТ 34.602-89 ТЕХНИЧЕСКОЕ ЗАДАНИЕ НА СОЗДАНИЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ [Електроний ресурс] – Режим доступу: <https://tzi.com.ua/downloads/34.602-89.pdf>

40. РД 50-34.698-90 АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ ТРЕБОВАНИЯ К СОДЕРЖАНИЮ ДОКУМЕНТОВ [Електроний ресурс] – Режим доступу: <https://tzi.com.ua/downloads/50-34.698-90.pdf>

41. Столингс, В. Криптография и защита сетей : принципы и практика : пер. с англ. / В. Столингс. – 2-е изд. – М. : Издат. дом «Вильямс», 2001. – 672 с.

42. Фергюсон, Н. Практическая криптография: пер. с англ. / Н. Фергюсон, Б. Шнайер. – М. : Издат. дом «Вильямс», 2005. – 424 с.

43. Фороузан, Б. А. Криптография и безопасность сетей : учеб. пособие / Б. А. Фороузан ; пер. с англ. под ред. А. Н. Берлина. – М. : Интернет – ун-т информ. технологий : Бином, 2010. – 783 с.

44. Anne Marie Willhite. Systems Engineering at MITRE Risk Management, RI, MP96Boooool20, September, 1998; Risk Matrix.

45. Managing the Threat of Denial-of-Service Attacks, CERT- Coordination Center, October 2003.
46. R. Witty, J. Dubiel, J. Girard, J. Graff, A. Hallawell ets. The Price of Information Security. Gartner Research, Strategic Analysis Report, K-l 1-6534, June, 2001.
47. A multipath protocol for secure and reliable data collection in wireless sensor networks : technical report / W. Lou, Y. Zhang , W. Liu, Y. Fang ; ECE department, Worcester Polytechnic Institute, June 2004.
48. Anil Kumar, V. Dynamic Broadcast Routing with Security Enhancement / V. Anil Kumar, B. Yakhoob, E. Pradeep // International Journal of Advances in Engineering & Technology. - May 2011. – Vol. 1, Iss. 2. – P. 20–27.
49. ATM Forum Private Network-Network Interface Specification Version 1.1 (PNNI 1.1). ATM Forum – af-pnni-0055.001, March, 2001
50. Dang, T. D. Fractal Analysis and Modeling of VoIP Traffic / T. D. Dang, B. Sonkoly, S. Molnar // Telecommunications Network Strategy and Planning Symposium. NETWORKS 2004, 11th International, 2004. – P. 217–222
51. Investigating the efficiency of cryptographic algorithms in online transactions // C. Lamprecht, A. Van Moorsel, P. Tomlinson, N. Thomas // I. J. of SIMULATION. – 2006. – Vol. 7, No. 2. – P. 63–75.
52. Lee, G. M. A survey of multipath routing for traffic engineering / G. M. Lee // Proc. of LNCS 3391. Springer-Verlag, 2005. - Vol. 4. – P. 635–661.
53. Lou, W. SPREAD: Enhancing data confidentiality in mobile ad hoc networks / W. Lou, W. Liu, Y. Fang // IEEE INFOCOM 2004, Hong Kong, China, March 2004.

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						91
Змн.	Арк.	№ докум.	Підпис	Дата		

54. Multipath Optimized Link State Routing for Mobile ad hoc Networks / Yijiazhi, Adnane Asmaa, David Sylvain, Parrein Benoit // Ad Hoc Networks 9, 1. – 2011. – P. 28–

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						92
Змн.	Арк.	№ докум.	Підпис	Дата		

					КБ.КВ.Б – 125 – 14 – ПЗ	Арк.
						93
Змн.	Арк.	№ докум.	Підпис	Дата		