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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Дугар Дениса Євгеновича*

академічної групи *125-16-3*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Політика безпеки інформації інформаційно- телекомунікаційної системи ТОВ "PegasGroup"*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доц. каф. БІТ Сафаров О.О.			
розділів:				
спеціальний	к.т.н., доц. каф. БІТ Сафаров О.О.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Тимофєєв Д. С.			

Дніпро
2020

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Дугар Денис Євгенович*** **академічної групи** ***125-16-3***
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Політика безпеки інформації інформаційно-телекомунікаційної системи ТОВ "PegasGroup"***

затверджену наказом ректора НТУ «Дніпровська політехніка» від _26.05.20__ № _275-с_

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз нормативно-правової бази в області інформаційної безпеки	29.03.2020
Розділ 2	Обстеження ОІД. Побудова моделі порушника та моделі загроз. Розробка політики безпеки інформації.	24.05.2020
Розділ 3	Розрахування економічної доцільності ведення розробленної політики безпеки інформації.	09.06.2020

Завдання видано _____ __Сафаров О. О._____
(підпис керівника) (прізвище, ініціали)

Дата видачі: 08.01.2020р.

Дата подання до екзаменаційної комісії: 15.06.2020р.

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

РЕФЕРАТ

Пояснювальна записка: 75 с., 3 рис., 15 табл., 4 додатка, 26 джерел.

Об’єкт розробки: інформаційно-телекомунікаційна система товариства з обмеженою відповідальністю «ПегасГруп».

Предмет розробки: політика безпеки інформації в інформаційно-телекомунікаційній системі товариства з обмеженою відповідальністю «ПегасГруп».

Мета дипломної роботи: підвищення рівня захищеності інформаційно-телекомунікаційної системи товариства з обмеженою відповідальністю «ПегасГруп».

В першому розділі сформовано питання і поставлена задача в галузі інформаційної безпеки, визначено необхідність та актуальність розробки політики безпеки інформації на підприємстві. Виконано аналіз нормативно-правової бази в сфері захисту інформації. Визначено нормативні документи, основні закони та державні стандарти, які мають бути задіяні в процесі розробки політики безпеки інформації на підприємстві.

В спеціальній частині наведено загальну характеристику обстежуваного об’єкту інформаційної діяльності, розроблено модель загроз, виконано аналіз та оцінка ризиків інформаційної безпеки, сформовано загальні положення політики безпеки інформації.

В економічній частині проведено розрахунок витрат на впровадження та експлуатацію політики безпеки інформації. Практичне значення роботи полягає в розробці, впровадженні та експлуатації політики безпеки інформації інформаційно-телекомунікаційної системи.

ІНФОРМАЦІЙНА БЕЗПЕКА, ЗАГРОЗИ, ВРАЗЛИВОСТІ, ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА, ПРОФІЛЬ ЗАХИЩЕНОСТІ, МОДЕЛЬ ЗАГРОЗ, ОЦІНКА РИЗИКУ.

ABSTRACT

Explanatory note: 75 p., 3 fig., 15 tab., 4 additions, 26 sources.

Object of research: information and telecommunication system of the limited liability company «PegasGroup».

Subject of research: information security policy in the information and telecommunication system of the limited liability company «PegasGroup».

The idea of work: increasing the level of protection of information and telecommunication system of the limited liability company «PegasGroup».

In the first section the question is formed and the task in the field of information security is set, the necessity and relevance of the development of information security policy at the enterprise is determined. The analysis of the regulatory framework in the field of information security. The normative documents, the basic laws and the state standards, which should be involved in the process of development of information security policy at the enterprise, are defined.

The special part provides a general description of the object of information activity, the threat model is developed, analysis and assessment of information security risks, formed the general provisions of information security policy.

In the economic part of the calculation of costs for the implementation and operation of information security policy. The practical significance of the work is the development, implementation and operation of information security policy of information and telecommunication system.

INFORMATION SECURITY, THREATS, VULNERABILITIES, INFORMATION AND TELECOMMUNICATION SYSTEM, THE PROFILE OF SECURITY, THE THREAT MODEL, RISK ASSESSMENT.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АРМ – автоматизоване робоче місце;

АС – автоматизована система;

ДТЗС – допоміжні технічні засоби та системи;

ІзОД – інформація з обмеженим доступом;

ІКС – інформаційно-комунікаційні системи;

ІТС – інформаційно-телекомунікаційна система;

КЗ – контрольована зона;

КЗЗ – комплекс засобів захисту;

КСЗІ – комплексна система захисту інформації;

НСД – несанкціонований доступ (дії)

ОІД – об’єкт інформаційної діяльності;

ОС – операційна система;

ОТЗ – основні технічні засоби;

ПБІ – політика безпеки інформації;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

ТЗ – технічне завдання.

ЗМІСТ с.

ВСТУП

У наш час дуже багато всього пов'язано з інформаційними технологіями, не тільки у повсякденному житті але й на підприємствах. Насамперед це необхідно в першу чергу для поліпшення виконання будь-яких завдань або зниження витрат на виробництво або обслуговування якогось процесу.

Але з спрощенням також приходить відповідальність за інформацію яка зберігається, оброблюється та стосується людей або фірми, на якій вони безпосередньо працюють.

Знаючи це можна зрозуміти, що деякі люди зацікавленні в отриманні секретних даних якогось окремо взятого підприємства.

Володіння незаконною секретною інформацією можна використовувати по-різному. Як приклад можна або продати конкурентам даної фірми, які точно будуть зацікавлені в таких даних, або використовувати для фінансових махінацій, які можуть призвести до повного краху виробництва. Таких варіантів багато, головне розуміти що в такому випадку зростає також необхідність на інформаційну безпеку і фахівців з нею.

Налагодження та підтримання працездатності систем безпеки, перевірка каналів зв'язку і передачі, досліджувати можливих загроз та подальші рішення, грамотне налаштування рівнів допуску та зменшення ймовірності несанкціонованого доступу є основними завданнями для інформаційно-телекомунікаційної системи компанії з обмеженою відповідальністю «PegasGroup».

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

У наш час, коли так багато конфіденційної інформації, яка оброблюється, передається та зберігається у великих об'ємах, також дуже популярні хакерські так кібератаки які націлені на будь-які підприємства. З ростом кількості таких атаки зростає також необхідність у спеціалістах у сфері захисту інформаційно-телекомунікаційних систем. Такі фахівці з безпеки створюють захисні механізми, які можуть протистояти атакам різних загроз у компанії.

Під інформаційною безпекою слід розуміти стан захисту життєво важливих інтересів людини, суспільства і держави, в якому запобігається нанесення шкоди через: неповноту, невчасність і неточності використовуваної інформації; негативний інформаційний вплив; негативні наслідки використання інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації. Одним з методів забезпечення безпеки інформації компанії є створення комплексної системи захисту інформації (КСЗІ).

КСЗІ слід вважати комплекс організаційних та інженерних заходів, програмного і апаратного забезпечення, що забезпечують захист інформації в АС. Відповідаючи вимогам законодавства України та створюючи КСЗІ, клієнт (який також є головою підприємства) отримує пакет документів, який складається з: акту контролю об'єкта інформаційної активності, моделі загроз, моделі зловмисника, політики безпеки, плану захисту інформації, графіка роботи щодо захисту інформації, специфікацій «Технічна інформація про створення КСЗІ», проектна та експлуатаційна документація, виконання робіт в кінці етапів і дозвіл переходу до наступного етапу створення КСЗІ, сертифікатів випробувань і сертифікатів відповідності.

Основною метою створення КСЗІ можна вважати досягнення ефективного захисту за рахунок використання всіх необхідних ресурсів, методів та інструментів,

що виключають несанкціонований доступ до інформації та створення умов для обробки інформації відповідно до чинних нормативно-правових актів України в сфері захисту інформації. КСЗІ складається з засобів і заходів, які реалізують методи та механізми для захисту інформації від:

- витоків через технічні канали, які включають акустичні та інші канали;

- несанкціоновані дії та несанкціонований доступ до інформації які можуть здійснюватися шляхом підключення до обладнання та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів безпеки з метою використання інформації або нав'язування хибної інформації, використання вбудованих пристроїв або програм, використання вірусів у комп'ютерній системі тощо

- особливий ефект на інформацію, який може бути реалізований шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту.

Кожна інформаційно-телекомунікаційна система має свій склад, структуру, клас АС, профілі інформаційної безпеки в комп'ютерних системах, обробку та зберігання інформації. Ось чому неможливо створити єдину структуру, яка буде регулювати методи і засоби забезпечення захисту інформації в ІТС. Схема впровадження інформаційної безпеки для компанії складається з п'яти компонентів: технічної, організаційної, дозвільної, профілактичної та юридичної. Оскільки всі елементи і підсистема взаємопов'язані в будь-якій системі, більшість завдань інформаційної безпеки виконуються за допомогою основної та допоміжної підсистем системи економічної безпеки підприємства.

Технічний компонент служить для захисту інформації і можливостей компанії, а також для виявлення фактів витоку інформації і незаконних дій персоналу і сторонніх осіб в цій компанії з використанням технічних засобів.

Організаційна складова повинна забезпечувати упорядковану поведінку персоналу компанії з секретною інформацією та іншими об'єктами захисту бізнес-одиниці. Дозволений компонент системи інформаційної безпеки повинен поширювати інформацію про компанію за ступенем секретності і визначати

ступінь доступу до неї. Компонент обережності необхідний для того, щоб уникнути наслідків дезінформації та подальшого прийняття невірних управлінських рішень, а також максимального зниження ймовірності втрати секретної інформації.

Правовий компонент покликаний забезпечити правовий захист інтересів компанії по захисту інформації, а також консолідацію прав компанії на комерційну таємницю в установчих документах, договорах та інших нормативних актах. Згідно з умовами, які забезпечують безпеку інформаційних ресурсів, компанія, що працює з персональними даними своїх клієнтів, повинна дотримуватися вимог щодо захисту персональних даних, оскільки ця інформація є дуже цікава для хакерів і порушників. За порушення безпеки персональних даних, наданих компанії для обробки, відповідальність передбачена відповідно до чинного законодавства України. За часів зростаючих загроз фірма повинна мати можливість розробляти і впроваджувати політику інформаційної безпеки. У свою чергу, політика інформаційної безпеки повинна

- розглядатися як документована інформація;
- бути повідомленим працівникам організації;
- бути доступними в порядку, встановленому для зацікавлених сторін.
- досягти цілей організації;
- містити цілі інформаційної безпеки або вказати основні положення, що визначають ці цілі;
- включати зобов'язання щодо дотримання поточних вимог інформаційної безпеки;
- Включити зобов'язання по постійному вдосконаленню системи управління інформаційною безпекою.

Актуальність теми роботи заснована на швидкому розвитку загроз інформаційної безпеки малих і середніх комерційних організацій. З цієї причини дотримання стандартів, інститутів, вимог і правил, які інтерпретуються в політиці безпеки, є найбільш важливим і найбільш ефективним важелем підвищення рівня безпеки інформаційної та телекомунікаційної системи.

1.2 Аналіз нормативно-правової бази в області інформаційної безпеки

Нормативно-правова база в сфері захисту інформації має велику кількість документів, що регламентують методи і методи збереження інформаційних властивостей, встановлює основні вимоги для розробки політики інформаційної безпеки, етапи побудови комплексної системи захисту інформації, вимоги для розробки технічних специфікацій, порядку проведення експертизи функціональної середовища ІТС, складання плану захисту і т. д. Закон України «Про інформацію» визначає поняття «захист інформації», а в статті 9 йдеться про те, що захист інформації є одним з видів інформаційної діяльності. Закон України «Про захист персональних даних» регулює вимоги, пов'язані із захистом і обробкою персональних даних, а також спрямований на захист прав і свобод людини і громадянина. Закон України «Про основні засади забезпечення кібербезпеки України» вперше визначає поняття «кібербезпека», «кіберзагроз», «кіберзлочинність», «критична інформаційна інфраструктура» тощо. Цей закон визначає правові та організаційні засади забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства і держави, а також національних інтересів України в кіберпросторі. Вперше криптографічний захист інформації згадувалася в Указі Президента України «Про Положення про порядок здійснення криптографічного захисту інформації в Україні», який визначає поняття «криптографічний захист інформації». Саме положення визначає порядок реалізації криптографічного захисту ІзОД, розкриття якої може завдати шкоди державі, суспільству або особистості. Указ Президента України «Про Положення про технічний захист інформації в Україні» визначає правові та організаційні засади технічного захисту інформації. Положення також визначає поняття «комплексна технічний захист інформації».

Постанова Кабінету Міністрів України «Про затвердження правил забезпечення захисту інформації в ІТ, телекомунікації та ІТ та телекомунікаційних системах» визначає, яка інформація повинна бути захищена в системі, які операції з інформацією повинні бути захищені від несанкціонованого доступу і як захист

забезпечується в секретна і службова інформаційна система, така як ця інформація, передається тощо. Перш ніж ви почнете створювати КСЗІ, ви повинні класифікувати засоби інформаційної діяльності. З цією метою створюється комісія з категоризації, яка, згідно з НД ТЗІ 1.6-005-2013, «Захист інформації на об'єктах інформаційної діяльності». Постанова про класифікацію об'єктів, в яких інформація з обмеженим доступом, яка не є державною таємницею, поширюється в ОІД.

Для створення КСЗІ необхідно враховувати вимоги нормативних документів в галузі захисту технічної інформації, в тому числі НД ТЗІ 3.7-00305. Процедура створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі визначає етапи побудови КСЗІ, НД ТЗІ 2.5.004-99 Критерії оцінки інформаційної безпеки. У комп'ютерних системах від несанкціонованого доступу визначаються критерії конфіденційності, цілісності, доступності, спостережливості і гарантії комп'ютерних систем для надання необхідних функціональних послуг, НД ТЗІ 2.5.005-99 Класифікація автоматизованих систем і стандартні функціональні профілі безпеки для інформації, що обробляється від несанкціонованого доступу, визначають класифікацію автоматизованих систем і пропонують стандартні функціональні профілі безпеки, які складаються з функціональних сервісів. Важливим кроком у створенні КСЗІ є розробка технічних специфікацій, яка інтерпретується як НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.

1.3 Постановка задачі

З урахуванням вищевикладеного можна визначити, що інформаційно-телекомунікаційна система ТОВ «PegasGroup» вимагає в рішенні дисертації наступних завдань:

1. Вивчити автоматизовану систему ТОВ «PegasGroup», розглядаючи її як організаційно-технічну систему, яка об'єднує в собі фізичне середовище,

комп'ютерна система і середовище для обробки інформації користувачів і технології її обробки.

2.Розробка моделі загроз і моделі зловмисника досліджуваної компанії.

3. Оцінка інформаційних ризиків за обраною методологією.

4. Створення політики інформаційної безпеки.

5. Перевірте ефективність реалізації політик безпеки шляхом переоцінки ризиків, пов'язаних з інформацією.

6. Визначення та аналіз економічної ефективності розробки політик інформаційної безпеки

1.4 Висновки

Визначено загальний стан розвитку загроз інформаційної безпеки компанії, сформовані основні завдання дипломної роботи та нормативно-правова база, що передбачає побудову етапів комплексних систем захисту інформації. Аналізується, а саме: розробка акту перевірки об'єкта інформаційної діяльності, побудова моделі загрози і моделі порушника, оцінка інформаційного ризику, постановка реалізація політики інформаційної безпеки, а також переоцінка інформаційних ризиків з урахуванням реалізації політики безпеки. Розробка коплексної системи захисту інформації є важливим кроком для забезпечення безпеки автоматизованих інформаційних систем телекомунікаційної системи компанії, вона вимагає контролю за дотриманням вимог, встановлених законодавством України у захист технічної інформації.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальні відомості про підприємство ТОВ «PegasGroup»

(ТОВ) «PegasGroup» (надалі Компанія), область діяльності якої – дистрибуція харчових товарів по всій Україні. Компанія займається логістичними послугами для великих магазинів та торгівельних марок.

Обьект має такі характеристики:

Офіс розташований за наступним адресом:Україна, м. Дніпро вул. Запорізьке шосе, 37, офіс № 317. Також офіс займає частину 3-го поверху з 5 поверхів будівлі. Форма власності: приватна власність.

Режим роботи підприємства:

Час роботи: 09.00 – 19.30

Робочі дні: понеділок – п’ятниця.

Підприємство складається з наступних підрозділів:

- відділ логістики
- бухгалтерія
- відділ опрацювання замовлень
- відділ збуту
- відділ програмного забезпечення

Організаційна структура підприємства представлена на рисунку 2.1.

Штат ТОВ «PegasGroup» налічує 27 осіб, серед них:

- Директор – 1 особа
- Начальник відділу логістики – 1 особа
- Логіст – 8 осіб
- Адміністратор – 1 особа
- Головній бухгалтер – 1 особа
- Бухгалтер – 5 осіб
- Менеджер колл-центру – 1 особа
- Оператор – 5 осіба

- Головний менеджер збуту – 1 особа
- Менеджер збуту – 3 особи

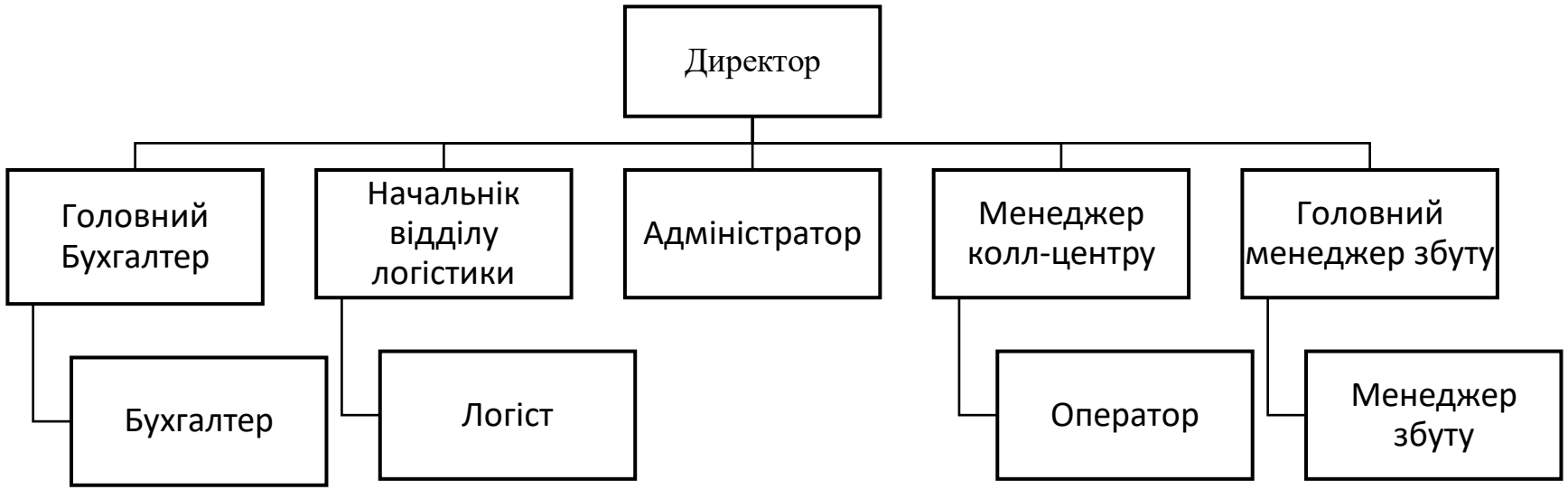


Рисунок 2.1 – Організаційна структура ТОВ «PegasGroup»

Таблиця 2.1 Опис будівель

Номер будівлі на малюнку	Етажність	Використання	Адреса
1	1	Порше Центр Дніпро	Запорізьке шосе, 37Д, Дніпро́, Дніпропетровська область, 49000
2	3	Paris Dakar ODessa COrp.	Запорізьке шосе, 37, Дніпро́, Дніпропетровська область, 49000
3	5	Корпорація Біосфера	Запорізьке шосе, 37, Дніпро́, Дніпропетровська область, 49000
4	2	Тойота Центр Дніпро "Алмаз мотор"	Запорізьке шосе, 35, Дніпро́, Дніпропетровська область, 49040
5	1	Автомийка Самообслуговування	Запорізьке шосе, 37б, Дніпро́, Дніпропетровська область, 49000
6	1	АТБ-Маркет	Запорізьке шосе, 45, Дніпро́, Дніпропетровська область, 49000

Фізичні характеристики будівлі :

-Зовнішні стіни будівлі виконані з трьошарової панелі, наружна частина-залізобетонний шар 60 мм, центральна частина - теплоізолюючий шар 200 мм - 220 мм, внутрішній шар - залізобетонний 80-100 мм;

-Внутрішні стіни виконана із гіпсобетону 80-100мм;

-Дах будівлі - вентелюючий суміжний дах, складений із спарених залізобетонних плит, вкладених між теплоізолятором. Вхід на дах здійснюється через спеціалі сходи на останньому поверсі будівлі, доступ до якої мають лише технічний персонал бізнес центру.

-Підлога представляє собою плиту міжповерхового перекриття, звукоізолюючий шар, арміруючий шар та гідроізолюючий шар, на який покладено кірамічну плитку;

-Головні двері входу мають розміри 900 мм х 2050 мм, виконані з металопластику та скла, оздоблені врізним замком;

-Міжкімнатні двустворчати двері мають розміри одного полотна 70 см * 200 см, виконані з зрощеного масива сосни, кожна міжкімнатна дверь має один врізний замок;

-Міжкімнатні одностворчаті двері мають розміри 60 см * 200 см, виконані з зрощеного масива сосни, кожна міжкімнатна дверь має один врізний замок;

-Вікна приміщщення поворотньо-відкривне виконані з металопластику, 1400 мм х 2100 мм, кожне вікно має змогу відкриватись, кількість пакетів - 3;

-Територія, навколо будівлі - відкрита.

Таблиця 2.2 Системи комунікації будівлі

Система комунікації	Вихід за межі КЗ	Характеристика
Система електро-постачання	+	Підключена до трансформаторної підстанції, знаходиться за межами КЗ
Система опалення	+	Міська система опалення, підключена до за межами КЗ. Труби опалення виконані з ПВХ.
Система каналізації	+	Підключена до міської мережі, яка знаходиться за межами КЗ
Система водопостачання	+	Підключена до міської мережі, яка знаходиться за межами КЗ
Інтернет	+	Інтернет провайдер Воля
Система сигналізації	-	Складається з пасиних інфрачервоних датчиків руху та датчиків температури. Блок керування та датчики- Ajax starterkit plus black.
Система кондиціонування	-	Кондиціонер спліт ElectrOlux серії FusiOn модель EACS-07HF/N3, кількість х3

Таблиця 2.3 Перелік та розміщення ОТЗ/ДТЗС

Назва ОТЗ/ДТЗС	Розміщення	Мінімальна відстань до КЗ /м
ПК PC_1	Відділ логістики	
ПК PC_2	Відділ логістики	
ПК PC_3	Відділ логістики	
ПК PC_4	Відділ логістики	
ПК PC_5	Відділ логістики	
ПК PC_6	Відділ логістики	
ПК PC_7	Відділ логістики	
ПК PC_8	Відділ логістики	
ПК PC_9	Відділ логістики	
ПК PC_10	Відділ логістики	
ПК PC_11	Відділ логістики	
ПК PC_12	Бухгалтерія	
ПК PC_13	Бухгалтерія	
ПК PC_14	Бухгалтерія	
ПК PC_15	Бухгалтерія	
ПК PC_16	Бухгалтерія	

Продовження таблиці 2.3

Назва ОТЗ/ДТЗС	Розміщення	Мінімальна відстань до КЗ /м
ПК PC_17	Бухгалтерія	
ПК PC_18	Відділ опрацювання замовлень	
ПК PC_19	Відділ опрацювання замовлень	
ПК PC_20	Відділ опрацювання замовлень	
ПК PC_21	Відділ опрацювання замовлень	
ПК PC_22	Відділ опрацювання замовлень	
ПК PC_23	Відділ опрацювання замовлень	
ПК PC_24	Відділ збуту	
ПК PC_25	Відділ збуту	
ПК PC_26	Відділ збуту	
ПК PC_27	Відділ збуту	
Комутатор SW1M	Відділ логістики	
Комутатор SW2	Відділ опрацювання замовлень	
Сервер SERVER_IN	Відділ логістики	

Продовження таблиці 2.3

Назва ОТЗ/ДТЗС	Розміщення	Мінімальна відстань до КЗ /м
Сервер SERVER_DB	Відділ логістики	
Роутер DL	Відділ логістики	
Кондиціонер 1	Відділ логістики	
Кондиціонер 2	Відділ опрацювання замовлень	
Кондиціонер 3	Відділ збуту	
Прінтер PR1	Відділ логістики	
Прінтер PR2	Бухгалтерія	
Прінтер PR3	Відділ збуту	
ІЧ датчик руху 1	Відділ логістики	
ІЧ датчик руху 2	Бухгалтерія	
ІЧ датчик руху 3	Відділ опрацювання замовлень	
ІЧ датчик руху 4	Відділ збуту	
Температурний датчик 1	Відділ логістики	
Температурний датчик 2	Відділ логістики	

Продовження таблиці 2.3

Назва ОТЗ/ДТЗС	Розміщення	Мінімальна відстань до КЗ /м
Температурний датчик 3	Відділ логістики	
Температурний датчик 4	Бухгалтерія	
Температурний датчик 5	Бухгалтерія	
Температурний датчик 6	Відділ опрацювання замовлень	
Температурний датчик 7	Відділ опрацювання замовлень	
Температурний датчик 8	Відділ збуту	
Температурний датчик 9	Відділ збуту	
Блок керування сигналізацією	Відділ логістики	
Розподільний блок електроживлення	Відділ логістики	

Таблиця 2.4 Умовні позначення

Колір	Позначення
	Основні технічні засоби
	Допоміжні технічні зачоби

2.2 Обстеження ОС

На підприємстві церкулює інформація з обмеженим доступом, доступ до якої контролюється розподільним сервером. Також на підприємстві наявні прінтери, доступ до яких має чітке розмежування.

В мережі ТОВ кожному комп’ютеру присвоєні імена, а саму мережу розділено на робочі групи: адміністратор, користувач.

Розмежування доступу робиться на основі відділів, в яких працюють співробітники.

Кожний відділ має доступ лише до певних файлів, програм та інформації, у кожного відділу є свої права та омеження. Обмін інформацією між відділами здійснюється за допомогою серверу або зовнішніх носіїв.

Таблиця 2.5 Технічні засоби

Назва	Характеристика	Умовні позначення	Кількість
Принтери	CanOn E4240 (2985C009)	PR1 - PR3	3

Продовженн таблиці 2.5

Назва	Характеристика	Умовні позначення	Кількість
Робоча станція 1	HP COmpaq dc7900 MT / Intel COre 2 DuO E8400 (2 ядра по 3.0GHz) / 4 GB DDR2 / 320 GB HDD	PC_24 - PC_27	4
Робоча станція 2	Dell OptiPlex 780 TOwer / Intel COre 2 DuO E7500 (2 ядра по 2.93 GHz) / 4 GB DDR3 / 320 GB HDD	PC_18 - PC_23	6
Робоча станція 3	Fujitsu EsprimO P710 E85+ TOwer / Intel COre i3-2120 (2 (4) ядра по 3.3 GHz) / 4 GB DDR3 / 60 GB SSD+320 GB HDD	PC_1 - PC_17	17
Комутатор	TP-LINK TL-SG1024DE 24-портовий гігабітний комутатор (10/100/1000 Мбіт / с)	SW1M SW2	2
Точка доступа	TP-LINK Archer A9	DL	1

2.2.1 Призначення серверу та особливості роботи.

Сервера компанії типу NAS(NetwOrk Attached StOrage), це сервера накопичувачі даннх. Основним призначенням цього серверу є надання сервісів для зберігання даних. Як правило, сучасні NAS використовують в якості носія інформації жорсткі диски в силу їх порівняно великих (щодо інших технологій зберігання інформації) доступних ємностей при порівняно низькій вартості зберігання за одиницю об’єму. Працює сервер на базі ОС Oracle SOlaris ZFS AdministratiOn Guide.

Таблиця 2.6 Класифікація інформації

Вид інформації	Режим доступу	Правовий режим	К	Ц	Д
Документація з маршрутів доставки	З обмеженим доступом	Конфедеційна	1	3	2
Документація про постачальників	З обмеженим доступом	Конфедеційна	2	1	2
База даних клієнтів	З обмеженим доступом	Конфедеційна	2	2	2
Звітність бухгалтерії	З обмеженим доступом	Конфедеційна	3	3	2
Прайс листи на продукцію	Відкрита				
Сертифікати на продукцію	Відкрита				

Таблиця 2.7 Класифікація доступу до інформації

Назва	Н1	Н2	Н3
Конфедеційність	Максимальне забезпечання конфедеційності інформації (К1)	Середній рівень забезпечення конфедеційності (К2)	Мінімальний рівень конфедеційності (К3)

Продовження таблиці 2.7

Назва	Н1	Н2	Н3
Цілістнітсь	Максимальне забезпечання цілістності інформації (Ц1)	Середній рівень забезпечення цілістності (Ц2)	Мінімальний рівень цілістності (Ц3)
Доступність	Максимальне забезпечання Доступності інформації (Д1)	Середній рівень забезпечення Доступності (Д2)	Мінімальний рівень Доступності (Д3)

2.2.2 Аналіз технології обробітку інформації «Документація з маршрутів доставки»

Документи з маршрутів доставки створюються на комп’ютерах PC_1 - PC_10. Для кожного співробітника виділяється певні регіони країни для опрацювання. Після постановки задачі на створення документу співробітники починають працювати.

Документи створюються на основі шаблонів документів які зберігаються на сервері. Для цього співробітники імпортують собі на робочі станції шоблони документів.

Після імпортування йде процес створення документу. Під час створення документу, його імпортують на компьютер директора компанії для того, щоб друкувати на прінтері. Обмін між комп’ютерами здійснюєть за допомогою серверів та зовнішніх носіїв.

Після створення документу його фінальну версію імпортують на ПК начальника відділу логістики, за допомогою зовнішніх носіїв для затвердження документа. Після затвердження начальником відділу логістики документи

імпортуються на ПК бухгалтера, якого затвердить головний бухгалтер. Бухгалтер підраховує економічну частину документа та віддає головному бухгалтеру на затвердження. Для імпортування використовують зовнішні носії та сервера компанії.

Після затвердження головним бухгалтером документ імпортують на компьютер директора компанії, для затвердження. Після затвердження імпортуються копії документів до відділу збуту для подальшого використання. Надалі документи передаються перевізникам та закріплюються у контракті з магазинами.

Таблиця 2.8 Види інформації

Номер	**Вид інформації**
1	Документація з маршрутів доставки
2	Документація про постачальників
3	База даних клієнтів
4	Звітність бухгалтерії
5	Прайс листи на продукцію
6	Сертифікати на продукцію

Таблиця 2.9 Встановлене ПЗ

Розміщення	Тип	Назва
Сервер	Операційна система	Oracle SOlaris ZFS AdministratiOn Guide
Робоча станція 1 PC_24 - PC_27	Операційна система	WindOws 10 10.0.18363.836 «May 12, 2020—KB4556799 (OS Builds 18362.836 and 18363.836)»
	ПЗ для роботи з документами	MicrOsOft Office 2019 (24 вересня 2018)
	Веб-браузер	Opera 66.0.3515.27
	Антивірус	Avast 20.2.2401 (WindOws) (1 квітня 2020)
Робоча станція 2 PC_18 - PC_23	Операційна система	WindOws 10 10.0.18363.836 «May 12, 2020—KB4556799 (OS Builds 18362.836 and 18363.836)»
	ПЗ для роботи з документами	MicrOsOft Office 2019 (24 вересня 2018)
	Веб-браузер	Opera 66.0.3515.27
	Антивірус	Avast 20.2.2401 (WindOws) (1 квітня 2020)

Продовження таблиці 2.9

Розміщення	Тип	Назва
Робоча станція 3 PC_1 - PC_17	Операційна система	WindOws 10 10.0.18363.836 «May 12, 2020—KB4556799 (OS Builds 18362.836 and 18363.836)»
	ПЗ для роботи з документами	MicrOsOft Office 2019 (24 вересня 2018)
	Веб-браузер	Opera 66.0.3515.27
	Антивірус	Avast 20.2.2401 (WindOws) (1 квітня 2020)
	ПЗ для автоматизації бухгалтерського обліку	1С:Бухгалтерія 8.1 клієнт

Таблиця 2.10 Середовище користувачів

Користувач	Роль	Рівень кваліфікації/освіта	Досвід (рік)
Директор компанії PC_1	Користувач	Вища спеціальна освіта	12
Начальник відділу Логістики PC_2	Користувач	Вища спеціальна освіта	7
Логіст PC_3	Користувач	Середня спеціальна освіта	3

Продовження таблиці 2.10

Користувач	Роль	Рівень кваліфікації/освіта	Досвід (рік)
Логіст PC_4	Користувач	Відсутність спеціальної підготовки	4
Логіст PC_5	Користувач	Середня спеціальна освіта	3
Логіст PC_6	Користувач	Відсутність спеціальної підготовки	5
Логіст PC_7	Користувач	Вища спеціальна освіта	6
Логіст PC_8	Користувач	Вища спеціальна освіта	3
Логіст PC_9	Користувач	Вища спеціальна освіта	4
Логіст PC_10	Користувач	Вища спеціальна освіта	2
Адміністратор PC_11	Адміністратор	Середня спеціальна освіта	5
Головний бухгалтер PC_12	Користувач	Вища спеціальна освіта	14

Продовження таблиці 2.10

Користувач	Роль	Рівень кваліфікації/освіта	Досвід (рік)
Бухгалтер PC_13	Користувач	Середня спеціальна освіта	6
Бухгалтер PC_14	Користувач	Вища спеціальна освіта	8
Бухгалтер PC_15	Користувач	Вища спеціальна освіта	5
Бухгалтер PC_16	Користувач	Вища спеціальна освіта	8
Бухгалтер PC_17	Користувач	Вища спеціальна освіта	7
Менеджер колл-центру PC_18	Користувач	Середня спеціальна освіта	5
Оператор PC_19	Користувач	Відсутність спеціальної підготовки	3
Оператор PC_20	Користувач	Відсутність спеціальної підготовки	2
Оператор PC_21	Користувач	Відсутність спеціальної підготовки	3

Продовження таблиці 2.10

Користувач	Роль	Рівень кваліфікації/освіта	Досвід (рік)
Менеджер збуту PC_25	Користувач	Відсутність спеціальної підготовки	5
Менеджер збуту PC_26	Користувач	Відсутність спеціальної підготовки	6
Менеджер збуту PC_27	Користувач	Відсутність спеціальної підготовки	5
Оператор PC_22	Користувач	Відсутність спеціальної підготовки	3
Оператор PC_23	Користувач	Відсутність спеціальної підготовки	4
Головний менеджер збуту PC_24	Користувач		9

Таблиця 2.11 Правила розмежування доступу

Користувач	**Інформація**	**Читання**	**Запис**	**Друкування**
Директор компанії PC_1	Документація з маршрутів доставки	+	+	+
	Документація про постачальників	+	+	+
	База даних клієнтів	+	+	+
	Звітність бухгалтерії	+	+	+
	Прайс листи на продукцію	+	+	+
	Сертифікати на продукцію	+	+	+
Начальник відділу Логістики PC_2	Документація з маршрутів доставки	+	+	
	Документація про постачальників	+	+	
	База даних клієнтів	+		
	Звітність бухгалтерії	+		
	Прайс листи на продукцію	+	+	
	Сертифікати на продукцію	+	+	-
Логіст PC_3-PC_10	Документація з маршрутів доставки	+	+	-

Продовження таблиці 2.11

Користувач	**Інформація**	**Читання**	**Запис**	**Друкування**
	Документація про постачальників	+	-	-
	База даних клієнтів	+	-	-
	Звітність бухгалтерії	-	-	-
	Прайс листи на продукцію	+	-	-
	Сертифікати на продукцію	+	-	-
Адміністратор PC_11	Документація з маршрутів доставки	+	+	+
	Документація про постачальників	+	+	+
	База даних клієнтів	+	+	+
	Звітність бухгалтерії	+	+	+
	Прайс листи на продукцію	+	+	+
	Сертифікати на продукцію	+	+	+
Головний бухгалтер PC_12	Документація з маршрутів доставки	+	-	-
	Документація про постачальників	+	+	+
	База даних клієнтів	+	-	-
	Звітність бухгалтерії	+	+	+

Продовження таблиці 2.11

Користувач	**Інформація**	**Читання**	**Запис**	**Друкування**
	Прайс листи на продукцію	+	+	-
	Сертифікати на продукцію	+	-	-
Бухгалтер PC_13 - PC_17	Документація з маршрутів доставки	+	-	-
	Документація про постачальників	+	-	-
	База даних клієнтів	+	-	-
	Звітність бухгалтерії	+	+	-
	Прайс листи на продукцію	+	-	-
	Сертифікати на продукцію	+	-	-
Менеджер колл-центру PC_18 Менеджер збуту PC_25-PC_27	Документація з маршрутів доставки	+	-	-
	Документація про постачальників	+	-	-
	База даних клієнтів	+	+	+
	Звітність бухгалтерії	+	-	-
	Прайс листи на продукцію	+	+	-
	Сертифікати на продукцію	+	+	-

Аналізуючи отримані дані та спираючись на НД ТЗІ 2.5.005-99 був визначений функціональний профіль захищеності в КС, що входять до складу АС класу 3, з підвищеними вимогами до забезпечення конфіденційності, цілісності і доступності оброблюваної інформації.

3.КЦД.2 = { КД-2, КА-2, КО-1, КВ-2, ЦД-1, ЦА-2, ЦО-1, ЦВ-2, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 } Згідно з НД ТЗІ 2.5.004-99:

КД-2 – Базова довірча конфіденційність. Ця послуга дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

КА-2 – Базова адміністративна конфіденційність. Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від захищених об'єктів до користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості управління.

КО-1 – Повторне використання об'єктів. Ця послуга дозволяє забезпечити коректність повторного використання розділюваних об'єктів, гарантуючи, що в разі, якщо розділюваний об'єкт виділяється новому користувачу або процесу, то він не містить інформації, яка залишилась від попереднього користувача або процесу.

КВ-2 – Базова конфіденційність при обміні. Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

ЦД-1 – Мінімальна довірча цілісність. Ця послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що

належать його домену. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

ЦА-2 – Базова адміністративна цілісність. Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від користувачів до захищених об'єктів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

ЦО-1 – Обмежений відкат. Ця послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкатити) захищений об'єкт до попереднього стану. Рівні даної послуги ранжируються на підставі множини операцій, для яких забезпечується відкат.

ЦВ-2 – Базова цілісність при обміні. Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

ДР-1 – Квоти. Ця послуга дозволяє користувачам керувати використанням послуг і ресурсів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування доступністю послуг КС.

ДВ-1 – Ручне відновлення. Ця послуга забезпечує повернення КС у відомий захищений стан після відмови або переривання обслуговування. Рівні даної послуги ранжируються на підставі міри автоматизації процесу відновлення.

НР-2 – Захищений журнал. Реєстрація дозволяє контролювати небезпечні для КС дії. Рівні даної послуги ранжируються залежно від повноти і вибірковості контролю, складності засобів аналізу даних журналів реєстрації і спроможності вияву потенційних порушень.

НИ-2 – Одиночна ідентифікація і автентифікація. Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача,

що намагається одержати доступ до КС. Рівні даної послуги ранжируються залежно від числа задіяних механізмів автентифікації.

НК-1 – Однонаправлений достовірний канал. Ця послуга дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ. Рівні даної послуги ранжируються залежно від гнучкості надання можливості КЗЗ або користувачу ініціювати захищений обмін.

НО-2 – Розподіл обов'язків адміністраторів. Ця послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Рівні даної послуги ранжируються на підставі вибірковості керування можливостями користувачів і адміністраторів.

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

НТ-2 – Самотестування при старті. Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Рівні даної послуги ранжируються на підставі можливості виконання тестів у процесі запуску або штатної роботи.

НВ-1 – Автентифікація вузла. Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ранжируються на підставі повноти реалізації.

Спираючись на отримані дані в таблиці 2.15 можна зробити підсумок, що належному захисту підлягають наступний перелік інформації (сума балів яких вище 7): картка клієнта на проведення робіт, щомісячний фінансовий звіт, щорічний фінансовий звіт, БД клієнтів, адміністративні дані сайту (логін і пароль від хостингу, доступи до FTP та ін.), звіт про нарахування зарплати, відомості про працівників, звіт виконаних робіт проекту та банківські дані підприємства (о/р, ЄДРПОУ та ін.).

Таблиця 2.12 Модель порушника внутрішнього

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума
Директор компанії PC_1	ПВЗ	МЗ	К2	З1	Ч4	Д2	15
Начальник відділу Логістики PC_2	ПВЗ	МЗ	К2	З1	Ч4	Д2	15
Логіст PC_3	ПВЗ	МЗ	К1	З1	Ч4	Д2	14
Логіст PC_4	ПВЗ	МЗ	К1	З1	Ч4	Д2	14
Логіст PC_5	ПВЗ	МЗ	К2	З1	Ч4	Д2	14
Логіст PC_6	ПВЗ	МЗ	К1	З1	Ч4	Д2	14
Логіст PC_7	ПВЗ	МЗ	К1	З1	Ч4	Д2	14

Продовження таблиці 2.12

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума
Логіст РС_8	ПВ3	М3	К1	З1	Ч4	Д2	14
Логіст РС_9	ПВ3	М3	К1	З1	Ч4	Д2	14
Логіст РС_10	ПВ3	М3	К1	З1	Ч4	Д2	14
Адміністратор РС_11	ПВ4	М3	К3	З2	Ч4	Д4	20
Головний бухгалтер РС_12	ПВ3	М3	К1	З1	Ч4	Д2	14
Бухгалтер РС_13	ПВ3	М3	К2	З1	Ч4	Д2	15
Бухгалтер РС_14	ПВ3	М3	К1	З1	Ч4	Д2	14
Бухгалтер РС_15	ПВ3	М3	К1	З1	Ч4	Д2	14

Продовження таблиці 2.12

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума
Бухгалтер РС_16	ПВЗ	МЗ	К1	З1	Ч4	Д2	14
Бухгалтер РС_17	ПВЗ	МЗ	К1	З1	Ч4	Д2	14
Менеджер колл-центру РС_18	ПВЗ	МЗ	К2	З1	Ч4	Д2	14
Оператор РС_19	ПВЗ	МЗ	К1	З1	Ч4	Д2	14
Оператор РС_20	ПВЗ	МЗ	К1	З1	Ч4	Д2	14
Оператор РС_21	ПВЗ	МЗ	К1	З1	Ч4	Д2	14

Продовження таблиці 2.12

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума
Головний менеджер збуту РС_24	ПВ3	М3	К2	З1	Ч4	Д2	15
Менеджер збуту РС_25	ПВ3	М3	К1	З1	Ч4	Д2	14
Менеджер збуту РС_26	ПВ3	М3	К1	З1	Ч4	Д2	14
Менеджер збуту РС_27	ПВ3	М3	К1	З1	Ч4	Д2	14
Внутрішня охорона	ПВ1	М3	К1	З3	Ч1	Д4	13
Прибиральниця	ПВ1	М3	К1	З1	Ч1	Д1	8

Таблиця 2.13 Модель порушника зовнішнього

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума
Технічний персонал	ПЗ2	М3	К1	З1	Ч1	Д1	9
Комунальний персонал бізнес центрц	ПЗ2	М3	К1	З1	Ч1	Д1	9
Наймані ремонті послуги	ПЗ2	М3	К1	З1	Ч1	Д1	9
Хакери	ПЗ3	М3	К3	З4	Ч4	Д4	21
Клієнти компанії	ПЗ1	М3	К1	З1	Ч1	Д1	8
Агенти конкурентів	ПЗ4	М3	К2	З3	Ч4	Д3	19
Прибиральники бізнес центру	ПЗ2	М3	К1	З1	Ч1	Д1	9
Відвідувачі	ПЗ1	М3	К1	З1	Ч1	Д1	8

Таблиця 2.14 Модель загроз

Загроза	Ймовірність	Рівень шкоди	К	Ц	Д
Збоїв роботи програмних та апаратних засобів	Середня	Високий	-	-	+
Випадкове делегування тому	Низька	Середній	+	-	-
Випадкове або навмисне делегування користувачеві привілеїв іншого користувача	Середня	Середній	+	+	+
Неправомірна зміна даних	Висока	Високий	-	+	-
Умисні дії персоналу направлені на вихід з ладу обладнання	Середня	Середній	-	-	+
Помилки програмного забезпечення	Низьке	Високий	+	+	+
Помилки персоналу	Висока	Середній	+	+	+

Продовження таблиці 2.14

Неправомірний доступ до інформації	Низька	Низький	+	-	-
Розробка та поширення вірусних програм	Низька	Низький	+	+	+
Розробка спеціального програмного забезпечення, використовуваного для здійснення неправомірного доступу	Низька	Високий	+	+	+
Піратське програмне забезпечення	Висока	Середній	+	+	+
Старе програмне забезпечення	Висока	Низький	+	+	+
Стихійні лиха	Висока	Високий	+	+	+

Висновок: З таблиці «модель порушника» видно, що найбільшу загрозу, що має відношення до проблеми захисту інформації, становить адмністратор компанії.

2.2.3 Опис основних загроз

Випадкове або навмисне делегування користувачеві привілеїв іншого користувача, може бути реалізовано через те, що співробітники, для підтримання темпу працездатності, передають привілеї для ускорення праці. Наприклад, системний адміністратор надає права користувачам для того, аби вони використовували інструменти для роботи не витрачаючи часу адміністратора.

Загроза призводить до поширення повноважень користувача і може привести до порушення КЦД інформації.

Піратське програмне забезпечення. Компанія не використовує ліцензійне програмне забезпечення для економії ресурсів. Використання неліцензійного ПЗ не гарантує цілісності продукту та може модифікувати інформацію, обробляємою в ІТС.

Старе програмне забезпечення. У компанії не має чіткого плану щодо оновлення ПЗ, адміністратор компанії оновлює ПЗ на свій розсуд. Не своєчасне оновлення може привести до порушення нормальної роботи з інформацією.

Помилки персоналу. Персонал компанії часто здійснюють помилки при роботі з ІТС та ресурсами. Наприклад : завчасне вимикання живлення ПК, помилки при праці в Інтернеті, завчасне відключення зовнішніх носіїв з ПК, надання доступу іншим співробітникам.

2.3 Розробка політики безпеки інформації

Політика безпеки інформації ТОВ «PegasGroup» створена з урахуванням всіх вимог чинного законодавства України, а також з виконанням рекомендацій, наведених у міжнародному стандарті ISO 27001.

Метою розробки політики безпеки є впровадження та ефективне управління інформаційною безпекою організації, яка спрямована на зниженні

ризиків інформаційної безпеки, забезпеченні неперервної роботи установи, дотриманні правил збереження інформаційних активів задля позитивних інформаційних відносин з партнерами і клієнтами, а найголовніше – захист інформаційних активів від зовнішніх та внутрішніх загроз.

У дипломній роботі розробка політики безпеки інформації в інформаційно-телекомунікаційній системі ТОВ «PegasGroup» виконується з урахуванням існуючої політики безпеки, яка містить в собі: політику управління інформаційною

безпекою, політику управління інцидентами інформаційної безпеки, політику безпеки інформації з обмеженим доступом.

2.3.1 Політика захисту персональних даних:

Прийнято та надано чинності: червень 2019 р. Відповідальний – системний адміністратор.

Власник документа – генеральний директор організації.

1 Опис. Політика захисту персональних даних складена відповідно до вимог Закону України «Про захист персональних даних» і визначає порядок оброблювання та заходи забезпечення безпеки персональних даних ТОВ «PegasGroup» (далі – Організація).

2 Призначення. Ця політика використовується у випадках, коли Організація оброблює персональні дані своїх Клієнтів, їх співробітників, тощо. В такому разі організація несе відповідальність за збереження захисту оброблювальних персональних даних.

3 Область застосування. Вимоги політики захисту персональних даних стосуються всіх працівників Організації, що працюють з персональними даними Клієнтів.

4 Політика.

4.1 Організація гарантує збереження конфіденційності, цілісності отриманих відомостей, що несуть персональні дані, а також унеможливлює несанкціонований доступ до них неуповноваженими особами.

4.2 Працівники Організації починають роботу з відомостям, що несуть персональні дані тільки у разі згоди Клієнта, які зазначені у відповідних документах.

4.3 Працівники Організації вносять до Бази даних тільки прізвище, ім’я, по-батькові, контактний телефон Клієнта і перелік виконаних робіт попередньо

шифруючи ці дані власним 6-значним паролем в базі даних. Пароль повинен містити латинські літери і цифри.

4.4 При передачі відомостей, що містять персональні дані (з використанням Wi-Fi каналу) працівник Організації повинен використовувати електронно-цифровий підпис (ЕЦП). Отримувач цих відомостей повинен використати спеціальний ключ ЕЦП, який надає доступ до них.

4.5 Отримуючи паперовий носій, що містить персональні дані, працівник Організації повинен залишити примітку в «Журналі обліку носіїв», в якому вказати своє ПІП, назву паперового носія, номер, дату отримання і поставити підпис.

4.6 Повертаючи паперовий носій, що містить персональні дані, працівник Організації повинен залишити примітку в «Журналі обліку носіїв», в якому вказати дату повернення і поставити підпис.

4.7 Відповідальність за цілісність і нерозголошення персональних даних паперового носія несе працівник Організації, який отримав цей носій. У разі порушення вимог ЗУ «Про захист персональних даних» на працівника Організації накладається відповідальність, встановлена законом (ст. 28 Закону України «Про захист персональних даних»).

4.8 Працівник Організації може видалити персональні дані Клієнта з інформаційних ресурсів у разі відкликання згоди останнього на обробку його даних.

5 Політика відповідальності.

Керівництво Організації повинне ознайомити своїх працівників з цією Політикою і оголосити відповідальність у разі невиконання вимог.

2.3.2 Політика безпеки обліку та зберігання носіїв інформації:

Прийнято та надано чинності: червень 2019 р. Відповідальний – системний адміністратор.

Власник документа – генеральний директор організації.

1 Опис. Політика безпеки обліку та зберігання носіїв інформації складена відповідно до вимог Постанови №736 Кабінету Міністрів України від 19.10.2016 «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію» і визначає порядок ведення обліку і зберігання носіїв інформації ТОВ «PegasGroup» (далі – Організація).

2 Призначення. Ця політика безпеки призначена для ведення контролю за носіями інформації: встановленні причасних у знищенні, модифікуванні та/або передачі службової інформації, визначенні місця збереження носіїв інформації.

3 Область застосування. Вимоги політики безпеки обліку та зберігання носіїв інформації стосуються всіх працівників Організації, що працюють з персональними даними Клієнтів.

4 Політика.

4.1 Працівник Організації, на початку своєї роботи з паперовим або електронним носієм інформації, повинен залишити примітку в «Журналі обліку носіїв», в якому вказати своє ПІП, назву паперового носія (або інвентарний номер електронного носія), номер, дату отримання і поставити підпис. Зробивши ці дії, відповідальна особа – фінансовий директор, видає працівнику вказаний носій інформації.

4.2 Працівник Організації, наприкінці своєї роботи з паперовим та/або електронним носієм інформації, повинен залишити примітку в «Журналі обліку носіїв», в якому вказати дату повернення і поставити підпис. Зробивши ці дії, відповідальна особа – фінансовий директор, приймає у працівника вказаний носій інформації і перевіряє його. У разі виявлення недостачі паперів та/або пошкодження носіїв, відповідальна особа повідомляє про це керівництво організації.

4.3 Працівник Організації, отримавши носій інформації, несе відповідальність за збереження цілісності і доступності носія. У разі, якщо працівник залишає своє робоче місце, він повинен повернути носій інформації

відповідальній особі і залишити відмітку в «Журналі обліку носіїв».

4.4 Працівник Організації повинен отримати та повернути носій інформації відповідальній особі з 10 години дня до 18 години вечора.

4.5 Відповідальна особа в проміжку з 18 години до 18 години 30 хвилини повинна провести облік носіїв інформації. У разі виникнення проблем повідомити про них керівництво організації.

4.6 Відповідальна особа за зберігання носіїв інформації повинна зберігати носії інформації в спеціальному сейфі, який обладнаний кодовим та механічним замком. Другий ключ від замка зберігається у керівництва Організації.

4.7 Друкування і розмноження документів, що становлять службову інформацію відбуваються згідно п.42 Постанови №736 Кабінету Міністрів України.

4.8 Працівники Організації повинні обробляти, зберігати, модифікувати та передавати інформацію з обмеженим доступом тільки з використанням ліцензованого ПЗ.

4.9 Працівники Організації повинні блокувати можливість ознайомлення з носіями, на яких міститься ІзОД, сторонніми особами.

4.10 Працівники Організації, винні у порушенні порядку ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, їх втраті або розголошенні службової інформації, що в них міститься, притягуються до дисциплінарної або іншої відповідальності, передбаченої законом.

5 Політика відповідальності.

Відповідальна особа за зберігання носіїв інформації ознайомлює працівників Організації з вимогами цієї Політики під розпис.

2.3.3 Політика забезпечення антивірусного захисту інформації:

Прийнято та надано чинності: червень 2019 р.

Відповідальний – системний адміністратор.

Власник документа – генеральний директор організації.

1 Опис. Політика забезпечення антивірусного захисту інформації ТОВ

«PegasGroup» (далі – Організація) визначає вимоги захисту інформаційних ресурсів антивірусним ПЗ від втручання шкідливих програм, що можуть призвести до призупинення роботи АС.

2 Призначення. Метою цієї політики є запобігання діяльності шкідливих програм і забезпечення антивірусного захисту інформаційних ресурсів

3 Область застосування. Вимоги політики забезпечення антивірусного захисту інформації стосуються всіх працівників, які працюють з інформаційними ресурсами Організації.

4 Політика.

4.1 Системний адміністратор повинен встановити і налаштувати антивірусне ПЗ на АРМ працівника Організації, а також встановити ПЗ для дистанційного контролю за КС цього працівника.

4.2 Системний адміністратор, налаштовуючи антивірусне ПЗ, повинен вказати наступні параметри:

– цілодобовий захист від вірусів та загроз: увімкнений;

– цілодобовий захист в Інтернеті: увімкнений

– часткове сканування файлів: щосереди та щоп’ятниці о 18 годині;

– повне сканування файлів: 1 понеділок на 2 тижні о 9.30;

– заборонити відімкнення та зміну параметрів антивірусного ПЗ.

4.3 Системний адміністратор повинен своєчасно встановлювати оновлення антивірусного ПЗ на АРМ працівників організації. Встановлення оновлень повинно відбуватись кожного дня з 9.30 до 10 години ранку.

4.4 Працівник Організації, отримавши і завантаживши файл з

корпоративної пошти, повинен перевірити цей файл на наявність вірусів, використовуючи антивірусне ПЗ.

4.5 Працівники Організації, оброблюючи інформацію з електронного носія, повинні проводити перевірку файлів на наявність вірусів.

4.6 Системний адміністратор, отримавши повідомлення в своїй КС про наявність вірусів на комп’ютері працівників Організації, повинен негайно ліквідувати загрозу, провести аналіз її виникнення і встановити відповідальних за скоєння цієї загрози\.

4.7 Системний адміністратор повинен встановлювати тільки ліцензоване програмне забезпечення на АРМ всіх працівників Організації.

5 Політика відповідальності.

Системний адміністратор повинен ознайомити працівників Організації з вимогами цієї політики і доповісти про відповідальність за недотримання цих вимог.

2.4 Висновок

У спеціальній частині було проведено обстеження фізичного, обчислювального, інформаційного середовища і середовища користувачів, аналіз інформаційних ризиків, за результатами яких було сформовано перелік інформаційних ресурсів, що становлять цінність організації.

3. ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Обґрунтування витрат на розробку політики безпеки інформації

Метою обґрунтування витрат на розробку політики безпеки інформації є розрахунок капітальних та експлуатаційних витрат, оцінка величини можливого збитку від атаки, визначення та аналіз показників економічної ефективності.

3.2 Розрахунки витрат на розробку політики безпеки інформації

При розробці та експлуатації політики безпеки інформації необхідно розрахувати витрати ТОВ «PegasGroup» (більш детально з діяльністю організації можна ознайомитись в розділі 2.1).

3.2.1 Розрахунок капітальних (фіксованих) витрат Капітальні (фіксовані) витрати на розробку та впровадження політики безпеки інформації складають:

$$К = К_{пр} + К_{аз} + К_{зпз} + К_{н} \quad (3.1)$$

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

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

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

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

Вихідні дані ТОВ «PegasGroup» становлять:

$К_{пр}$ = 10000 грн (вартість розроблення політики безпеки інформації та залучення до цього зовнішніх консультантів);

$К_{аз}$ = 13500 грн (вартість нового сейфу);

$$К_{зпз} = 61579 \begin{cases} 32029 \text{ грн. за ліцензоване антивірусне ПЗ } Eset\ NOD32 \\ 28450 \text{ грн. за ліцензоване ПЗ } Office\ 365 \\ 1100 \text{ грн. ЕЦП} \end{cases}$$

$К_{н} = 250$ грн (витрати на встановлення обладнання та налагодження системи інформаційної безпеки).

Визначимо капітальні витрати:

$$К = 10000 + 13500 + 250 + 61579 = 85329 \text{ грн.}$$

3.2.2 Розрахунок річних поточних (експлуатаційних) витрат

Річні поточні витрати складаються з:

$$С = С_а + С_{ел} + С_о + С_{тос} \quad (3.2)$$

де $С_а$ – річний фонд амортизаційних відрахувань;

$С_{ел}$ – вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$$С_{ел} = Р * F_р * Ц_е \quad (3.3)$$

де Р – встановлена потужність апаратури інформаційної безпеки, кВт;

$F_р$ – річний фонд робочого часу системи інформаційної безпеки; Це – тариф на електроенергію, грн/кВт·годин;

$C_о$ – витрати на залучення сторонніх організацій для виконання деяких видів обслуговування, навчання та сертифікацію обслуговуючого персоналу;

$C_{тос}$ – витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки.

Річний фонд амортизаційних відрахувань ($C_а$) складає 25% від капітальних витрат:

$$C_а = 54729 * 0.25 = 13682.25 \text{ грн.}$$

Потужність (Р) комп'ютерів та ноутбуків становить 1,12 кВт. За 40-годинного робочого тижня річний фонд робочого часу системи інформаційної безпеки ($F_р$) становить 1920.

Тариф на електроенергію ($Ц_е$) складає 1,68 грн/кВт·годин. Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($C_{ел}$) становить:

$$C_{ел} = 1.12 *1920 *1.68 = 3612.67 \text{ грн}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки ($C_о$) складають 6000 грн.

$$C_о = 6000 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки ($С_{тос}$) визначаються ТОВ «PegasGroup» і складають 2% від вартості капітальних витрат.

$$С_{тос} = 54729 * 0.02 = 1094.58 \text{ грн}$$

Визначаемо річні поточні витрати:

$$С = 13682.25 + 3612.67 + 6000 + 1094.58 = 24389.5 \text{грн}$$

3.3 Оцінка величини можливого збитку від атаки

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = П_п + П_в + V \qquad (3.4)$$

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

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

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

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

$$П_п = \frac{\Sigma з_с * ч_с}{F} * t_п \quad (3.5)$$

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

$З_с$ – місячна заробітна плата співробітника атакованого вузла або сегмента корпоративної мережі з нарахуванням єдиного соціального внеску, грн на місяць;

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

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин. Розрахунок витрат на заробітну плату співробітників за місяць з нарахуванням ЄСВ наведено в таблиці 3.1

Таблиця 3.1 – Витрати на заробітну плату співробітників за місяць з нарахуванням ЄСВ

Посада	Кількість спіробітників, осіб	Місячна заробітна плата, грн	Витрати на заробітну плату, грн	Єдиний соціальний внесок, грн	Витрати на заробістну плату з урахуванням ЄСВ, грн
Начальник відділу логістики	1	15000	15000	3300	18300
Логіст	8	8000	64000	14080	78080
Адміністратор	1	20000	20000	4400	24400

Продовження таблиці 3.1

Посада	Кількість співробітників, осіб	Місячна заробітна плата, грн	Витрати на заробітну плату, грн	Єдиний соціальний внесок, грн	Витрати на заробістну плату з урахуванням ЄСВ, грн
Головний бухгалтер	1	18000	18000	3960	21960
Бухгалтер	5	12000	60000	13200	73200
Менеджер колл-центру	1	10000	10000	2200	12200
Оператор	5	8000	40000	8800	48800
Головний менеджер збуту	1	12000	12000	2640	14640
Менеджер збуту	3	8000	24000	5280	29280
Всього					320860

Визначимо оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі:

$$П_п = (320860 / 176) * 3 = 5469.2 \text{ гр}$$

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

$$П_в = П_{ви} + П_{пв} + П_{зч} \quad (3.6)$$

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

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;
$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

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

$$П_{ви} = \frac{\Sigma З_с * Ч_с}{F} * t_{ви} \quad (3.7)$$

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

$$П_{ви} = (320860 / 176) * 4 = 7292.27 \text{ грн.}$$

Витрати на відновлення вузла або сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати системного адміністратора:

$$П_{пв} = \frac{\Sigma З_О * Ч_О}{F} * t_в \quad (3.8)$$

де $З_о$ – місячна заробітна плата системного адміністратора з нарахуванням єдиного соціального внеску, грн на місяць;

$Ч_о$ – чисельність обслуговуючого персоналу, осіб;

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

$$П_{пв} = (24400 / 176) * 2 = 277.27 \text{ грн.}$$

Визначимо вартість відновлення працездатності вузла або сегмента корпоративної мережі:

$$П_в = 7292.27 + 277.27 + 0 = 7569.54 \text{ грн.}$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із середньогодинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі:

$$V = \frac{O}{F_г} * (t_п + t_в + t_{ви}) \qquad (3.9)$$

де О – обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн у рік;

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

V = 10000000 / 2080 * (3 + 4 + 2) = 43269.23 грн.

Визначимо упущену вигоду від простою атакованого вузла або сегмента корпоративної мережі:

U = 7569.54 + 7592.27 + 43269.23 = 58431.04 грн

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

$$B = \sum \sum U * N * I \qquad (3.10)$$

де N – середнє число можливих атак на рік; I – число атакованих вузлів або сегментів корпоративної мережі.

B = 58431.04 * 1 * 3 = 233724.16 грн.

3.4 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = (B * R) – C \qquad (3.11)$$

де B – загальний збиток від атаки на вузол або сегмент корпоративної мережі організації;

R – очікувана ймовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

C – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

E = (233724.16 * 0.5) – 24389.5= 92472.58 грн.

3.5 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Оцінка економічної ефективності системи захисту інформації, розглянутої у спеціальній частині дипломної роботи, здійснюється на основі визначення та аналізу наступних показників:

а) коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI (Return On Investment for Security);

б) термін окупності капітальних інвестицій T_O.

Коефіцієнт повернення інвестицій показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки. Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі, а отже:

$$\text{ROSI} = \frac{E}{K} \tag{3.12}$$

де ROSI – коефіцієнт повернення інвестицій;

Е – загальний ефект від впровадження системи інформаційної безпеки, тис. грн;

К – капітальні інвестиції, що забезпечили цей ефект, тис. грн

$$\text{ROSI} = 92472.58 / 85329 = 1.08$$

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

$$\text{To} = \frac{K}{E} = \frac{1}{ROSI} \tag{3.13}$$

де То – термін окупності капітальних інвестицій.

То = 85329 / 92472.58 = 0.92, що становить 11 місяців 5 днів.

3.6 Висновок

В економічному розділі була визначена економічна ефективність розробки та впровадження політики безпеки інформації в ТОВ «PegasGroup». Було розраховано капітальні та експлуатаційні витрати, які склали 85329 грн та 27125,02 грн відповідно. Оцінено величину можливого збитку від реалізованої атаки через упущену вигоду – 24389.5грн. Визначено термін окупності капітальних інвестицій. Він склав 11 місяців 5 днів. Таким чином можна вважати, що впровадження політики безпеки інформації на підприємство є економічно доцільним рішенням, яке ефективно захистить інформаційні активи від негативних зовнішніх та внутрішніх впливів.

ВИСНОВКИ

В перші частині дипломної роботи було визначено поняття інформаційної безпеки, сформовано складові схеми реалізації інформаційної безпеки підприємства, а також було охарактеризовано конкретні цілі, вимоги та задачі, що висуваються до політики безпеки. Проаналізовано нормативно-правову базу в сфері захисту інформації, а також визначено задачі, які необхідно вирішити в цій роботі.

В спеціальній частині було обґрунтовано необхідність розробки та впровадження політики безпеки інформації в ТОВ «PegasGroup». Крім цього, було виконано Обстеження середовищ функціонування ІТС, за результатами якого було визначено функціональний профіль захищеності КС, спираючись на який побудовано модель загроз та сформовано модель порушника.

Для мінімізації ймовірності реалізації проаналізованих та Оцінених ризиків була розроблена політика безпеки інформації ТОВ «PegasGroup», яка складається з документів «політика захисту персональних даних», «політика забезпечення антивірусного захисту інформації» та «політика безпеки Обліку та зберігання носіїв інформації». Була повторно проведена Оцінка інформаційних ризиків, яка показала ефективність після впровадження політики безпеки інформації, а також наведено порівняльний графік доцільності розробки ПБІ.

В економічній частині було обґрунтовано доцільність витрат на розробку ПБІ, а також проведені розрахунки капітальних та експлуатаційних витрат, оцінено величину можливого збитку від атаки, визначено ефект від впровадження політики безпеки інформації, а також проаналізована та визначена економічна ефективність системи захисту інформації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 09.01.2007 № 537-V // Відомості Верховної Ради України. – 2007. – № 12. [Електронний ресурс]. – Режим доступу https://zakon.rada.gov.ua/laws/show/537-16

2. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу – [Чинний від 1999.04.28]. – К. : ДСТСЗІ СБУ, 1999. – № 22. – (Нормативний документ системи технічного захисту інформації).

3. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі – [Чинний від 2005.08.11]. – К. : ДСТСЗІ СБУ, 2005. – № 125. – (Нормативний документ системи технічного захисту інформації).

4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР // Відомості Верховної Ради України. – 1994. – № 31. [Електронний ресурс]. – Режим доступу https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

5. Вінницький апеляційний адміністративний суд. Захист інформаційних систем [Електронний ресурс]. - Режим доступу http://www.vaas.gov.ua/news/zaxist-informacijnix-sistem-vazhlive-zavdannya- sogodennya/

6. ДССЗЗІ України. Порядок створення комплексних систем захисту інформації, проведення експертизи та видачі Експертних висновків і Атестатів відповідності [Електронний ресурс]. - Режим доступу http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=3 9479&cat_id=38689&ctime=1127824089206

7. Закон України «Про інформацію» від 02.10.1992 №2657-XII //

Відомості Верховної Ради України. – 1992. – № 48. [Електронний ресурс]. – Режим доступу https://zakon.rada.gov.ua/laws/show/2657-12

8. Закон України «Про захист персональних даних» від 01.06.2010 №2297-VI // Відомості Верховної Ради України. – 2010. – № 34. [Електронний ресурс]. – Режим доступу https://zakon.rada.gov.ua/laws/show/2297-17

9. Закон України «Про основні засади забезпечення кібербезпеки України» від 21.06.2018 № 2163-VIII // Відомості Верховної Ради України. – 2017. – № 45. [Електронний ресурс]. – Режим доступу http://zakon5.rada.gov.ua/laws/show/2163-19

10. Указ Президента України «Про Положення про порядок здійснення криптографічного захисту інформації в Україні» від 22.05.1998 №505/98 // Відомості Верховної Ради України. – 1998. [Електронний ресурс]. – Режим доступу https://zakon.rada.gov.ua/laws/show/505/98

11. Указ Президента України «Про Положення про технічний захист інформації в Україні» від 27.09.1999 №1229/99 // Відомості Верховної Ради України. – 1999. [Електронний ресурс]. – Режим доступу https://zakon.rada.gov.ua/laws/show/1229/99

12. Постанова Кабінету Міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373 // Офіційний вісник України. – 2006. – № 13.

13. НД ТЗІ 2.5.004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. – [Чинний від 1999.04.28]. – К. : ДСТСЗІ СБУ, 1999. – № 22. – (Нормативний документ системи технічного захисту інформації).

14. НД ТЗІ 2.5.005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. – [Чинний від 1999.04.28]. – К. : ДСТСЗІ СБУ,

1999. – № 22. – (Нормативний документ системи технічного захисту інформації).

15. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. – [Чинний від 1999.04.28]. – К. : ДСТСЗІ СБУ, 1999. № 22. – (Нормативний документ системи технічного захисту інформації).

16. НД ТЗІ 1.6-005-2013 Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці.– [Чинний від 2013.04.15]. – К. : ДССЗЗІ, 2013. № 215. – (Нормативний документ системи технічного захисту інформації).

17. Приставка Ф., Павленко П., Казмирчук С., Коломієць М. «Дослід засобів оцінювання ризиків безпеки ресурсів інформаційних систем», [Електронний ресурс]. – Режим доступу http://er.nau.edu.ua/bitstream/NAU/37138/1/2017_%D0%98%D0%A1%D0%A1%D0%9B%D0%95%D0%94%D0%9E%D0%92%D0%90%D0%9D%D0%98%D0%95%20%D0%A1%D0%A0%D0%95%D0%94%D0%A1%D0%A2%D0%92%20%D0%9E%D0%A6%D0%95%D0%9D%D0%98%D0%92%D0%90%D0%9D%D0%98%D0%AF.pdf

18. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою // ISO/IEC 27001, який прийнято як ДСТУ ISO/IEC 27001:2015

19. Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека / Упорядн.: І.В. Шереметьєва, Д.П. Пілова, Н.М. Романюк. – Дніпро: Національний технічний університет "Дніпровська політехніка", 2017. – 17 с.

20. Методичні рекомендації до виконання кваліфікаційних робіт бакалаврів спеціальності 125 Кібербезпека/ Упорял.Ж О. В. Герасіна, Д. С. Тимофєєв, О. В. Кручінін, Ю. А. Мілінчук – Дніпро: НТУ «ДП», 2020. – 47 с.

21. Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки // ISO/IEC 27002, який прийнято як ДСТУ ISO/IEC 27002:2015

22. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки // ISO/IEC 27005, який прийнято як ДСТУ ISO/IEC 27005:2015

23. Захист інформації. Технічний захист інформації. Основні положення // ДСТУ 3396.0-96

24. Захист інформації. Технічний захист інформації. Порядок проведення робіт // ДСТУ 3396.1-96

25. Захист інформації. Технічний захист інформації. Терміни та визначення // ДСТУ 3396.2-97

26. Закон України «Про електронні документи та електронний документообіг» від 07.11.2018 №851-IV // Відомості Верховної Ради України. – 2003. – № 36. [Електронний ресурс]. – Режим доступу https://zakon.rada.gov.ua/laws/show/851-15

ДОДАТОК А. ВІДОМІСТЬ МАТЕРІАЛІВ ДИПЛОМНОЇ РОБОТИ

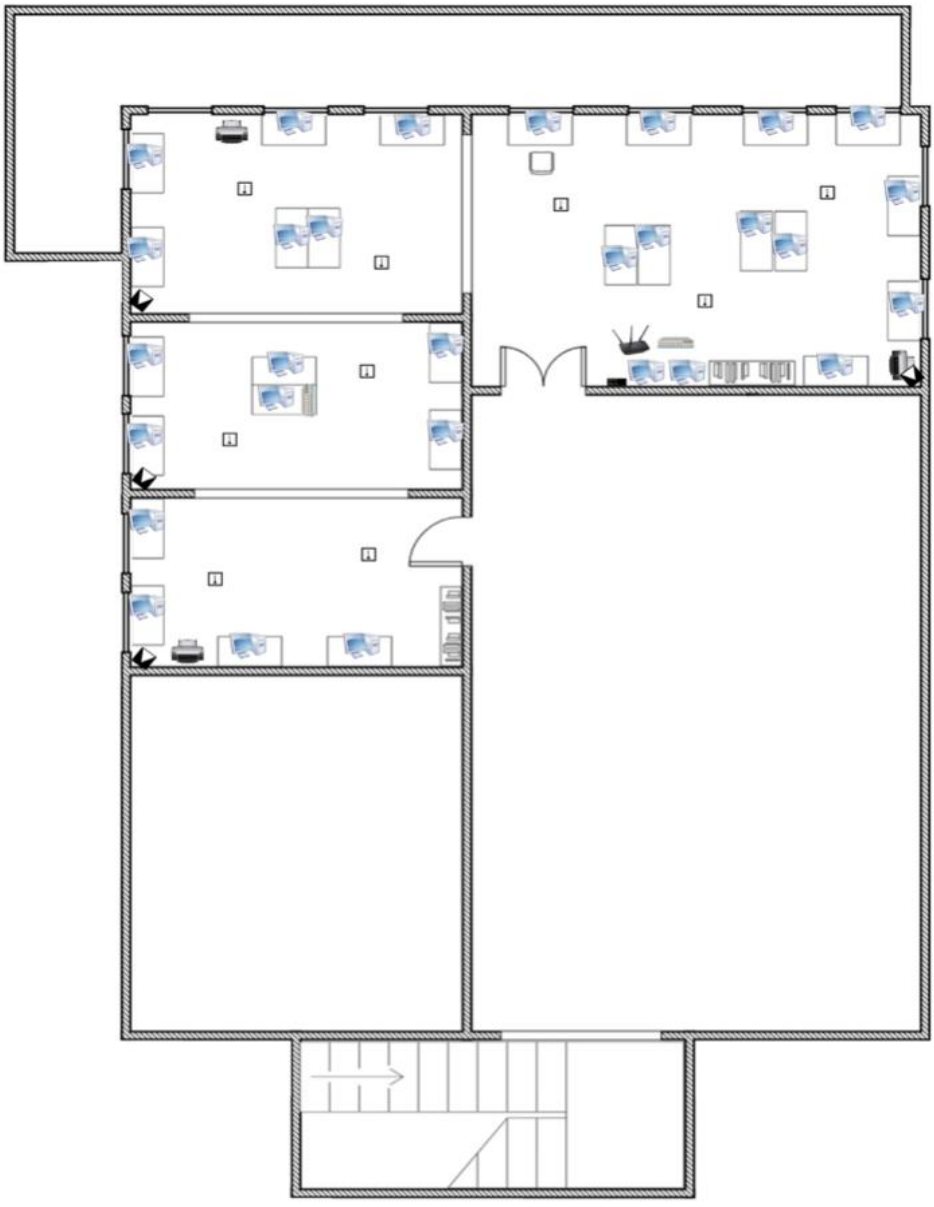
№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	1	
4	А4	Вступ	1	
5	А4	Стан питання. Постановка задачі	7	
6	А4	Спеціальна частина	43	
7	А4	Економічна частина	10	
8	А4	Висновки	1	
9	А4	Перелік посилань	4	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. СИТУАЦІЙНИЙ ПЛАН ТОВ «PEGASGROUP»

1. **Ситуаційний план**

ДОДАТОК В. ГЕНЕРАЛЬНИЙ ПЛАН ТОВ «PEGASGROUP»

2. **Генеральний план. Основні технічні та допоміжні технічні засоби.**



ДОДАТОК Г ПЕРЕЛІК ДОКУМЕНТІВ НА ОПТИЧНОМУ НОСІЇ

1. Пояснювальна записка Дугар Д.Є.docx
2. Пояснювальна записка Дугар Д.Є.pdf
3. Презентація Дугар Д.Є.pptx

ДОДАТОК Ґ. ВІДГУК КЕРІВНИКА ЕКОНОМІЧНОГО РОЗДІЛУ

Керівник розділу _____ _____

(підпис) (прізвище ініціали)