**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** *Черкаського Давида Олександровича*

**академічної групи** *125-18-3*

**спеціальності** *125 Кібербезпека*

**спеціалізації**[1]

**за освітньо-професійною програмою** *Кібербезпека*

**на тему** *Розробка політики безпеки інформації для інформаційно-комунікаційної системи приватного підприємства "Альфа Транс"*

| Керівники | Прізвище, ініціали | Оцінка за шкалою | | Підпис |
|---|---|---|---|---|
| | | рейтинговою | інституційною | |
| кваліфікаційної роботи | д.т.н., проф. Корнієнко В.І. | | | |
| розділів: | | | | |
| спеціальний | д.т.н., проф. Корнієнко В.І. | | | |
| економічний | к.е.н., доц. Романюк Н.М. | | | |
| **Рецензент** | | | | |
| **Нормоконтролер** | ст. викл. Мєшков В.І. | | | |

**Дніпро**
**2022**

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

«_____»_____20___року

# ЗАВДАННЯ
## на кваліфікаційну роботу
## ступеня бакалавра

**студенту** *Черкаському Давиду Олександровичу* **академічної групи** *125-18-3*
(прізвище ім'я по-батькові) (шифр)

**спеціальності** *125 Кібербезпека*
(код і назва спеціальності)

**на тему** ***Розробка політики безпеки інформації для інформаційно-комунікаційної системи приватного підприємства "Альфа Транс"***

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

| Розділ | Зміст | Термін виконання |
|---|---|---|
| Розділ 1 | Виконати розгляд ситуації в галузі інформаційної безпеки, обґрунтувати важливість та актуальність розробки політики безпеки інформації на підприємстві. Виконати аналіз нормативно-правової бази у сфері захисту інформації. Виділити основні закони, нормативні документи та державні стандарти, що мають бути застосовані в процесі створення політики безпеки інформації на підприємстві. | 29.03.2022 |
| Розділ 2 | Привести загальні характеристики підприємства, розробити модель загроз, провести аналіз та оцінку ризиків інформаційної безпеки, розробити основні положення політики безпеки інформації. | 24.05.2022 |
| Розділ 3 | В економічному розділі виконати розрахунок капітальних та експлуатаційних витрат на впровадження політики безпеки інформації. | 14.06.2022 |

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

**Дата видачі: 08.01.2022р.**

**Дата подання до екзаменаційної комісії: 15.06.2022р.**

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

# РЕФЕРАТ

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

Об'єкт досліджень: інформаційно-телекомунікаційна система приватного підприємства «Альфа Транс».

Предмет розробки: політика безпеки інформації в інформаційно-телекомунікаційній системі приватного підприємства «Альфа Транс».

Мета: розробка та впровадження політики безпеки інформації в інформаційно-телекомунікаційній системі приватного підприємства «Альфа Транс».

В першому розділі проведено розгляд ситуації в галузі інформаційної безпеки, обґрунтовано важливість та актуальність розробки політики безпеки інформації на підприємстві. Виконано аналіз нормативно-правової бази у сфері захисту інформації. Виділені основні закони, нормативні документи та державні стандарти, що мають бути застосовані в процесі створення політики безпеки інформації на підприємстві.

В спеціальній частині приведено загальна характеристика підприємства, розроблено модель загроз, проведено аналіз та оцінка ризиків інформаційної безпеки, розроблено основні положення політики безпеки інформації.

В економічному розділі виконано розрахунок капітальних та експлуатаційних витрат на впровадження політики безпеки інформації.

Практичне значення роботи полягає у розробці та впровадженні політики безпеки інформації інформаційно-телекомунікаційної системи.

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

# ABSTRACT

Explanatory note: ___ pp., ___ pic., ___ table, ___ app, ___ sources.

Object of research: information and telecommunication system of the private enterprise "Alfa Trans".

Subject of development: information security policy in the information and telecommunication system of the private enterprise "Alfa Trans".

Purpose: development and implementation of information security policy in the information and telecommunication system of the private enterprise "Alfa Trans".

The first section examines the situation in the field of information security, substantiates the importance and relevance of information security policy development at the enterprise. The analysis of the legal framework in the field of information protection is performed. The basic laws, normative documents and state standards that should be applied in the process of creating information security policy at the enterprise are highlighted.

In the special part the general characteristic of the enterprise is resulted, the model of threats is developed, the analysis and an estimation of risks of information security is carried out, the basic provisions of a policy of information security are developed.

In the economic section, the calculation of capital and operating costs for the implementation of information security policy is performed.

The practical significance of the work lies in the development and implementation of information security policy of the information and telecommunication system.

INFORMATION SECURITY, REGULATORY AND LEGAL SECURITY, INFORMATION AND TELECOMMUNICATIONS SYSTEM, VULNERABILITIES, THREATS, THREATS AND THREATS

# СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ВПА – відділ планування автотранспорту

ІД – інформаційна діяльність;

ІзОД – інформація з обмеженим доступом;

ІКС – інформаційно-комунікаційні системи;

КЗ – контрольована зона;

КЗЗ – комплекс засобів захисту;

КСЗІ – комплексна система захисту інформації;

ОІД – об’єкт інформаційної діяльності;

ПЗ – програмне забезпечення;

СЗІ – служба захисту інформації;

ТЗ – технічне завдання;

ТЗІ – технічний захист інформації.

ЗМІСТ

# ВСТУП

Сучасний етап розвитку суспільства характеризується зростаючою роллю інформаційної сфери, що представляє собою сукупність інформації, інформаційної інфраструктури, суб'єктів, що здійснюють формування, поширення й використання інформації, а також; системи регулювання суспільних відносин, що виникають при цьому. На сьогодні інформаційна сфера є системоутворюючим чинником життя суспільства, активно впливає на стан політичної, економічної, оборонної й інших складових безпеки держави. Сучасні інформаційні технології надають нові можливості з обробки, передачі та зберігання інформації та підвищують рівень доступності інформаційних ресурсів для користувача. Однак нові технології інформації можуть бути не тільки корисними, але й небезпечними для інформаційних систем та мереж.

На даний час приватна й ділова інформація має комерційну вартість і тому важливою є проблема її захисту від несанкціонованого доступу та атак. Нині спостерігається тенденція до підвищення кількості атак та несанкціонованого доступу, які захоплюють контроль над віддаленою інформаційною системою, копіюють та передають зловмисникам персональні дані, іншу конфіденційну або, навіть, секретну інформацію. Проблема комплексного захисту інформації сучасних інформаційно-комунікаційних систем (ІКС) стає ще актуальнішою, якщо мова йде про захист великої кількості оперативної інформації, що обробляється в сучасних комп'ютерних системах.

Саме тому у роботі розглядається питання збереження інформаційних ресурсів на приватному підприємстві «Альфа Транс», як складова КСЗІ.

# РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

## 1.1 Стан питання

На даний час все більшого значення набуває забезпечення інформаційної безпеки підприємства. Це пов'язано із зростаючим обсягом інформації, вдосконаленням засобів її зберігання, передачі та обробки. Наявність значної частини інформації в електронній формі, використання локальних і глобальних мереж створюють якісно нові загрози конфіденційної інформації.

Під інформаційною безпекою розуміється захищеність інформації та підтримуючої її інфраструктури від будь-яких випадкових або зловмисних дій, результатом яких може бути нанесення збитку самій інформації, її власникам або підтримуючій інфраструктурі [1].

На виконання вимог законодавства України з питань захисту інформації [2, 3] в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах державних органів, комерційних установ та організацій України на даний час активно створюються комплексні системи захисту інформації (КСЗІ). Ці системи являють собою сукупність організаційних заходів та технічних засобів, спрямованих на забезпечення захисту інформації з обмеженим доступом, яка обробляється, зберігається та передається в автоматизованих системах, від загроз несанкціонованого доступу до неї [3, 4].

Комплексна система захисту інформації включає заходи та засоби, що реалізують способи, методи, механізми захисту інформації від:

– витоку інформації технічними каналами (побічні електромагнітні випромінювання, акустоелектричних канали і т.д.);

– несанкціонованих дій та несанкціонованого доступу до інформації (підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, застосування закладних пристроїв чи програм і т.д.);

– спеціального впливу на інформацію (формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту).

Для кожної конкретної інформаційно-комунікаційної системи склад, структура та вимоги до системи захисту визначаються властивостями оброблюваної інформації, класом автоматизованої системи та умовами її експлуатації. Кінцевою метою всіх заходів щодо захисту інформації, які реалізуються, є забезпечення безпеки інформації під час її оброблення в ІКС. Захист інформації має бути забезпечений на всіх стадіях життєвого циклу ІКСМ, на всіх технологічних етапах оброблення інформації і в усіх режимах функціонування.

Можна виділити цілу низку джерел загроз інформаційній безпеці сучасного підприємства:

– протизаконна діяльність деяких економічних структур у сфері формування, поширення і використання інформації;

– порушення встановлених регламентів збору, обробки та передачі інформації;

– навмисні дії та ненавмисні помилки персоналу інформаційних систем;

– помилки в проєктуванні інформаційних систем;

– відмова технічних засобів і збої програмного забезпечення ІКС тощо.

Також необхідно враховувати, що загроза інформаційним системам підприємства може настати з боку наступних суб'єктів:

– працівники підприємства, що використовують своє службове становище (коли законні права за посадою використовуються для незаконних операцій з інформацією);

– працівники підприємства, що не мають права в силу своїх службових обов'язків, але здійснили несанкціонований доступ до конфіденційної інформації;

– особи, які не пов'язані з підприємством трудовою угодою (контрактом).

Всі методи забезпечення інформаційної безпеки підприємства можна об'єднати у три групи: правові, організаційні та програмно-технічні [1].

Правові методи включають сукупність нормативно-правових актів, які регулюють відносини, пов'язані з використанням інформації в діяльності підприємства. З розвитком правового регулювання процесів інформаційного обміну набагато простіше встановлювати партнерські стосунки, шукати контрагентів, реалізовувати і закуповувати продукцію. Захист інформації є невід'ємною складовою бізнесу.

Програмно-технічні методи реалізуються за допомогою засобів програмного та апаратного забезпечення. Технічні методи захисту припускають використання засобів програмно-технічного характеру, спрямованих, передусім, на обмеження доступу користувача, який працює з інформаційними системами підприємства, до тієї інформації, звертатися до якої він не має права.

Організаційні методи полягають в забезпеченні збереження конфіденційної інформації підприємства шляхом формування корпоративної системи захисту і пов'язані з обмеженням можливого несанкціонованого фізичного доступу до інформаційних систем.

Захист інформації, забезпечення інформаційної безпеки повинно носити системний характер, тобто різні засоби захисту (апаратні, програмні, фізичні, організаційні) повинні застосовуватися одночасно і під єдиним управлінням.

Отже, пріоритетним напрямом у процесі забезпечення інформаційної безпеки підприємства є збереження в таємниці комерційно важливої інформації, що дозволяє успішно конкурувати на ринку виробництва та збуту товарів і послуг.

Сучасне підприємство повинно вміти належним чином будувати політику інформаційної безпеки, тобто розробляти і ефективно впроваджувати комплекс превентивних заходів по захисту конфіденційних

даних та інформаційних процесів. Така політика передбачає відповідні вимоги на адресу персоналу, менеджерів і технічних служб [5].

Важливим є визначення етапів побудови політики інформаційної безпеки, а саме:

– реєстрація всіх ресурсів, які мають бути захищені;

– аналіз та створення переліку можливих загроз для кожного ресурсу;

– оцінка ймовірності появи кожної загрози;

– вжиття заходів, які дозволяють економічно ефективно захистити інформаційну систему.

На практиці інформаційна безпека включає сукупність напрямів, методів, засобів і заходів, що знижують вразливість інформації і перешкоджають несанкціонованому доступу до інформації, її розголошенню або витоку.

Структура системи залежить від об'єму та цінності інформації, характеру можливих загроз безпеки інформації, необхідної надійності захисту і вартості системи. Більшість фахівців у галузі захисту інформації вважають, що інформаційна безпека підтримується на належному рівні, якщо всі інформаційні ресурси системи дотримуються відповідного рівня конфіденційності, цілісності (неможливості навмисної або випадкової її модифікації) і доступності.

Можна виділити такі підсистеми ефективного захисту інформації на підприємстві [1]:

1. Підсистема антивірусного захисту шлюзів входу в мережу Інтернет, файлових серверів, робочих місць користувачів, централізованого управління, періодичного оновлення антивірусних баз даних.

2. Підсистема управління контролем доступу та ідентифікацією в інформаційній системі.

3. Підсистема міжмережного екранування, яка дозволяє реалізувати безпеку міжмережної взаємодії через використання програмних і програмно-апаратних міжмережних екранів.

4. Підсистема криптографічного захисту, яка гарантує безпеку передачі інформації завдяки шифруванню даних.

5. Підсистема забезпечення цілісності інформації та програмного середовища шляхом застосування відповідних засобів для фіксації та контролю стану програмного комплексу, управління зберіганням даних для резервного копіювання та архівування.

6. Підсистема захисту від інсайдерів, яка контролює дії порушників, реалізує інформаційну безпеку при управлінні доступом і реєстрації.

7. Підсистема захисту систем управління базами даних.

8. Підсистема виявлення вторгнень і спроб несанкціонованого доступу до інформаційних ресурсів підприємства. Підсистема забезпечує реалізацію захисних заходів з протидії атакам хакерів і поширенню спаму.

9. Підсистема захисту мобільних пристроїв.

10. Підсистема моніторингу подій інформаційної безпеки, яка дозволяє своєчасно виявляти загрози інформаційній системі та оперативно реагувати на них.

## 1.2 Аналіз нормативно-правової бази у сфері захисту інформації

Для забезпечення захисту інформації існує ціла низка напрямів забезпечення інформаційної безпеки, які направлені на зниження ймовірності виникнення загрози та порушення базових властивостей інформації (конфіденційності, цілісності та доступності). Нормативно-правова база, як первинний етап при побудові комплексної системи захисту інформації сучасних ІКС є найважливішою складовою для забезпечення ефективного і надійного захисту інформації та інформаційних ресурсів [6].

Нормативно-правова база регламентує та визначає порядок захисту визначених політикою безпеки властивостей інформації під час створення та експлуатації інформаційної системи; регламентує порядок ефективного знешкодження і попередження загроз для ресурсів шляхом побудови

комплексної системи захисту інформації; статус інформаційної системи з точки зору інформаційної безпеки; права, обов'язки й відповідальність персоналу, роботи яких пов’язані з інформаційною безпекою; правові положення окремих видів процесу керування та управління доступом в захищених ІКС; порядок створення й використання захищених ІКС; етапи побудови КСЗІ [7].

В травні 2018 року набув чинності закон «Про основні засади забезпечення кібербезпеки України». В ньому були визначенні поняття «кібербезпека» та «критично важливі об’єкти інфраструктури» [8].

У відповідності до ст .4 постанови Кабінету Міністрів України від 29 березня 2006 р. № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» захисту підлягає інформація, вимога щодо захисту якої встановлена законом, у тому числі конфіденційна інформація про фізичну особу.

Персональні дані являються конфіденційною інформацією. У випадку їх обробки в інформаційній (автоматизованій) системі, необхідно керуватися вимогами ст. 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», що вимагає від власника системи побудови КСЗІ. Відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

Під час створення комплексної системи захисту інформації слід керуватися низкою нормативно-правових документів та актів. Базовими нормативними документами при організації та побудови комплексної системи захисту інформації в ІКСМ є: Закон України "Про інформацію"; Закон України "Про захист інформації в інформаційно-телекомунікаційних системах"; НД ТЗІ 1.1-002-99: Загальні положення з захисту інформації в комп’ютерних системах від НСД; НД ТЗІ 1.1-003-99: Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу; НД ТЗІ 1.4-001-2000: Типове положення про службу захисту інформації в

автоматизованій системі; НД ТЗІ 2.5-005-99: Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого; НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»; НД ТЗІ 3.7-001-99: Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі [6, 9 – 14].

Дослідження показали, що всі вище зазначені нормативні-документи визначають основи та положення організації захисту інформації на всіх етапах життєвого циклу ІКС. Основою побудови комплексної системи захисту інформації сучасних ІКС, згідно нормативних документів є надання нормативно-методологічної бази для вибору і реалізації вимог до захисту інформації та інформаційних ресурсів в ІКС. Порядок вибору вимог до захисту інформації в ІКС визначається згідно НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» [10, 11].

Основою для надійного та ефективного захисту являється вибір стандартного функціонального профілю захищеності. Під поняттям функціонального профілю захищеності розуміється перелік мінімально необхідних рівнів послуг та механізмів, які повинна реалізовувати система захисту ІКС.

Функціональний профіль захищеності повинен задовольняти певні вимоги щодо захищеності інформації, яка обробляється в захищеній ІКС. Стандартні функціональні профілі вибираються на основі існуючих вимог щодо захисту інформації та інформаційних ресурсів від певних загроз і відомих на сьогоднішній день функціональних послуг, що дозволяють протистояти даним загрозам і забезпечувати виконання вимог, які пред'являються.

Комплексні системи захисту інформації в інформаційних (автоматизованих) системах організацій повинні створюватися згідно до вимог, що викладені в НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» [7].

Встановлений цим документом порядок є обов'язковим для всіх суб'єктів системи ТЗІ в Україні незалежно від їхньої організаційно-правової форми та форми власності, АІС в яких обробляється інформація, яка є власністю держави, належить до державної чи іншої таємниці або окремих видів інформації, необхідність захисту якої визначено законодавством. Якщо в АІС обробляються інші види інформації, то вимоги цього нормативного документа суб'єкти системи ТЗІ можуть використовувати як рекомендації.

Порядок створення КСЗІ в АІС розглядається НД ТЗІ 3.7-003-05 як сукупність впорядкованих у часі, взаємопов'язаних, об'єднаних в окремі етапи робіт, виконання яких необхідне й достатнє для КСЗІ, що створюється.

Етапи робіт, які виконуються під час створення КСЗІ в конкретній АІС, їх зміст та результати, терміни виконання визначаються ТЗ на створення КСЗІ на підставі НД ТЗІ 3.7-003-05. Етапами робіт, які виконуються під час створення КСЗІ є наступні:

1. Формування загальних вимог до КСЗІ в ІТС.
    1.1 Обґрунтування необхідності створення КСЗІ.
    1.2. Обстеження середовищ функціонування ІТС.
    1.3 Формування завдання на створення КСЗІ.
2. Розробка політики безпеки інформації в ІТС.
    2.1 Вивчення об'єкта, на якому створюється КСЗІ, проведення науково-дослідних робіт.
    2.2 Вибір варіанту КСЗІ.
    2.3 Оформлення політики безпеки.
3. Розробка технічного завдання на створення КСЗІ.
4. Розробка проєкту КСЗІ.

4.2. Ескізний проєкт КСЗІ.

4.3. Технічний проєкт КСЗІ.

4.4. Робочий проєкт КСЗІ.

5. Введення КСЗІ в дію та оцінка захищеності інформації в ІТС.

5.1 Підготовка КСЗІ до введення в дію.

5.2 Навчання користувачів.

5.3 Комплектування КСЗІ.

5.4 Будівельно-монтажні роботи.

5.5 Пусконалагоджувальні роботи.

5.6 Попередні випробування.

5.7 Дослідна експлуатація.

5.8 Державна експертиза КСЗІ.

6. Супроводження КСЗІ.

На етапі «Формування загальних вимог до КСЗІ в ІТС» виконується обґрунтування необхідності створення КСЗІ. Підставою для визначення необхідності створення КСЗІ є норми та вимоги чинного законодавства, які встановлюють обов'язковість обмеження доступу до певних видів інформації або забезпечення її цілісності чи доступності, або прийняте власником інформації рішення щодо цього, якщо нормативно-правові акти надають йому право діяти на власний розсуд.

Вихідні дані для обґрунтування необхідності створення КСЗІ у загальному випадку одержуються за результатами:

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

– визначення наявності у складі інформації, яка підлягає автоматизованій обробці, таких її видів, що потребують обмеження доступу

до неї або забезпечення цілісності чи доступності відповідно до вимог нормативно-правових актів;

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

На підставі проведеного аналізу приймається рішення про необхідність створення КСЗІ.

Під час виконання робот по обстеженню середовищ функціонування ІТС, ІТС розглядається як організаційно-технічна система, яка поєднує обчислювальну систему, фізичне середовище, середовище користувачів, оброблювану інформацію і технологію її обробки.

Метою обстеження є підготовка засадничих даних для формування вимог до КСЗІ у вигляді опису кожного середовища функціонування ІТС та виявлення в ньому елементів, які безпосередньо чи опосередковано можуть впливати на безпеку інформації, виявлення взаємного впливу елементів різних середовищ, документування результатів обстеження для використання на наступних етапах робіт.

На етапі формування завдання на створення КСЗІ:

– визначаються завдання захисту інформації в ІТС, мета створення КСЗІ, варіант вирішення задач захисту (відповідно до ДСТУ 3396.1), основні напрями забезпечення захисту;

– здійснюється аналіз ризиків (вивчення моделі загроз і моделі порушника, можливих наслідків від реалізації потенційних загроз, величини можливих збитків та ін.) і визначається перелік суттєвих загроз;

Етап «Розробка політики безпеки інформації в ІТС» включає наступні роботи:

– вивчення об’єкта, на якому створюється КСЗІ, проведення науково-дослідних робіт. На цьому етапі розробник КСЗІ проводить детальне вивчення об’єкта, на якому створюється КСЗІ, уточнює моделі загроз, потенційного порушника та результати аналізу можливості керування ризиками, які виконані на попередніх етапах, а також виконує у разі

необхідності додаткові науково-дослідні роботи, пов'язані з пошуком шляхів реалізації завдання на створення КСЗІ, оформлює і затверджує звіти з НДР, що виконувалися.

– вибір варіанту КСЗІ. У загальному випадку за результатами робіт попереднього етапу готуються альтернативні варіанти концепції створення КСЗІ і планів їх реалізації, здійснюється оцінка переваг і недоліків кожного варіанту, вибір найбільш оптимального варіанту. Концепція оформлюється у вигляді звіту.

– оформлення політики безпеки.

При оформленні політики безпеки здійснюється:

– вибір основних рішень з протидії всім суттєвим загрозам, формування загальних вимог, правил, обмежень, рекомендацій і т.п., які регламентують використання захищених технологій обробки інформації в ІТС, окремих заходів і засобів захисту інформації, діяльність користувачів всіх категорій;

– документальне оформлення політики безпеки інформації.

Політика безпеки може розроблятись для ІТС в цілому або, якщо мають місце особливості функціонування окремих компонентів КСЗІ, для окремої компоненти, для окремої функціональної задачі, для окремої технології обробки інформації тощо. Політика безпеки розробляється згідно з положеннями НД ТЗІ 1.1- 002-99 та рекомендаціями НД ТЗІ 1.4-001-2000.

Методологія розроблення політики безпеки включає в себе наступні роботи [12]:

– розробка концепції безпеки інформації в АС;

– аналіз ризиків;

– визначення вимог до заходів, методів та засобів захисту;

– вибір основних рішень з забезпечення безпеки інформації;

– організація виконання відновлювальних робіт і забезпечення неперервного функціонування АС;

– документальне оформлення політики безпеки.

## 1.3 Постановка задачі

Враховуючи вищезазначене, для забезпечення надійної системи інформаційної безпеки на підприємстві ПП «Альфа Транс» необхідно провести обстеження середовищ функціонування ІТС .

Складовою частиною комплексної системи захисту інформації є політика безпеки інформації. Вразливими складовими АС є:

– обладнання – ЕОМ та їхні складові частини (процесори, монітори, термінали, робочі станції та ін.), периферійні пристрої;

– програмне забезпечення – завантажувальні модулі, СКБД, операційні системи та інші системні програми, діагностичні і тестові програми тощо;

– дані – тимчасового і постійного зберігання, на магнітних носіях, друковані, архівні і резервні копії, системні журнали, технічна, експлуатаційна і розпорядча документація та ін.;

– персонал і користувачі АС.

Виходячи з цього необхідно створити політики безпеки, які будуть відображені в спеціальній частині роботи.

## 1.4 Висновок

Проведено аналіз сучасного стану нормативно-правової бази безпеки інформації інформаційно-комунікаційних систем. Розглянуто основні документи з точки зору організації та побудови комплексної системи захисту інформації.

З огляду на раніше наведене можна зробити висновок, що для довгострокового успішного функціонування підприємства необхідною умовою є зниження ризиків та загроз інформації підприємства до мінімуму. А це може бути досягнене за рахунок створення ефективної моделі його подальшого функціонування з точки зору безпеки інформації.

# РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

## 2.1 Загальні відомості про підприємство ПП «Альфа Транс»

Дослідження роботи ґрунтується на базі ПП «Альфа Транс», що знаходиться за адресою: вул. Академіка Чекмарьова, 3, м. Дніпро, 49000, Україна.

ПП «Альфа Транс» засноване в 2011 році. Основним видом діяльності підприємства є надання транспортно-експедиційних послуг.

Форма власності: приватна власність.

У склад підприємства входять наступні підрозділи:

- відділ з планування автотранспорту;
- відділ транспортно-експедиційної діяльності;
- відділ взаєморозрахунків;
- бухгалтерія;
- відділ персоналу;
- відділ матеріально технічного забезпечення;
- відділ інформаційних технологій;
- відділ економічної безпеки.

Організаційна структура підприємства наведена на рисунку 2.1.

Всього штат співробітників ПП «Альфа Транс» налічує 43 особи, в тому числі:

- генеральний директор – 1;
- комерційний директор – 1;
- директор з економіки і фінансів – 1;
- начальник відділу з планування автотранспорту– 1;
- спеціаліст з організації автотранспортних перевезень – 1;
- ведучий спеціаліст з планування автотранспорту – 2;
- спеціаліст з планування автотранспорту – 12;
- начальник відділу транспортно-експедиційної діяльності – 1;
- начальник сектору з роботи зі сторонніми перевізниками – 1;

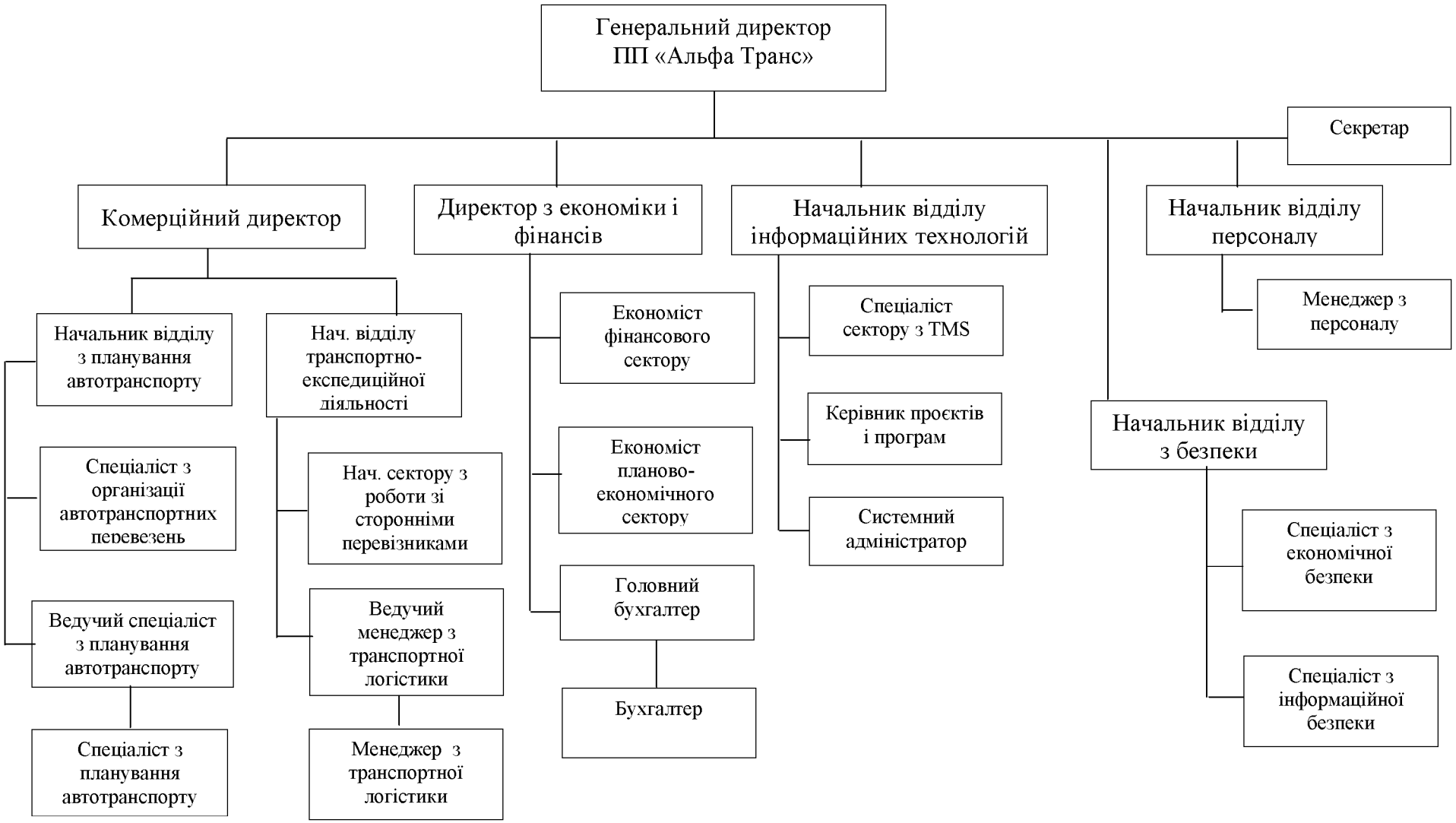



Рисунок 2.1 – Організаційна структура підприємства

- ведучий менеджер з транспортної логістики – 2;
- менеджер з транспортної логістики – 3;
- економіст фінансового сектору – 2;
- економіст планово-економічного сектору – 1;
- головний бухгалтер – 1;
- бухгалтер – 3;
- начальник відділу інформаційних технологій – 1;
- спеціаліст сектору з TMS – 1;
- керівник проєктів і програм – 1;
- системний адміністратор – 1;
- начальник відділу персоналу – 1;
- менеджер з персоналу – 1;
- начальник відділу з безпеки – 1;
- спеціаліст з економічної безпеки – 1;
- спеціаліст з інформаційної безпеки – 1;
- секретар – 1.

Основний бізнес-процес підприємства ПП «Альфа Транс» полягає в наступному. Замовлення на перевезення вантажу та наряд на автотранспорт, який формує робітник автоколони, надходять у електронному вигляді у відділ з планування автотранспорту. Спеціаліст з планування на підставі замовлень та наряду, що містить відомості про справний транспорт, виконує планування маршрутів доставки товарів автотранспортом і формування маршрутних листів для загрузки в електронній формі. На підставі маршрутного листа спеціаліст з організації автотранспортних перевезень формує подорожній лист в електронній формі, а потім друкує його для передачі водієві. На підставі маршрутного листа формується акт виконаних робіт, що служить підставою для взаєморозрахунку між ПП «Альфа Транс» і замовником, який виконується у відділі взаєморозрахунків.

Інформація, що підтримує основний бізнес-процес підприємства

«Альфа Транс», обробляється в АС «TMS ORTEC TD», до складу якої входять підсистеми:

- управління нормативно-довідковою інформацією;
- управління потребами в перевезенні вантажів;
- управління завданнями на перевезення вантажів;
- автоматичне й ручне планування маршрутів доставки;
- формування рейсів;
- управління ресурсами для забезпечення рейсів;
- контроль за виконанням рейсів;
- управління тарифною політикою компанії;
- управління взаємодіями;
- управління доступом;
- одержання аналітичної звітності;
- візуалізація інформації на електронних картах.

Підсистема «Управління нормативно-довідковою інформацією забезпечує роботу всіх інших функціональних підсистем. В рамках даної підсистеми створюється, обробляється і зберігається наступна інформація:

- ділові партнери компанії (замовники, перевізники);
- контактні особи, адреси;
- правила тарифікації, що залежать від параметрів перевезення;
- номенклатура;
- користувачі;
- групи тарифів;
- маршрути.

Також на підприємстві функціонує АС "1С: Бухгалтерія +Кадри". Вона використовується для вирішення всіх завдань, що стоять перед бухгалтерською та економічною службами підприємства, а також завдань з обліку матеріально-технічного забезпечення, активів підприємства, персоналу і розрахунку заробітної плати.

Підприємство працює з понеділка по суботу. Вихідний день - неділя. Графік роботи з понеділка по п'ятницю з 9.00 до 18.00. Перерва з 13.00 - 14.00. Субота - короткий день. Графік роботи з 9.00 - 14.00.

Прибирання приміщення проводиться прибиральницею кожен день, крім неділі. Вранці з 7.30 - 9.00.

Охорона працює цілодобово, зі зміною о 12 годині. Ключі від офісу знаходяться у директора і охоронців. Доступ сторонніх осіб в приміщення здійснюється тільки в робочий час через пост охорони, який розташований при вході.

## 2.2 Обґрунтування необхідності створення комплексної системи захисту інформації

Відповідно до п. 1.2 розділу 1 створення КСЗІ на ПП «Альфа Транс» необхідно для роботи компанії на простору ринку та для збереження цілісності, конфіденційності та доступності інформації.

Значна частина інформації підприємства представлена в електронній формі, серед якої є відомості, віднесені до інформації з обмеженим доступом (ІзОД).

В останній час на підприємстві відбулося різке збільшення заказів на перевезення. На підставі цього збільшилися обсяги інформаційних потоків даних, що обробляється автоматизованим способом і передається каналами зв'язку. Взаємодія з клієнтами здійснюється за допомогою загальнодоступних глобальних інформаційних мереж.

За рахунок використання більш оперативної й повної інформації є можливість підвищити ефективність діяльності компаній.

З метою визначення необхідного рівня захисту інформації, що обробляється технічними засобами та/або озвучується на об'єкті, було проведене категоріювання об'єкта інформаційної діяльності (ОІД). Відповідно до НД ТЗІ 1.6-005-2013 підприємству була надана IV категорія.

До четвертої категорії відносяться об'єкти, в яких циркулює конфіденційна інформація [15].

## 2.3 Обстеження на об’єкті інформаційної діяльності

В останній час на підприємстві відбулося різке збільшення заказів на перевезення. На підставі цього збільшилися обсяги інформації та відбулося збільшення штату відділу з планування автотранспорту та відділу транспортно-експедиційної діяльності.

У зв’язку з цим керівництвом підприємства прийняте рішення щодо обстеження вищезазначених відділів. Метою обстеження є вивчення їх ІД, визначення об`єктів захисту – ІзОД, виявлення загроз, їхній аналіз та побудова окремої моделі загроз.

Підставою для проведення обстеження об’єкта інформаційної діяльності була послідовність виконання етапів створення КСЗІ відповідно до НД ТЗІ 3.7-003-05 [7] та Наказ керівника підприємства.

Для проведення обстеження ОІД необхідно:

– провести аналіз умов функціювання підприємства, його розташування на місцевості (ситуаційного плану) для визначення можливих джерел загроз;

– дослідити засоби забезпечення ІД, які мають вихід за межі контрольованої території;

– вивчити схеми систем життєзабезпечення підприємства, а також інженерних комунікацій;

– дослідити інформаційні потоки, технологічні процеси передачі, одержання, використання, розповсюдження і зберігання інформації;

– визначити наявність та технічний стан засобів забезпечення ТЗІ;

– перевірити наявність на підприємстві нормативних документів, які забезпечують функціювання системи захисту інформації, а також нормативної та експлуатаційної документації, яка забезпечує ІД;

– визначити технічні засоби і системи, застосування яких не обґрунтоване службовою необхідністю і які підлягають демонтуванню;

– визначити технічні засоби, що потребують переобладнання та встановлення засобів ТЗІ.

Матеріали обстеження необхідно використовувати під час розроблення окремої моделі загроз, які повинні включати:

– генеральний та ситуаційний плани підприємства, схеми розташування засобів і систем забезпечення ІД, а також інженерних комунікацій, які виходять за межі контрольованої території;

– схеми та описи каналів витоку інформації, каналів спеціального впливу і шляхів несанкціонованого доступу до ІзОД;

– оцінку шкоди, яка передбачається від реалізації загроз.

### 2.3.1 Обстеження фізичного середовища функціонування ІТС

При обстеженні фізичного середовища здійснено аналіз взаємного розташування засобів обробки інформації ІТС на об'єктах інформаційної діяльності, комунікацій, систем життєзабезпечення та зв'язку, а також режим функціонування цих об'єктів.

Аналізу підлягали наступні характеристики фізичного середовища:

– територіальне розташування компонентів ІТС (генеральний план, ситуаційний план);
– наявність охорони території та пропускний режим;
– наявність категорійних приміщень, в яких повинні розміщуватися компоненти ІТС;
– режим доступу до компонентів фізичного середовища ІТС.

Ситуаційний план ОІД наведений на рисунку 2.2.

До підприємства прилягають дві вулиці: на північному заході проспект Гагаріна (має односторонній рух для автотранспорту, ширина проїжджої частини 3 м, і двосторонній рух для електротранспорту) та на південному

заході вулиця Академіка Чекмарьова (має двосторонній рух для автотранспорту, ширина проїжджої частини 2,5 м). ОІД розташований на другому поверсі двоповерхової будівлі. На першому поверсі знаходиться супермаркет «АТБ-Маркет». Парковка розташовується на південно-західному напрямку на відстані 4 м від ОІД і є об'єктом загального користування.

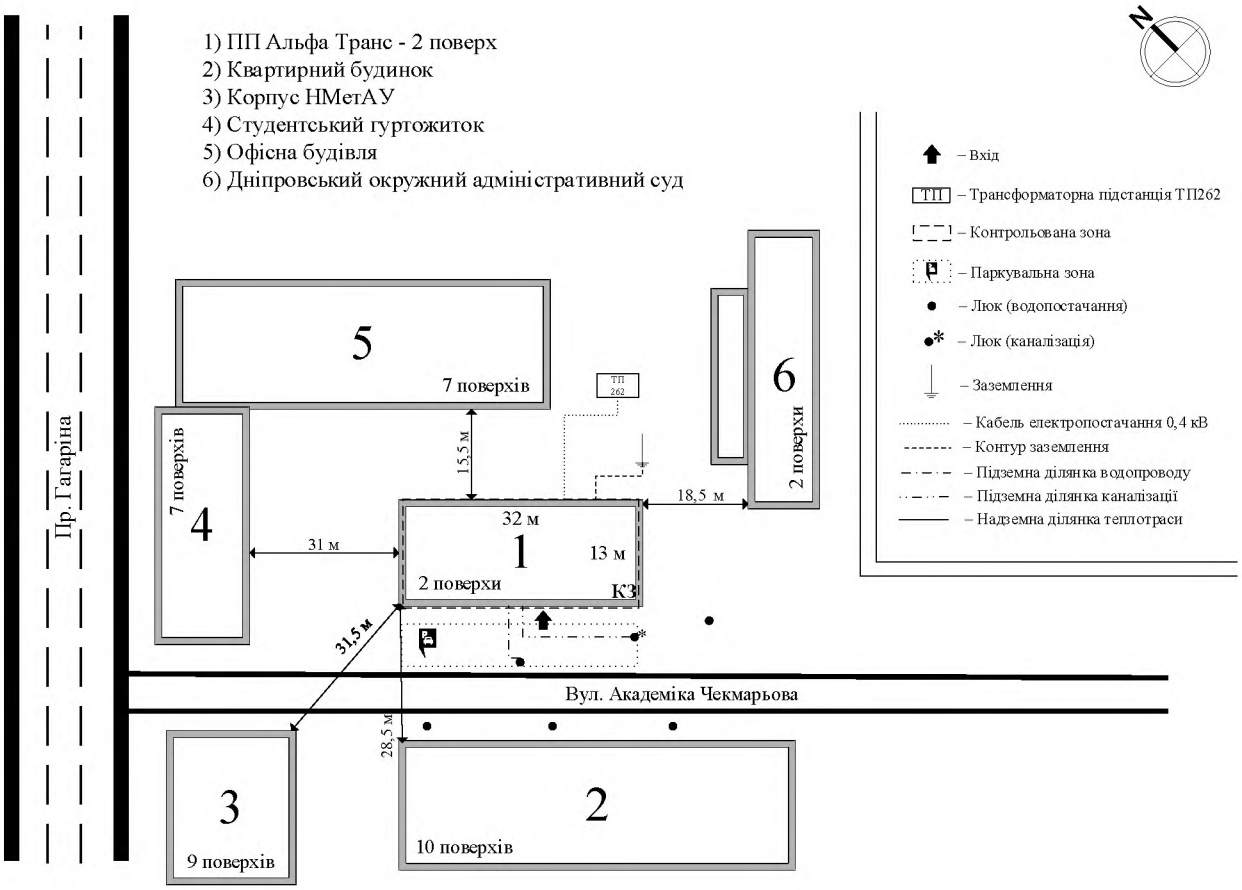



Рисунок 2.2 – Ситуаційний план ОІД

На південь від об'єкта розташовується проїжджа частина вулиці Академіка Чекмарьова та квартирний будинок на протилежній стороні (на відстані 28,5 м від ОІД). На сході – Дніпропетровський окружний адміністративний суд (на відстані 18,5 м від ОІД). На північному заході розташовується студентський гуртожиток для іноземних студентів (на відстані 31 м від ОІД). На півночі - офісна будівля (на відстані 15,5 м від ОІД).

Будівля з червоної цегли, обшита профнастилом, має плоский дах і

пожежну драбину. Територія охороняється службою внутрішньої охорони підприємства. До будівлі підведені наступні системи комунікацій: система водопостачання, система каналізації, система електропостачання, система опалення, система сигналізації і телефонна лінія. Режим контрольованої зони об'єкта зони забезпечується контрольно-пропускним пунктом на вході ОІД.

Контрольована зона (КЗ) визначена наказом керівника підприємства № 3 від 10.02.2011 р і обмежена першим (контрольно-пропускний пункт) і другим поверхом будівлі. ОІД обладнаний системою охоронно-пожежної сигналізації та контролю доступу.

Генеральний план ОІД приведено на рисунку 2.3.

Фундамент будівлі – бетонний, зовнішні стіни – цегляні, внутрішні перегородки – цегляні стіни, обшиті гіпсокартоном. Товщина зовнішніх стін - 0,4 м. Товщина внутрішніх перегородок – 0,25 м. Висота перекриття – 3 м. Перекриття між поверхами – залізобетонні плити. Дах будівлі – горизонтальна, покрита руберойдом з теплоізоляцією. Покриття підлоги – лінолеум.

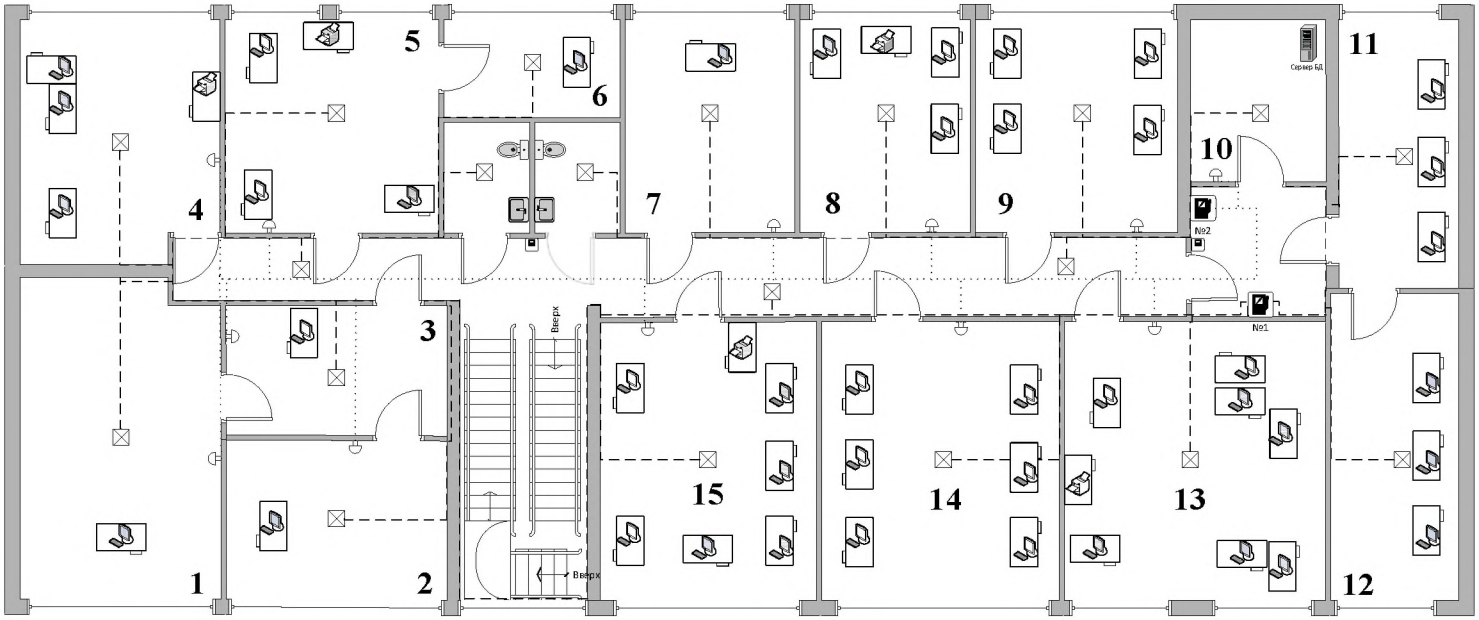
Вікна (14 шт., Розміром 1100 × 2600 мм) – металопластикові, що відкриваються, з двокамерним склопакетом. Товщина скла 3 мм. На всіх вікнах знаходяться жалюзі, а також датчики на відкриття та розбиття скла.

Внутрішні двері (19 шт.) – дерев'яні одностулкові, розміром 900 × 2100 мм, товщиною 50 мм. Всі двері обладнані врізаним замком. На кожен замок виділено по 2 копії ключа. Дублікати ключів зберігаються на пункті охорони. Зовнішні металеві двостулкові двері (1 шт.) з врізаним замком, розміром 2000 × 2100 мм, товщиною 100 мм. Товщина металу – 5 мм.

Опис систем інженерних комунікацій підприємства наведений у таблиці 2.1.

Електроживлення будівлі здійснюється від трансформаторної підстанції, яка знаходиться за межами офісного приміщення. Система опалення, система водопостачання і система заземлення мають вихід за межі виділеного приміщення.

Генеральний план ПП «Альфа Транс»




| Умовне позначення | Значення |
|---|---|
| | Електричний щит ( №1, №2) |
| | Світильник |
| | Датчик пожежної сигналізації |
| | Ручна пожежна сигналізація |
| – – – | Лінія електропередачі з щитка №1 |
| ..... | Лінія електропередачі з щитка №2 |
| | Комп'ютер |
| | Принтер |

1) Генеральний директор
2) Директор з економіки та фінансів
3) Приймальна
4) Відділ з безпеки
5) Бухгалтерія
6) Головний бухгалтер
7) Комерційний директор
8) Відділ взаєморозрахунків
9) Відділ персоналу
10) Серверна
11) Відділ інформаційних технологій
12) Економічна служба
13) Відділ з планування автотранспорту
14) Відділ з планування автотранспорту
15) Відділ транспортно-експедиційної діяльності

Рисунок 2.3 – Генеральний план ОІД

Таблиця 2.1 – Системи інженерних комунікацій підприємства

| | |
|---|---|
| Система електропостачання | Підключена до трансформаторної підстанції КП «Дніпрообленерго» ТП №-262 підземним кабелем, яка має сторонніх споживачів і перебуває за межами КЗ |
| Система опалення | Підключена до мережі централізованого опалення КП «Теплоенерго», знаходиться за межами КЗ (пластикові труби, однотрубна вертикальна система опалення) |
| Система каналізації | Підключена до міської мережі КП «Міськводоканалу», яка знаходитися за межами КЗ (підземне підключення до люка) |
| Система водопостачання | Підключена до системи КП «Міськводоканалу» (підземне підключення до люка). |
| Система заземлення | Всі прилади, комп'ютери заземлені на загальний контур заземлення, який є замкнутим і виходить за межі КЗ. |
| Телефонна лінія | Підключена до АТС-597 «Укртелеком» кабелем діаметром 24 мм маркування ТПП 100 * 2 * 0.4. На офіс відведено 4 номери. |
| Internet | Кабельне підключення, виходить за межі контрольованої зони |

Електроживлення ОІД здійснюється від електрощита, що знаходиться на другому поверсі. Електрика заведено від підстанції ТП №-262 підземним кабелем на перший поверх будівлі. Вертикально по стіні через залізобетонні перекриття проведені лінії електромережі до щита розподілу на другому поверсі.

### 2.3.2 Обстеження ІТС ПП «Альфа Транс»

ІТС підприємства являє собою локальну мережу – з’єднуються пристрої, що розташовані в межах ОІД. До складу локальної мережі входять 43 персональних комп'ютерів, сервер баз даних, що відповідає за обробку та зберігання інформації, мережеве і друкарське обладнання. Схема обладнання ІТС зображена на рисунку 2.4. Розміщення ПК по приміщеннях підприємства наведено в таблиці 2.2.

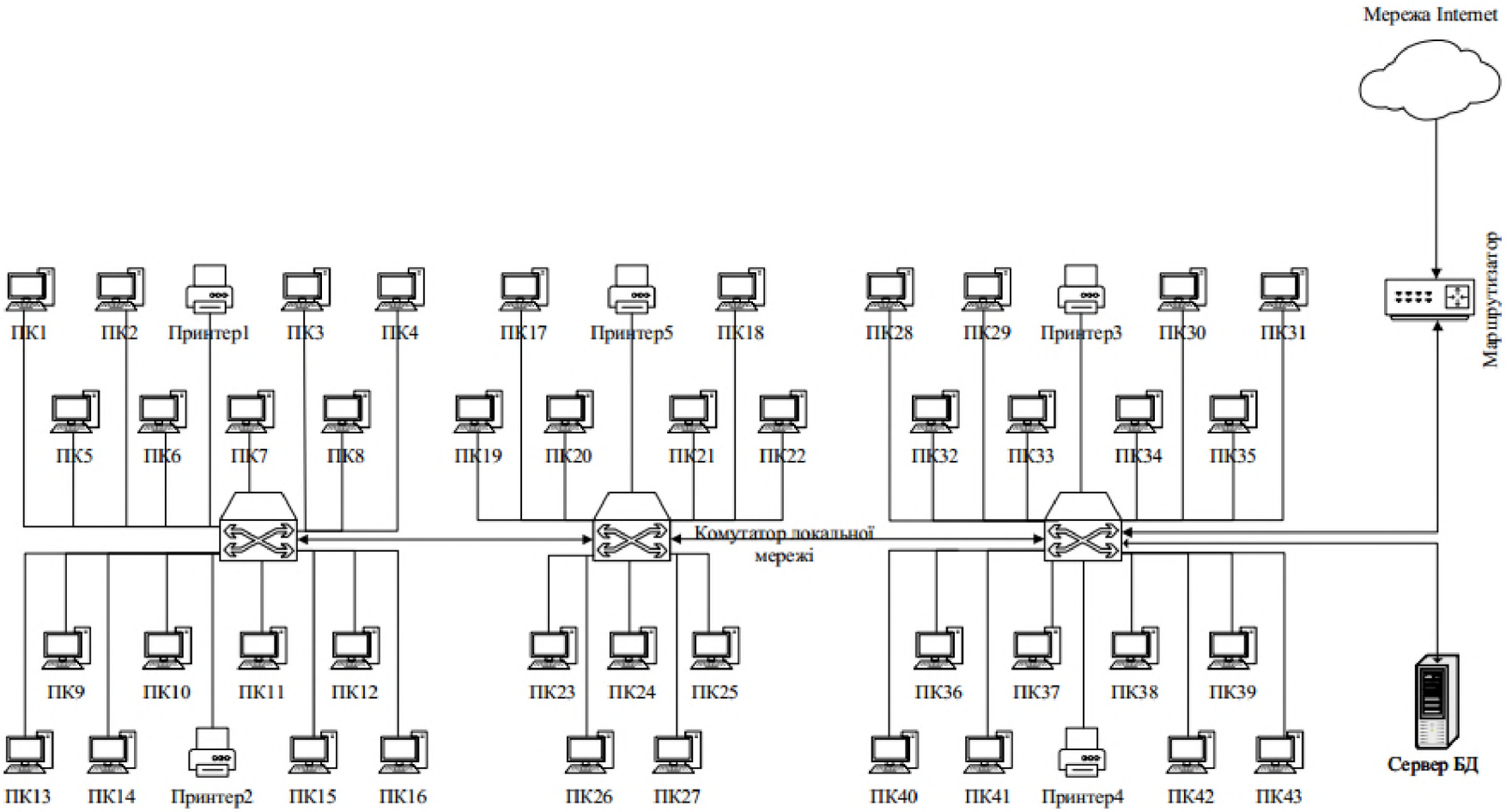



Рисунок 2.4 – Схема обладнання ІТС ПП «Альфа Транс»

Таблиця 2.2 – Розміщення ПК по приміщеннях підприємства

| № з/п | Посада | Номер приміщення | Номер комп'ютера в ІТС |
|---|---|---|---|
| 1 | Генеральний директор | 1 | ПК1 |
| 2 | Директор з економіки і фінансів | 2 | ПК2 |
| 3 | Секретар | 3 | ПК3 |
| 4 | Начальник відділу з безпеки | 4 | ПК4 |
| 5 | Спеціаліст з економічної безпеки | 4 | ПК5 |
| 6 | Спеціаліст з інформаційної безпеки | 4 | ПК6 |
| 7 | Бухгалтер | 5 | ПК7-ПК9 |
| 8 | Головний бухгалтер | 6 | ПК10 |
| 9 | Комерційний директор | 7 | ПК11 |
| 10 | Економіст фінансового сектору | 8 | ПК12, ПК13 |
| 11 | Економіст планово-економічного сектору | 8 | ПК14 |
| 12 | Начальник відділу транспортно-експедиційної діяльності | 9 | ПК15 |
| 13 | Начальник відділу інформаційних технологій | 9 | ПК16 |
| 14 | Начальник відділу персоналу | 9 | ПК17 |
| 15 | Менеджер з персоналу | 9 | ПК18 |
| 16 | Спеціаліст сектору з TMS | 11 | ПК19 |
| 17 | Керівник проєктів і програм | 11 | ПК20 |
| 18 | Системний адміністратор | 11 | ПК21 |
| 19 | Начальник відділу з планування автотранспорту | 12 | ПК22 |
| 20 | Ведучий спеціаліст з планування автотранспорту | 12 | ПК23, ПК24 |
| 21 | Спеціаліст з організації автотранспортних перевезень | 13 | ПК25 |
| 22 | Спеціаліст з планування автотранспорту | 13, 14 | ПК26-ПК37 |
| 23 | Начальник сектору з роботи зі сторонніми перевізниками | 15 | ПК38 |
| 24 | Ведучий менеджер з транспортної логістики | 15 | ПК39-ПК40 |
| 25 | Менеджер з транспортної логістики | 15 | ПК41-ПК43 |

За класифікацією АС за сукупністю її характеристик відноситься до 3 класу: розподілений багатомашинний комплекс, який обробляє інформацію різних ступенів обмеження доступу, розрахований на багато користувачів. Особливість класу – необхідність передачі інформації через незахищене середовище або, в загальному випадку, наявність вузлів, що реалізують різну політику безпеки [11].

Згідно із НД ТЗІ 3.7-003-05 політика безпеки може розроблятись для ІТС в цілому або, якщо мають місце особливості функціонування окремих компонентів КСЗІ, для окремої компоненти, для окремої функціональної задачі, для окремої технології обробки інформації тощо [7]. Виходячи з цього, а також з того, на підприємстві відбулося різке збільшення заказів на перевезення, що призвело до збільшення обсягів інформації та її видів, штату відділу з планування автотранспорту, керівництво прийняло рішення щодо обстеження цього підрозділу з метою доповнення КСЗІ вже існуючої на ПП «Альфа Транс».

### 2.3.3 Обстеження інформації, що обробляється у ІТС, і технологія її обробки

При обстеженні інформаційного середовища аналізу підлягала інформація, яка обробляється, а також зберігається в ІТС (дані і програмне забезпечення).

Службова, таємна інформація, інформація, що є власністю держави, а також відомості, що становлять державну таємницю, в АС ПП «Альфа Транс» не циркулює.

За режимом доступу інформація, що обробляється в АС: відкрита і з обмеженим доступом. За правовим режимом до інформації з обмеженим доступом належить конфіденційна інформація [7].

ПП «Альфа Транс» має конфіденційну інформацію. Згідно ЗУ «Про інформацію» конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних

осіб і поширюються за їх бажанням відповідно до передбачених ними умов.

Згідно з НД ТЗІ 1.1-003-99: конфіденційність інформації – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем.

У ПП «Альфа Транс» циркулює інформація з обмеженим доступом і комерційна таємниця, а, отже, її збереження і захист повинні забезпечуватися відповідно до Цивільного, Господарського кодексів і таких законів України: «Про захист персональних даних», «Про інформацію», «Про захист від недобросовісної конкуренції ».

Захист інформації ОІД необхідно забезпечити для:

– запобігання перехоплення конфіденційної інформації та ознайомлення з нею;

– захисту і зберігання конфіденційної інформації відповідно до закону;

– запобігання несанкціонованого копіювання, модифікації і знищення інформації;

– запобігання викрадення роздрукованих документів і магнітних носіїв з конфіденційною інформацією;

– запобігання помилок в програмному забезпеченні і роботі з ним;

– запобігання неправомірних дій з боку персоналу, контроль за виконанням правил, зазначених в політиці безпеки.

Основними джерелами конфіденційної інформації є:

1) персонал підприємства, допущений до конфіденційної інформації;

2) носії конфіденційної інформації (документи, пристрої);

3) технічні засоби, призначені для зберігання і обробки інформації;

4) засоби комунікації, які використовуються з метою передачі інформації;

5) повідомлення, що передаються по каналах зв'язку, що містять конфіденційну інформацію.

Перелік програмного забезпечення системи обробки інформації наведений у таблиці 2.3.

Таблиця 2.3 – Перелік програмного забезпечення системи обробки інформації ПП «Альфа Транс»

| Найменування програмного забезпечення | Тип ліцензії | Місцезнаходження |
|---|---|---|
| Windows 10 Pro | OLP | ПК1, ПК2, ПК10, ПК11, ПК22 – ПК43 |
| Windows 7 Pro | OLP | ПК3 – ПК9, ПК12 – ПК2 |
| Windows Server 2019 | Standard | Сервер БД |
| Microsoft Office 365 | OLP | ПК1 – ПК43 |
| 1С:Бухгалтерія + Кадри, версія 8.3 | Пропріетарна комерційна | ПК7 – ПК10, ПК17 – ПК18, ПК21 |
| TMS ORTEC TD (Transport Management Systems) | Пропріетарна комерційна | ПК21, ПК22 – ПК43 |
| Google Chrome | Не потребує | ПК1 – ПК43 |

Аналіз технології обробки інформації виявив особливості обігу електронних документів, були визначені і описані інформаційні потоки і середовища, через які вони передаються, джерела утворення потоків і місця призначення. Фіксувалися види носіїв інформації та порядок їх використання під час функціонування ІТС.

Наведемо опис інформаційних потоків у відділі з планування автотранспорту.

Замовлення на перевезення вантажу та наряд на автотранспорт, який формує робітник автоколони, надходять у електронному вигляді у відділ з планування автотранспорту через Інтернет. Спеціаліст з планування автотранспорту на підставі замовлень, а також наряду на автотранспорт (відомостей про справний транспорт) виконує планування маршрутів доставки товарів автотранспортом і формування маршрутних листів для загрузки в електронній формі. На підставі маршрутного листа спеціаліст з організації автотранспортних перевезень формує подорожній лист в електронній формі, а потім друкує його для передачі водієві. Подорожній лист в електронній формі

додається у реєстр рейсів. На підставі маршрутного листа формується акт виконаних робіт, що служить підставою для взаєморозрахунку між ПП «Альфа Транс» і замовником, який виконується у відділі взаєморозрахунків.

Далі наведено опис життєвих циклів кожного з видів інформації.

Опис життєвого циклу замовлень на перевезення вантажу.

Замовлення, що надходять від клієнтів на надання послуг з вантажоперевезення.

1) Надходження. Замовлення надходять від клієнтів на електронну пошту. Інформація створюється в системі в форматі xls.

2) Обробка. Інформація обробляється програмним засобом Microsoft Excel.

3) Використання. Інформація використовується для створення маршрутного листа.

4) Зберігання. Інформація зберігається на сервері бази даних. Термін зберігання визначається політикою підприємства.

5) Відправлення. Після закінчення терміну зберігання відправляється в архів.

Опис життєвого циклу наряду на автотранспорт.

Наряд на автотранспорт, що надходить від начальника автоколони, що знаходиться за межами КЗ.

1) Надходження. Наряд на автотранспорт надходить один раз на добу на електронну пошту. Інформація створюється в системі Microsoft Excel в форматі csv.

2) Обробка. Інформація імпортується в систему «TMS ORTEC TD».

3) Використання. Інформація використовується для створення маршрутного листа.

4) Зберігання. Інформація зберігається на сервері бази даних. Термін зберігання визначається політикою підприємства.

5) Відправлення. Після закінчення терміну зберігання відправляється в архів.

Опис життєвого циклу маршрутних листів.

1) Надходження. Інформація створюється в системі «TMS ORTEC TD» фахівцем з планування перевезень на підставі замовлення.

2) Обробка. Інформація обробляється програмним засобом «TMS ORTEC TD».

3) Використання. Інформація використовується для створення подорожнього листа.

4) Зберігання. Інформація зберігається на сервері бази даних. Термін зберігання визначається політикою підприємства.

5) Відправлення. Після закінчення терміну зберігання відправляється в архів.

Опис життєвого циклу реєстру рейсів.

1) Надходження. Інформація створюється в системі «TMS ORTEC TD» фахівцем з планування перевезень на підставі електронних маршрутних листів.

2) Обробка. Інформація обробляється програмним засобом «TMS ORTEC TD».

3) Використання. Інформація використовується програмною системою «1С: Бухгалтерія».

4) Зберігання. Інформація зберігається на сервері бази даних. Термін зберігання визначається політикою підприємства.

5) Відправлення. Після закінчення терміну зберігання відправляється в архів.

Опис життєвого циклу подорожніх листів.

1) Надходження. Інформація створюється в системі «TMS ORTEC TD» спеціалістом з організації автотранспортних перевезень на підставі маршрутного листа.

2) Обробка. Інформація обробляється програмним засобом «TMS ORTEC TD».

3) Використання. Інформація використовується для створення паперового подорожнього листа.

4) Зберігання. Інформація зберігається на сервері бази даних. Термін зберігання визначається політикою підприємства.

5) Відправлення. Інформація експортується з системи на паперовий носій у вигляді подорожнього листа водієві автотранспортного засобу, а також у програмну систему «1С: Бухгалтерія».

### 2.3.4 Обстеження середовища користувачів ІТС

При обстеженні середовища користувачів здійснювався аналіз:

- функціонального і кількісного складу користувачів;
- повноважень користувачів про допуск до відомостей, що обробляються в ІТС, доступу до ІТС та її окремих компонентів;
- рівня можливостей різних категорій користувачів послуг (можуть бути доступні) їм засобами ІТС.

Персонал відділу з планування автотранспорту складається з 16 осіб. Матриця доступу працівників до інформації наведено в таблиці 2.4.

Таблиця 2.4 – Матриця доступу працівників до інформації ВПА

| Інформація | Посада | | | |
|---|---|---|---|---|
| | Начальник відділу | Спеціаліст з організації автотранс-портних перевезень | Ведучий спеціаліст з планування автотранспорту | Спеціаліст з планування автотранс-порту |
| Замовлення на перевезення | О, М, В | О | О, М, В | О, М, В |
| Маршрутний лист | О, М, В | О | О, М, В | О, М, В |
| Подорожній лист | О, М, В | О, М, В | О | О |

| | | | | |
|---|---|---|---|---|
| Наряд на автотранспорт | О, М, В | О, М, В | О | О |
| Реєстр рейсів | О, М, В | О | О, М, В | О |
| Інформація про тарифи на перевезення | О, М, В | О | О, М, В | О |
| Інформація про контрагентів | О, М, В | О | О, М, В | О |
| Внутрішні документи (накази, службові записки, інструкції) | О, М, В | О, М, В | О, М, В | О |

О – ознайомлення, М – модифікація, В – видалення.

## 2.4 Аналіз та оцінка інформаційних ризиків

Для аналізу та оцінки інформаційних ризиків проведемо класифікацію інформації, що обробляється в АС.

Щоб визначити найцінніший ресурс в ІТС було обрано модель класифікації, в основі якої лежить розподіл інформації за основними властивостями. Класифікація інформації наведено у таблицях 2.5 – 2.7.

Таблиця 2.5 – Класифікація інформації за розголошенням чи конфіденційністю

| Клас | Ступінь важливості | Кількість балів | Характеристика |
|---|---|---|---|
| К5 | Критична інформація | 5 | Розголошення інформації призведе до краху підприємства або дуже значних матеріальних втрат |

| | | | |
|---|---|---|---|
| К4 | Дуже важлива інформація | 4 | Розголошення призведе до значних матеріальних втрат, якщо не будуть прийняті відповідні заходи |
| К3 | Важлива інформація | 3 | Розголошення призведе до деяких матеріальних або моральних втрат, якщо не будуть прийняті відповідні заходи |
| К2 | Значима інформація | 2 | Приносить моральну шкоду, може бути використана в певний момент |
| К1 | Малозначима інформація | 1 | Може принести моральну шкоду в дуже рідкісних випадках |
| К0 | Незначна інформація | 0 | Не впливає на роботу суб'єкта |

Таблиця 2.6 – Класифікація інформації за цілісністю або несанкціонованою модифікацією

| Клас | Ступінь важливості | Кількість балів | Характеристика |
|---|---|---|---|
| Ц4 | Критична інформація | 4 | Несанкціонована зміна призведе до некоректної роботи всього підприємства або значної його частини; наслідки такої модифікації незворотні |
| Ц3 | Дуже важлива інформація | 3 | Несанкціонована зміна призводить до невірної роботи підприємства або його частини через деякий час, якщо не будуть виконані певні дії; наслідки такої модифікації незворотні |
| Ц2 | Важлива інформація | 2 | Несанкціонована зміна приводить до некоректної роботи підприємства через |

| | | | |
|---|---|---|---|
| | | | деякий час, якщо не будуть виконані деякі дії; наслідки такої модифікації оборотні |
| Ц1 | Значима інформація | 1 | Несанкціонована зміна позначиться через деякий час, але не призведе до збою в системі; наслідки такої модифікації оборотні |
| Ц0 | Незначна інформація | 0 | Несанкціоноване зміна не позначиться на роботі системи |

Таблиця 2.7 – Класифікація інформації за доступністю або наявністю

| Клас | Ступінь важливості | Кількість балів | Характеристика |
|---|---|---|---|
| Д4 | Критична інформація | 4 | Робота суб'єкта буде зупинена |
| Д3 | Дуже важлива інформація | 3 | Суб'єкт буде працювати, але короткий час |
| Д2 | Важлива інформація | 2 | Суб'єкт може працювати без цієї інформації певний час, але вона скоро знадобиться |
| Д1 | Корисна інформація | 1 | Без інформації можна працювати, але її використання економить час |
| Д0 | Не суттєва інформація | 0 | Застаріла або невикористовувана інформація, що не впливає на роботу суб'єктів |

Оцінка інформації, яка циркулює у ВПА, у відповідності до моделі класифікації, наведена у таблиці 2.8.

Таблиця 2.8 – Оцінка інформації, яка циркулює у ВПА, у відповідності до моделі класифікації

| Інформація | Вимоги до властивостей | | | Сума балів |
|---|---|---|---|---|
| | К | Ц | Д | |
| Замовлення на перевезення | 3 | 2 | 4 | 9 |
| Маршрутний лист | 2 | 4 | 4 | 10 |
| Подорожній лист | 1 | 3 | 2 | 6 |
| Наряд на автотранспорт | 2 | 2 | 4 | 7 |
| Реєстр рейсів | 4 | 1 | 2 | 7 |
| Інформація про тарифи на перевезення | 3 | 3 | 2 | 8 |
| Інформація про контрагентів | 2 | 2 | 2 | 6 |
| Внутрішні документи (накази, службові записки, інструкції) | 1 | 1 | 1 | 3 |

К –конфіденційність; Ц – цілісність; Д –доступність.

Враховуючи отримані дані та відповідно до НД ТЗІ 2.5-005-99 [10] був обраний стандартний 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.1 = { КД-2, КО-1, КВ-1, ЦД-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }

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.

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-1 – мінімальна 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.

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-1 – мінімальна 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.

З наведених у таблиці 2.8 даних можна зробити висновок про найважливішу інформацію підприємства (якщо сума балів більш ніж 6) — маршрутний лист, замовлення на перевезення, інформація про тарифи на

перевезення, наряд на автотранспорт, реєстр рейсів. Саме ця інформація повинна бути забезпечена найбільшим рівнем захисту.

Проаналізуємо модель загроз.

Для аналізу інформаційних ризиків застосуємо модель їх ранжування та класифікації. Джерела загроз можна розділити на антропогенні, техногенні та стихійні, котрим можна привласнити рівень небезпеки $К_{неб.}$ Для антропогенних джерел: К1 – доступність до об'єкту, К2 – кваліфікація і мотивація, К3 – фатальність наслідків, для техногенних джерел К1 – можливість виникнення, К2 – наявність необхідних умов, К3 – фатальність наслідків, для стихійних джерел К1 – особливості місцевості, К2 – наявність необхідних умов, К3 – фатальність наслідків. Кожному критерію надається оцінка від 1 до 5, а потім для джерела можна порахувати коефіцієнт $К_{неб}$ за допомогою формули

$$К_{неб} = \frac{К1 \times К2 \times К3}{125} \quad (2.1)$$

де 125 – максимальне число добутку показників К.

Виконаємо ранжування джерел загроз.

Таблиця 2.9 – Антропогенні джерела загроз

| Джерело загрози | Доступність до об'єкту (К1) | Кваліфікація і мотивація (К2) | Фатальність (К3) | $К_{неб}$ |
|---|---|---|---|---|
| Внутрішні джерела | | | | |
| Начальник відділу | 5 | 5 | 4 | 0,800 |
| Спеціаліст з організації автотранспортних перевезень | 5 | 4 | 3 | 0,480 |
| Ведучий спеціаліст з планування автотранспорту | 5 | 5 | 4 | 0,800 |
| Спеціаліст з планування | 5 | 4 | 3 | 0,480 |

| | | | | |
|---|---|---|---|---|
| автотранспорту | | | | |
| Системний адміністратор | 5 | 5 | 5 | 1,000 |
| Інші працівники (не працівники ВПА) | 2 | 2 | 2 | 0,064 |
| Допоміжний склад (прибиральники, охорона) | 4 | 1 | 2 | 0,064 |
| Зовнішні джерела | | | | |
| Контрагенти | 1 | 1 | 1 | 0,008 |
| Технічний персонал з надання послуг ремонту обладнання | 5 | 4 | 5 | 0,8 |
| Злочинці / кримінальні структури | 2 | 2 | 3 | 0,096 |

Таблиця 2.10 – Техногенні джерела загроз

| Джерело загрози | Можливість виникнення (К1) | Наявність необхідних умов (К2) | Фатальність (К3) | $К_{неб}$ |
|---|---|---|---|---|
| Система телефонного зв'язку | 4 | 4 | 2 | 0,256 |
| Система доступу до Internet | 3 | 3 | 3 | 0,216 |
| Неякісні технічні засоби передачі, обробки, зберігання інформації | 3 | 3 | 4 | 0,288 |
| Неякісні програмні засоби | 2 | 2 | 3 | 0,096 |
| Мережі інженерних комунікацій | 3 | 4 | 4 | 0,384 |

Таблиця 2.11 – Стихійні джерела загроз

| Джерело загрози | Особливості місцевості (К1) | Наявність необхідних умов (К2) | Фатальність (К3) | $К_{неб}$ |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| Пожежа | 3 | 3 | 4 | 0,288 |
| Ураган | 2 | 3 | 4 | 0,192 |
| Повінь | 2 | 2 | 2 | 0,064 |
| Замелетрус | 1 | 1 | 2 | 0,016 |
| Інші форс-мажорні обставини | 1 | 1 | 2 | 0,016 |

Наведемо класифікацію для вразливостей, в критерії якої входять К1 – фатальність, інформативність для об'єктивних вразливостей, К2 – доступність і К3 – кількість. Критеріям надається та ж сама система оцінювання та коефіцієнт $К_{неб}$ вираховується за допомогою тієї ж формули (2.1), що наведена вище. Самі вразливості можна розділити на об'єктивні, суб'єктивні та випадкові. Далі виконаємо ранжування вразливостей.

Таблиця 2.12 – Об'єктивні вразливості

| Вразливість | Інформа-тивність (К1) | Доступ-ність (К2) | Кількість (К3) | $К_{неб}$ |
|---|---|---|---|---|
| Вразливості, що обумовлені особливостями об'єкта захисту | | | | |
| 1. Місцезнаходженням об'єкта | 2 | 2 | 2 | 0,064 |
| 2. Організацією каналів обміну інформацією | 3 | 2 | 2 | 0,096 |
| Вразливості, що активізуються | | | | |
| 1. Апаратні закладки | 3 | 3 | 2 | 0,144 |
| 2. Програмні закладки | 3 | 4 | 2 | 0,192 |

Таблиця 2.13 – Суб'єктивні вразливості

| Вразливість | Фаталь-ність (К1) | Доступ-ність (К2) | Кількість (К3) | $К_{неб}$ |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| Помилки користувачів системи | 3 | 3 | 3 | 0,216 |
| Помилки адміністраторів / IT персоналу | 4 | 4 | 2 | 0,256 |
| Використання системи з метою порушення її роботи | 4 | 3 | 2 | 0,192 |
| Порушення використання носіїв передачі даних і обміну повідомленнями | 3 | 3 | 3 | 0,216 |
| Злом паролів | 3 | 3 | 2 | 0,144 |
| Несанкціонована спроба доступу | 4 | 3 | 2 | 0,192 |

Таблиця 2.14 – Випадкові вразливості

| Вразливість | Фаталь-ність (К1) | Доступ-ність (К2) | Кількість (К3) | $К_{неб}$ |
|---|---|---|---|---|
| Збої і відмови комп'ютерного обладнання | 4 | 4 | 3 | 0,384 |
| Збої і відмови мережевого обладнання | 4 | 3 | 2 | 0,192 |
| Збої програмного забезпечення | 3 | 3 | 4 | 0,288 |
| Пошкодження обладнання | 3 | 2 | 3 | 0,144 |
| Збої і відмови сервера баз даних | 5 | 4 | 3 | 0,480 |

Відштовхуючись від отриманих даних, з’являється можливість виключити певні антропогенні та стихійні джерела загроз як маловірогідні.

Наведемо для найбільш важливих ресурсів ІТС відділу планування автотранспорту загрози і вразливості у таблиці 2.15.

Таблиця 2.15 – Найважливіші ресурси та їх вразливості і загрози

| Ресурс | Вразливість | Загроза | Властивість інформації |
|---|---|---|---|
| Замовлення на | Збої і відмови Internet-обладнання, некоректне | Знищення та копіювання | К, Ц, Д |

| | | | |
|---|---|---|---|
| перевезення | поводження з інформацією | | |
| Наряд на автотранспорт | Збої і відмови Internet-обладнання, некоректне поводження з інформацією | Відсутність доступу, втрата та копіювання | К, Ц, Д |
| Маршрутний лист | Збої і відмови сервера баз даних | Відсутність доступу, втрата | Ц, Д |
| Реєстр рейсів | Збої програмного забезпечення, неблагонадійність адміністратора системи | Відсутність доступу, знищення, розкриття | К, Ц, Д |
| Інформація про тарифи на перевезення | Збої і відмови сервера баз даних, неблагонадійність співробітників | Відсутність доступу, розголошення | К, Д |

Для оцінки ризику було обрано методику RiskWatch. Отже, оцінка ризику за методикою RiskWatch розраховується як оцінка очікуваних річних втрат для одного конкретного ресурсу від реалізації однієї загрози ALE [16]:

$$ALE = AV \times EF \times F, \quad (2.1)$$

де AV – вартість даного ресурсу. Цей показник може мати якісну і кількісну характеристику. Для показника AV було обрано якісну характеристику (важливість інформації), а потім цю якість прив'язано до чисельної шкали, тобто перетворено показник у кількісний: 1 – найменш важлива інформація, 2 – інформація середньої важливості, 3 – найбільш важлива.

EF – коефіцієнт дії, що показує, яка частина від вартості активу піддається ризику (втратить внаслідок події). EF також визначається за допомогою якісної шкали: 1 – мінімальний вплив, 2 – середній вплив, 3 – максимальний вплив;

F – частота виникнення небажаної події, або ймовірність виникнення збитку, й оцінюється наступним чином: 1 – низька ймовірність реалізації

(менше 25%), 2 – середня (від 25 до 60%), 3 – велика ймовірність реалізації (більше 60%).

Таблиця 2.16 – Оцінка ризику за методикою RiskWatch

| Ресурс | Загроза | AV | EF | F | ALE |
|---|---|---|---|---|---|
| Замовлення на перевезення | Знищення та копіювання | 2 | 2 | 2 | 8 |
| Наряд на автотранспорт | Відсутність доступу, втрата та копіювання | 1 | 2 | 2 | 4 |
| Маршрутний лист | Відсутність доступу, втрата | 2 | 3 | 2 | 12 |
| Реєстр рейсів | Відсутність доступу, знищення, розкриття | 3 | 3 | 2 | 18 |
| Інформація про тарифи на перевезення | Відсутність доступу, розголошення | 2 | 2 | 2 | 8 |

З наведених вище розрахунків можна зробити висновок, що найбільшу вірогідність виникнення мають ризики, які направлені на загрози відсутності доступу, знищення та розкриття інформації.

## 2.5 Розробка політики безпеки інформації

Забезпечення інформаційної безпеки ПП «Альфа Транс», організовується з урахуванням рекомендацій стандарту ISO 27001 [17], а також нормативних вимог чинного законодавства України.

Метою управління інформаційною безпекою є забезпечення принципів управління та підтримка інформаційної безпеки згідно з вимогами бізнесу та відповідними законами й нормативами.

У кваліфікаційній роботі розробка політики безпеки інформації в інформаційно-телекомунікаційній системі ПП «Альфа Транс» виконується з урахуванням вже існуючої на підприємстві політикою інформаційної безпеки, а саме: політика класифікації інформаційних активів, політика безпеки персоналу, політика захисту від шкідливого і мобільного коду, політика використання корпоративної електронної пошти, політика управління інцидентами інформаційної безпеки тощо.

Згідно з обраним у роботі стандартним функціональним профілем захищеності в АС класу 3 з підвищеними вимогами до забезпечення конфіденційності, цілісності і доступності оброблюваної інформації 3.КДЦ.1 та враховуючи включені до нього функціональні послуги (див. п.2.4), та відповідно до НД ТЗІ 2.5-005-99 [10] в процесі розробки політики безпеки інформації в інформаційно-телекомунікаційній системі підприємства необхідно приділити окрему увагу до її складових, що пов'язані із забезпеченням захисту інформації від витоку, некоректного поводження, помилкового знищення чи модифікації, забезпечення своєчасного і безперешкодного доступу до неї авторизованих користувачів і сервісів тощо.

1) Політика безпеки документів в паперовому та електронному вигляді.

Введено до експлуатації вперше.

Відповідальний – спеціаліст з інформаційної безпеки.

Власник документа: керівник відділу безпеки.

1 Опис. Політика безпеки документів створюється для гарантування того, що всі конфіденційні матеріали видаляються з робочого простору кінцевого користувача та блокуються, коли інформація не використовується.

2 Призначення. Метою цієї політики є встановлення мінімальних вимог для підтримки чистого столу щодо паперових документів і зовнішніх носіїв інформації, а також чистого екрану щодо ІТ-систем, в яких зберігається, обробляється і передається інформація, що належить підприємству. Тобто ІзОД буде знаходитися в захищеному середовищі.

3 Область застосування. Правила політики стосуються всіх працівників підприємства.

4 Політика.

4.1 Під час відсутності працівника на робочому місці не повинні бути залишені документи та фізичні носії інформації. Знімні носії інформації під час відсутності користувача повинні зберігатися у зачиненому висувному ящику.

4.2 Під час відсутності користувача, робоча станція мусить бути заблокованою.

4.3 Приміщення, в котрих зберігається ІзОД повинні бути зачинені коли не використовуються для роботи.

4.4 Роздруковані документи, що містять ІзОД, не повинні залишатися в принтері.

4.5 Документи в паперовому та електронному вигляді повинні бути належним рівнем захищені відповідно до присвоєння рівня класифікації.

4.6 Електронні і паперові документи, в яких підприємство більше не має потреби, підлягають знищенню. З цією метою власники інформаційних активів переглядають їхню значимість і придатність регулярно, з періодичністю не рідше одного разу на рік. Власники інформаційних ресурсів також повинні брати до уваги мінімальний термін зберігання електронних і паперових документів, визначений законодавством.

4.7 Методи знищення електронних і паперових документів визначаються відділом ІБ. Методи знищення документів повинні гарантувати неможливість їх повторного використання.

5 Політика відповідальності.

Керівництво підприємства зобов'язане попередити співробітників про відповідальність та дисциплінарні заходи у разі невиконання правил ПБІ.

2) Політика використання глобальної мережі Інтернет

Введено до експлуатації вперше.

Відповідальний – спеціаліст з інформаційної безпеки.

Власник документа: керівник відділу безпеки.

1 Опис. Правила користування глобальною мережею Інтернет.

2 Призначення. Запобігання зараження вірусним ПО, витоку конфіденційної інформації, захисту від небажаних повідомлень, що масово розсилаються.

3 Область застосування. Правила політики стосуються всіх працівників підприємства.

4 Політика.

4.1 Доступ до мережі Інтернет повинен бути організований лише з використанням засобів доступу і захисту, авторизованих на підприємстві.

4.2 Доступ в Інтернет здійснюється тільки за допомогою авторизованого в на підприємстві провайдера.

4.3 Електронна пошта повинна використовуватися тільки для забезпечення цілей бізнесу, в службової необхідності, і не повинна використовуватися в будь-яких інших цілях.

4.4 Доступ працівників до електронної пошти повинен бути узгоджений з відділом інформаційної безпеки.

4.5 Механізми захисту повинні забезпечувати належний рівень конфіденційності, цілісності і доступності, відповідно до системи класифікації інформаційних активів.

5 Політика відповідальності.

Керівництво підприємства зобов'язане попередити співробітників про відповідальність та дисциплінарні заходи у разі невиконання правил ПБІ.

3) Політика забезпечення безперервності діяльності підприємства.

Введено до експлуатації вперше.

Відповідальний – системний адміністратор.

Власник документа: керівник відділу ІТ.

1 Опис. Визначити вимоги для належного рівня інформаційної безпеки в разі повної або часткової втрати даних.

2 Призначення. Запобігання фінансовим збиткам підприємства у разі припинення основного бізнес-процесу.

3 Область застосування. Правила політики стосується працівників відділу інформаційних технологій підприємства.

4 Політика.

4.1 Визначити перелік інформації, що підлягає резервному копіюванню.

4.2 Розробити і затвердити процедури резервного копіювання інформації, яка зберігається, передається і обробляється в IT-системах підприємства, щодо періодичності проведення резервного копіювання, місця і періодичності зберігання резервних копій.

4.3 Визначити періодичність проведення тестового відновлення даних з резервних копій.

4.4 Встановити резервне обладнання (сервер баз даних) для запобігання припинення бізнес-процесу в разі відмови основного обладнання.

4.5 Встановити програмне забезпечення для роботи з резервним обладнанням.

4.6 Назначити відповідальних співробітників з запуску резервного обладнання і забезпечити їх навчання.

## 2.6 Аналіз інформаційних ризиків після впровадження політики безпеки

Проведемо оцінку інформаційних ризиків після впровадження ПБІ на підприємстві за допомогою використаної методики RiskWatch [16]. Результати оцінки наведені у таблиці 2.17.

Таблиця 2.17 – Оцінка ризику за методикою RiskWatch після впровадження політики безпеки інформації

| Ресурс | Загроза | AV | EF | F | ALE |
|---|---|---|---|---|---|
| Замовлення на перевезення | Знищення та копіювання | 2 | 2 | 1 | 4 |
| Наряд на | Відсутність доступу, | 1 | 2 | 1 | 2 |

| | | | | | |
|---|---|---|---|---|---|
| автотранспорт | втрата та копіювання | | | | |
| Маршрутний лист | Відсутність доступу, втрата | 2 | 3 | 1 | 6 |
| Реєстр рейсів | Відсутність доступу, знищення, розкриття | 3 | 3 | 1 | 9 |
| Інформація про тарифи на перевезення | Відсутність доступу, розголошення | 2 | 2 | 1 | 4 |

Можна зробити висновок, що після впровадження ПБІ вдалося знизити очікуваний річний збиток (ALE) в 2 та більше разів. Порівняння очікуваних річних збитків до та після впровадження політики безпеки інформації наведено у таблиці 2.18.

Таблиця 2.18 – Порівняння очікуваних річних збитків до та після впровадження політики безпеки інформації

| Ресурс | Збитки до впровадження політики безпеки інформації, ALE | Збитки після впровадження політики безпеки інформації, $ALE_1$ |
|---|---|---|
| Замовлення на перевезення | 8 | 4 |
| Наряд на автотранспорт | 4 | 2 |
| Маршрутний лист | 12 | 6 |
| Реєстр рейсів | 18 | 9 |
| Інформація про тарифи на перевезення | 8 | 4 |

Отже, можна зробити висновок, що впровадження політики безпеки інформації можна вважати доцільним з точки зору зниження вірогідності реалізації ризиків.

## 2.7 Висновок

У другому розділі було проведено аналіз фізичного середовища, опис компонентів АС та отримано дані про найцінніші ресурси інформаційно-телекомунікаційної системи Приватного підприємства «ПП «Альфа Транс»

Також, для підприємства був обраний функціональний профіль захищеності автоматизованої системи, був проведений аналіз інформаційних ризиків з ранжуванням джерел вразливостей та загроз, була зроблена оцінка інформаційних ризиків за допомогою методики RiskWatch.

З метою зниження вірогідності реалізації найнебезпечніших інформаційних ризиків була створена політика безпеки інформації.

Приведено повторний аналіз інформаційних ризиків після впровадження політики безпеки інформації, який обгрунтував доцільність її впровадження і створив порівняльну характеристику оцінок інформаційних ризиків до і після впровадження ПБІ.

# РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

## 3.1 Обґрунтування витрат на розробку політики безпеки інформації

Як показав приведений після впровадження ПБІ аналіз інформаційних ризиків, ПБІ доцільно розробляти та впроваджувати задля суттєвого зниження вірогідності реалізації небезпечних ризиків, підвищення рівня безпеки інформації в ІТС та захищеності цінних інформаційних ресурсів. Не дивлячись на складність розробки та впровадження ПБІ, це поміркований крок для забезпечення безпеки інформації на довгострокову перспективу.

## 3.2 Розрахунки витрат на розробку політики безпеки інформації

### 3.2.1 Розрахунок капітальних (фіксованих) витрат

Капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

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

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

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

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

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

$К_{пр}$ = 7500 грн (вартість розробки проекту інформаційної безпеки та залучення зовнішніх консультантів);

$К_{зпз}$ = 12200 грн (вартість закупівлі Windows Server 2019 );

$К_{аз}$ = 39600 грн (вартість закупівлі файлового серверу);

$К_н$ = 100 грн (витрати на встановлення обладнання та налагодження системи інформаційної безпеки)

Підрахуємо капітальні витрати:

$$К = 7500 + 12200 + 39600 + 100 = 59400 \text{ грн}$$

3.2.2 Розрахунок річних поточних (експлуатаційних) витрат

Річні поточні (експлуатаційні) витрати складаються з наступних витрат:

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

де $С_а$ – річний фонд амортизаційних відрахувань;

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

$$С_{ел} = Р \text{ х } F_р \text{ х } Ц_е, \qquad (3.3)$$

де Р – встановлена потужність апаратури інформаційної безпеки, кВт;

$F_р$ – річний фонд робочого часу системи інформаційної безпеки;

$Ц_е$ – тариф на електроенергію, грн./кВт годин;

$С_о$ – витрати на залучення сторонніх організацій для навчання співробітників компанії за допомогою запрошення спеціалістів інформаційної безпеки, які організовують створення політики безпеки;

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

Са – річний фонд амортизаційних відрахувань, складає 25%;

$$Са = К \text{ х } 0,25 = 59400 \text{ х } 0,25 = 14850 \text{ грн};$$

$С_е$ – вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року (Р файлового серверу = 0.665 кВт, Fр = 8736 робочих годин (робота цілодобово), $Ц_е$ = 1,44 грн);

$$С_{ел} = Р \times F_р \times Ц_е = 0.665 \times 8736 \times 1.44 = 8365{,}59 \text{ грн};$$

$$С_0 = 7000 \text{ грн}$$

$С_{тос}$ – витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки, визначаються ПП «Альфа Транс» і становлять 3% від вартості капітальних витрат.

$$С_{тос} = К \times 0{,}03 = 59400 \times 0{,}03 = 1782 \text{ грн};$$

Підрахуємо річні поточні (експлуатаційні) витрати:

$$С = С_а + С_{ел} + С_0 + С_{тос} = 14850 + 8365{,}59 + 7000 + 1782 = 31997{,}59 \text{ грн};$$

### 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 корпоративної мережі, грн;

V – втрати від зниження обсягу надання послуг на перевезення за час простою файлового сервера корпоративної мережі, грн.

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

$$П_п = \frac{\sum З_с * Ч_с}{F} \cdot t_п \ , \qquad (3.5)$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 160-176 ч).

$З_с$ – 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 за місяць з нарахуванням єдиного соціального внеску наведено в таблиці 3.1.

Таблиця 3.1 – Витрати на заробітну плату за місяць з нарахуванням єдиного соціального внеску

| Посада | Кількість співробіт-ників, осіб | Місячна заробітна плата, грн | Витрати на заробітну плату, грн | Єдиний соціальний внесок, грн | Витрати на заробітну плату з урахуванням ЄСВ, грн |
|---|---|---|---|---|---|
| Ведучій спеціаліст з планування автотранспорту | 2 | 11 000 | 22 000 | 4 840 | 26 840 |
| Спеціаліст з планування автотранспорту | 12 | 8 000 | 96 000 | 21 120 | 117 120 |
| Спеціаліст з організації перевезень | 1 | 10 000 | 10 000 | 2 200 | 12 200 |

| | |
|---|---|
| Всього | 156 160 |

$$П_{п} = 156160 / 168 * 3 = 2788,57 \text{ грн}$$

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

$$П_{ви} = \frac{\sum З_{с} * Ч_{с}}{F} \cdot t_{ви} \ , \quad (3.7)$$

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

$$П_{ви} = 156160 /168 * 4 = 3718,10 \text{ грн}$$

Витрати на відновлення файлового сервера корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_{в}$ і розміром середньогодинної заробітної плати системного адміністратора:

$$П_{пв} = \frac{\sum З_о * Ч_о}{F} \cdot t_в \ , \qquad (3.8)$$

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

$Ч_о$ – чисельність персоналу, осіб;

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

Розрахунок витрат на заробітну плату системного адміністратора з нарахуванням ЄСВ:

$$З_{о1} = 16200 + 16200*022 = 19764 \text{ грн}$$

Розрахунок витрат на заробітну плату спеціаліста ІТ з нарахуванням ЄСВ:

$$З_{о2} = 10000+10000 * 0,22 = 12200 \text{ грн}$$

$$П_{ПВ} = (19764 + 12200 ) / 168 *2 =380,52 \text{ грн}$$

$$П_{В} = 3718,10 + 380,52 + 0 =4098,62 \text{ грн}$$

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:

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

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

О – обсяг чистого прибутку/дохід від реалізації/ атакованого вузла або сегмента корпоративної мережі, грн у рік, або оподаткований прибуток атакованого вузла або сегмента корпоративної мережі;

$$V = 4000000 / 2080 *(3 + 4 + 2) = 17307,69 \text{ грн}$$

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

$$U = П_п + П_в + V = 2788,57 + 4098,62 + 17307,69 = 24194,88 \text{ грн}$$

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

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

де I – число атакованих вузлів корпоративної мережі;

N – середнє число можливих атак на рік.

$$B = 24194,88 * 6 * 1 = 145169,30 \text{ грн}$$

## 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:

$$E = B \cdot R - C, \quad (3.11)$$

де $B$ – загальний збиток від атаки на вузол або сегмент корпоративної мережі, тис. грн;

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

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

$$E = 145169,30 * 0,5 - 31997,59 = 40587,06 \text{ грн}$$

## 3.5 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

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

а) коефіцієнт повернення інвестицій у сфері інформаційної безпеки 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.

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

де ROSI – коефіцієнт повернення інвестицій, частки одиниці;

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

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

$$ROSI = 40587,06 / 59400 = 0,68$$

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

$$T_o = \frac{K}{E} = \frac{1}{RC} \qquad (3.13)$$

де $T_o$ – термін окупності капітальних інвестицій, років.

$T_o$ = 59400 / 40587,06 =1,46 років, що становить 1 рік 6 місяців

## 3.6 Висновок

В цьому розділі проаналізовано доцільність впровадження політики інформаційної безпеки на підприємстві. Визначено її економічну ефективність.

Розраховано капітальні та експлуатаційній витрати на впровадження інформаційної політики безпеки, які склали 59400 грн. та 31997,59 грн. відповідно.

Загальний збиток від атаки на підприємство через упущену вигоду складає 145169,30 грн.

Термін окупності капітальних інвестицій складає 1 рік і 6 місяців.

Отже, економічна доцільність обґрунтована і впровадження інформаційної політики безпеки може бути ефективною та успішною.

# ВИСНОВКИ

В першій частині був проаналізований стан справ України та світу щодо питання безпеки інформації, були наведені статистичні дані та приклади інцидентів витоку інформації з обмеженим доступом.

Була створена обґрунтована основа розробки політики безпеки інформації на приватному підприємстві «Альфа Транс».

В спеціальній частині були проведені обстеження ПП «Альфа Транс», створено класифікацію інформації, що циркулює на підприємстві, та ранжування ризиків та загроз найціннішим інформаційним ресурсам підприємства, був обраний функціональний профіль захищеності автоматизованої системи підприємства.

Були проаналізовані та оцінені інформаційні ризики, які пов'язані з найбільш вагомими вразливостями та загрозами інформаційно-телекомунікаційної системи. Оцінка виконувалась за допомогою методики RiskWatch.

Для мінімізування ймовірності виникнення та реалізації інформаційних ризиків, була розроблена політика безпеки інформації ПП «Альфа Транс», яка складається з документів «Політика безпеки документів в паперовому та електронному вигляді», «Політика використання глобальної мережі Інтернет», «Політика забезпечення безперервності діяльності підприємства».

Була проведена повторна оцінка інформаційних ризиків після впровадження ПБІ та наведена порівняльна характеристика показників для наочного відображення доцільності створення ПБІ.

В економічній частині були проведені розрахунки капітальних (фіксованих) та річних поточних (експлуатаційних) витрат на розробку та впровадження політики безпеки інформації, загальний збиток від атаки на підприємство, а також оцінка економічної ефективності системи захисту інформації.

# ПЕРЕЛІК ПОСИЛАНЬ

1. Легомінова С. В. Теоретичні засади інформаційної безпеки підприємства / С. Легомінова // Економіка. Менеджмент. Бізнес. – 2015. – № 3 – С. 87-92.

2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» // Відомості Верховної Ради України. – 1994. – № 31.

3. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою Кабінету Міністрів України від 29.03.2006 № 373 // Офіційний вісник України. – 2006. – № 13.

4. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-003-99. [Чинний від 1999.04.28]. – К. : ДСТСЗІ СБУ, 1999. – (Нормативний документ системи технічного захисту інформації).

5. Литвинюк, А. А. Основи інформаційної безпеки. Комплексна система захисту інформації: структура, встановлення та підтримка функціонування// А. А. Литвинюк.— [Електронний ресурс].— Режим доступу: http://www.cvk.gov.ua/visnyk/pdf/2008_4/visnik_st_08.pdf.

6. Юдін О.К. Інформаційна безпека. Нормативно-правове-забезпечення: Підручник. - К.: Вид-во Видавництво Національного авіаційного університету «НАУ-друк», 2011. - 640 с.

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

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

9. Загальні положення з захисту інформації в комп'ютерних системах від НСД: НД ТЗІ 1.1-002-99. — [Чинний від 1999.04.28]. — К. : ДСТСЗІ СБУ, 1999 — № 22. — (Нормативний документ системи технічного захисту інформації).

10. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу: НД ТЗІ 2.5-005-99. – [Чинний від 1999.04.28]. – К. : ДСТСЗІ СБУ, 1999. – № 22. – (Нормативний документ системи технічного захисту інформації).

11. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5-004-99. — [Чинний від 1999.04.28]. — К. : ДСТСЗІ СБУ, 1999. — № 22. — (Нормативний документ системи технічного захисту інформації).

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

13. Про захист інформації в автоматизованих системах: Закон України від 05.07.1994 № 81/94-ВР//ВВР. 1994. — № 31. — С. 287.

14. Типове положення про службу захисту інформації в автоматизованій системі: 1.4-001-2000. — [Чинний від 2000.12.04]. — К. : ДСТСЗІ СБУ, 2000. — № 53.— (Нормативний документ системи технічного захисту інформації).

15. 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", [Електронний ресурс]. – Режим доступу http://www.dsszzi.gov.ua/dsszzi/control/uk/publisharticle?art_id=890&cat_id=94

16. Пузиренко О. Г. Застосування моделей оцінювання ризиків інформаційної безпеки в інформаційно-телекомунікаційних системах /О.Г. Пузиренко, С.О. Івко, О.О. Лаврут, О.К. Климович // Системи обробки

інформації. – 2015. – №3. – С.75 – 79. [Електронний ресурс]. – Режим доступу http://www.hups.mil.gov.ua/periodic-app/article/12129/soi_2015_3_17.pdf

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

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

| № | Формат | Найменування | Кількість листів | Примітка |
|---|---|---|---|---|
| 1 | А4 | Реферат | 3 | |
| 2 | А4 | Список умовних скорочень | 1 | |
| 3 | А4 | Зміст | 2 | |
| 4 | А4 | Вступ | 1 | |
| 5 | А4 | 1 Розділ | 12 | |
| 6 | А4 | 2 Розділ | 37 | |
| 7 | А4 | 3 Розділ | 9 | |
| 8 | А4 | Висновки | 1 | |
| 9 | А4 | Перелік посилань | 3 | |
| 10 | А4 | Додаток А | 1 | |
| 11 | А4 | Додаток Б | 1 | |
| 12 | А4 | Додаток В | 1 | |
| 13 | А4 | Додаток Г | 1 | |

# ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

Презентація.pptx

# ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

# ДОДАТОК Г. ВІДГУК
на кваліфікаційну роботу бакалавра на тему:
Розробка політики безпеки інформації для інформаційно-комунікаційної системи приватного підприємства "Альфа Транс"
ст. гр. 125-18-3 Черкаського Давида Олександровича

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

Об'єкт досліджень: інформаційно-телекомунікаційна система приватного підприємства «Альфа Транс».

Мета: розробка та впровадження політики безпеки інформації в інформаційно-телекомунікаційній системі приватного підприємства «Альфа Транс».

В першому розділі проведено розгляд ситуації в галузі інформаційної безпеки, обґрунтовано важливість та актуальність розробки політики безпеки інформації на підприємстві. Виконано аналіз нормативно-правової бази у сфері захисту інформації. Виділені основні закони, нормативні документи та державні стандарти, що мають бути застосовані в процесі створення політики безпеки інформації на підприємстві.

В спеціальній частині приведено загальна характеристика підприємства, розроблено модель загроз, проведено аналіз та оцінка ризиків інформаційної безпеки, розроблено основні положення політики безпеки інформації.

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

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

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

Керівник