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

**Інститут електроенергетики**
**Факультет інформаційних технологій**
**Кафедра безпеки інформації та телекомунікацій**

# ПОЯСНЮВАЛЬНА ЗАПИСКА
## кваліфікаційної роботи ступеня бакалавра

**студента** *Бурдюгова Микити Олександровича*

**академічної групи** *125-20-1*

**спеціальності** *125 Кібербезпека*

**спеціалізації**[1]

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

**на тему** *Розробка політики безпеки інформації інформаційно-комунікаційної системи ТОВ «ТоргСервіс»*

| Керівники | Прізвище, ініціали | Оцінка за шкалою | | Підпис |
|---|---|---|---|---|
| | | рейтинговою | інституційною | |
| кваліфікаційної роботи | к.т.н., доц. Ковальова Ю.В. | | | |
| розділів: | | | | |
| спеціальний | к.т.н., доц. Ковальова Ю.В. | | | |
| економічний | к. е. н., доц. Пілова Д.П. | | | |

| | | | | |
|---|---|---|---|---|
| **Рецензент** | | | | |

| | | | | |
|---|---|---|---|---|
| **Нормоконтролер** | ст. викл. Мєшков В.І. | | | |

**Дніпро**
**2024**

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

«_____»_____20___року

# ЗАВДАННЯ
## на кваліфікаційну роботу ступеня бакалавра

**студенту** ***Бурдюгову М.О.*** **академічної групи** ***125-20-1***
(прізвище та ініціали) (шифр)

**спеціальності** ***125 Кібербезпека***

**спеціалізації**

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

**на тему** ***Розробка політики безпеки інформації інформаційно-комунікаційної системи ТОВ «ТоргСервіс»***

Затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № _____

| Розділ | Зміст | Термін виконання |
|---|---|---|
| 1 | Стан питання, аналіз нормативно-правової бази, постановка задачі. | 26.05.2024 |
| 2 | Розробка політики безпеки інформації, визначення профілю захищеності, аналіз загроз. | 19.06.2024 |
| 3 | Розрахунок річних витрат на розробку політики безпеки, оцінка величини збитку. Розрахунок ефективності. | 26.06.2024 |

Завдання видано _____ Ковальова Ю.В.
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: 06.05.2024

Дата подання до екзаменаційної комісії: 01.07.2024

Прийнято до виконання _____ Бурдюгов М.О.
(підпис студента) (прізвище, ініціали)

# РЕФЕРАТ

Пояснювальна записка містить 100 сторінок, 8 рисунків, 22 таблиці, 4 додатки, 20 джерел.

Об'єкт розробки: політика безпеки інформації інформаційно-комунікаційної системи.

Мета кваліфікаційної роботи: підвищення рівня інформаційної безпеки ІКС ТОВ «ТоргСервіс».

В першому розділі кваліфікаційної роботи визначено актуальність роботи, проаналізовано стан питання інформаційної безпеки в ІКС, визначено основні проблеми захисту інформації та шляхи їх вирішення. Виконано аналіз нормативно-правової бази у сфері захисту інформації.

У спеціальній частині роботи було виконано обстеження об'єкту інформаційної діяльності, проаналізовано інформаційні потоки, проведено аналіз загроз та вразливостей системи, побудувана модель порушника. Також обґрунтовано вибір стандартного функціонально профіля захищеності та розроблено інструкції політики безпеки.

В економічній частині було розраховані витрати на розробку та впровадження політики безпеки інформації інформаційно-комунікаційної системи ТОВ «ТоргСервіс».

Практична цінність кваліфікаційної роботи полягає у підвищенні рівня інформаційної безпеки та зниженні ризиків завдяки впровадженню запропонованої політики безпеки інформації інформаційно-комунікаційної системи підприємства.

ІНФОРМАЦІЙНА БЕЗПЕКА, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ПОЛІТИКА БЕЗПЕКИ ІНФОРМАЦІЇ.

# ABSTRACT

The explanatory note consists of 100 pages, 8 images, 22 tables, 4 appendices, 20 sources.

Object of development: the information security policy of the information and communication system.

The purpose of the qualification work: to increase the level of information security of the ICS of the TorgService LLC.

In the first part of the qualification work, the relevance of the work is determined, the state of the information security issue in ICS is analyzed, the main problems of information protection and ways to solve them are determined. The analysis of the legal framework in the field of information protection was carried out.

In the special part of the work, an inspection of the object of information activity was carried out, information flows were analyzed, an analysis of system threats and vulnerabilities was carried out, and user violator model was built. The choice of a standard functional security profile is also justified and security policy instructions are developed.

In the economic part, the costs for the development and implementation of the information security policy of the information and communication system of TorgService LLC were calculated.

The practical value of the qualification work is to increase the level of information security and reduce the risks of information security due to the implementation of information security policy.

INFORMATION SAFETY, MODEL OF THREATS, USER VIOLATOR MODEL, INFORMATION SECURITY POLICY.

# СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ДФ – дестабілізуючі фактори;

ІБ – інформаційна безпека;

ІзОД – інформація з обмеженим доступом;

ІКС – інформаційно-комунікаційна система;

ІС – інформаційна система;

ІТ – інформаційні технології;

КЗЗ – комплекс засобів захисту;

КСЗІ – комплексна система захисту інформації;

КТЗІ – комплекс технічного захисту інформації;

НД – нормативний документ;

НСД – несанкціонований доступ;

ОІД – об’єкт інформаційної діяльності;

ПБ – політика безпеки;

ТЗІ – технічний захист інформації;

ФПЗ – функціональні послуги захисту;

DBF – Database Firewall;

DLP – Data Leak Prevention.

# ЗМІСТ

# ВСТУП

Розвиток глобального процесу інформатизації суспільства, що спостерігається в останні десятиліття, спричинив нову глобальну проблему – інформаційну безпеку. Багато найважливіших інтересів підприємства в даний час значною мірою визначається станом навколишнього інформаційного середовища. Цілеспрямовані або ненавмисні впливи на інформаційну сферу з боку зовнішніх або внутрішніх джерел можуть завдавати серйозної шкоди цим інтересам і становлять загрози та ризики для безпеки. Тому інформаційна безпека в сучасних умовах є однією з необхідних умов нормального функціонування підприємства.

Усе більш очевидною стає залежність загального рівня економічної безпеки підприємства від інформаційної складової. Практика показує, що будь-яка недружня акція, спрямована проти інтересів господарського суб'єкта, починається зі збору інформації: навіть дрібне розкрадання звичайно випереджає вивчення особою зі злочинними задумами можливості протиправних дій, і без відповідного інформаційного забезпечення не представляються такі деструктивні прояви, як відведення активів підприємства або рейдерське захоплення.

Невипадково питання інформаційної безпеки вже давно входять до головних пріоритетів практично всіх великих компаній. Останнім часом більше керівників середнього і малого вітчизняного бізнесу починають усвідомлювати реальну небезпеку ризиків, пов'язаних з інсайдерською інформацією, системами її обробки і співробітниками, що беруть участь у цьому процесі.

# РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

## 1.1 Стан питання

Статистика у сфері інформаційної безпеки свідчить, що близько 80% зловмисників належить до інсайдерів. У компаніях телекомунікаційної галузі на їх дії припадає близько 90% фінансових втрат.

Людський фактор завжди був і є одним із найважливіших ризиків будь-якого бізнесу, оскільки більшість інцидентів відбуваються саме з вини співробітників. Навмисний відплив часто важко відрізнити від ненавмисного, однак це не завжди потрібно, оскільки наслідки для підприємства при будь-якому із цих варіантів можуть бути катастрофічними. Те, що більшість керівників не знають джерел внутрішніх загроз, говорить про те, що бізнесом приділяється недостатньо уваги інформаційній безпеці, що, утім, є одним із найважливіших факторів існування підприємства. Аналіз, проведений на підприємствах середнього бізнесу, показав, що випадкові кібератаки виникають частіше і потенційно можуть нашкодити більше, ніж навмисні атаки інсайдерів. У результаті дослідження з'ясовано, що більшість підприємств приділяють набагато більше уваги захисту від навмисних внутрішніх атак, ніж від більш частих і потенційно більш руйнівних випадкових внутрішніх інцидентів.

Поза увагою залишаються питання потенційних внутрішніх ризиків, що виходять від співробітників, які мають доступ до критично важливих систем і секретної інформації. Хоча керівники усвідомлюють існування таких ризиків, турбота про зовнішню інформаційну безпеку часто переважує інші питання. Але значною є кількість порушень та випадків несанкціонованого доступу і використання інформації самими співробітниками, що ставить під загрозу основу бізнесу багатьох підприємств.

Із 500 керівників підприємств у сфері IT, що брали участь у дослідженні, більшість відзначили, що вони не знають джерел і причин виникнення внутрішніх загроз. При цьому підприємства намагаються оцінити потенційний фінансовий збиток від цих загроз та їх вплив на операційну діяльність. Половина опитаних

упевнені, що більшість внутрішніх загроз створюється ненавмисно, 20% вважають загрози навмисними, 25%, – що навмисних і ненавмисних загроз приблизно нарівно, 5% утруднилися з відповіддю. Однак у пункті, де пропонувалося перелічити найбільші загрози за їх важливістю, майже 85% респондентів не могли точно сказати, чи були навмисними або випадковими внутрішні інциденти, спровоковані підрядчиками або тимчасовими співробітниками.

Дослідження також показало, що приблизно раз на місяць на підприємствах трапляється один інцидент, який можна віднести до одного з 10 можливих типів загроз. Більше за все відбувається випадків ненавмисної втрати даних через недбалість співробітників – таких інцидентів відбувається 15-20 на рік. Внутрішні зловмисні атаки і шпигунство – 10 випадків на рік, зловживання доступом до інформації – 20 випадків на рік. Якщо говорити про сферу діяльності, то на досліджуваних підприємствах відбувається до 20-30 інцидентів щорічно. Результати дослідження свідчать, що універсального рішення для усунення внутрішніх ризиків не існує. Кожне підприємство має виробити власний комплексний підхід з урахуванням особливостей структури і специфіки діяльності [1].

Хоча навмисних атак зловмисників стає все більше, практика показує, що випадкові помилки, неуважність до правил безпеки впливають на діяльність підприємства набагато більше, ніж атаки шахраїв.

Фахівці у сфері інформаційної безпеки дотримуються двох думок. Перша полягає у наступному: інформаційною безпекою на підприємстві можна взагалі не займатися, не витрачаючи коштів. У цьому випадку не виключений такий варіант, що прийнятий ризик себе цілком виправдає. Другий погляд: необхідно витратити на створення системи захисту інформації чимало грошей (навчання персоналу, програмне забезпечення тощо) і тим самим забезпечити належний рівень безпеки. Але при цьому також залишиться деяка вразливість, що рано або пізно призведе до відпливу або розкрадання конфіденційної інформації.

В обґрунтуванні витрат на інформаційну безпеку можна використати нижченаведений підхід. Необхідно застосувати на практиці інструментарій визначення рівня інформаційної безпеки. Керівництво підприємства залучається до оцінки вартості інформаційних ресурсів, визначення оцінки потенційного збитку від порушень інформаційної безпеки. Від результатів цих оцінок буде багато в чому залежати подальша діяльність керівників у сфері інформаційної безпеки. Якщо інформація нічого не коштує, істотних загроз для інформаційних активів немає, а потенційний збиток мінімальний, то проблемою забезпечення інформаційної безпеки можна не займатися. Якщо ж інформація має значну вартість, загрози і потенційний збиток ясні, тоді постає питання про внесення в бюджет витрат на підсистему інформаційної безпеки. У цьому випадку слід заручитися підтримкою керівництва підприємства в усвідомленні проблем інформаційної безпеки й побудові системи захисту інформації.

Надійно гарантувати бізнес від перерахованих негативних явищ можна тільки на основі формування ефективної системи забезпечення інформаційної безпеки. Однак тут існують певні проблеми, що належать, швидше за все, до організаційно-фінансових. Першою і найбільшою проблемою у створенні системи інформаційної безпеки є відсутність розуміння в керівництва необхідності створення такої системи. Багато керівників підприємств не усвідомлюють, що створювати систему інформаційної безпеки просто необхідно, бо своєчасне створення її позбавить підприємство збитків, а іноді навіть і врятує бізнес [2].

Друга проблема при створенні системи інформаційної безпеки – відсутність достатньої кількості фінансових коштів. Відсутність фінансування з мінімального бюджету для створення системи інформаційної безпеки зустрічається також дуже часто. Приміром, у США і країнах Євросоюзу на створення системи інформаційної безпеки і підтримку її в актуальному стані виділяється від 30% прибутку компанії. В Україні ж якщо фінанси і виділяються, то одноразово й у недостатній кількості. Їх може вистачити хіба що на продовження ліцензії на антивірусні програми. І лише деякі підприємства, які можна вважати скоріше

винятком із правил, планують і приймають бюджет своєї системи інформаційної безпеки виходячи з реальних потреб.

Третьою найнебезпечнішою проблемою є ситуація, коли є розуміння керівництва та необхідні кошти, але створення системи інформаційної безпеки доручають фахівцям, що не мають ані відповідної освіти, ані достатнього досвіду. Найчастіше це бувають системні адміністратори або відділ технічної підтримки. Вони, у свою чергу, розцінюють це як установку і налаштування антивірусу. Наявність внутрішнього зловмисника, найчастіше, узагалі не береться до уваги. Відповідно до статистики 70% порушень здійснюється внутрішніми зловмисниками. Ще частіше без належної уваги залишаються канали зв'язку, і переписка керівництва підприємства з діловими партнерами, із клієнтами стає незахищеною. У результаті таких дій кошти витрачені, а інформаційна безпека на колишньому рівні.

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

При створенні ефективної системи забезпечення інформаційної безпеки підприємства, одну з важливих ролей виконує нормативно-правова база України.

Нормативна база інформаційної безпеки повинна виконувати в першу чергу три основні функції:

1 Регулювати взаємовідносини між суб'єктами інформаційної безпеки, визначати їх права, обов'язки та відповідальність.

2 Нормативно забезпечувати дії суб'єктів інформаційної безпеки на всіх рівнях, а саме - людини, суспільства, держави.

3 Встановлювати порядок застосування різних сил і засобів забезпечення інформаційної безпеки.

Першим розглянемо Закон України «Про інформацію» [3]. Він установлює загальні правові основи одержання, використання, поширення та зберігання інформації, закріплює право особи на інформацію в усіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначає статус учасників інформаційних відносин, регулює доступ до інформації та забезпечує її охорону, захищає особу і суспільство від неправдивої інформації.

Закон визначає інформацію як документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому середовищі. Відповідно об'єктами інформаційних відносин є документована або публічно оголошувана інформація про події та явища в галузі політики, економіки, культури, охорони здоров'я, а також у соціальній, екологічній, міжнародній та інших сферах.

Усі громадяни України, юридичні особи та державні органи мають право на інформацію. Але реалізація права на інформацію громадянами, юридичними особами і державою не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб.

Положення Закону України «Про інформацію» конкретизуються в інших законах про інформаційну діяльність та охорону прав інтелектуальної власності, які мають більш конкретний характер, а також у низці інших законодавчих і нормативних актів.

Наступний закон, що регулює суспільні відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-комунікаційних системах з метою забезпечення дотримання права власності фізичних і юридичних осіб на інформацію та їх права доступу до неї, а також права власника інформації на її захист, є Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [4] .

Згідно цього закону, об'єктами захисту є інформація, що обробляється в ІС, права власників цієї інформації і власників ІС, права користувача. Захисту підлягає будь-яка інформація в ІС, необхідність захисту якої визначається її власником або чинним законодавством.

Доступ до інформації, яка зберігається, обробляється і передається в ІС, здійснюється лише відповідно до правил розмежування доступу, встановлених власником інформації або уповноваженим їм особою. Без дозволу власника доступ до інформації, яка обробляється в ІС, здійснюється лише у випадках, передбачених чинним законодавством.

Власник ІС повинен забезпечити захист інформації згідно вимогам і правилам, обумовлюваною угодою з власником інформації або уповноваженим їм особою, і зобов'язаний повідомити його про всі факти порушення її захисту. Власник інформації має право контролювати дотримання вимог по захисту інформації і забороняти або припиняти обробку інформації у разі порушення цих вимог.

Власник інформації і уповноваженим їм на те особи визначають користувачів інформації, що належить йому, і встановлюють їх повноваження. Власник ІС дає користувачам можливість доступу до інформації, що обробляється в ІС, згідно повноваженням, встановленим власником інформації. Розпорядник ІС інформує власника інформації про технічні можливості захисту в його ІС і типових правилах, встановлених для персоналу ІС.

Закон України «Про телекомунікації» встановлює правову основу діяльності у сфері телекомунікацій. Закон визначає повноваження держави щодо управління та регулювання зазначеної діяльності, а також права, обов'язки та засади відповідальності фізичних і юридичних осіб, які беруть участь у даній діяльності або користуються телекомунікаційними послугами [5].

Наступний закон – Закон України «Про захист персональних даних», регулює правові відносини, пов’язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв’язку з обробкою персональних даних [6].

Цей Закон поширюється на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів, а також на обробку персональних даних, що містяться у картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів.

Закон України «Про доступ до публічної інформації» [7] визначає порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників

публічної інформації, визначених цим Законом, та інформації, що становить суспільний інтерес.

Для встановлення основних організаційно-правових засад електронного документообігу та використання електронних документів потрібно прийняти до уваги Закон України «Про електронні документи та електронний документообіг»

Наступною важливою складовою є нормативні документи системного технічного захисту інформації. НД ТЗІ 2.5-001-99 «Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту» [8]. Цей нормативний документ (НД) містить специфікації функціональних послуг захисту (ФПЗ) інформаційних ресурсів АТС, а також специфікації рівнів стійкості механізмів захисту інформації, які ці ФПЗ реалізують. Дія цього документу поширюється на програмно-керовані АТС, що функціонують на мережі електрозв'язку загального користування, а також у складі відомчих (корпоративних, установчих) приводних телефонних мереж, у яких зберігається та циркулює інформація, що підлягає технічному захисту.

Документ призначений для замовників, розроблювачів, виготовлювачів і постачальників АТС, операторів мереж електрозв'язку загального користування національного, регіонального і місцевого рівнів, юридичних осіб – власників і користувачів АТС, а також організацій і підприємств, що здійснюють оцінку захищеності інформації на АТС від НСД, витоків і спеціальних впливів через технічні канали. Вимоги цього НД є обов'язковими для підприємств, організацій, юридичних осіб, діючих на терені України незалежно від їх форм власності та відомчої підпорядкованості, які здійснюють діяльність, пов'язану з розробкою, виготовленням, експлуатацією АТС, а також проводять оцінку захищеності інформації на АТС від НСД, витоків та спеціальних впливів через технічні канали.

НД ТЗІ 2.5-002-99 «Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту» [9]. Цей нормативний документ (НД) установлює вимоги до гарантій захисту інформації,

що циркулює на програмно - керованих АТС загального користування, а також на установчих (відомчих, корпоративних) АТС.

Положення НД поширюються на програмно-керовані АТС (далі - АТС), у яких зберігається та циркулює інформація, що підлягає технічному захисту

Захист елементів АТС від фізичного доступу, ушкоджень, розкрадань і підмін у цьому НД розглядається в загальному вигляді і лише як необхідна обмежувальна міра в процесі здійснення заходів щодо ТЗІ. Передбачається, що вжиті заходи щодо обмеження фізичного доступу до зони станційного устаткування достатні, щоб виключити можливість несанкціонованого доступу (НСД) в цю зону неуповноважених осіб.

Документ призначений для замовників, розроблювачів, виготовлювачів і постачальників АТС, операторів зв'язку національного, регіонального і місцевого рівнів, юридичних осіб - власників і користувачів АТС, а також для організацій і підприємств, що здійснюють оцінку захищеності інформації на АТС від НСД, витоків і спеціальних впливів через технічні канали.

Вимоги цього НД є обов'язковими для підприємств, організацій, юридичних осіб, діючих на терені України незалежно від їх форм власності та відомчої підпорядкованості, які здійснюють діяльність, пов'язану з розробкою, виготовленням, експлуатацією АТС, а також проводять оцінку захищеності інформації на АТС від НСД, витоків та спеціальних впливів через технічні канали.

НД ТЗІ 2.5-003-99 «Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту» [10]. Установлює вимоги до довірчих оцінок коректності реалізації захисту інформації, що циркулює на програмно-керованих АТС загального користування, а також на установчих (відомчих, корпоративних) АТС.

Положення НД поширюються на програмно-керовані АТС (далі - АТС), у яких зберігається та циркулює інформація, що підлягає технічному захисту.

Захист елементів АТС від фізичного доступу, ушкоджень, розкрадань і підмін у цьому НД розглядається в загальному вигляді і лише як необхідна

обмежувальна міра в процесі здійснення заходів щодо ТЗІ. Передбачається, що вжиті заходи щодо обмеження фізичного доступу до зони станційного устаткування достатні, щоб виключити можливість несанкціонованого доступу (НСД) в цю зону неуповноважених осіб.

Документ призначений для замовників, розроблювачів, виготовлювачів і постачальників АТС, операторів зв'язку національного, регіонального і місцевого рівнів, юридичних осіб - власників і користувачів АТС, а також для організацій і підприємств, що здійснюють оцінку захищеності інформації на АТС від НСД, витоків і спеціальних впливів через технічні канали.

Вимоги цього НД є обов'язковими для підприємств, організацій, юридичних осіб, діючих на терені України незалежно від їх форм власності та відомчої підпорядкованості, які здійснюють діяльність, пов'язану з розробкою, виготовленням, експлуатацією АТС, а також проводять оцінку захищеності інформації на АТС від НСД, витоків та спеціальних впливів через технічні канали.

Наступний НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» [11] установлює критерії оцінки захищеності інформації, оброблюваної в комп'ютерних системах, від несанкціонованого доступу. Критерії є методологічною базою для визначення вимог з захисту інформації в комп'ютерних системах від несанкціонованого доступу; створення захищених комп'ютерних систем і засобів захисту від несанкціонованого доступу; оцінки захищеності інформації в комп'ютерних системах і їх придатності для обробки критичної інформації (інформації, що вимагає захисту). Критерії надають: 1. Порівняльну шкалу для оцінки надійності механізмів захисту інформації від несанкціонованого доступу, реалізованих в комп'ютерних системах. 2. Базу (орієнтири) для розробки комп'ютерних систем, в яких мають бути реалізовані функції захисту інформації. Критерії можуть застосовуватися до всього спектра комп'ютерних систем, включаючи однорідні системи, багатопроцесорні системи, бази даних, вбудовані системи, розподілені системи, мережі, об'єктно-орієнтовані системи та ін. Цей документ призначено

для постачальників (розробників), споживачів (замовників, користувачів) комп'ютерних систем, які використовуються для обробки (в тому числі збирання, зберігання, передачі і т. ін.) критичної інформації, а також для органів, що здійснюють функції оцінювання захищеності такої інформації та контролю за її обробкою. Цей документ відображає сучасний стан проблеми і підходів до її розв'язання. З розвитком нових тенденцій в галузі і за умови достатньої обґрунтованості документ є відкритим для включення до його складу Адміністрацією Державної служби спеціального зв'язку та захисту інформації України нових послуг.

НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» [12]. Установлює принципи класифікації автоматизованих систем і утворення стандартних функціональних профілів захищеності оброблюваної інформації від несанкціонованого доступу.

Призначений для постачальників (розробників), споживачів (замовників, користувачів) автоматизованих систем, які використовуються для обробки ( в тому числі збирання, зберігання, передачі і т. ін.) критичної інформації (інформації, яка потребує захисту), а також для державних органів, які здійснюють функції контролю за обробкою такої інформації. Мета цього документа — надання нормативно-методологічної бази для вибору і реалізації вимог з захисту інформації в автоматизованій системі.

Далі розглянемо стандарти, розроблені відповідно до чинного законодавства України, що встановлюють для загального і багаторазового застосування правила, загальні принципи або характеристики, які стосуються діяльності чи її результатів, з метою досягнення оптимального ступеня впорядкованості, розроблені на основі консенсусу та затверджені уповноваженим органом.

ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. Цей стандарт установлює об’єкт, мету, основні організаційно-технічні положення забезпечення технічного захисту інформації (ТЗІ), неправомірний

доступ до якої може завдати шкоди громадянам, організаціям (юридичним особам) та державі, а також категорії нормативних документів системи ТЗІ [13].

Вимоги стандарту обов'язкові для підприємств та установ усіх форм власності і підпорядкування, громадян - суб'єктів підприємницької діяльності, органів державної влади, органів місцевого самоврядування, військових частин усіх військових формувань, представництв України за кордоном, які володіють, користуються та розпоряджаються інформацією, що підлягає технічному захисту.

За допомогою ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт, можна встановити вимоги щодо порядку проведення робіт з технічного захисту інформації (ТЗІ) [14].

Вимоги стандарту обов`язкові для підприємств та установ усіх форм власності й підпорядкування, громадян-суб`єктів підприємницької діяльності, органів державної влади, органів місцевого самоврядування, військових частин усіх військових формувань, представництв України за кордоном, які володіють, користуються та розпоряджаються інформацією, що підлягає технічному захисту.

ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення [15]. Встановлює терміни та визначення понять у сфері технічного захисту інформації (ТЗІ). Терміни, регламентовані у цьому стандарті, обов'язкові для використання в усіх видах організаційної та нормативної документації, а також для робіт зі стандартизації, і рекомендовані для використання у довідковій та навчально-методичній літературі, що належить до сфери технічного захисту інформації.

Терміни стандарту є обов'язковими для використання підприємствами та установами усіх форм власності і підпорядкування, громадянами - суб'єктами підприємницької діяльності, міністерствами (відомствами), центральними і місцевими органами державної виконавчої влади, військовими частинами усіх військових формувань, представництвами України за кордоном, які володіють, використовують та розпоряджаються інформацією, що становить державну чи іншу передбачену законом таємницю або є конфіденційною інформацією, яка належить державі.

Для розробки і реалізації політики інформаційної безпеки без порушення вимог законодавства потрібно керуватися міжнародними стандартами, такими як ISO 27001 та ISO 27002.

ISO 27001 визначає вимоги до створення, впровадження, підтримки функціонування і безперервне покращення системи менеджменту інформаційної безпеки в рамках контексту організації. Міжнародний Стандарт також включає вимоги для оцінки і обробки ризиків інформаційної безпеки, адаптування до потреб організації. Вимоги, встановлені Міжнародним Стандартом, є загальними і передбачені для застосування будь-якими організаціями, незалежно від їх типу, розміру чи характеру [16].

ISO 27002 надає кращі практичні поради щодо менеджменту інформаційної безпеки для тих, хто відповідає за створення, реалізацію або обслуговування систем менеджменту інформаційної безпеки. Інформаційна безпека визначається стандартом, як «збереження конфіденційності (упевненості в тому, що інформація доступна лише тим, хто уповноважений мати такий доступ), цілісності (гарантії точності і повноти інформації, а також методів її обробки) і доступності (гарантії того, що уповноважені користувачі мають право доступу до інформації і зв'язаними з нею ресурсами)» [17].

## 1.3 Постановка задачі. Висновки до першого розділу

В першому розділі кваліфікаційної роботи була розглянута статистика інформаційних загроз на підприємствах, розпізнання внутрішніх загроз керівниками, декілька поглядів керівників організацій, щодо забезпечення інформаційної безпеки на підприємстві, також була розглянута статистика інцидентів здійснення атак, шахрайства та інших маніпуляцій зі сторони злочинців.

Був проведений аналіз нормативно-правової бази України у сфері захисту інформації, розглянуті державні, а також міжнародні стандарти, за допомогою яких регулюються інформаційні відносини на підприємстві, забезпечуються норми зберігання, обробки, поширення інформації.

В ході виконання даної роботи необхідно:

– провести обстеження об’єкту інформаційної діяльності;

– проаналізувати інформаційні потоки;

– виконати аналіз загроз та вразливостей системи;

– побудувати модель порушника;

– проаналізувати ризики для виявлення слабких місць у системі забезпечення інформаційної безпеки;

– обґрунтувати вибір стандартного функціонально профіля захищеності;

– проаналізувати виконання вимог стандартного функціонального профіля захищеності;

– розробити інструкції політики безпеки, щоб мінімізувати реалізацію ризиків втрати, викривлення, розголошення інформації, яка несе у собі життєвоважливі інтереси для підприємства.

# РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

## 2.1 Обґрунтування необхідності створення КСЗІ

Згідно Закону України «Про захист інформації» в ІКС ТОВ «ТоргСервіс» оброблюється і зберігається інформація з обмеженим доступом.

Згідно Законів України «Про захист інформації в інформаційно-телекомунікаційних системах» та «Про захист персональних даних» порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються власником інформації. Власник інформації та інформаційної системи сам може визначити необхідність створення КСЗІ та КЗЗ, якщо це не суперечить чинному законодавству.

Згідно з НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» у ТОВ «ТоргСервіс» АС відносяться до третього класу, оскільки представляє собою розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності. Передача інформації здійснюється через незахищене середовище.

Комплексна система захисту інформації (КСЗІ) – це сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС.

Комплекс технічного захисту інформації (КТЗІ) – сукупність організаційних, інженерних і технічних заходів та засобів, призначених для захисту від витоку ІзОД технічними каналами на об’єктах інформаційної діяльності.

Інформація з обмеженим доступом (ІзОД) – інформація, що становить державну або іншу передбачену законом таємницю, а також конфіденційна інформація, що є власністю держави або вимога щодо захисту якої встановлена законом [18].

Для забезпечення безпеки інформації під час її обробки в АС створюється КСЗІ, процес управління якою повинен підтримуватись протягом всього життєвого циклу АС.

Комплекс засобів захисту (КЗЗ) – сукупність всіх програмно-апаратних засобів, задіяних під час реалізації політики безпеки.

Політика безпеки (ПБ) – набір законів, правил, обмежень, рекомендацій тощо, які регламентують порядок обробки інформації.

Згідно з Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» на ТОВ «ТоргСервіс» циркулює інформація з обмеженим доступом (персональні данні персоналу та клієнтів), вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю та конфіденційна інформація вимога щодо захисту якої встановлюється її власником.

Така інформація повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством. Тобто, перед створенням КСЗІ, треба визначити чи є на підприємстві інформація, яка підлягає захисту.

До організаційних заходів КСЗІ можна віднести:

1 Складання посадових інструкцій для користувачів та обслуговуючого персоналу;

2 Створення правил адміністрування системи, обліку, зберігання, розмноження, знищення носіїв інформації, ідентифікація користувачів;

3 Розробка порядку дій у випадках виявлення спроб НСД до ІС або виходу з ладу засобів захисту інформації;

4 Навчання користувачів правилам інформаційної безпеки.

Вибір інженерно-технічних заходів КСЗІ залежить від рівня захисту інформації. До них можна віднести:

1 Програмно-апаратні засоби захисту;

2 Розмежування потоків інформації між сегментами мережі;

3 Засоби шифрування і захисту від НСД;

4 СКУД та охоронно-пожежна сигналізація.

Процес створення КСЗІ полягає у здійсненні комплексу взаємоузгоджених заходів, спрямованих на розроблення і впровадження інформаційної технології, яка забезпечує обробку інформації в ІКС згідно з вимогами, встановленими нормативно-правовими актами та НД у сфері захисту інформації [19].

2.2 Загальні відомості про підприємство

Товариство з обмеженою відповідальністю «ТоргСервіс» займається постачанням пакувальних матеріалів та обладнання як для малих організацій та складів, так і для великих підприємств. Надає послуги з доставлення пакувальних матеріалів по місту на власному транспорті або за межі міста завдяки різним компаніям доставки.

Характеристика об’єкта:

Офіс ТОВ «ТоргСервіс» знаходиться в одноповерховій будівлі. В цій же будівлі також знаходяться офіси інших компаній.

Об’єкт: ТОВ «ТоргСервіс»

Адреса: вул. Стартова , 7, м. Дніпро, 49041, Україна.

Форма власності: приватна власність.

Режим роботи підприємства:

Час роботи: 09.00 – 18.00

Перерва: з 13.00 до 14.00

Робочі дні: понеділок – п’ятниця.

Штат співробітників підприємства складається з 10 чоловік:

- директор – 1;
- заступник директора – 1;
- директор з розвитку – 1;
- бухгалтер – 1;
- менеджер з продажів – 1;
- секретар – 1;

– адміністратор – 1.

2.3 Обстеження ОІД

На ситуаційному плані на рисунку 2.1 відображено положення об'єкту інформаційної діяльності відносно об'єктів місцевості.

Офіс знаходиться в одноповерховому самостійному приміщенні (вул. Стартова 7). На ситуаційному плані на рисунку 2 відображено положення об'єкту інформаційної діяльності відносно об'єктів місцевості.

Навпроти головного входу з північно-західної сторони, на відстані 80м, розташований торгівельний майданчик будівельних матеріалів.

Зі Східної сторони на відстані 70 м, знаходиться підприємство «Стройекс».

З південної сторони підприємство «New Holland», будівля знаходиться на відстані 78 м.

На південно-західній стороні, на відстані 22 м знаходиться службова будівля підприємства «New Holland».

На південно-сході, на відстані 78 м знаходяться складські приміщення.

На заході на відстані 146 м знаходиться трансформаторна підстанція.

Фізичні характеристики будівлі і приміщень:

– зовнішні стіни а також стіна, що граничить з коридором – біла цегла, завтовшки 700мм;

– внутрішні стіни – біла цегла, завтовшки 160мм;

– дах будівлі плоский, викладений руберойдом. Вхід на дах здійснюється через пожежні сходи або горище;

– підлога – залізобетонні плити перекриття, завтовшки 350мм, укриті лінолеумом;

– двері головного входу мають розміри 1200 мм * 2000мм, виконані зі звареної листової сталі, оздоблені 2 замками з різними ключами; міжкімнатні двері мають розміри 1200 мм * 2000мм, виконані з ламінованого МДФ;

– територія, навколо будівлі - відкрита, не обмежена забором;

– перебування транспорту на цій території не обмежено та не контролюється;

– територію навколо будівлі впорядковано, вона має асфальтове покриття.

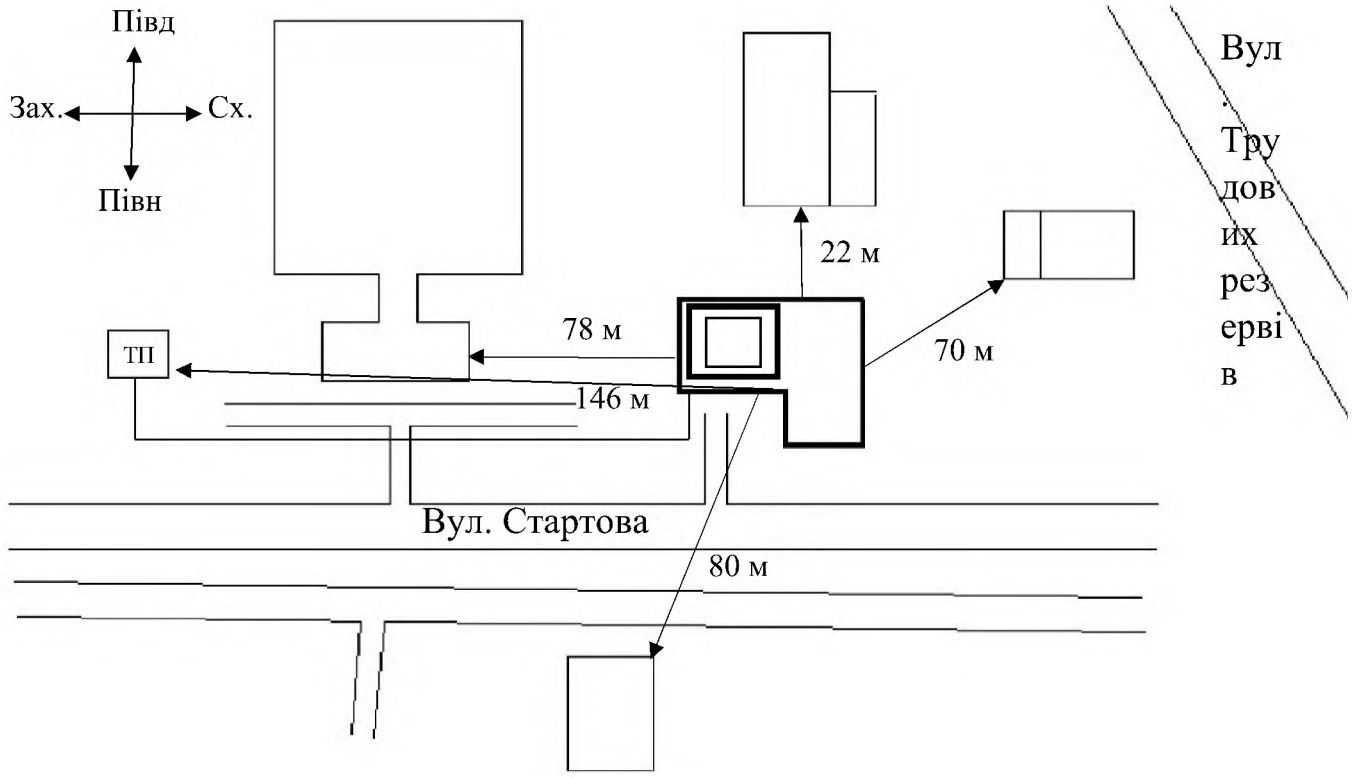



Рисунок 2.1– Ситуаційний план

Таблиця 2.1 - Умовні позначення

| **Позначка на плані** | **Значення** |
|---|---|
| ▬▬ | Лінія електропостачання |
| ▬▬ | Контур заземлення |
| ТП | Трансформаторна підстанція |

Таблиця 2.2 – Системи комунікації, життєзабезпечення та зв'язку

| **Система комунікації** | **Вихід за межі КЗ** | **Характеристика** |
|---|---|---|
| Система електро-постачання | + | Підключена до трансформаторної підстанції, яка має сторонніх споживачів і знаходиться за межами КЗ |
| Система опалення | + | Автономна система, що підключена до міської мережі водопостачання, яка проходить через все приміщення, та виходить за межі КЗ до системи міського водоканалу |
| Система каналізації | + | Підключена до міської мережі, яка знаходиться за межами КЗ |
| Система водопостачання | + | Підключена до міського водоканалу, яка знаходиться за межами КЗ |
| Система заземлення | + | Всі прилади, комп'ютери заземлені до спільного контуру заземлення, який є замкнутим і виходить за межі КЗ до трансформаторної підстанції |
| Телефонна лінія та Інтернет | + | Підключені до АТС «Воля» |
| Система вентиляції | + | Приточно-витяжна |

Продовження табл. 2.2

| **Система комунікації** | **Вихід за межі КЗ** | **Характеристика** |
|---|---|---|
| Система сигналізації | - | Складається з датчиків відкриття (магнітно-контактний датчик), датчиків руху (пасивні інфрачервоні) та системи кабелів |
| Система кондиціонування | + | Спліт-система, що складається з двох блоків: зовнішнього та внутрішнього |
| Система відео-спостереження | – | Складається з чотирьох відеокамер, системи кабелів, квадратору з монітором, плати відеозахоплення та відео-реєстратору, на якому зберігається відзнята інформація. Все обладнання знаходяться в межах КЗ |
| Протипожежна система | + | Складається з системи оповіщувачів та датчиків, дані з яких обробляються протипожежним приймально-контрольним пристроєм, що знаходиться на пості реєстратури |
| Кабелі комп'ютерної мережі | + | Кабель локальної мережі комп'ютерів являє собою неекранована вита пара (1000BASE-T) категорії 5е |
| Опалення | + | Труби опалення виконані з поліпропіленового матеріалу. Це унеможливлює витік інформації по вібро-акустичному каналу |

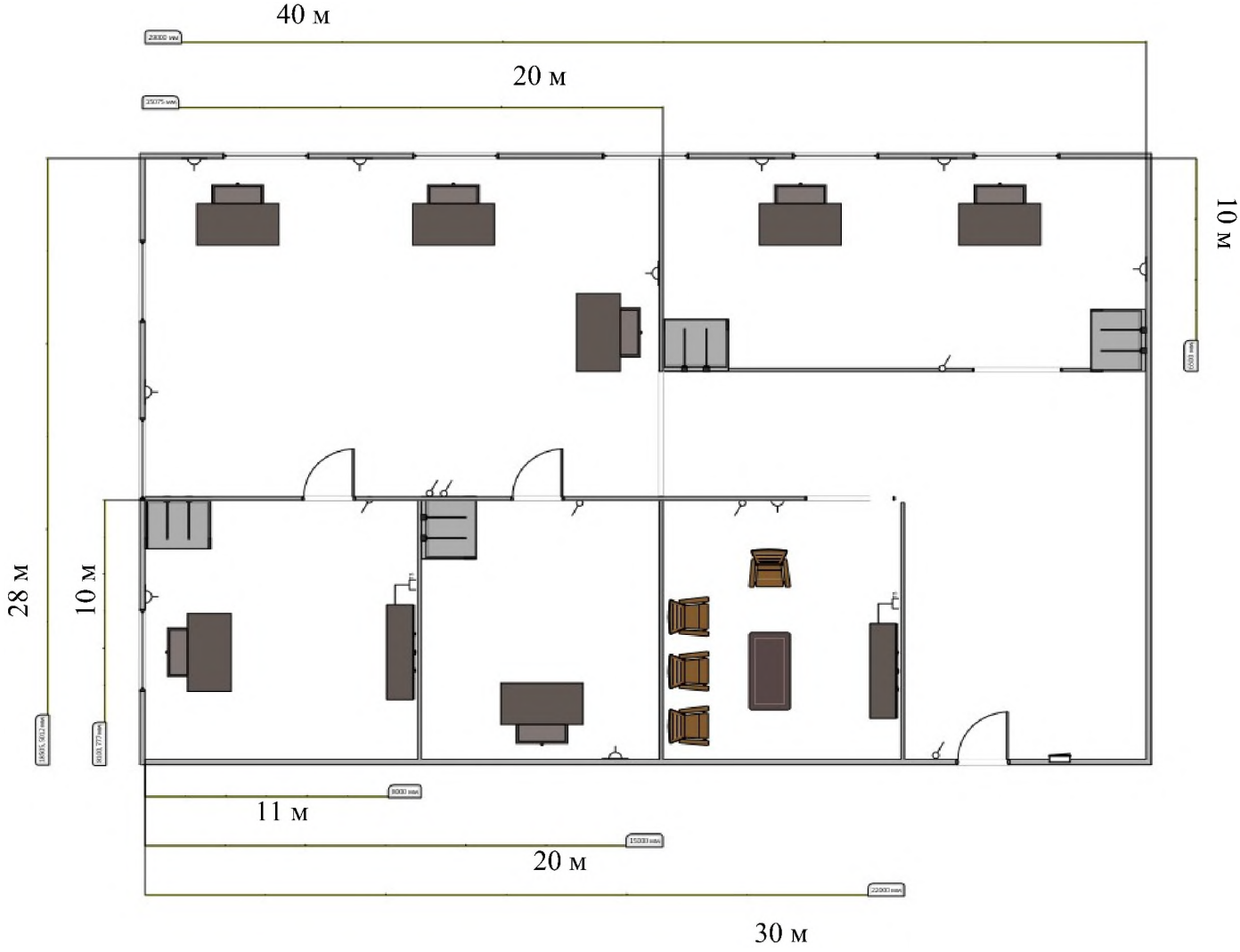



Рисунок 2.2 – Генеральний план

Таблиця 2.3 – Умовні позначення для генерального плану

| **Позначка** | **Пояснення** |
|---|---|
|  | Вимикач |
|  | Розетка |
|  | Телевізійна розетка |

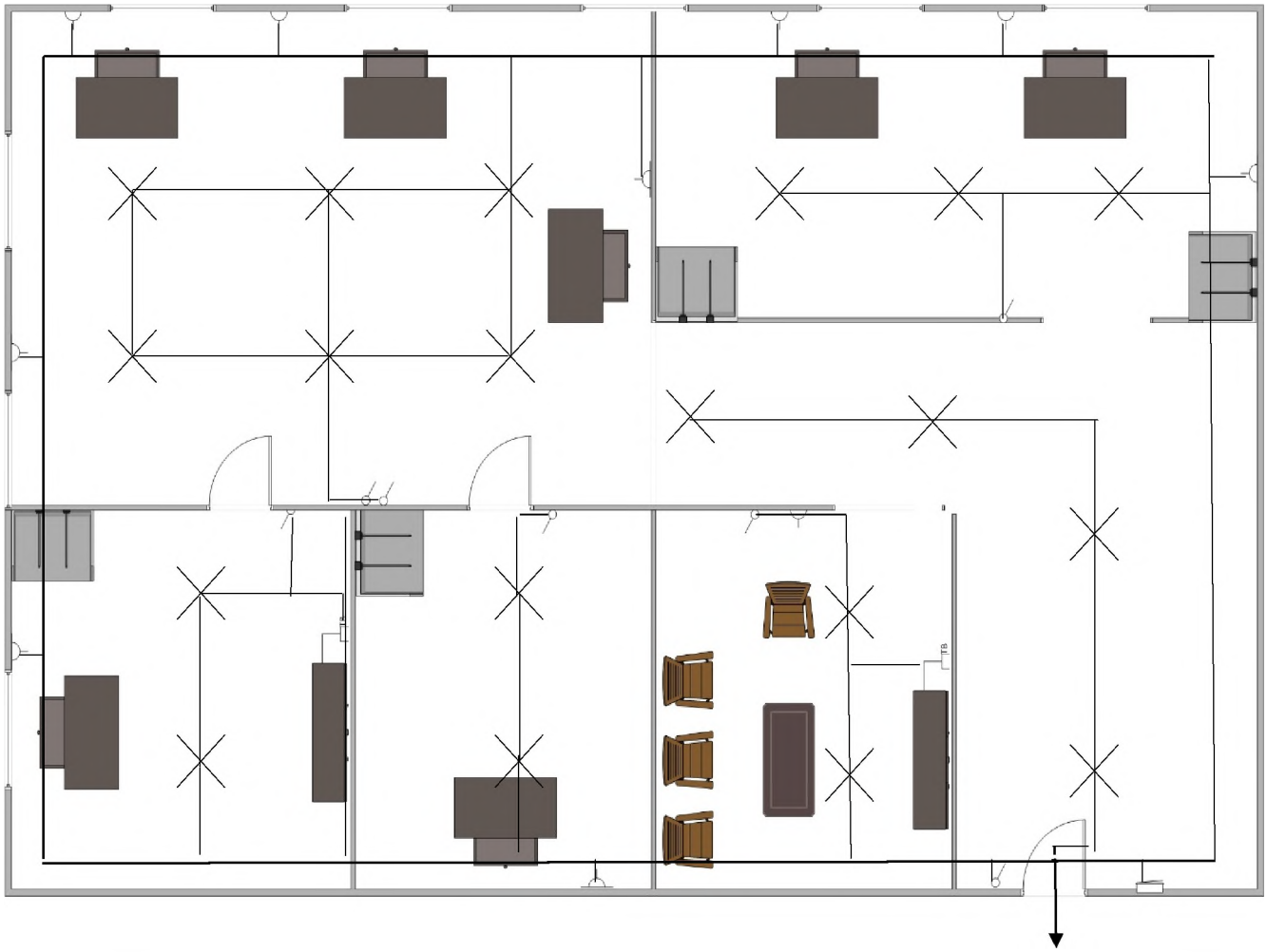


Рисунок 2.3 - Схема електропостачання

Таблиця 2.4 – Умовні позначення для схеми електропостачання

| **Позначка** | **Пояснення** |
|---|---|
|  | Вимикач |
|  | Розетка |
|  | Телевізійна розетка |
|  | Освітлювач |

Рисунок 2.4 - Схема підключення комп’ютерної мережі

Таблиця 2.5 – Умовні позначення для схеми підключення комп’ютерної мережі

| **Позначка** | **Пояснення** |
|---|---|
|  | Вимикач |
|  | Розетка |
|  | Телевізійна розетка |
|  | PC1 -PC7 |
|  | Концентратор |

Рисунок 2.5 - Схема підключення пожежної охорони

Таблиця 2.6 – Умовні позначення схеми пожежної охорони

| **Позначка** | **Пояснення** |
|---|---|
|  | Пожежна сигналізація |
|  | Оповіщувач ручний |
|  | Оповіщувач звуковий |
|  | Прийомно-контрольний прилад |

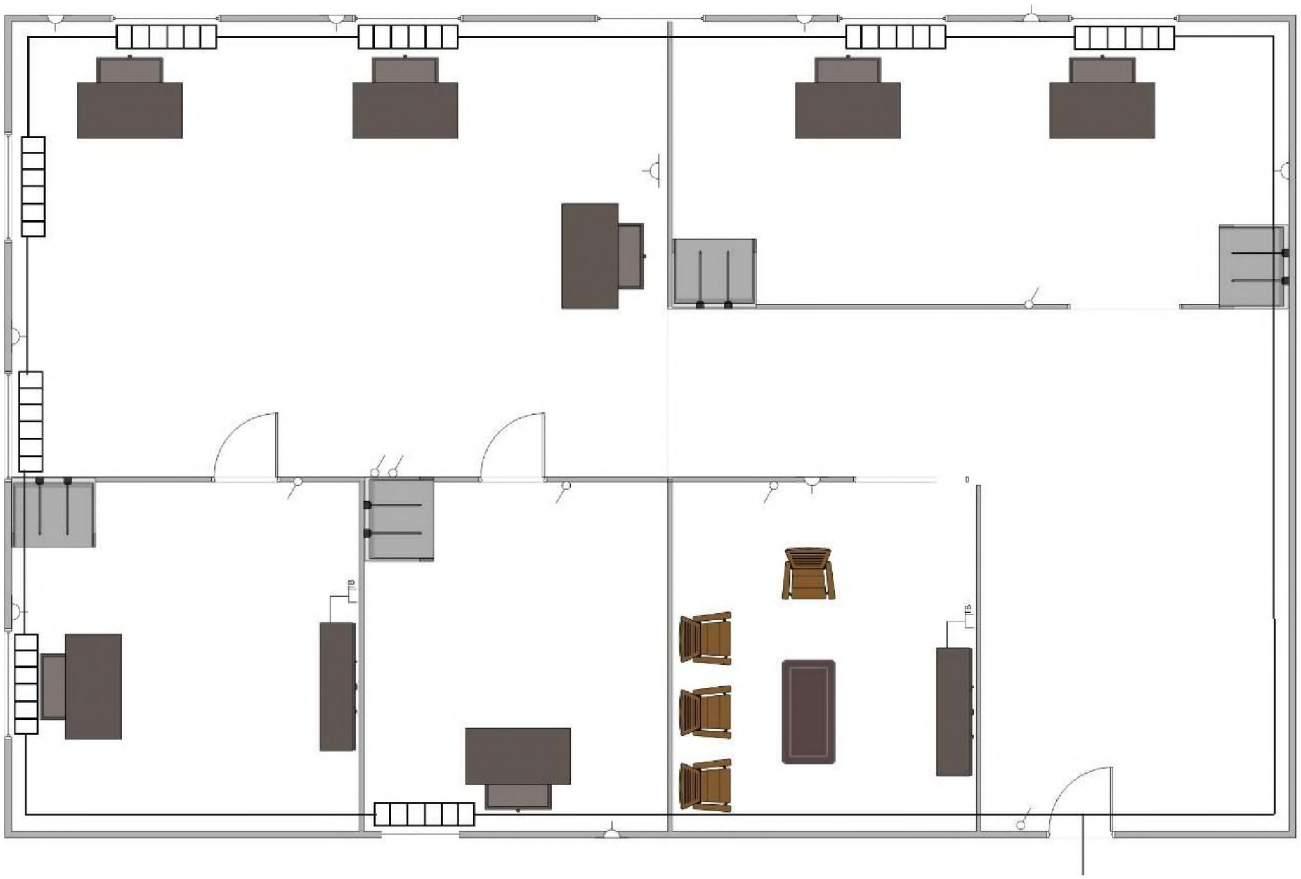
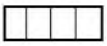


Рисунок 2.6 – Схема підключення системи опалення

Таблиця 2.7 – Умовні позначення для схеми підключення системи опалення

| **Позначка** | **Пояснення** |
|---|---|
|  | Радіатор |
|  | Труби |

На досліджуваному ОІД циркулює інформація з обмеженим доступом: конфіденційна.

В мережі ТОВ кожному комп'ютеру присвоєні імена, а саму мережу розділено на три (робочі) групи (директор, адміністратор, останні користувачі). Кожна з цих груп має доступ лише до певних файлів, програм та інформації в цілому, у кожного користувача свої права доступу. Вихід комп'ютерів до мережі Інтернет забезпечується по постійним віртуальним каналам комутації кадрів.

Цінна для об’єкта інформація дублюється на комп’ютерах співробітників з подібними правами доступу або на спеціальних знімних носіях, які зберігаються в опечатаному сейфі. Відповідальність за сейфи несе керівництво.

У разі обміну, конфіденційну інформацію зберігають на спеціальні змінні носії і передають їх через вповноважених (відповідальних) за ці носії співробітників. Це може бути і сам директор. Також обмін інформацією може відбуватись за допомогою електронної пошти. В приміщенні також є МФУ.

Склад обчислюваної системи вказано в таблиці 2.8.

Таблиця 2.8 – Склад та характеристики обчислюваної системи

| **Назва** | **Характеристика** | **Умовні позначення** | **Кількість** |
|---|---|---|---|
| Принтери | Модель: HP DeskJet Ink Advantage 2135 (F5S29C) | PR1-PR2 | 2 |
| БФП | Модель: Canon imageRUNNER iR2204n with USB cable | M1 | 1 |
| Комутатор | Модель: Cisco SB SRW224G4-K9-EU | SW1 | 1 |
| ADSL модем | Модель: TP-LINK TD-8616 | Mod1 | 1 |
| Ноутбук | Asus X751SV (X751SV-TY002D)/ RAM 4 ГБ / HDD 500 ГБ / Windows 11 Pro 64-bit | PC1-PC7 | 7 |
| Сервер | HPE ProLiant ML10 Gen9 : Intel Xeon Quad-Core E3-1225 v5 (3.3 - 3.7 ГГц)/ 8 ГБ/ 2 x 1 ТБ (3.5», SATA 3, 7200 об/хв) HPE LFF | SRV1 | 1 |

Встановлене на робочих станціях та сервері програмне забезпечення відображено у таблиці 2.9.

Таблиця 2.9 – Встановлене програмне забезпечення

| **Розміщення** | **Тип** | **Назва** |
|---|---|---|
| Сервер БД | Операційна система | Microsoft Windows Server 2022 |
| | ПЗ для роботи з документами | Microsoft Office 2021 |
| | ПЗ для автоматизації бухгалтерського обліку | Dilovod |
| | Антивірус | ESET SmartSecurity |
| Робочі станції | Операційна система | Microsoft Windows 11 Enterprise Edition Service Pack 1 |
| | ПЗ для роботи з документами | Microsoft Office 2021 |
| | Веб-браузер | Google Chrome |
| | ПЗ для автоматизації бухгалтерського обліку | Dilovod |
| | Антивірус | ESET SmartSecurity |

Всі документи створюються відповідними працівниками на своїх робочих станціях за допомогою встановленого ПЗ та роздруковуються на принтерах чи розмножуються на БФП. Електрона копія зберігається або на робочий станції працівника або в спеціально відведеному місці (папка на диску) на сервері для документів, роздрукований паперовий варіант зберігається в шафі або в сейфі. Після втрати необхідності в документі він знищується.

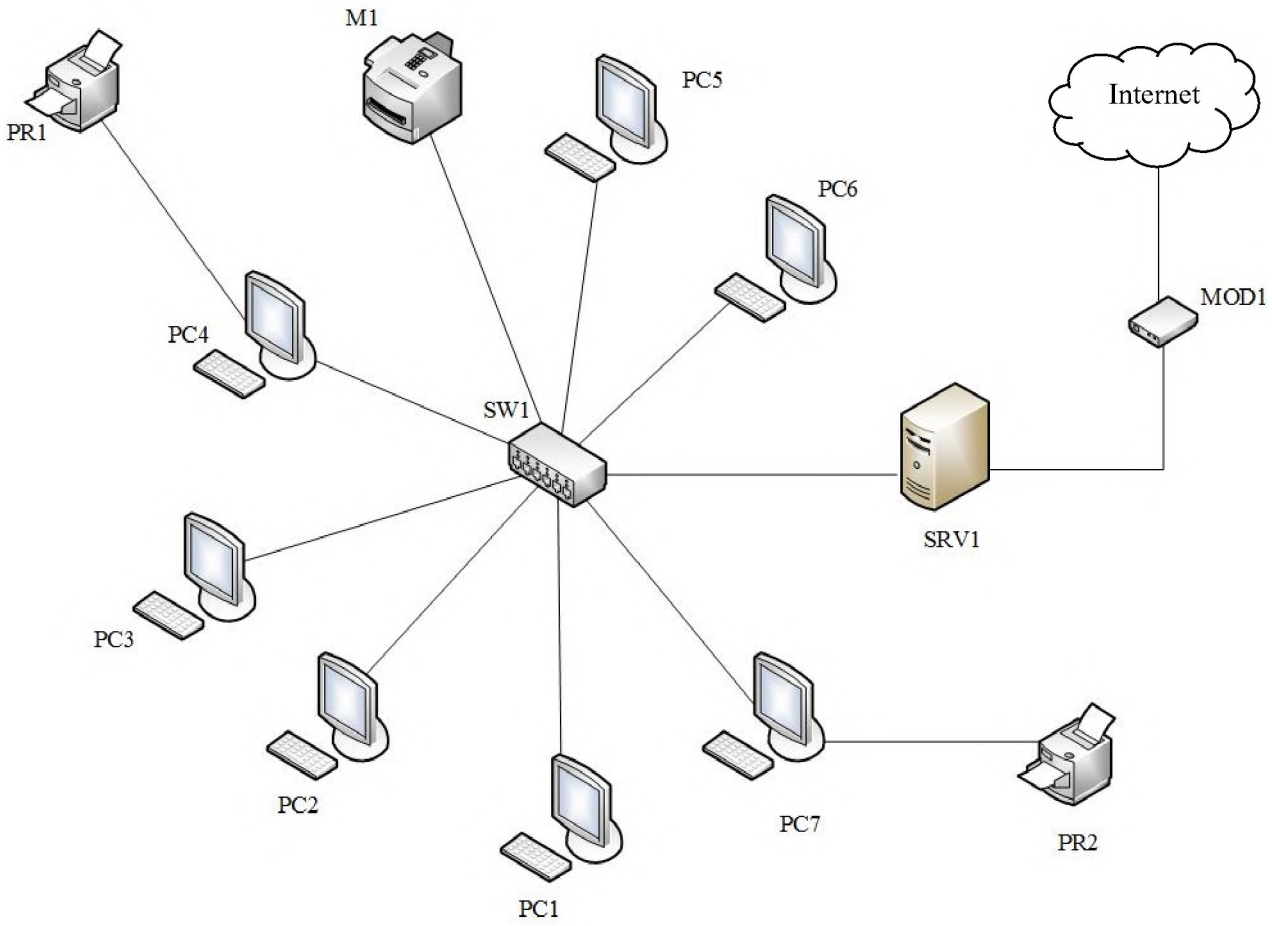



Рисунок 2.7 – Логічна схема інформаційно-комунікаційної системи

Умовні позначення:

- PC від 1 до 7 – робоча станція;
- PR від 1 до 2 – принтер;
- M1 – багатофункціональний пристрій;
- Mod1 – ADSL модем;
- SW1 – мережевий комутатор;
- SRV1 – сервер.

У таблиці 2.10 представлений перелік інформації, що циркулює на підприємстві та її класифікація.

Таблиця 2.10 - Класифікація інформації

| № | Вид інформації | Режим доступу | Вид зберігання | Вимоги |
|---|---|---|---|---|
| 1 | Особисті дані персоналу | ІзОД | Паперовий та електронний | КЦД |
| 2 | БД підприємства | ІзОД | Паперовий та електронний | КЦД |
| 3 | Договори, укладені з клієнтами (партнерами) | ІзОД | Паперовий та електронний | КЦД |
| 4 | Інформація бухгалтерської звітності | ІзОД | Паперовий та електронний | КЦД |
| 5 | Інформація про стан мережі, її компонентів | ІзОД | Електронний | КЦД |
| 6 | Інформація про засоби захисту інформації | ІзОД | Паперовий та електронний | КЦД |
| 7 | Трудові договори | ІзОД | Паперовий | КЦД |
| 8 | Інформація, пов’язана з виробничою діяльністю | ІзОД | Паперовий та електронний | КЦД |
| 9 | Інформація про послуги та їх вартість | Відкрита | Паперовий та електронний | ЦД |
| 10 | Інформація про діяльність підприємства | Відкрита | Паперовий та електронний | ЦД |
| 11 | Статутні документи підприємства | Відкрита | Паперовий та електронний | ЦД |

К – вимоги до конфіденційності;

Ц – вимоги до цілісності;

Д – вимоги до доступності.

На рисунку 2.8 представлений аналіз потоків, тобто те, як здійснюється циркуляція інформації між відділами та директором.

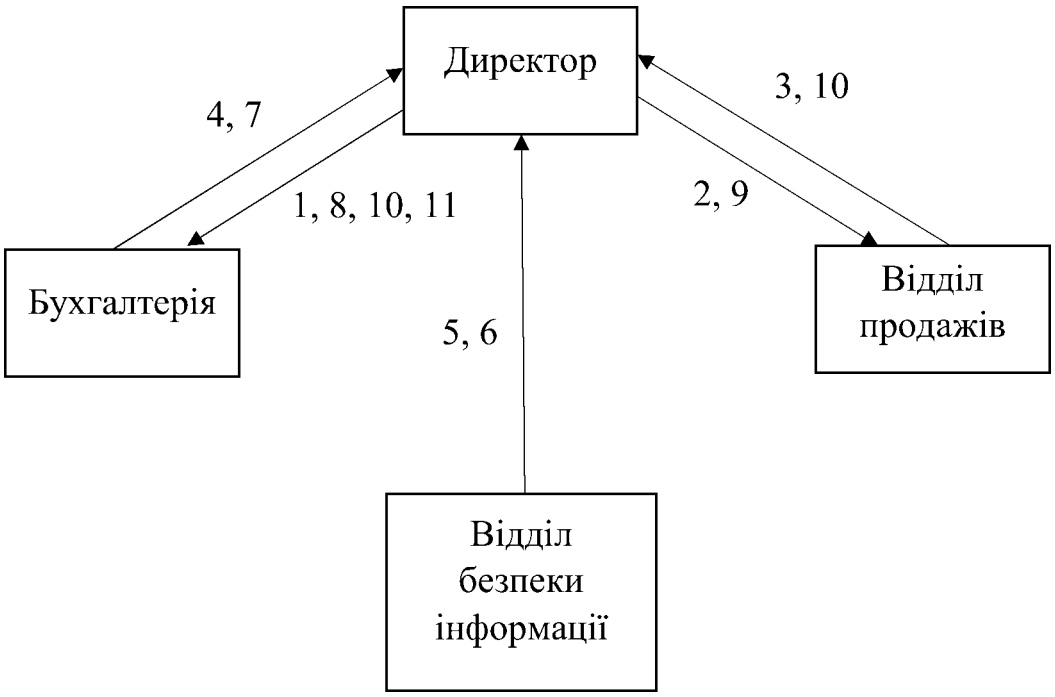



Рисунок 2.8 – Аналіз інформаційних потоків

Таблиця 2.11 – Пояснення до рисунку 2.8

| **№ виду інформації** | **Пояснення** |
|---|---|
| 1 | Особисті дані персоналу |
| 2 | БД підприємства |
| 3 | Договори, укладені з клієнтами (партнерами) |
| 4 | Інформація бухгалтерської звітності |
| 5 | Інформація про стан мережі, її компонентів |

Продовження табл. 2.11

| № виду інформації | Пояснення |
|---|---|
| 6 | Інформація про засоби захисту інформації |
| 7 | Трудові договори |
| 8 | Інформація, пов'язана з виробничою діяльністю |
| 9 | Інформація про послуги та їх вартість |
| 10 | Інформація про діяльність підприємства |
| 11 | Статутні документи підприємства |

В таблиці 2.12 «Матриця доступу до інформації» вказано, як авторизовані користувачі мережі можуть здійснювати керування інформацією.

Таблиця 2.12 – Матриця доступу до інформації

| Посада / Інформація | Директор | Заступник директора | Директор з розвитку | Бухгалтер | Менеджер з продажів | Секретар | Адміністратор |
|---|---|---|---|---|---|---|---|
| | **1** | **2** | **3** | **4** | **5** | **6** | **7** |
| **1** | R,W,D | R,W | R | R | - | R,W | - |
| **2** | R,W,D | R,W | R | R,W | R,W | R | - |
| **3** | R,W,D | R,W | R,W | R | R,W,D | - | - |
| **4** | R,W | R | - | R,W | - | - | - |
| **5** | R | R | - | - | - | - | R,W,D |
| **6** | R,W,D | R | - | - | - | - | R,W,D |
| **7** | R,W,D | R,W,D | R | R | - | R,W,D | - |

Продовження табл. 2.12

| Посада / Інформація | Директор | Заступник директора | Директор з розвитку | Бухгалтер | Менеджер з продажів | Секретар | Адміністратор |
|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 8 | R,W,D | R,W | R | - | - | - | - |
| 9 | R,W,D | R,W,D | R | R | R | R,W,D | R |
| 10 | R,W,D | R,W | R | R | R | R,W,D | R |
| 11 | R,W,D | R,W,D | R | R | R | R,W,D | R |

R – read (право на зчитування);

W – write (право на редагування);

D – delete (право на видалення).

## 2.4 Аналіз загроз та вразливостей

Загроза (threat) — будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків АС.

Загрози інформаційної безпеки класифікуються за низькою ознак:

– за складовими інформаційної безпеки
– за компонентами інформаційних систем, на які загрози націлені
– за характером впливу
– за розміщенням джерела загроз

Розглянемо класифікацію загроз інформаційної безпеки за її складовими. Класифікація загроз інформаційної безпеки за її складовими полягає у визначенні загроз (загрози), які безпосередньо направлені на таки складові інформаційної безпеки, як цілісність, доступність, конфіденційність. Усі загрози, що класифікуються за іншими ознаками можуть впливати на усі складові інформаційної безпеки.

Також загрози інформаційної безпеки можуть бути розділені за компонентами інформаційних систем, на які вони націлені. Класифікація загроз інформаційної безпеки за компонентами інформаційних систем, на які загрози націлені полягає у визначенні загроз (загрози), які безпосередньо направлені на такі складові інформаційної системи, як інформація, що обробляється в обчислювальної системі, обчислювальна система, програмне забезпечення, апаратура, персонал та інші.

В якості прикладів загроз компонентам інформаційних систем, що суттєво впливають на стан захищеності інформації, можна навести такі:

– зміна архітектури системи
– зміна складу та/або можливостей апаратних і програмних засобів
– підключення до мережі (особливо глобальної)
– відмінності в категорії та/або кваліфікації персоналу

Загрози інформаційної безпеки за характером впливу класифікують, як випадкові та навмисні дії природного або техногенного характеру.

Випадкові загрози – це загрози, які не пов'язані з умисними діями зловмисників та реалізуються у випадкові моменти часу. Випадкові загрози поділяють на загрози від аварій та стихійних лих, збоїв та відмов технічних засобів, помилок при розробці елементів інформаційної системи, алгоритмічні та програмні помилки, помилки користувачів чи обслуговуючого персоналу та інші(за статистикою – до 65% збитків у порівнянні з іншими загрозами). Реалізація цих загроз веде до найбільшої втрати інформації (за статистикою – до 80% збитків у порівнянні з іншими загрозами). Це – знищення, порушення цілісності, доступності, інколи – конфіденційності інформації.

Навмисні загрози – це цілеспрямовані дії зловмисника. Цей клас загроз динамічний, постійно оновлюється новими загрозами, як правило, недостатньо вивчений.

Навмисні загрози поділяють на:

– «спеціальні впливи»;
– несанкціонований доступ до інформації;

– використання технічних каналів витоку інформації;

– несанкціоновану зміну структури та інші.

Спроба реалізації будь якої навмисної загрози по відношенню до об'єкту інформаційної діяльності підпадає під дію відповідних статей Карного кодексу України.

«Спеціальні впливи». Загрози інформаційної безпеці від традиційних «спеціальних впливів» до цього часу залишаються актуальними. Частіше за все їх використовують для отримання інформації про систему захисту інформації або її знищення з метою подальшого проникнення до інформаційної системи [20].

Методами «спеціальних впливів» є: підслуховування, візуальне спостереження, викрадення документів або носіїв інформації, викрадення програм або атрибутів системи захисту інформації, підкуп або шантаж співробітників, сбір та аналіз відходів машинних носіїв інформації, підпалення та інші.

Розрізняють два класи загроз інформації за розміщенням їх джерела в середині інформаційної системи, або поза неї.

Найбільш небезпечною загрозою вважається внутрішня загроза, джерелом якої є співробітники установи – користувачі інформаційної системи. Серед користувачів є специфічна категорія – керівництво. Часто, керівники вимагають собі підвищені привілеї в системі, а також не визнають щодо себе жодних обмежень. До того ж, адміністратори системи формально підпорядковані керівництву, а не навпаки.

Потенційні можливості легального користувача в ІКС значно більші, ніж у будь-якого зовнішнього порушника. Користувач має в системі певні повноваження. Користувач має багато інформації про систему, а іншу інформацію може порівняно легко отримати (когось спитати, підслухати, «неформально» проконсультуватись – йому це значно простіше, ніж будь-якій сторонній особі). Користувач, як правило, незадоволений обмеженнями своїх прав у системі. Користувач цікавиться інформаційними технологіями і бажає перевірити свої досягнення на практиці. Часто користувач не дуже кваліфікований, і все, що він буде робити, фактично зведеться до методу спроб і помилок.

### 2.4.1 Аналіз загроз

Модель загроз (model of threats) — абстрактний формалізований або неформалізований опис методів і засобів здійснення загроз.

Носіями загроз безпеки інформації є джерела загроз. У якості джерел загроз можуть виступати як суб'єкти (особистість), так і об'єктивні прояви. Причому, джерела загроз можуть перебувати як усередині організації, що захищається, – внутрішні джерела, так і поза неї – зовнішні джерела. Розподіл джерел на суб'єктивні й об'єктивні виправдане виходячи із приводу провини або ризику збитку інформації. А розподіл на внутрішні й зовнішні джерела виправдане тому, що для однієї й тієї ж загрози методи парирування для зовнішніх і внутрішніх джерел можу бути різними.

Всі джерела загроз безпеки інформації можна розділити на три основні групи:

– Обумовлені діями суб'єкта (антропогенні джерела загроз);

– Обумовлені технічними засобами (техногенні джерела загроз);

– Обумовлені стихійними джерелами.

Антропогенними джерелами загроз безпеки інформації виступають суб'єкти, дії яких можуть бути кваліфіковані як навмисні або випадкові злочини. Тільки в цьому випадку можна говорить про заподіяння збитку. Ця група найбільш велика й становить найбільший інтерес із погляду організації захисту, тому що дії суб'єкта завжди можна оцінити, спрогнозувати й вжити адекватні заходи. Методи протидії в цьому випадку керовані й прямо залежать від волі організаторів захисту інформації.

У якості антропогенного джерела загроз можна розглядати суб'єкт, що має доступ (санкціонований або несанкціонований) до роботи зі штатними засобами об'єкту, що захищається. Техногенні виникають внаслідок використання техніки. Загрози, пов’язані з втратою або псуванням інформації внаслідок виходу з ладу обладнання важко спрогнозувати і попередити.

Стихійні лиха - це група джерел, яка представляє обставини, що мають непереборну силу и не піддаються попередженню. Найчастіше сюди відносять

стихійні лиха та природні катаклізми, техногенні катастрофи, пожежі. Вони не піддаються прогнозуванню, тому заходи захисту від їх наслідків повинні виконуватися постійно.

Суб'єкти (джерела), дії яких можуть привести до порушення безпеки інформації, можуть бути як зовнішні, так і внутрішні. Зовнішні джерела можуть бути випадковими або навмисними й мати різний рівень кваліфікації.

Внутрішні суб'єкти (джерела), як правило, являють собою висококваліфікованих фахівців в області розробки й експлуатації програмного забезпечення й технічних засобів, знайомих зі специфікою розв'язуваних задач, структурою й основними функціями й принципами роботи програмно-апаратних засобів захисту інформації, які мають можливість використання штатного устаткування й технічних засобів мережі.

При розгляданні моделі загроз, також слід приділити увагу дестабілізуючим факторам. Дестабілізуючі фактори (ДФ) – це такі явища чи події, що можуть з'являтися на будь-якому етапі життєвого циклу АС і наслідком яких можуть бути загрози інформації. У продовження життєвого циклу АС може виникати багато ДФ всілякої природи.

Тому, на основі аналізу архітектури, технології й умов функціонування АС і всіх можливих у принципі ДФ зручно ввести поняття типу ДФ, що дозволяє класифікувати ДФ за способами їхньої реалізації. Вважаючи, що ця класифікація ДФ є вичерпною, виділимо наступні типи ДФ:

– кількісна недостатність – фізична недостатність компонентів АС для забезпечення необхідного рівня захищеності оброблюваної інформації;

– якісна недостатність – недосконаліть конструкції чи організації компонентів АС, внаслідок чого не забезпечується необхідний рівень захищеності оброблюваної інформації;

– відмова елементів АС – порушення працездатності елементів, що

– збій елементів АС – тимчасове порушення працездатності елементів, що призводить до неправильного виконання ними в цей момент своїх функцій;

– помилки елементів АС – неправильне (одноразове чи систематичне) виконання елементами своїх функцій внаслідок специфічного (постійного і/або тимчасового) їхнього стану;

– стихійні лиха – випадково виникаючі неконтрольовані явища, що

– призводять до фізичних руйнувань;

В таблиці 2.13 представлена модель загроз, вона допомагає виявити через які загрози джерела загроз можуть нести найбільшу небезпеку. Така таблиця в подальшому допоможе розробити заходи для мінімізації цих загроз.

Таблиця 2.13 – Аналіз загроз

| **Джерело загроз** | **Загроза** | **К** | **Д** | **Ц** | **$К_1$** | **$К_2$** | **$К_3$** | **$К_{неб}$** |
|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| **Антропогенні, зовнішні** | | | | | | | | |
| Кримінальні структури | Крадіжка (копіювання) інформації | + | + | + | 3 | 1 | 2 | 0,048 |
| | Знищення інформації | + | + | + | 3 | 1 | 2 | 0,048 |
| | Змінення інформації | + | + | + | 1 | 2 | 2 | 0,032 |
| | Порушення доступності (блокування) інформації | + | + | + | 1 | 1 | 2 | 0,016 |
| | Заперечення достовірності інформації | + | + | + | 1 | 1 | 2 | 0,016 |
| | Нав'язування помилкової інформації | + | + | + | 1 | 1 | 2 | 0,016 |

Продовження табл. 2.13

| **Джерело загроз** | **Загроза** | **К** | **Д** | **Ц** | **$К_1$** | **$К_2$** | **$К_3$** | **$К_{неб}$** |
|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| Хакери | Крадіжка (копіювання) інформації | + | + | + | 3 | 2 | 3 | 0,144 |
| | Знищення інформації | + | + | + | 4 | 2 | 3 | 0,192 |
| | Змінення інформації | + | + | + | 3 | 3 | 3 | 0,216 |
| | Порушення доступності (блокування) інформації | + | + | + | 3 | 2 | 2 | 0,096 |
| | Заперечення достовірності інформації | + | + | + | 3 | 3 | 3 | 0,216 |
| | Нав'язування помилкової інформації | + | + | + | 3 | 3 | 3 | 0,216 |
| Конкуренти | Крадіжка (копіювання) інформації | + | + | + | 2 | 4 | 2 | 0,128 |
| | Знищення інформації | + | + | + | 2 | 4 | 2 | 0,128 |
| | Змінення інформації | + | + | + | 2 | 3 | 2 | 0,096 |
| | Порушення доступності (блокування) інформації | + | + | + | 1 | 4 | 2 | 0,064 |
| | Заперечення достовірності інформації | + | + | + | 2 | 4 | 1 | 0,064 |

Продовження табл. 2.13

| **Джерело загроз** | **Загроза** | **К** | **Д** | **Ц** | **$К_1$** | **$К_2$** | **$К_3$** | **$К_{неб}$** |
|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| | Нав'язування помилкової інформації | + | + | + | 1 | 3 | 2 | 0,048 |
| Відвідувачі | Крадіжка (копіювання) інформації | + | + | + | 3 | 2 | 2 | 0,096 |
| | Знищення інформації | + | + | + | 3 | 2 | 2 | 0,096 |
| | Змінення інформації | + | + | + | 3 | 2 | 2 | 0,096 |
| | Порушення доступності (блокування) інформації | + | + | + | 2 | 2 | 2 | 0,064 |
| | Заперечення достовірності інформації | + | + | + | 3 | 1 | 2 | 0,048 |
| | Нав'язування помилкової інформації | + | + | + | 2 | 1 | 2 | 0,032 |
| Будь-які особи, що знаходяться за межами КЗ | Крадіжка (копіювання) інформації | + | + | + | 1 | 1 | 2 | 0,016 |
| | Знищення інформації | + | + | + | 1 | 1 | 2 | 0,016 |
| | Змінення інформації | + | + | + | 1 | 1 | 2 | 0,016 |
| | Порушення доступності (блокування) інформації | + | + | + | 1 | 1 | 2 | 0,016 |

Продовження табл. 2.13

| **Джерело загроз** | **Загроза** | **К** | **Д** | **Ц** | **$К_1$** | **$К_2$** | **$К_3$** | **$К_{неб}$** |
|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| | Заперечення достовірності інформації | + | + | + | 1 | 1 | 1 | 0,008 |
| | Нав'язування помилкової інформації | + | + | + | 1 | 2 | 2 | 0,032 |
| **Антропогенні, внутрішні (авторизовані користувачі)** | | | | | | | | |
| Директор | Крадіжка (копіювання) інформації | + | + | + | 5 | 3 | 3 | 0,36 |
| | Знищення інформації | + | + | + | 5 | 4 | 4 | 0,64 |
| | Змінення інформації | + | + | + | 5 | 3 | 4 | 0,48 |
| | Порушення доступності (блокування) інформації | + | + | + | 5 | 3 | 4 | 0,48 |
| | Заперечення достовірності інформації | + | + | + | 5 | 3 | 4 | 0,48 |
| | Нав'язування помилкової інформації | + | + | + | 5 | 3 | 4 | 0,48 |
| Основний персонал (користувачі мережі) | Крадіжка (копіювання) інформації | + | + | + | 4 | 3 | 3 | 0,288 |
| | Знищення інформації | + | + | + | 4 | 3 | 4 | 0,384 |
| | Змінення інформації | + | + | + | 4 | 3 | 4 | 0,384 |

Продовження табл. 2.13

| **Джерело загроз** | **Загроза** | **К** | **Д** | **Ц** | **$К_1$** | **$К_2$** | **$К_3$** | **$К_{неб}$** |
|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| | Порушення доступності (блокування) інформації | + | + | + | 4 | 2 | 3 | 0,192 |
| | Заперечення достовірності інформації | + | + | + | 3 | 3 | 3 | 0,216 |
| | Нав'язування помилкової інформації | + | + | + | 4 | 2 | 3 | 0,192 |
| Адміністратор | Крадіжка (копіювання) інформації | + | + | + | 5 | 5 | 4 | 0,8 |
| | Знищення інформації | + | + | + | 5 | 5 | 4 | 0,8 |
| | Змінення інформації | + | + | + | 5 | 5 | 4 | 0,8 |
| | Порушення доступності (блокування) інформації | + | + | + | 5 | 5 | 4 | 0,8 |
| | Заперечення достовірності інформації | + | + | + | 5 | 4 | 4 | 0,64 |
| | Нав'язування помилкової інформації | + | + | + | 5 | 5 | 4 | 0,8 |

Продовження табл. 2.13

| **Джерело загроз** | **Загроза** | **К** | **Д** | **Ц** | **$К_1$** | **$К_2$** | **$К_3$** | **$К_{неб}$** |
|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| **Антропогенні, внутрішні (персонал, який не є авторизованими користувачами)** | | | | | | | | |
| Прибиральниця та охорона | Крадіжка (копіювання) інформації | + | + | - | 4 | 1 | 2 | 0,064 |
| | Знищення інформації | + | + | - | 3 | 1 | 2 | 0,048 |
| | Змінення інформації | + | + | - | 4 | 1 | 1 | 0,032 |
| | Порушення доступності (блокування) інформації | + | + | - | 3 | 2 | 2 | 0,096 |
| | Заперечення інформації | + | + | - | 4 | 1 | 2 | 0,064 |
| | Нав'язування помилкової інформації | + | + | - | 4 | 2 | 2 | 0,128 |
| **Техногенні, зовнішні** | | | | | | | | |
| Засоби зв'язку | Крадіжка (копіювання) інформації | + | - | + | 2 | 2 | 2 | 0,064 |
| | Знищення інформації | + | - | + | 2 | 1 | 2 | 0,032 |
| | Змінення інформації | + | - | + | 2 | 2 | 1 | 0,032 |
| | Порушення доступності (блокування) інформації | + | - | + | 3 | 2 | 2 | 0,096 |

Продовження табл. 2.13

| **Джерело загроз** | **Загроза** | **К** | **Д** | **Ц** | **$К_1$** | **$К_2$** | **$К_3$** | **$К_{неб}$** |
|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| | Заперечення інформації | + | - | + | 2 | 1 | 1 | 0,016 |
| | Нав'язування помилкової інформації | + | - | + | 2 | 2 | 2 | 0,064 |
| Мережі інженерних комунікацій (система опалення, каналізації, водопостачання, заземлення) | Крадіжка (копіювання) інформації | + | - | + | 3 | 2 | 3 | 0,144 |
| | Знищення інформації | + | - | + | 3 | 2 | 2 | 0,096 |
| | Змінення інформації | + | - | + | 3 | 1 | 2 | 0,048 |
| | Порушення доступності (блокування) інформації | + | - | + | 1 | 2 | 2 | 0,032 |
| | Заперечення інформації | + | - | + | 3 | 1 | 2 | 0,048 |
| | Нав'язування помилкової інформації | + | - | + | 3 | 1 | 1 | 0,024 |
| **Техногенні, внутрішні** | | | | | | | | |
| Неякісне апаратне забезпечення | Крадіжка (копіювання) інформації | + | + | + | 4 | 2 | 2 | 0,128 |
| | Знищення інформації | + | + | + | 4 | 3 | 2 | 0,192 |
| | Змінення інформації | + | + | + | 4 | 2 | 3 | 0,192 |

Продовження табл. 2.13

| **Джерело загроз** | **Загроза** | **К** | **Д** | **Ц** | **$К_1$** | **$К_2$** | **$К_3$** | **$К_{неб}$** |
|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| | Порушення доступності (блокування) інформації | + | + | + | 4 | 3 | 2 | 0,192 |
| | Заперечення інформації | + | + | + | 4 | 1 | 2 | 0,128 |
| | Нав'язування помилкової інформації | + | + | + | 4 | 2 | 2 | 0,128 |
| Неякісне програмне забезпечення | Крадіжка (копіювання) інформації | + | + | + | 4 | 2 | 2 | 0,128 |
| | Знищення інформації | + | + | + | 4 | 2 | 3 | 0,192 |
| | Змінення інформації | + | + | + | 4 | 2 | 2 | 0,128 |
| | Порушення доступності (блокування) інформації | + | + | + | 4 | 3 | 2 | 0,192 |
| | Заперечення інформації | + | + | + | 3 | 2 | 2 | 0,096 |
| | Нав'язування помилкової інформації | + | + | + | 4 | 3 | 2 | 0,192 |

Продовження табл. 2.13

| **Джерело загроз** | **Загроза** | **К** | **Д** | **Ц** | **$К_1$** | **$К_2$** | **$К_3$** | **$К_{неб}$** |
|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| **Стихійні** | | | | | | | | |
| Пожежі | | - | + | - | 2 | 2 | 2 | 0,064 |
| Землетруси | | - | + | - | 2 | 1 | 1 | 0,016 |
| Підтоплення | | - | + | - | 1 | 1 | 2 | 0,016 |
| Урагани | | - | + | - | 1 | 1 | 2 | 0,016 |
| Різні непередбачені обставини | | - | + | - | 2 | 1 | 2 | 0,032 |
| Інші форс-мажорні обставини | | - | + | - | 2 | 1 | 2 | 0,032 |

$(К1)_f$ – Фатальність, визначає міра впливу уразливості на неможливість усунення наслідків реалізації загрози. Для об'єктивних вразливостей це інформативність – здатність вразливості повністю (без спотворень) передати корисний інформаційний сигнал.

$(К2)_f$ – Доступність, визначає зручність (можливість) використання вразливості джерелом загроз (багато габаритні розміри, складність, вартість необхідних засобів, можливість використання не спеціалізованої апаратури).

$(К3)_f$ – Кількість, визначає кількість елементів об'єкту, яким характерна та або інша вразливість.

$$(К_{неб})_f = \frac{К_1 \times К_2 \times К_3}{125}. \quad (1.1)$$

Розглянемо наступну таблицю 2.14, враховуючи дані таблиці 2.8, виділимо загрози, які найбільше піддаються впливу зі сторони джерел загроз.

Таблиця 2.14 – Загрози, що найбільше піддаються впливу

| **Джерело загроз** | **Загроза** | **$К_{неб}$** |
|---|---|---|
| Кримінальні структури | Крадіжка (копіювання) інформації | 0,048 |
| | Знищення інформації | |

Продовження табл. 2.14

| Джерело загроз | Загроза | $К_{неб}$ |
|---|---|---|
| **Антропогенні, зовнішні** | | |
| Хакери | Змінення інформації | 0,216 |
| | Заперечення достовірності інформації | |
| | Нав'язування помилкової інформації | |
| Конкуренти | Крадіжка (копіювання) інформації | 0,128 |
| | Знищення інформації | |
| Відвідувачі | Крадіжка (копіювання) інформації | 0,096 |
| | Знищення інформації | |
| | Змінення інформації | |
| Будь які особи, що знаходяться за межами КЗ | Нав'язування помилкової інформації | 0,032 |
| **Антропогенні, внутрішні** | | |
| Директор | Знищення інформації | 0,64 |
| Основний персонал (користувачі мережі) | Знищення інформації | 0,384 |
| | Змінення інформації | |
| Адміністратор | Крадіжка (копіювання) інформації | 0,8 |
| | Знищення інформації | |
| | Змінення інформації | |
| | Порушення доступності (блокування) інформації | |
| | Нав'язування помилкової інформації | |

Продовження табл. 2.14

| Джерело загроз | Загроза | $К_{неб}$ |
|---|---|---|
| **Антропогенні, внутрішні (персонал, який не є авторизованими користувачами)** | | |
| Прибиральниця та охорона | Нав'язування помилкової інформації | 0,128 |
| **Техногенні, зовнішні** | | |
| Засоби зв’язку | Порушення доступності (блокування) інформації | 0,096 |
| Мережі інженерних комунікацій (система опалення, каналізації, водопостачання, заземлення) | Крадіжка (копіювання) інформації | 0,144 |
| Неякісне апаратне забезпечення | Крадіжка (копіювання) інформації | 0,192 |
| | Знищення інформації | |
| | Змінення інформації | |
| | Порушення доступності (блокування) інформації | |
| Неякісне програмне забезпечення | Знищення інформації | 0,192 |
| | Порушення доступності (блокування) інформації | |
| | Нав'язування помилкової інформації | |

2.4.2 Моделі порушника

Модель порушника (user violator model) — абстрактний формалізований або неформалізований опис порушника.

Порушник (user violator) – користувач, який здійснює НСД до інформації. Оскільки під порушником розуміється людина, то цілком зрозуміло, що створення його формалізованої моделі дуже складна задача. Тому, звичайно, мова може йти тільки про неформальну або описову модель порушника.

Порушник – це особа, яка може отримати доступ до роботи з включеними в склад АС засобами. Вона може помилково, унаслідок необізнаності, цілеспрямовано, за злим умислом або без нього, використовуючи різні можливості, методи та засоби здійснити спробу виконати операції, які призвели або можуть призвести до порушення властивостей інформації, що визначені політикою безпеки.

Зрозуміло, що в кожному конкретному випадку для кожного об'єкта визначаються імовірні загрози і моделі потенціальних порушників – «провідників» цих загроз, включаючи можливі сценарії їх здійснення. Цей етап дуже складний, оскільки від служби безпеки необхідно для кожного об'єкта вибрати з декількох можливих типів порушників один, на який і буде орієнтована система безпеки, що проектується. Відповідно до нормативних документів модель порушника – це абстрактний формалізований або неформалізований опис порушника.

Модель порушника відображає його практичні та потенційні можливості, апріорні знання, час та місце дії тощо.

При розробці моделі порушника визначаються:

– припущення щодо категорії осіб, до яких може належати порушник;

– припущення щодо мотивів дій порушника (цілей, які він переслідує);

– припущення щодо рівня кваліфікації та обізнаності порушника та його технічної оснащеності (щодо методів та засобів, які використовуються при здійсненні порушень);

– обмеження та припущення щодо характеру можливих дій порушників (за часом та місцем дії та інші).

Припускається, що у своєму рівні порушник – це фахівець вищої кваліфікації, який має повну інформацію про систему.

Звичайно розглядаються 5 типів порушників. Спочатку їх поділяють на дві групи: зовнішні і внутрішні порушники.

Зовнішні порушники включають:

– добре озброєну й оснащену силову групу, що діє зовні швидко і напролом;

– поодинокий порушник, що не має допуску на об'єкт і намагається діяти потайки й обережно, так як він усвідомлює, що сили реагування мають перед ним переваги.

Серед потенціальних внутрішніх порушників можна відзначити:

– допоміжний персонал об'єкту, що допущений на об'єкт, але не допущений до життєвоважливого центру АС;

– основний персонал, що допущений до житєвоважливого центру (найбільш небезпечний тип порушників);

– співробітників служби безпеки, які часто формально і не допущені до житєвоважливого центру, але реально мають достатньо широкі можливості для збору необхідної інформації і скоєння акції.

Категорія осіб, до якої може належати порушник:

– внутрішні порушники;

– користувачі,

– інженерний склад,

– співробітники відділів, що супроводжують ПЗ,

– технічний персонал, що обслуговує будинок,

– співробітники служби безпеки,

– керівники;

– зовнішні порушники.

Мета порушника:

– отримання необхідної інформації;

– отримання можливості вносити зміни в інформаційні потоки у відповідності зі своїми намірами;

– нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

Повноваження порушника в АС:

– запуск фіксованого набору задач (програм);

– створення і запуск власних програмних засобів;

– керування функціонуванням і внесення змін у конфігурацію системи;

– підключення чи зміна конфігурації апаратних засобів.

Технічна оснащеність порушника:

– апаратні засоби;

– програмні засоби;

– спеціальні засоби.

Кваліфікація порушника:

– для аналізу загроз завжди приймається висока кваліфікація.

Таблиця 2.15 – Модель порушника

| **Джерело загрози** | **Загрози** | | | **Інформація, яка зазнає впливу від джерел загроз** |
|---|---|---|---|---|
| | **К** | **Д** | **Ц** | |
| 1 | 2 | 3 | 4 | 5 |
| Директор | + | + | + | 1,2,3,5,6,7,8 |
| Заступник директора | + | + | + | 1,2,3,4,5,6,8 |
| Директор з розвитку | + | + | + | 2,3,7,8 |

Продовження табл. 2.15

| | | | | |
|---|---|---|---|---|
| Бухгалтер | + | + | + | 1,2,3,4,7 |
| Менеджер з продажів | + | + | + | 2,3 |
| Секретар | + | + | + | 1,2,7 |
| Адміністратор | + | + | + | 1,2,3,5,6,8 |
| Прибиральники та охорона | + | + | - | 2,3,8 |
| Кримінальні структури | + | + | + | 1,2,3,4,5,6,7,8 |
| Хакери | + | + | + | 1,2,3,4,5,6,7,8 |
| Конкуренти | + | + | + | 2,3,4,8 |
| Відвідувачі | + | + | + | 1,2,3,4,5,6,7,8 |
| Будь які особи, що знаходяться за межами КЗ | + | + | + | 1,2,3,4,5,6,7,8 |

Для того, щоб розуміти, яка інформація найбільше зазнає впливу від джерел загроз, продублюємо таблицю 2.10 – Класифікація інформації.

Таблицю 2.16 – Класифікація інформації

| **№** | **Вид інформації** | **Режим доступу** | **Вид зберігання** | **Вимоги** |
|---|---|---|---|---|
| 1 | Особисті дані персоналу | ІзОД | Паперовий та електронний | КЦД |
| 2 | БД підприємства | ІзОД | Паперовий та електронний | КЦД |

Продовження табл. 2.16

| № | Вид інформації | Режим доступу | Вид зберігання | Вимоги |
|---|---|---|---|---|
| 3 | Договори, укладені з клієнтами (партнерами) | ІзОД | Паперовий та електронний | КЦД |
| 4 | Інформація бухгалтерської звітності | ІзОД | Паперовий та електронний | КЦД |
| 5 | Інформація про стан мережі, її компонентів | ІзОД | Електронний | КЦД |
| 6 | Інформація про засоби захисту інформації | ІзОД | Паперовий та електронний | КЦД |
| 7 | Трудові договори | ІзОД | Паперовий | КЦД |
| 8 | Інформація, пов'язана з виробничою діяльністю | ІзОД | Паперовий та електронний | КЦД |
| 9 | Інформація про послуги та їх вартість | Відкрита | Паперовий та електронний | ЦД |
| 10 | Інформація про діяльність підприємства | Відкрита | Паперовий та електронний | ЦД |
| 11 | Статутні документи підприємства | Відкрита | Паперовий та електронний | ЦД |

В таблиці 2.17, за результатами моделей загроз та порушника, виділено найбільш значущі джерела загроз ІБ.

Таблиця 2.17 – Джерела загроз

| Джерела загроз | Небезпека |
|---|---|
| **Антропогенні** | |
| Директор | 0,48 |
| Адміністратор | 0,8 |
| Основний персонал (користувачі системи) | 0,288 |
| Прибиральники та охорона | 0,064 |
| Кримінальні структури | 0,016 |
| Конкуренти | 0,128 |
| Хакери | 0,144 |
| **Техногенні** | |
| Засоби зв'язку | 0,064 |
| Мережі інженерних комунікацій (система опалення, каналізації, водопостачання, заземлення) | 0,096 |
| Допоміжні засоби (протипожежна сигналізація, телефонія) | 0,128 |
| Неякісне програмне забезпечення | 0,128 |
| Неякісне апаратне забезпечення | 0,128 |
| **Стихійні** | |
| Пожежі | 0,064 |
| Землетруси | 0,016 |
| Підтоплення | 0,016 |
| Урагани | 0,016 |
| Різні непередбачені обставини | 0,032 |
| Інші форс-мажорні обставини | 0,032 |

Виходячи з таблиці 2.17, серед антропогенних джерел загроз найбільшу небезпеку становить адміністратор, він має коефіцієнт 0,8 та директор, у якого коефіцієнт становить 0,48. Серед техногенних джерел загроз, найбільший коефіцієнт отримали такі джерела загроз, як «Допоміжні засоби (протипожежна сигналізація, телефонія)», «Неякісне програмне забезпечення», «Неякісне апаратне забезпечення», у всіх них коефіцієнт становить 0,128. Та серед стихійних джерел загроз, найбільші коефіцієнт небезпеки 0,016 отримали землетруси, підтоплення та урагани.

## 2.5 Аналіз ризиків

Ризик (risk) — функція ймовірності реалізації певної загрози, виду і величини завданих збитків.

Аналіз ризиків передбачає вивчення моделі загроз для інформації та моделі порушників, можливих наслідків від реалізації потенційних загроз (рівня можливої заподіяної ними шкоди) і формування на його підставі моделі захисту інформації в ІКС. Під час проведення аналізу ризиків необхідним є виконання наступних робіт.

При ідентифікація загроз з об'єктами захисту встановлюється відповідність моделі загроз і об'єктів захисту, тобто складається матриця загрози/компоненти (ресурси) ІКС. Кожному елементу матриці повинен бути зіставлений опис можливого впливу загрози на відповідний компонент або ресурс ІКС. У процесі упорядкування матриці може уточнюватися список загроз і об'єктів захисту, внаслідок чого коригуватись модель загроз.

Під час оцінки ризиків повинні бути отримані оцінки гранично припустимого й існуючого (реального) ризику здійснення кожної загрози впродовж певного проміжку часу, тобто ймовірності її здійснення впродовж цього інтервалу. Для оцінки ймовірності реалізації загрози рекомендується вводити декілька дискретних ступенів (градацій). Оцінку слід робити за припущення, що кожна подія має найгірший, з точки зору власника інформації, що потребує захисту, закон розподілу, а також за умови відсутності заходів захисту інформації.

На практиці для більшості загроз неможливо одержати достатньо об'єктивні дані про ймовірність їхньої реалізації і доводиться обмежуватися якісними оцінками. У цьому випадку значення ймовірності реалізації загрози визначається в кожному конкретному випадку експертним методом або емпіричним шляхом, на підставі досвіду експлуатації подібних систем, шляхом реєстрації певних подій і визначення частоти їхнього повторення тощо.

Оцінка може мати числове або смислове значення (наприклад, ймовірність реалізації загрози – незначна, низька, висока, неприпустимо висока).

У будь-якому випадку існуючий ризик не повинен перевищувати гранично допустимий для кожної загрози. Перевищення свідчить про необхідність впровадження додаткових заходів захисту. Мають бути розроблені рекомендації щодо зниження ймовірності виникнення або реалізації загроз та величини ризиків.

Спочатку потрібно оцінити наслідки (цінність активів) у визначеному масштабі (0-4), кожного активу, якому загрожують (стовпчик «b» в таблиці 2.18). Наступним кроком потрібно оцінити імовірність входження загрози у визначеному масштабі (0-4), кожної загрози (стовпчик «c» в таблиці 2.18). Далі необхідно підрахувати міру ризику, множенням (b x c). Загрози можуть бути ранжовані в порядку їх зв'язаної міри ризику. В таблиці 2.11 використано 1, як найнижчий наслідок і найнижчу імовірність загрози. [21].

Таблиця 2.18 – Аналіз ризиків

| **Загрози** | **Наслідки (активи) Цінність (b)** | **Імовірність поширення загроз (c)** | **Міра ризику (d)** | **Ранжування загрози (e)** |
|---|---|---|---|---|
| Крадіжка (копіювання) інформації | 2 | 3 | 6 | 1 |
| Знищення інформації | 3 | 2 | 6 | 1 |
| Змінення інформації | 2 | 2 | 4 | 2 |

Продовження табл. 2.18

| **Загрози** | **Наслідки (активи) Цінність (b)** | **Імовірність поширення загроз (c)** | **Міра ризику (d)** | **Ранжування загрози (e)** |
|---|---|---|---|---|
| Порушення доступності (блокування) інформації | 2 | 1 | 2 | 3 |
| Заперечення достовірності інформації | 1 | 2 | 2 | 3 |
| Нав'язування помилкової інформації | 1 | 1 | 1 | 3 |

Для стовпців «b» і «c»:

1 – Низький

2 – Середній

3 – Високий

Для стовпця «e»:

1: 5 – 6 – Високий

2: 3 – 4 – Середній

3: 1 – 2 – Низький

Згідно таблиці 2.18, найбільші значення важливості отримали загрози «Крадіжка (копіювання) інформації» та «Знищення інформації» - 1 (ранжування здійснювалося в порядку пріоритетності, тобто 1 є найважливіше значення). Тому вони несуть в собі найбільший ризик для підприємства.

## 2.6 Профіль захищеності

Функціональний профіль захищеності складається з трьох частин: буквено-числового ідентифікатора, знаку рівності і переліку рівнів послуг, взятого в фігурні дужки. Ідентифікатор у свою чергу включає: позначення класу АС (1, 2

або 3), буквену частину, що характеризує види загроз, від яких забезпечується захист (К, і/або Ц, і/або Д), номер профілю і необов'язкове буквене позначення версії. Всі частини ідентифікатора відділяються один від одного крапкою.

Версія може служити, зокрема, для вказівки на підсилення певної послуги всередині профілю. Наприклад, нарощування можливостей реєстрації приведе до появи нової версії. Тим не менше, при внесенні деяких істотних змін, особливо додання нових послуг, може або привести до появи нового профілю, або до того, що профіль буде відноситись до іншого класу чи підкласу АС.

Перелік функціональних послуг безпеки та рівнів гарантій, їх структура і семантичне позначення наведені в НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу».

Після проведення обстеження ТОВ «ТоргСервіс» була вивчена його інформаційна діяльність, були вивчені об'єкти захисту – ІзОД, виявлені загрози, зроблений їх аналіз та побудована окрема модель загроз.

Стандартний функціональний профіль захищеності являє собою перелік мінімально необхідних рівнів послуг, які повинен реалізовувати КЗЗ обчислювальної системи АС, щоб задовольняти певні вимоги щодо захищеності інформації, яка обробляється в даній АС.

Стандартні функціональні профілі будуються на підставі існуючих вимог щодо захисту певної інформації від певних загроз і відомих на сьогоднішній день функціональних послуг, що дозволяють протистояти даним загрозам і забезпечувати виконання вимог, які пред'являються.

Для стандартних функціональних профілів захищеності не вимагається ні зв'язаної з ними політики безпеки, ні рівня гарантій, хоч їх наявність і допускається в разі необхідності. Політика безпеки КС, що реалізує певний стандартний профіль, має бути «успадкована» з відповідних документів, що встановлюють вимоги до порядку обробки певної інформації в АС. Так, один і той же профіль захищеності може використовуватись для опису функціональних

вимог з захисту оброблюваної інформації і для ОС, і для СУБД, в той час, як їх політика безпеки, зокрема визначення об’єктів, буде різною.

При утворенні нових профілів слід дотримуватися вимог, описаних в НД ТЗІ 2.5-004-99 [22].

Згідно з нормативними документами НД ТЗІ 2.5-004-99 і НД ТЗІ 2.5-005-99 треба визначити критерії захищеності даної АС. На досліджуваному ОІД АС належить до третього класу, а вимоги до захисту інформації (конфіденційність, цілісність та доступність),то обраний профіль має вигляд:

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 }

2.6.1 Аналіз виконання послуг профіля захищеності

Розглянемо таблицю 2.19, в якій наведені критерії, що виконуються.

Таблиця 2.19 – Критерії, що виконуються

| **Критерії** | **Пояснення** |
|---|---|
| КД-2. Базова довірча конфіденційність | Є розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта; адміністратор може вказати, які конкретні користувачі мають право одержувати інформацію від об'єкта. Виконується, так як є множина об'єктів КС. |
| КО-1. Повторне використання об'єктів | Виконуються, так як інформація, що знаходиться на звільненому об`єкті не стає недосяжною для інших користувачів. |
| КВ-1. Мінімальна конфіденційність при обміні | Виконується, якщо відомо, що при обміні інформацією використовуються захищені (зашифровані) лінії передачі. |
| ЦД-1. Мінімальна довірча цілісність | Виконується, так як користувач сам ранжує інформацію. |
| ЦО-1. Обмежений відкат | Виконується тому, що користувачу дозволяється відкатити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу. |

Продовження табл. 2.19

| Критерії | Пояснення |
|---|---|
| ЦВ-1. Мінімальна цілісність при обміні | Виконується автоматично в певних механізмах системи (наприклад: оновлення ОС, антивірусу). |
| ДР-1. Квоти | Виконується, так як користувач з правами адміністратора контролює кількість виділених ресурсів. |
| ДВ-1. Ручне відновлення | Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути КС до нормального функціонування<br>Виконується автоматично системними засобами до моменту останнього оновлення |
| НР-2. Захищений журнал | Виконується, так як для доступу до журналу треба мати права адміністратор, щоб потрапити до реєстру. |
| НК-1. Однонаправлений достовірний канал | Реалізується, так як використовується користувачем логін і пароль для входу в систему. Зв'язок з використанням даного каналу відбувається виключно користувачем, а не роботом. |
| НО-1. Виділення адміністратора | Реалізується, так як визначаються ролі адміністратора і звичайного користувача. |
| НЦ-2. КЗЗ з гарантованою цілісністю | Виконується, тому що КЗЗ має власного домену для підтримання захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування. |
| НТ-2. Самотестування при старті | Реалізується, бо йде перевірка файлів при запуску системи. |
| НВ-1: Автентифікація вузла | Виконується, так як йде оновлення операційної системи з офіційних серверів постачальника ОС. |

Також розглянемо таблицю 2.20, в якій наведені критерії не виконуються.

Таблиця 2.20 – Критерії, що не виконуються

| Критерії | Пояснення |
|---|---|
| КД-1. Мінімальна довірча конфіденційність | КЗЗ обмежує потоки інформації фіксованому списку процесів, ґрунтуючись на атрибутах доступу об'єктів і процесів; КЗЗ надає користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретні процеси або групи процесів, які мають право одержувати інформацію від об'єкта. |
| КД-3. Повна довірча конфіденційність | Адміністратор може вказати, права доступу для кожного конкретного користувача і групи користувачів. Не виконується тому, що ця політика відноситься до всіх об’єктів КС, а в нас тільки множина об’єктів. |
| КА–1. Мінімальна адміністративна конфіденційність<br>КА-2. Базова адміністративна конфіденційність | Політика адміністративної конфіденційності повинна визначати множину об'єктів ІКС, до яких вона відноситься. КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу процесу і захищеного об'єкта. КЗЗ повинен надавати можливість адміністратору для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретні процеси і/або групи процесів, які мають право одержувати інформацію від об'єкта. |
| КА-3. Повна адміністративна конфіденційність | Адміністратор або користувач, що має відповідні повноваження, може вказати конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта. Не виконується тому, що ця політика відноситься до всіх об’єктів КС, а в нас тільки множина об’єктів. |
| КК-1. Виявлення прихованих каналів | Має бути документована максимальна пропускна здатність кожного знайденого прихованого каналу, одержана на підставі теоретичної оцінки або вимірів. Не виконується тому, що ми не були ознайомлені з документальними системами, в яких знаходяться всі приховані канали. |

Продовження табл. 2.20

| Критерії | Пояснення |
|---|---|
| ЦД-2. Базова довірча цілісність | КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу процесу і захищеного об'єкта. Не реалізується, так як не має накладення обмежень на те, який процес або група процесів може модифікувати об’єкт. |
| ЦА-1. Мінімальна адміністративна цілісність | Адміністратор може керувати потоками інформації від користувачів до захищених об'єктів. |
| ДР-2. Недопущення захоплення ресурсів | Політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу. Не виконується тому, що ця політика охоплює всі об’єкти КС. |
| ДС-1. Стійкість при обмежених відмовах | Повинна визначати множину компонентів КС, до яких вона відноситься, і типи їх відмов, після яких КС в змозі продовжувати функціонування. |
| ДС-2. Стійкість з погіршенням характеристик обслуговування | Не реалізується, так як політика охоплює всі компоненти КС. Наприклад, якщо зламався вінчестер, то комп’ютер не змозі працювати далі. |
| ДЗ-1. Модернізація | Політика КЗЗ повинна визначати політику проведення модернізації ІКС. Адміністратор або користувачі, яким надані відповідні повноваження, повинні мати можливість провести модернізацію ІКС. Модернізація не повинна призводити до необхідності ще раз проводити інсталяцію ІКС або до переривання виконання КЗЗ функцій захисту. |
| ДЗ-2. Обмежена гаряча заміна | Визначає множину компонентів КС, які можуть бути замінені без переривання обслуговування. Не виконується. Наприклад, якщо зламався вінчестер, то має відбутися відновлення його, при цьому буде переривання обслуговування деяких програм. А це суперечить цьому критерію. |
| ДВ-2. Автоматизоване відновлення | Не виконується, так як не ознайомлені з процедурами, які можуть бути використані автоматизовані процедури для повернення КС до нормального функціонування. |

Продовження табл. 2.20

| Критерії | Пояснення |
|---|---|
| НР-1. Зовнішній аналіз | КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки. |
| НР-3. Сигналізація про небезпеку | Не виконується, бо немає механізму, який забезпечує роботу захисту системи. |
| НИ-1. Зовнішня ідентифікація і автентифікація | Не виконується, так як КЗЗ з використанням захищеного механізму не одержує від зовнішнього джерела логін і пароль користувача. |
| НК-2. Двонаправлений достовірний канал | Не реалізується тому, що після входу в КС не можемо переконатися, що система наша, а не зловмисника. |
| НО-2. Розподіл обов'язків адміністраторів | Не реалізується, так як у нас один адміністратор. |
| НЦ-1. КЗЗ з контролем цілісності | Рівень даної послуги є необхідною умовою для абсолютно всіх рівнів усіх інших послуг. КЗЗ повинен мати можливість перевіряти свою цілісність і у разі виявлення її порушення переводити систему в стан, з якого її може вивести тільки адміністратор. |
| НТ-1. Самотестування за запитом | КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій за запитом користувача, що має відповідні повноваження. |
| НВ-2: Автентифікація джерела даних | Не виконується, так як вбудований в систему антивірус не перевіряє надходжуючі оновлення. |
| НВ-3: Автентифікація з підтвердженням | Не виконується тому, що нема незалежної третьої сторони, все приймається адміністратором або уповноваженої особи. |
| НА-1: Базова автентифікація відправника | Не реалізується, бо система приймає документи, запити навіть без електронного підпису, але приймати чи не приймати, система дає на рішення адміністратору або уповноваженій особі. Залежить від політики безпеки. |

Продовження табл. 2.20

| Критерії | Пояснення |
|---|---|
| НП-1: Базова автентифікація отримувача | Встановлення належності має виконуватися на підставі затвердженого протоколу автентифікації. Не виконується. Залежить від політики безпеки. |

2.7 Розробка політики безпеки

1 Мета політики безпеки

Встановити правила користування бездротовою мережею підприємства ТОВ «ТоргСервіс», необхідні вимоги для безпечної роботи з конфіденційною інформацією та безпечної роботи мережі в цілому. Всі користувачі, що використовують бездротову мережу для доступу до інформаційних ресурсів, мають виконувати вимогу даної інструкції.

2 Область дії

Область дії даної інструкції є бездротова мережа підприємства та всі користувачі, що користуються нею.

3 Відповідальні особи політики безпеки

Відповідальною особою за виконання інструкції системним адміністратором є заступник директора.

4 Інструкція

Перед підключенням до бездротової мережі, на мобільній робочій станції мають бути встановлені критичні оновлення ОС та ПО, що використовується для обробки чи доступу до інформації, мають бути встановлені актуальні бази даних антивірусних систем.

При обробленні інформації, що є конфіденційною, користувач має контролювати, щоб сторонні особи, що не мають доступу до цієї інформації, не мали можливості несанкціоновано ознайомитися з екрану монітору.

Після включення адаптеру бездротової мережі, користувач має бути ввести свої автентифікаційні дані.

Паролі для доступу до бездротової мережі видаються заступником директора згідно документу «політика використання паролів».

Після проходження процедури автентифікації користувач отримує право доступу до інформації циркулюючої в ІКС підприємства.

Мобільна робоча станція, що використовується для доступу до ІКС підприємства зобов'язана мати пароль для доступу до ОС, пароль на BIOS.

Після виконання необхідної роботи з інформацією, користувач має відключитись від бездротової мережі

5 Затвердження політики

Політика безпеки розробляється системним адміністратором та підписується директором підприємства при прийнятті усіх розділів політики.

6 Дії з виконання інструкції інформаційної безпеки

Системний адміністратор контролює підключення до бездротової мережі, та має засоби моніторингу та виконання політики доступу. Заступник директор контролює виконання інструкції шляхом регулярного обходу приміщень.

7 Відповідальність

Системний адміністратор та заступник директору несуть відповідальність за виконання інструкції.

**Політика використання паролів**

1 Опис

Паролі – один з найважливіших аспектів інформаційної безпеки, так як погано підібраний пароль підвищує потенційний ризик несанкціонованого доступу в інформаційну систему компанії. Всі користувачі ІКС ТОВ «ТоргСервіс» (включаючи підрядників і третю сторону) несуть відповідальність за виконання вимог цієї політики.

2 Мета

Мета цієї політики встановити стандарти створення сильних паролів, їх захист, збереження і частоту зміни.

3 Область застосування

Ця політика належить до всього персоналу, хто має або відповідальний за доступ до конфіденційної інформації усіх рівнів (або будь-яка форма доступу, яка підтримує або вимагає пароля) на будь-якій системі, обладнанні, що має доступ (або що зберігає конфіденційну інформацію) до Вашої корпоративної мережі.

4. Політика

4.1 Паролі системних облікових записів (адміністратора домену, локального адміністратора, root і т. д.) повинні змінюватися щокварталу.

4.2 Всі паролі системних облікових записів, а також паролі додатків і активного обладнання необхідно зберігати в базі даних в зашифрованому вигляді, доступ до якої обмежений.

4.3 Термін дії паролів облікових записів домену повинен становити не більше 9 місяців. Рекомендований інтервал зміни пароля 6 місяців.

4.4 Пароль облікового запису користувача, який має адміністративні привілеї, отримані за допомогою членства в групі або за допомогою програм, таких як sudo, повинен бути унікальний по відношенню до інших паролів облікових записів даного користувача.

5 Інструкції

Інструкція по створенню пароля. ТОВ «ТоргСервіс» використовує паролі для різних цілей. Серед них: доступ до облікового запису користувача, до веб-інтерфейсів, до електронної пошти, для захисту зберігача екрану, паролі голосової пошти та доступ до маршрутизаторів. Оскільки дуже мало систем підтримують токени з одноразовими паролями (динамічні паролі, які використовуються тільки один раз), слід знати як вибрати стійкий пароль.

Погані, слабкі паролі володіють наступними ознаками:

– містять менше восьми символів;

– є словом, яке міститься в словниках (в т.ч. іноземних);

– є найбільш вживаним словом;

– містять прізвище, кличку тварини, імена друзів, співробітників, вигаданих персонажів і т. д.;

**Інструкція з організації антивірусного захисту**

1 Вступ

Ця Інструкція визначає вимоги до організації антивірусного захисту в ІКС ТОВ «ТоргСервіс» та встановлює відповідальність керівників і співробітників, що експлуатують та супроводжуючих ІКС, за виконання вимог цієї Інструкції.

2 Загальні положення

Для забезпечення інформаційної безпеки до використання в ІКС ТОВ «ТоргСервіс» допускаються тільки ліцензійні антивірусні засоби, централізовано закуплені у розробників (постачальників) зазначених коштів, рекомендовані до застосування СІП.

У разі необхідності використання антивірусних засобів, що не увійшли до переліку рекомендованих, необхідно узгодити їх застосування з системним адміністратором.

Установка засобів антивірусного контролю на ПК здійснюється системним адміністратором на всі ПК ІКС ТОВ «ТоргСервіс». Налаштування параметрів засобів антивірусного контролю здійснюється системним адміністратором щодо застосування конкретних антивірусних засобів.

3 Застосування засобів антивірусного контролю

Обов'язковому антивірусному контролю підлягають усі ПК, а також будь-яка інформація (текстові файли будь-яких форматів, файли даних, виконувані файли), одержувана і передана по телекомунікаційних каналах, а також інформація на знімних носіях (CD-ROM і т.п.).

Антивірусний контроль ПК повинен проводитися щоденно в автоматичному режимі при початковій завантаженні ПК.

Оновлення баз антивірусних засобів повинно проводитися регулярно в автоматичному режимі, для чого спеціалістом служби техпідтримки повинен бути налаштований доступ до серверів оновлень розробника антивірусного засобу. У разі неможливості налаштувати доступ до серверів оновлень розробника антивірусного засобу, спеціалісту служби техпідтримки необхідно один раз на

тиждень здійснювати установку пакетів оновлень вірусних баз, контроль їх підключення до антивірусного пакету і перевірку ПК на наявність вірусів.

У разі виявлення при проведенні антивірусної перевірки наявності в системі комп'ютерного вірусу співробітники ТОВ «ТоргСервіс» зобов'язані:

– негайно поставити до відома фахівця служби техпідтримки і припинити будь-які дії на персональному комп'ютері призупинити роботу;

– негайно поставити до відома керівника, відповідального за забезпечення інформаційної безпеки свого підрозділу, а також фахівця служби техпідтримки.

У разі виявлення наявності в системі комп'ютерного вірусу фахівці служби техпідтримки зобов'язані:

– спільно з власником заражених вірусом файлів провести аналіз необхідності подальшого їх використання;

– забезпечити видалення вірусу із системи;

– у разі виявлення нового вірусу, що не піддається лікуванню застосовуваними антивірусними засобами, спеціаліст служби техпідтримки повинен направити заражений вірусом файл системному адміністратору для подальшої передачі його в організацію, з якою укладено договір на антивірусну підтримку;

– за фактом виявлення вірусу повинна бути складена службова записка системному адміністратору, в якій потрібно вказати Можливий джерело (відправника, власника і т.д.) вірусу, тип зараженого файлу, характер міститься у файлі інформації, тип вірусу і виконані антивірусні заходи.

Користувачеві ІКС забороняється без схвалення системного адміністратора:

Встановлення (зміна) системного та прикладного програмного забезпечення повинна здійснюватися тільки в присутності спеціаліста служби техпідтримки. Встановлюване (змінюване) програмне забезпечення повинне бути попередньо перевірено спеціалістом служби техпідтримки на відсутність вірусів. Безпосередньо після встановлення (зміни) системного програмного забезпечення ІКС ТОВ «ТоргСервіс», повинна проводитися антивірусна перевірка:

– на захищаються ПК – відповідальним за забезпечення інформаційної безпеки;

– на інших ПК – особою, що встановила (змінила) програмне забезпечення, - у присутності і під контролем керівника даного підрозділу ТОВ «ТоргСервіс» або співробітника, ним уповноваженої.

У разі виявлення при проведенні антивірусної перевірки наявності в системі комп'ютерного вірусу співробітники ТОВ «ТоргСервіс» зобов'язані:

– негайно поставити до відома фахівця служби техпідтримки і припинити будь-які дії на персональному комп'ютері призупинити роботу;

– негайно поставити до відома керівника, відповідального за забезпечення інформаційної безпеки свого підрозділу, а також фахівця служби техпідтримки.

Користувач зобов'язаний:

– щодня при початковій завантаженні ПК переконатися в наявності резидентного антивірусного монітора і в разі його відсутності повідомити про це системного адміністратора;

– самостійно запускати позапланову антивірусну перевірку ПК при отриманні від системного адміністратора повідомлення про наявність в системі вірусу, а також при виникненні підозри на наявність вірусу.

4 Відповідальність

Відповідальність за організацію антивірусного контролю в ТОВ «ТоргСервіс», що експлуатує ІКС, відповідно до вимог цієї Інструкції покладається на керівника. Відповідальність за проведення заходів з антивірусного контролю та дотримання вимог цієї Інструкції покладається на відповідального за забезпечення інформаційної безпеки і всіх співробітників підрозділів, які є користувачами ІКС.

Періодичний контроль за станом антивірусного захисту в ІКС, а також за дотриманням встановленого порядку антивірусного контролю та виконанням співробітниками підрозділів ТОВ «ТоргСервіс» вимог цієї Інструкції здійснюється системним адміністратором.

Співробітники ТОВ «ТоргСервіс», які порушили вимоги цього документа, притягуються до відповідальності відповідно до чинного законодавства України.

**Інструкції щодо захисту підприємства від внутрішніх загроз для бухгалтерії**

Бухгалтер зобов'язаний:

1 Підписати угоду щодо нерозголошення інформації, яка становить комерційну таємницю, що є власністю ТОВ «ТоргСервіс».

2 Самостійно і в повному обсязі вести облік необоротних активів, запасів, коштів, розрахунків та інших активів, власного капіталу та зобов'язань, доходів та витрат за прийнятою на підприємстві формою бухгалтерського обліку з додержанням єдиних методологічних засад бухгалтерського обліку та з урахуванням особливостей діяльності ТОВ «ТоргСервіс» й технології оброблення даних.

3 Забезпечити повне та достовірне відображення інформації, що міститься у прийнятих до обліку первинних документах, на рахунках бухгалтерського обліку.

4 За погодженням з директором ТОВ «ТоргСервіс» подавати в банківські установи документи для перерахування коштів згідно з визначеними податками й платежами.

5 Брати участь у проведенні інвентаризації активів і зобов'язань, оформленні матеріалів, пов'язаних з нестачею та відшкодуванням втрат під нестачі, крадіжки й псування активів підприємства.

6 Готувати дані для включення їх до фінансової звітності, здійснювати складання окремих її форм, а також форм іншої періодичної звітності, яка грунтується на даних бухгалтерського обліку.

7 Забезпечити підготовку оброблених документів, реєстрів і звітності для зберігання їх протягом установленого терміну.

**Інструкції щодо захисту підприємства від внутрішніх загроз для заступника директора**

В обов’язки заступника директора додаються наступні положення:

1 Робота зі співробітниками підприємства, незалежно від ступеня конфіденційності інформації, до якої дані співробітники допущені (допускалися або будуть допускатися), проводиться:

– при прийомі кандидата на роботу, пов'язану з доступом до конфіденційної інформації (перекладі на цю роботу штатного працівника підприємства, не допущеного до такої інформації);

– в ході виконання співробітником підприємства, допущеним до конфіденційної інформації, посадових (функціональних) обов'язків;

– безпосередньо перед звільненням і в процесі звільнення працівника з підприємства.

2 В перелік основних методів перевірки і оцінки відповідності кандидата вимогам додати:

3 Вивчення матеріалів особової справи, анкетних, автобіографічних та інших персональних даних, резюме та інших документів кандидата;

5 Підвищення відповідальності працівників усіх категорій за збереження в таємниці довірених по службі відомостей конфіденційного характеру;

6 Проведення профілактичної роботи із запобігання (виключення) витоку конфіденційної інформації шляхом її розголошення;

7 Підвищення рівня теоретичних знань і практичних навичок співробітників в питаннях захисту конфіденційної інформації;

**Інструкції щодо захисту підприємства від внутрішніх загроз для системного адміністратора**

Системного адміністратор зобов’язаний:

1 Підписати угоду щодо нерозголошення конфіденційної інформації, що є власністю ТОВ «ТоргСервіс».

2 Забезпечувати конфіденційність, цілісність, доступність комп'ютерних баз даних.

3 Здійснювати систематичний аналіз керованих апаратних засобів і програмного забезпечення.

4 Усувати аварійні ситуації, пов'язані з пошкодженням ПЗ та баз даних.

5 Впровадити на сервері міжмережевий екран для фільтрації можливого шкідливого трафіку.

6 Забезпечити застосування системи резервного копіювання.

7 Затвердити усі програми, що використовуються для доступу до мережі Internet і налаштувати на них необхідні рівні безпеки.

8 Забезпечувати безперервну роботу серверу.

9 Створювати та змінювати паролі на всі робочі станції та облікові записи домену та на персонал, що з ними працює.

10 Створювати пароль відповідно до вимог «Політики використання паролів».

11 Впровадити на сервері систему контролю версіями.

12 Забезпечити доступ на сервер розробникам, які працюють віддалено.

**Інструкція з використання електронних ресурсів комп'ютерної мережі**

1 Загальні положення

1.1 Метою цієї інструкції є регулювання роботи системного адміністратора і користувачів, розподілу мережевих ресурсів колективного користування та підтримки необхідного рівня захисту інформації, її збереження, і дотримання прав доступу до інформації. Більш ефективного використання мережевих ресурсів і зменшення ризику навмисного чи ненавмисного неправильного їх використання.

1.2 До роботи в системі допускаються особи, призначені начальником відповідного відділу, які пройшли інструктаж та реєстрацію.

1.3 Робота в системі кожному працівникові дозволена тільки на певних комп'ютерах і тільки з дозволеними програмами і мережевими ресурсами. Якщо потрібно працювати на інших комп'ютерах і з іншими програмами, необхідно отримати дозвіл системного адміністратора.

1.4 Кожен користувач створює пароль для входу в комп'ютерну мережу. При цьому пароль повинен містити мінімум 8 символів, містити букви і цифри.

1.5 Кожен користувач повинен користуватися лише своїм іменем користувача та паролем для входу в локальну мережу та мережу Інтернет, передача їх будь-кому заборонено.

1.6 Для роботи на комп'ютері окрім користувача необхідний дозвіл системного адміністратора. Ніхто не може давати дозвіл на навіть тимчасову роботу на комп'ютері, без дозволу системного адміністратора або начальника відділу.

1.7 У разі порушення правил користування мережею, користувач повідомляє системного адміністратора, який проводить розслідування причин і виявлення винуватців порушень і вживає заходи щодо припинення подібних порушень. Якщо винуватцем порушення є користувач даного комп'ютера, адміністратор має право відсторонити винуватця від користування комп'ютером або вжити інші заходи.

1.8 Системний адміністратор - особа, що обслуговує сервер і стежить за правильним функціонуванням мережі. Системний адміністратор дає дозвіл на підключення комп'ютера до мережі, видає IP-адреса комп'ютера, створює

обліковий запис електронної пошти для користувача. Самовільне підключення є серйозним порушенням правил користування мережею.

2 Обов’язки користувачів мережі

2.1 Дотримуватися правил роботи в мережі, обумовлені цією інструкцією.

2.2 При доступі до зовнішніх ресурсів мережі, дотримуватися правил, встановлених системними адміністраторами для використовуваних ресурсів.

2.3 Негайно повідомляти системного адміністратора про виявлені проблеми у використанні наданих ресурсів, а також про факти порушення цієї інструкції ким-небудь. Адміністратор, при необхідності, за допомогою інших фахівців, повинен провести розслідування зазначених фактів і вжити відповідних заходів.

2.4 Не розголошувати відому їм конфіденційну інформацію (імена користувачів, паролі), необхідну для безпечної роботи в мережі.

2.5 Негайно відключати від мережі комп'ютер, який підозрюється в зараженні вірусом. Комп'ютер не повинен підключатися до мережі до тих пір, поки системний адміністратор не переконаються у видаленні вірусу.

2.6 Виконувати приписи, спрямовані на забезпечення безпеки мережі.

3 Заборонено

3.1 Дозволяти стороннім особам користуватися довіреним їм комп'ютером.

3.2 Використовувати мережеві програми, не призначені для виконання прямих службових обов'язків без узгодження з системним адміністратором.

3.3 Самостійно встановлювати або видаляти встановлені системним адміністратором мережеві програми на комп'ютерах, змінювати налаштування операційної системи та програм, що впливають на роботу мережевого обладнання та мережевих ресурсів.

3.4 Пошкоджувати, знищувати або фальсифікувати інформацію, що не належить користувачу.

3.5 Самовільно підключати комп'ютер до мережі, а також змінювати IP-адреса комп'ютера, виданий системним адміністратором.

Отже, для мінімізації загроз «Крадіжка (копіювання) інформації» та «Знищення інформації», які були виявлені на етапі «Аналіз ризиків», потрібно виконати:

1 Використання надійних паролів та їх регулярна зміна;

2 Встановити більш надійну антивірусну програму;

3 Встановити систему безпеки з контролем доступу;

4 Встановити firewall, для контролю потоку інформації з/в захищуваної мережі;

5 Впровадити до застосування DLP (Data Leak Prevention) и DBF (Database Firewall) для захисту файлів та баз даних;

6 Впровадження системи контролю і безпеки робочих станцій, для усунення загрози, зв’язаної з несанкціонованою користувачевою активністю (McAfee Endpoint Security);

2.8 Аналіз ризиків після впровадження політики безпеки

Розглянемо таблицю 2.21, в ній показано, як змінилися показники ризиків після застосування інструкцій політики безпеки.

Таблиця 2.21 – Аналіз ризиків після впровадження політики безпеки

| **Загрози** | **Наслідки (активи) Цінність (b)** | **Імовірність поширення загроз (c)** | **Міра ризику (d)** | **Ранжування загрози (e)** |
|---|---|---|---|---|
| Крадіжка (копіювання) інформації | 2 | **2** | **4** | **2** |
| Знищення інформації | 3 | **1** | **3** | **2** |
| Змінення інформації | 2 | **1** | **2** | **3** |
| Порушення доступності (блокування) інформації | 2 | **1** | **2** | **3** |
| Заперечення достовірності інформації | 1 | **1** | **1** | **3** |
| Нав'язування помилкової інформації | 1 | 1 | **1** | **3** |

Для стовпців «b» і «c»:

1– Низький

2– Середній

3– Високий

Для стовпця «e»:

1: 5 – 6 – Високий

2: 3 – 4 – Середній

3: 1 – 2 – Низький

Загрози «Крадіжка (копіювання) інформації» та «Знищення інформації», що представляли найбільший ризик для підприємства, які були виявлені у пункті «2.5

– Аналіз ризиків», тепер мають інші показники, менші, ніж до того, як були застосовані інструкції.

Тож тепер «Крадіжка (копіювання) інформації» має оцінку «Ранжування загрози» 2, що означає середній рівень, замість 1 - високого. Та загроза «Знищення інформації» має також має середній рівень, замість високого.

2.9 Висновки до другого розділу

Під час виконання другого розділу було виконано обґрунтування створення необхідності комплексної системи захисту інформації, встановлено яка інформація циркулює на підприємстві «ТоргСервіс». Згідно з Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» на ТОВ «ТоргСервіс» циркулює інформація з обмеженим доступом (персональні данні персоналу та клієнтів), вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю та конфіденційна інформація вимога щодо захисту якої встановлюється її власником. Були розглянуті загальні відомості про підприємство, проведено обстеження об’єкту інформаційної діяльності, зроблена класифікація інформації, зроблений аналіз інформаційних потоків, що циркулюють на підприємстві, виконаний аналіз загроз та вразливостей системи, розроблена модель загроз та модель порушника, проведений аналіз ризиків для виявлення слабких місць у системі забезпечення інформаційної безпеки. Також в ході виконання другого розділу був розглянутий профіль захищеності, розроблені інструкції політики безпеки та мінімізація реалізації ризиків втрати, викривлення, розголошення інформації, яка несе у собі життєвоважливі інтереси для підприємства.

# РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

## 3.1 Обґрунтування витрат на реалізацію політики безпеки

Метою економічного розділу є розрахунок витрат на створення та впровадження політики безпеки інформації в ІКС підприємства.

Завданням був розрахунок капітальних та експлуатаційних витрат на розробку та впровадження ПБ.

В кваліфікаційній роботі розглянуті засоби для протидії атакам, пов'язаних з використанням зовнішніх носіїв авторизованими користувачами підприємства.

Мета економічної частини:

- визначити капітальні витрати для програмного забезпечення, що використовується для протидії атакам, пов'язаним з використанням зовнішніх носіїв авторизованими користувачами підприємства
- визначити експлуатаційні витрати для програмного забезпечення, що використовується для протидії атакам, пов'язаним з використанням зовнішніх носіїв авторизованими користувачами підприємства
- розрахувати рівень передбачуваних збитків від атак на ІКС підприємства.

## 3.2 Розрахунок капітальних витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

Фіксовані витрати на впровадження системи розраховуватимуться за формулою:

$$К = К_{пр} + К_{навч} + К_{н} + К_{зпз}, \text{ грн.} \quad (3.1)$$

де $К_{пр}$ – вартість впровадження, грн.;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, грн.;

$К_{н}$ – витрати на встановлення та налагодження ПЗ, грн.;

$К_{зпз}$ – вартість закупівель, грн.

Розрахунок капітальних витрат буде проводитися на прикладі впровадження засобів захисту інформації та додаткового програмного забезпечення: резервне копіювання, контроль стану обладнання, інструктаж з ІБ, встановлення та налаштування ПЗ (DLP і DBF, Firewall тощо).

3.2.1 Розрахунок заробітної плати системного адміністратора

Обліком носіїв інформації, резервним копіюванням, встановленням фаєрволу, антивірусу, налагодженням та встановленням ПЗ та обліком носіїв інформації займається системний адміністратор.

Заробітна плата при простій часовій системі оплати праці визначається за формулою:

$$З = ТС* Ф, \quad (3.2)$$

де ТС – тарифна ставка привласненого робітникові кваліфікаційного розряду в одиницю часу (година, день, місяць), грн.;

Ф – фактично відпрацьований час;

Почасова тарифна ставка системного адміністратора складає ТС = 250 грн/год.

Час на налагодження резервного копіювання займає 4 год.:

$$З = ТС* Ф = 250*4 = 1000 \text{ грн.}$$

Час на розробку алгоритму захисту від витоку інформації займає 15 год.:

$$З = ТС* Ф = 250*15 = 3750 \text{ грн.}$$

Час на впровадження запропонованої політики безпеки займає 10 год.:

$$З = ТС* Ф = 250*10 = 2500 \text{ грн.}$$

Час на встановлення Firewall займе 2 год.:

$$З = ТС* Ф = 250*2 = 500 \text{ грн.}$$

Час на встановлення антивірусної програми McAfee займе 2 год.:

$$З = ТС* Ф = 250*2 = 500 \text{ грн.}$$

Час на встановлення Symantec DLP займе 4 год.:

$$З = ТС* Ф = 250*4 = 1000 \text{ грн.}$$

3.2.2 Розрахунок капітальних витрат

В таблиці 3.1 наведена кількісно-вартісна характеристика заходів, що впроваджується на підприємстві.

Таблиця 3.1 – Кількісно-вартісна характеристика заходів

| Міри | Характеристика | Вартість |
|---|---|---|
| Резервне копіювання | Kingston USB3.2 Gen 2 DataTraveler Max (DTMAX/512GB) (2929 грн. * 4 шт.) | 11716 грн. |
| Контроль інформації з/в захищуваної мережі (міжмережевий екран) | Zyxel ZyWALL ATP100 (ATP100-EU0112F) (31349 грн.) | 31349 грн. |
| Антивірусний захист | McAfee Internet Security 2023 (810 грн. * 7) | 5670 грн. |
| Проведення аналізу і контролю над конфіденційною інформацією | Symantec DLP (830,69 грн.) | 830,69 грн. |

Фіксовані витрати на проєктування та впровадження заходів захисту інформації складатимуть:

Резервне копіювання:

$$К = 1000 + 11716 = 12716 \text{ грн.}$$

Розробка алгоритму захисту від витоку інформації:

$$К = 3750 \text{ грн.}$$

Впровадження запропонованої ПБ:

$$К = 2500 \text{ грн.}$$

Міжмережевий екран Zyxel ZyWALL ATP100:

$$К = 500 + 31349 = 31849 \text{ грн.}$$

Антивірусний захист McAfee Internet Security 2023:

$$К = 500 + 5670 = 6170 \text{ грн.}$$

Контроль над конфіденційною інформацією Symantec DLP:

$$К = 1000 + 830,69 = 1830,69 \text{ грн.}$$

Загальні затрати складуть:

$$К = 58815,69 \text{ грн.}$$

## 3.3 Розрахунок експлуатаційних витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проєктування за визначений період (наприклад, рік), що виражені у грошовій формі.

Під «витратами на керування системою» маються на увазі витрати, пов'язані з керуванням й адмініструванням компонентів системи інформаційної безпеки. До цієї статті витрат можна віднести наступні витрати:

- навчання адміністративного персоналу й кінцевих користувачів;
- амортизаційні відрахування від вартості обладнання та ПЗ;
- заробітна плата персоналу;
- навчальні курси й сертифікація обслуговуючого персоналу;
- технічне й організаційне адміністрування й сервіс.

До експлуатаційних витрат віднесено:

- заробітну плату співробітника системного адміністратора;
- витрати на ліцензію антивірусу;
- витрати на резервне копіювання;
- витрати на розробку та впровадження алгоритму захисту;
- витрати на ліцензію іншого ПЗ.

Річні поточні витрати на функціонування системи заходів протидії загрозам інформації визначаються за формулою (3.3):

$$C = C_1 + C_2 + \ldots + C_n, \text{ грн}, \quad (3.3)$$

де С – вартість підтримки заходу протидії загрозам інформації;

n – порядковий номер заходів протидії загрозам інформації.

Обліком носіїв інформації, резервним копіюванням, підтримкою антивірусу та інших ПЗ займається системний адміністратор.

Заробітна плата системного адміністратора складає $З_{СА} = 250$ грн/год.

Час на резервне копіювання займе 1 год/тиждень:

$$С = ТС^* Ф = 250*1*50 = 12500 \text{ грн.}$$

Час на підтримку міжмережевого екрану займе 1 год/тиждень, затрати:

С = ТС* Ф = 250*1*50 = 12500 грн.

Час на підтримку антивірусного захисту займе 2 год/тиждень, затрати:

С = ТС* Ф = 250*2* 50 = 25000 грн.

Час на коригування алгоритму - 1 год/тиждень:

С = ТС* Ф = 250*1*50 = 12500 грн.

Час на підтримку займе Symantec DLP 1 год/тиждень, затрати:

С = ТС* Ф = 250*1*50 = 12500 грн.

Значення загальних річних поточних витрат складає:

С = 12500 + 12500 + 25000 + 12500 + 12500 = 75000 грн.

## 3.4 Визначення збитку від поломок обладнання

Запобігти поломкам обладнання практично неможливо. Природньо, первинна передумова наступна: витрати на ремонт або заміну деяких деталей обладнання не повинні перевищувати вартість самого обладнання.

Вихідні дані для підрахунку збитку:

- час простою внаслідок поломки, $t_п$ (в годинах), $t_п$ = 6 год.;
- час відновлення після поломки, $t_в$ (в годинах), $t_в$ = 4 год.;
- час повторного введення втраченої інформації, $t_{ви}$ (в годинах), $t_{ви}$ = 4 год.;
- заробітна плата обслуговуючого персоналу, $Z_0$ (грн. в місяць з податками), $Z_0$ = 35000 грн.;
- заробітна плата співробітників, $Z_с$ (грн. в місяць з податками), $Z_с$ = 25000 грн.;
- кількість обслуговуючого персоналу, $N_0$, $N_0$ = 1;
- число співробітників, $N_с$, $N_с$ = 9;
- прибуток , $О$ (грн. на рік), $О$ = 7000000 грн.;
- вартість заміни обладнання та запасних частин, виправлення помилок в роботі системи, $П_{зч}$ (грн.), $П_{зч}$ = 8000 грн;
- число зламаного обладнання, $I$, $I$ = 3;
- число поломок на рік, $n$, $n$ = 4.

Вартість втрат від зниження продуктивності співробітників несправного обладнання розраховується за формулою 3.4:

$$П_п = \frac{\sum Z_c}{\frac{N_c}{160}} \cdot t_п, \text{ грн.}, \quad (3.4)$$

де місячний фонд робочого часу при 40-а годинному робочому тижні 160 годин.

Підставивши вихідні дані отримаємо:

$$П_п = (9*25000/160)*6 = 8437,5 \text{ грн.}$$

Вартість відновлення зламаного обладнання розраховується за формулою 3.5:

$$П_в = П_{ви} + П_{пв} + П_{зч}, \text{ грн.} \quad (3.5)$$

де $П_{ви}$ – вартість повторного введення інформації (формула 3.6),

$П_{пв}$ – вартість відновлення обладнання (формула 3.7).

$$П_{ви} = \frac{\sum Z_c}{\frac{N_c}{160}} \cdot t_{ви}, \text{ грн.} \quad (3.6)$$

$$П_{пв} = \frac{\sum Z_o}{\frac{N_o}{160}} \cdot t_в, \text{ грн.} \quad (3.7)$$

Отримаємо:

$$П_{ви} = (9*25000/160)*4 = 5625 \text{ грн.}$$

$$П_{пв} = (1*35000/160)*4 = 875 \text{ грн.}$$

Вартість заміни обладнання та запасних частин, виправлення помилок в системі, $П_{зч}$ (грн.)

$$П_{зч} = 8000 \text{ грн.}$$

Підставивши отримані результати в загальну формулу отримаємо:

$$П_в = 5625 + 875 + 8000 = 14500 \text{ грн.}$$

Втрачена вигода від простою зламаного обладнання становить та розраховується за формулою 3.8 й 3.9 відповідно:

$$U = П_п + П_в + V, \text{ грн.} \quad (3.8)$$

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

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

V = (7000000/2080)*(6+4+4) = 47115,38 грн.

U = 8437,5 + 14500 + 47115,38 = 70052,88 грн.

Таким чином, загальний збиток від поломки обладнання, повторного введення інформації в системі, виявлення та усунення помилок в системі складе (формула 3.10):

$$ОУ = \sum_n \sum_I U, \text{ грн.} \quad (3.10)$$

ОУ = 4 * 3 * 70052,88 = 840634,56 грн.

3.5 Загальний ефект від впровадження політики безпеки

Загальний ефект від впровадження алгоритму для компанії визначається за формулою 3.11 з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = ОУ \cdot R - C, \text{ грн,} \quad (3.11)$$

де *ОУ*– загальний збиток від атаки на вузол або сегмент корпоративної мережі, грн.;

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

*C* – щорічні витрати на експлуатацію моделі підтримки прийняття рішень оцінки загроз інформаційній безпеці для компанії, грн.

Таким чином, загальний ефект від впровадження становить:

*E* = 840634,56 * 0,25 – 75000 = 135158,64 грн.

3.6 Визначення та аналіз показників економічної ефективності

Оцінка економічної ефективності моделі, розглянутої у спеціальній частині кваліфікаційної роботи, здійснюється на основі визначення та аналізу коефіцієнта повернення інвестицій *ROSI* (Return on Investment for Security) за формулою 3.12 та терміну окупності капітальних інвестицій $T_o$ за формулою 3.13.

$$ROSI = \frac{E}{K}, \text{ частки одиниці,} \quad (3.12)$$

де $E$ – загальний ефект від впровадження системи захисту, грн.;

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

Підставивши відповідні значення, маємо:

$$ROSI = 135158,64 / 58815,69 = 2,3$$

Організація здійснює фінансування капітальних інвестицій за рахунок реінвестування власних коштів (частини прибутку та амортизаційних відрахувань).

Проєкт визнається економічно доцільним, якщо розрахунковий коефіцієнт ефективності перевищує річний рівень прибутковості.

Отже, проєкт є економічно доцільним.

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

$$T_O = \frac{K}{E} = \frac{1}{ROSI}, \text{ років.} \quad (3.13)$$

Підставимо значення:

$$T_o = 1 / 2,3 = 0,43 \text{ (5,2 місяця).}$$

## 3.7 Висновки до третього розділу

У даному розділі була показана економічна доцільність впровадження запропонованої політики безпеки інформації інформаційно-комунікаційної системи, що доведено шляхом розрахунку:

- капітальних витрат на придбання та установку програмного забезпечення;
- експлуатаційних витрат на утримання та обслуговування програмного забезпечення;
- передбачуваних збитків від атак.

Розрахунки показали, що у випадку атаки на корпоративну мережу підприємства вартість збитків буде значно вищою, ніж вартість запропонованих засобів захисту.

Загальний ефект від впровадження системи інформаційної безпеки становить 135158,64 грн. Термін окупності складає трохи більше п’яти місяців.

Таким чином, можемо зробити висновок, що запропонована система є економічно вигідною і рекомендується до впровадження на підприємстві.

# ВИСНОВКИ

В ході виконання кваліфікаційної роботи була розглянута статистика інформаційних загроз на підприємствах, розпізнання внутрішніх загроз керівниками, декілька поглядів керівників організацій, щодо забезпечення інформаційної безпеки на підприємстві, також була розглянута статистика інцидентів здійснення атак, шахрайства та інших маніпуляцій зі сторони злочинців.

Був проведений аналіз нормативно-правової бази України у сфері захисту інформації, розглянуті державні, а також міжнародні стандарти, за допомогою яких регулюються інформаційні відносини на підприємстві, забезпечуються норми зберігання, обробки, поширення інформації.

Було виконано:

– обстеження об’єкту інформаційної діяльності;

– аналіз інформаційних потоків;

– аналіз загроз та вразливостей системи;

– побудувана модель порушника;

– аналіз ризиків для виявлення слабких місць у системі забезпечення інформаційної безпеки;

– обґрунтування вибору стандартного функціонально профіля захищеності;

– аналіз виконання вимог стандартного функціонального профіля захищеності;

– розроблені інструкції політики безпеки, для мінімізації реалізації ризиків втрати, викривлення, розголошення інформації, яка несе у собі життєвоважливі інтереси для підприємства.

Також було виконано обґрунтування створення необхідності комплексної системи захисту інформації та встановлено яка інформація циркулює на підприємстві ТОВ «ТоргСервіс». «Згідно з Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» на ТОВ «ТоргСервіс»

циркулює інформація з обмеженим доступом (персональні данні персоналу та клієнтів), вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю та конфіденційна інформація вимога щодо захисту якої встановлюється її власником». Були розглянуті загальні відомості про підприємство, проведено обстеження об'єкту інформаційної діяльності, зроблена класифікація інформації, зроблений аналіз інформаційних потоків, що циркулюють на підприємстві, виконаний аналіз загроз та вразливостей системи, розроблена модель загроз та модель порушника, проведений аналіз ризиків для виявлення слабких місць у системі забезпечення інформаційної безпеки.

Був зроблений підрахунок капітальних витрат на створення політики безпеки підприємства за рік.

# ПЕРЕЛІК ПОСИЛАНЬ

1. Ю.О. Коваленко – «Забезпечення інформаційної безпеки на підприємстві».

2. Берлач А. Безпека бізнесу. – К.: Університет «Україна», 2007.

3. Закон України «Про інформацію».

4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».

5. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».

6. Закон України «Про телекомунікації».

7. Закон України «Про захист персональних даних».

8. Закон України «Про доступ до публічної інформації».

9. НД ТЗІ 2.5-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту.

10. НД ТЗІ 2.5-002-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту.

11. НД ТЗІ 2.5-003-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту.

12. Наступний НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

13. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

14. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.

15. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт, можна встановити вимоги щодо порядку проведення робіт з технічного захисту інформації (ТЗІ).

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

17. ISO 27001

18. ISO 27002

19. Літнарович Р. М. Сучасні технології інформаційної безпеки – Навчальний посібник – Рівне, 2011.

20. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

| № | Формат | Найменування | Кількість листів | Примітки |
|---|---|---|---|---|
| *Документація* | | | | |
| 1 | А4 | Реферат | 2 | |
| 2 | А4 | Список умовних скорочень | 1 | |
| 3 | А4 | Зміст | 1 | |
| 4 | А4 | Вступ | 1 | |
| 5 | А4 | Розділ 1 | 13 | |
| 6 | А4 | Розділ 2 | 62 | |
| 7 | А4 | Розділ 3 | 9 | |
| 8 | А4 | Висновки | 2 | |
| 9 | А4 | Перелік посилань | 2 | |
| 10 | А4 | Додаток А | 1 | |
| 11 | А4 | Додаток Б | 1 | |
| 12 | А4 | Додаток В | 1 | |
| 13 | А4 | Додаток Г | 2 | |

ДОДАТОК Б. Перелік документів на оптичному носії.

1. Презентація_ Бурдюгов.ppt
2. Кваліфікаційна робота_ Бурдюгов.doc

# ДОДАТОК В. Відгук керівника економічного розділу

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (прізвище, ініціали)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

# В І Д Г У К

на кваліфікаційну роботу студента групи 125-20-1 Бурдюгова М.О. на тему: «Розробка політики безпеки інформації інформаційно-комунікаційної системи ТОВ «ТоргСервіс»

Пояснювальна записка містить 100 сторінок, 8 рисунків, 22 таблиці, 4 додатки, 20 джерел.

Метою кваліфікаційної роботи є підвищення рівня інформаційної безпеки інформаційно-комунікаційної системи ТОВ «ТоргСервіс».

В ході виконання кваліфікаційної роботи було визначено актуальність роботи, проаналізовано стан питання інформаційної безпеки в інформаційно-комунікаційній системи, розглянута статистика інформаційних загроз на підприємствах, проведено аналіз нормативно-правової бази України у сфері захисту інформації, розглянуті державні, а також міжнародні стандарти, за допомогою яких регулюються інформаційні відносини на підприємстві, забезпечуються норми зберігання, обробки, поширення інформації.

У спеціальній частині роботи було виконано обстеження об'єкту інформаційної діяльності, проаналізовано інформаційні потоки, проведено аналіз загроз та вразливостей системи, побудована модель порушника. Також обґрунтовано вибір стандартного функціонально профіля захищеності та розроблено інструкції політики безпеки.

В економічній частині було розраховані витрати на розробку та впровадження політики безпеки інформації інформаційно-комунікаційної системи ТОВ «ТоргСервіс».

Практична цінність кваліфікаційної роботи полягає у підвищенні рівня інформаційної безпеки та зниженні ризиків завдяки впровадженню політики забезпечення інформаційної безпеки.

В якості недоліків слід відзначити окремі невідповідності вимогам при оформленні та нечітке розкриття теми міжнародних стандартів у сфері захисту інформації.

Рівень запозичень у кваліфікаційній роботі відповідає вимогам «Положення про систему виявлення та запобігання плагіату».

В цілому робота задовольняє усім вимогам, а її автор Бурдюгов М.О. заслуговує на оцінку «  » та присвоєння кваліфікації «Бакалавр з кібербезпеки» за спеціальністю 125 Кібербезпека.

**Керівник роботи,**
**к.т.н., доц.** **Ковальова Ю.В.**