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 *Левітан Ольги Сергіївни*

академічної групи *125-18-3*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Політика безпеки інформації інформаційно-телекомунікаційної системи ТОВ «ЛевіДрім»*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.ф.-м.н., проф. Кагадій Т.С.	90	відмінно	
розділів:				
спеціальний	ст. викл Тимофєєв Д.С.	90	відмінно	
економічний	к.е.н., доц. Пілова Д.П.	95	відмінно	

Рецензент				

Нормоконтролер	ст. викл Тимофєєв Д.С.	95	відмінно	

Дніпро
2022

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту *Левітан О.С.* **академічної групи** *125-18-3*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації

за освітньо-професійною програмою *Кібербезпека*

на тему *Політика безпеки інформації інформаційно-телекомунікаційної системи ТОВ «ЛевіДрім»*

Затверджену наказом ректора НТУ «Дніпровська політехніка» від 18.05.2022№ 268-с

Розділ	**Зміст**	**Термін виконання**
Розділ 1	Проаналізувати стан питання, нормативно-правову базу. Виконати постановку задачі	15.05.2022
Розділ 2	Виконати обстеження об'єкту інформаційної діяльності, розробити моделі порушника та загроз, розробити елементи політики безпеки інформації	26.05.2022
Розділ 3	Виконати техніко-економічне обґрунтування доцільності запровадження політики безпеки підприємства	02.06.2022

Завдання видано _____ Кагадій Т.С.
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: 20.01.2022
Дата подання до екзаменаційної комісії: 09.06.2022

Прийнято до виконання _____ Левітан О.С.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 65 с., 8 рис., 18 табл., 9 додатків, 15 джерел.

Об'єкт розробки: інформаційно-телекомунікаційна система ТОВ «ЛевіДрім».

Предмет розробки: елементи політики безпеки інформації інформаційно-телекомунікаційної системи ТОВ «ЛевіДрім»

Мета кваліфікаційної роботи: забезпечення достатнього рівня захисту інформації у інформаційно- телекомунікаційній системі підприємства.

У першому розділі розглянуто загальний стан питання, наведена причина створення КСЗІ та політики безпеки інформації, проаналізована нормативно-правова база у сфері захисту інформації. Виконано постановку задачі.

У другому розділі виконано обстеження об'єкту інформаційної діяльності (ОІД), де циркулює інформація з обмеженим доступом (ІзОД), аналіз відомостей про підприємство та особливості обробки інформації, яка циркулює в компанії. Виходячи з цих даних, проаналізовано потенційні загрози та вразливості, розроблені моделі порушника та модель загроз. Згідно отриманих даних сформовані основні елементи політики безпеки інформації для інформаційно-телекомунікаційної системи (ІТС) за для мінімізації втрат ресурсів компанії.

В економічній частині здійснені розрахунки капітальних витрат на внесення основних елементів політики безпеки інформації та визначена доцільність їх впровадження.

Практична значимість роботи полягає у забезпеченні організаційної складової системи захисту інформації на підприємстві мінімізації потенційних втрат від реалізації загроз інформації з урахуванням особливостей її обробки в ІТС.

МОДЕЛЬ ПОРУШНИКА, ПОЛІТИКА БЕЗПЕКИ ІНФОРМАЦІЇ, АКТ ОБСЕЖЕННЯ, КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ІНФОРМАЦІЙНІ ПОТОКИ, МОДЕЛЬ ЗАГРОЗ, ЗАХИСТ ІНФОРМАЦІЇ, ОБ'ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

ABSTRACT

Explanatory note: 65 p., 8 pictures, 18 tables, 9 applications, 15 sources.

Object of development: information and telecommunication system LLC «LeviDream».

Subject of development: ensuring a sufficient level of information security policy in the information and telecommunication system LLC «LeviDream».

The purpose of the qualification work: increasing the overall level of information security in the information and telecommunication system.

The first section considers the general state of the issue, gives the reason for the creation information security policy, the relevance of creation and analyzes the legal framework in the field of information protection.

The second section examines the object of information activities, which circulates information with limited access and analysis of enterprise information and features of processing information circulating in the company. Based on these data, potential threats and vulnerabilities are analyzed, and a model of the violator is developed. According to the obtained data, the main elements of the information security policy for this information and telecommunication system are formed in order to minimize the loss of the company`s resources.

In the economic part, the main calculations of capital expenditures for the introduction of the main elements of information security policy to determine the feasibility of their implementation.

The practical significance of the work is to increase the level of information security to minimize the potential costs of information threats, taking into account the nature of its processing in the information and telecommunication system.

THREAT MODEL, INFORMATION SECURITY POLICY, INSPECTION ACT, VULNERABILITIES, INFORMATION SECURITY, COMPREHENSIVE INFORMATION SECURITY SYSTEM, OBJECT OF INFORMATION ACTIVITY, THREAD OF EXECUTION.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС- автоматизована система;

ДТЗС – допоміжні технічні засоби і системи;

ІзОД- інформація з обмеженим доступом;

ІТС- інформаційно-телекомунікаційна система;

КСЗІ – комплексна система захисту інформації;

НСД – несанкціонований доступ;

ОІД- об’єкт інформаційної діяльності;

ПБ – політика безпеки;

ПЗ- програмне забезпечення;

ПК- персональний комп’ютер;

ОІД- об’єкт інформаційної діяльності.

ЗМІСТ

ДОДАТОК Е. Перелік матеріалів на оптичному носії

ДОДАТОК Є. Відгук керівника економічного розділу

ДОДАТОК Ж. Відгук керівника кваліфікаційної роботи

ВСТУП

Об’єкт розробки: інформаційно-телекомунікаційна система ТОВ «ЛевіДрім».

Предмет розробки: елементи політики безпеки інформації інформаційно-телекомунікаційної системи ТОВ «ЛевіДрім»

Мета кваліфікаційної роботи: забезпечення достатнього рівня захисту інформації у інформаційно- телекомунікаційній системі підприємства.

КСЗІ (комплексна система захисту інформації) — сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС. [1]

На сьогоднішній день захист інформації стає більш складнішою проблемою, оскільки відбувається масове розповсюдження засобів електронної обчислювальної техніки, розповсюдження інформації про шифрувальні технології, використання неперевіреного програмного забезпечення (наприклад, що містить віруси), хакерські атаки, отриманням спаму, халатністю співробітників, що виникає доволі часто. Рідше втрата даних викликана такими причинами, як збій в роботі апаратно-програмного забезпечення або крадіжка обладнання. В результаті компанії зазнають значних втрат. Для визначення наявності у складі інформації видів, що потребують обмеження доступу, створюють КСЗІ (Комплексну систему захисту інформації) – взаємопов'язану сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації, – яка згідно з НД ТЗІ 3.7-003-2005 регламентується 6 етапами [2]:

1) формулювання загальних вимог до створення КСЗІ;
2) створення чи розробка політики безпеки;
3) розробка технічного завдання на створення КСЗІ;
4) створення КСЗІ;
5) впровадження КСЗІ (оцінка ефективності функціонування КСЗІ);
6) супроводження системи.

Розробка політики безпеки є одним із етапів побудови комплексної системи захисту інформації (КСЗІ). Метою політики є реалізація заходів, направлених на

захист підприємства від можливого нанесення йому та його клієнтам матеріальної, репутаційної чи іншої шкоди, яка може бути нанесена за допомогою випадкового чи навмисного впливу на об’єкти захисту. Зазначена мета досягається шляхом забезпечення властивостей об’єктів захисту, таких як доступність, цілісність та конфіденційність. Необхідний рівень доступності, цілісності та конфіденційності забезпечується впровадженням організаційних та технічних заходів, розроблених на підставі оцінки властивих об’єктам захисту ризиків інформаційної безпеки. Чим точніше буде розроблена політика безпеки- тим меншою буде ймовірність витоку інформації.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ.

1.1 Стан питання

Кіберзлочинці системно атакують банки, бізнес та держави в усьому світі. Лише з початку 2021 року фахівці Держспецзв'язку заблокували понад мільйон атак різних видів на державні ресурси та понад 250 DDoS-атак. У гонитві за мільйонними викупами хакери вдосконалюють свої навички, а лідери держав шукають спосіб їм протистояти на міжнародному рівні.

Зберегти конфіденційність інформації можна лише завдяки професійній стратегії з кіберзахисту. [3]

Атака хакерів – поширений злочин в цифровому світі. Негативний вплив може торкнутися фінансів, ділової репутації, прав на об'єкти інтелектуальної власності компанії, пошкодження обладнання тощо. Зловмисники можуть отримати доступ до закритих даних та шантажувати власників компанії. У 2021 році найпоширенішими є кібератаки саме на конфіденційні дані компаній та розголошення даних. Щоб подолати наслідки дій злочинців потрібен довгий час, значні кошти та можливості. Подекуди і це не допомагає. Домовленості з шахраями після атаки та викупи не дають гарантій, що викрадена інформація не стане надбанням суспільства, а злочинці не спробують атакувати знову.

За даними команди з технологій кібербезпеки Cybereason [14] 80% компаній потрапляють на гачок шахраїв, та, сплативши викуп один раз, змушені робити це постійно, бо атаки починаються з новою силою. Злочинці претендують на більші суми. Інститут Національної Безпеки США зафіксував, що у 2018 році середня сума викупу становила 5 тисяч доларів, а у 2021 – вже 200 тисяч доларів. Але як повідомляє провайдер фінансової інформації Bloomberg, страховій компанії CNA Financial довелося поставити невтішний рекорд – її власники віддали хакерам 40 мільйонів доларів.

Щоб врахувати індивідуальні особливості, притаманні окремій організації, та грамотно розробити стратегію кіберзахисту, потрібно розуміти, які найбільш типові хакерські атаки:

- Розсилка спаму, вірусів.
- DDoS-атаки, коли сайт атакується не з одного джерела, а одночасно з багатьох напрямів, гальмуючи його роботу.

- Злам мережі, електронної пошти, хмарних сервісів.
- Незаконний доступ до таємної інформації та фішинг.
- Загрози пристроям та ПЗ.

Із такими проблемами сьогодні стикається не лише великий та середній бізнес. 43% кібератак націлені на малі підприємства. Тобто будь-яка компанія може потрапити під атаку хакерів, якщо її власники не подбали про безпеку. [4]

Інформація та інформаційні ресурси, у процесі функціонування сучасних ІТС зазнають впливу цілого ряду загроз, внаслідок чого виникають порушення її цілісності, доступності з боку авторизованих та неавторизованих користувачів. Для забезпечення захисту інформації існує ціла низка напрямів забезпечення інформаційної безпеки, які направлені на зниження ймовірності виникнення загрози та порушення базових властивостей інформації. Нормативно-правове забезпечення, як первинний етап при побудові комплексної системи захисту інформації сучасних ІТС є найважливішою складовою для забезпечення ефективного і надійного захисту інформації та інформаційних ресурсів.

Під поняттям нормативно-правового забезпечення слід розуміти сукупність правових норм, що визначають порядок створення, правовий статус і функціонування захищених ІТС, регламентують порядок одержання, перетворення та використання інформації і інформаційних ресурсів.

Тобто нормативно-правове забезпечення регламентує та визначає порядок захисту визначених політикою безпеки властивостей інформації (конфіденційності, цілісності та доступності) під час створення та експлуатації інформаційної мережі; регламентує порядок ефективного знешкодження і попередження загроз для ресурсів шляхом побудови комплексної системи захисту інформації; статус інформаційної системи з точки зору інформаційної безпеки; права, обов'язки й відповідальність персоналу роботи яких пов'язані з інформаційною безпекою; правові положення окремих видів процесу керування та управління доступом в захищених ІТС; порядок створення й використання захищених ІТС; етапи побудови КСЗІ.

Під час створення комплексної системи захисту інформації, як сукупності організаційних і інженерних заходів, програмно-апаратних засобів слід керуватися низкою нормативно-правових документів та актів. Базовими нормативними документами при організації та побудови комплексної системи захисту інформації в ІТС є:

Закон України «Про інформацію» - цей Закон регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації. [5];

Закон України «Про захист інформації в автоматизованих системах» - цей Закон регулює відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах [6];

НД ТЗІ 1.1-002-99: Загальні положення з захисту інформації в комп'ютерних системах від НСД (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. No 22) - Цей нормативний документ технічного захисту інформації (НД ТЗІ) визначає методологічні основи (концепцію) вирішення завдань захисту інформації в комп'ютерних системах і створення нормативних і методологічних документів, регламентуючих питання:

-визначення вимог щодо захисту комп'ютерних систем від несанкціонованого доступу;

-створення захищених комп'ютерних систем і засобів їх захисту від несанкціонованого доступу;

-оцінки захищеності комп'ютерних систем і їх придатності для вирішення завдань споживача. [7] ;

НД ТЗІ 1.1-003-99: Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. No 22) - цей документ установлює терміни і визначення понять у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

Терміни, що установлюються цим документом, обов'язкові для застосування в усіх видах документації і літератури, що входять до системи технічного захисту інформації.

Для кожного поняття встановлено один термін. Застосування синонімів терміна не допускається.

Для довідки наведені іноземні еквіваленти термінів, що запроваджуються, а також алфавітні покажчики термінів. [8];

НД ТЗІ 1.4-001-2000: Типове положення про службу захисту інформації в автоматизованій системі (введено в дію Наказом ДСТСЗІ СБУ від 04.12.2000 р. No 53)- Цей нормативний документ системи технічного захисту інформації (НД ТЗІ) встановлює вимоги до структури та змісту нормативного документу, що регламентує діяльність служби захисту інформації в автоматизованій системі - "Положення про службу захисту інформації в автоматизованій системі". [9];

НД ТЗІ 2.5-005-99: Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. No 22)- Цей документ установлює принципи класифікації автоматизованих систем і утворення стандартних функціональних профілів захищеності оброблюваної інформації від несанкціонованого доступу.

Цей документ 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. [10];

НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. No 22) - Цей нормативний документ — установлює критерії оцінки захищеності інформації, оброблюваної в комп'ютерних системах, від несанкціонованого доступу.

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. [11];

НД ТЗІ 3.7-001-99: Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі (введено в дію Наказом ДСТСЗІ СБУ від 28.04.199 р. No 22) - Цей нормативний документ встановлює вимоги до порядку розробки, складу і змісту технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі, призначеній для оброблення, зберігання і передачі (далі — оброблення) інформації з обмеженим доступом або інформації, захист якої гарантується державою.

Положення цього документа розповсюджуються на державні органи, Збройні Сили, інші військові формування, МВС, Раду Міністрів Автономної Республіки Крим і органи місцевого самоврядування, а також підприємства, установи і організації всіх форм власності, які володіють, користуються і розпоряджаються інформацією, яка належить до державних інформаційних ресурсів, або інформацією, вимога щодо захисту якої встановлена законом. Власники (користувачі) іншої інформації, положення цього документа застосовують на свій розсуд. [8] .

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

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

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

Державним центром кіберзахисту було проаналізовано статистику категорій подій ІБ та їх типи за останній рік. Результати наведено на Рис 1.1, звідки можна зробити висновок, що найпоширенішими атаками є: шкідливий програмний код, збір інформації зловмисником та інше. Також було проаналізовано категорії детектувань аномалій на основі поведінкового аналізу. Результати наведено на Рис. 1.1.2, звідки висновок, що найпоширенішими атаками є сканування та порушення мережевої політики безпеки.

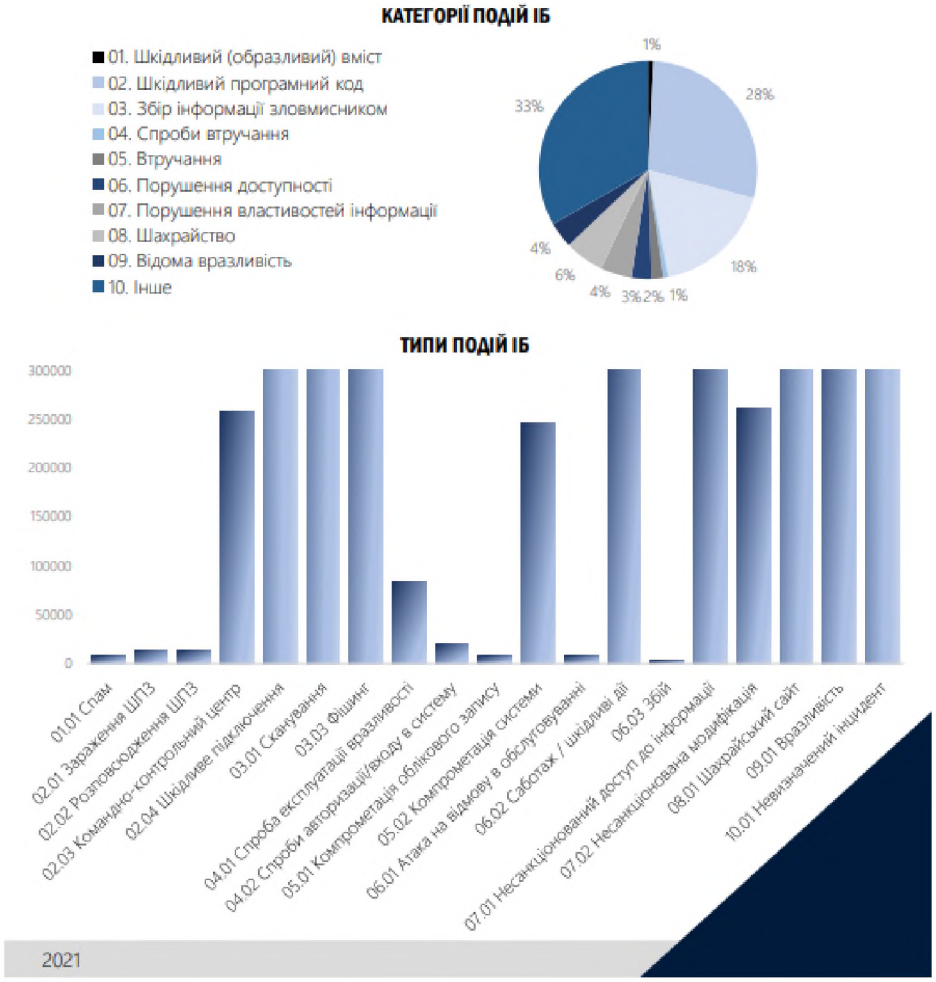


Рис 1.1 Статистика зібраних та опрацьованих даних

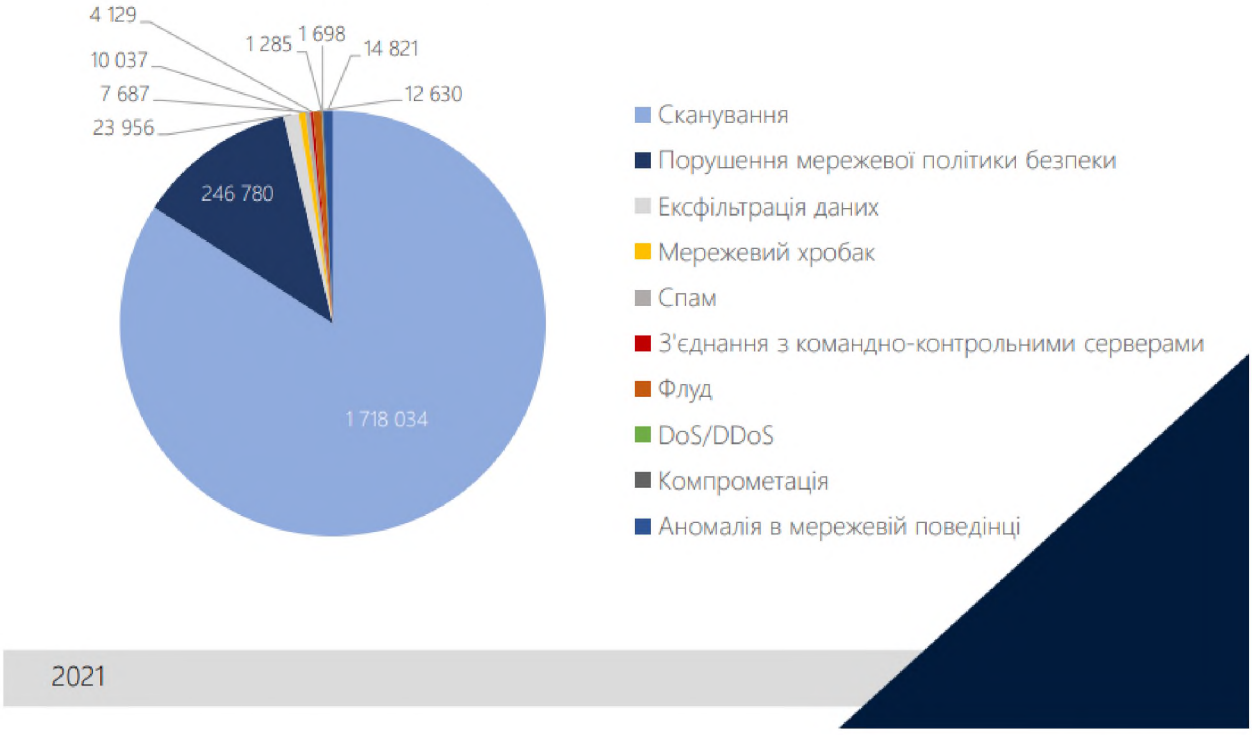


Рис. 1.1.2 Категорії детектувань на основі поведінкового аналізу

1.2 Визначення необхідних умов створення КСЗІ

Комплексна система захисту інформації (КСЗІ) — сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в ІТС. [1]

До складу КСЗІ входять заходи та засоби, які реалізують методи, механізми захисту інформації від несанкціонованих дій та несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм, використання комп'ютерних вірусів та ін;

Для організації робіт зі створення КСЗІ в ІТС створюється служба захисту інформації, порядок створення, завдання, функції, структура та повноваження якої визначено в НД 1.4-001-2000.

Розглянемо основні етапи створення КСЗІ

При створенні КСЗІ дозволяється виключати окремі етапи робіт або поєднувати декілька етапів, а також включати нові етапи робіт. За необхідністю дозволяється змінювати послідовність виконання окремих етапів – виконувати одночасно декілька етапів робіт, окремі етапи виконувати до завершення попередніх і т.п., якщо це не призводить до зниження якості робіт і не суперечить цілям їх виконання.

- Формування загальних вимог до КСЗІ в ІТС;
- Розробка політики безпеки інформації в ІТС;
- Розробка технічного завдання на створення КСЗІ;
- Розробка проекту КСЗІ;
- Введення КСЗІ в дію та оцінка захищеності інформації в ІТС.

1.3 Висновок до першого розділу

У цьому розділі було зазначено стан питання та визначено необхідні умови для створення КСЗІ в ІТС. Після повного аналізу, обстеження та вияву усіх можливих загроз можна розпочати розробку елементів КСЗІ ІТС підприємства.

Задача полягає у розробці політики безпеки підприємства ТОВ «ЛевіДрім» та рекомендацій з впровадження її на ОІД.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Повні відомості про підприємство

Товариство з обмеженою відповідальністю «ЛевіДрім» займається оптовою закупівлею та продажом метизної продукції по всій Україні. Головний офіс знаходиться за адресою: м. Дніпро, вулиця Метизна, 19. Підприємство було створене у 2000 році і має велику кількість клієнтів. Саме через це підприємство потребує якісного та надійного захисту від усіх витоків інформації. Це дуже важливо для репутації компанії, бо клієнти користуються послугами щодня.

Характеристика підприємства:

Офіс компанії займає перший поверх будівлі.

Адреса: вул. Метизна, 19. Дніпро, Дніпропетровська область, 49000.

Графік роботи:

Понеділок-П'ятниця: з 9 до 18:30.

Обідня перерва: з 12 до 13.

Керівником підприємства було призначено комісію з категоріювання. За результатами обстеження об'єкту було присвоєно IV категорію. Акт категоріювання наведено у ДОДАТКУ Д.

Керівником підприємства було прийнято рішення про створення КСЗІ та видано відповідний наказ, який наведено у ДОДАТКУ Ґ.

2.2 Обстеження фізичного середовища

Об'єктом інформаційної діяльності (ОІД) є товариство з обмеженою відповідальністю «ЛевіДрім».

Ситуаційний план наведено у ДОДАТКУ Б.

Адреса підприємства: вул. Метизна, 19. Дніпро, Дніпропетровська область, 49000. Знаходиться на першому поверсі трьох поверхового будинку.

Генеральний план наведено у ДОДАТКУ В.

Площа ОІД: 115 $м^2$

Висота стель – 3 м, стінні перегородки- 150 мм, стіни зовнішні з цегли – 400 мм.

Вікна: 9 шт, металопластикові, подвійні, з розміром 1500 мм * 2000 мм

Вхідні двері до підприємства: металопластикові, потрійне скло, з розміром 1500 мм * 2000 мм

Міжкімнатні двері: 3 шт, матеріал – МФД, з розміром 2000 мм * 800 мм

Підлога: ламінат

Контрольована зона (КЗ) обмежена стінами ОІД. Режим КЗ здійснюється за допомогою охоронної системи, постійною відео реєстрацією подій, у неробочий час вхідні двері закриті на вирізний замок та захищені металевими ролетами. Ключі від ОІД має лише директор, заступник директора та бухгалтер.

Підключені комунікації:

ОІД має доступ до мережі Інтернет, підключення здійснюється оптично-волокнистим кабелем, доступ надає компанія «Воля».

Система опалення централізована, труби стояку йдуть з 0 поверху до КЗ, а потім до офісів вище.

Система заземлення у будівлі відсутня.

Система охорони та сигналізації:

- Датчик диму;
- Магнітоконтактні датчики на відкриття на дверях та вікнах;
- Інфрачервоні датчики руху;
- Камери відеоспостереження;
- Головна централь з клавіатурою.

План системи охоронно-пожежної сигналізації наведено у ДОДАТКУ Ґ.

Таблиця 2.1 Відстань від інших будівель до КЗ

№	Відстань від КЗ, м	Адреса	Призначення будівлі
1	65	Вул. Метизна 23	Будівля з комерційними приміщеннями для оренди
2	80	Вул. Метизна 17	Житловий будинок

Продовження таблиці 2.1

№	Відстань від КЗ, м	Адреса	Призначення будівлі
3	37	Вул. Метизна 34	Житловий будинок
4	40	Вул. Метизна 38	Житловий будинок
5	120	Вул. Гончара 12	Будівля з комерційними приміщеннями для оренди
6	90	Вул. Гончара 16	Житловий будинок
7	110	Вул. Метизна 30	Салон краси

2.3 Організаційна структура підприємства та його аналіз

Кількість працівників на підприємстві- 6 чоловік:

- Генеральний директор
- Бухгалтер
- 2 менеджери з продажу
- Системний адміністратор

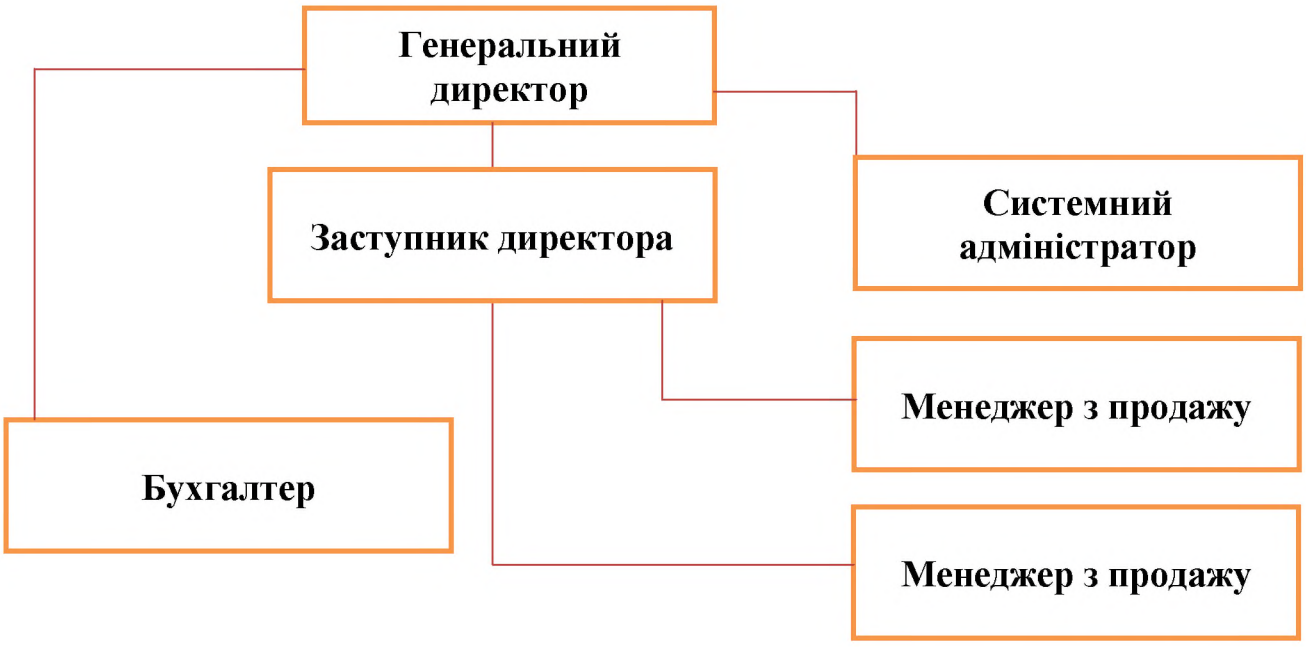


Рис 2.1 Організаційна структура підприємства

До обов'язків генерального директора входить: укладання договорів, підбір персоналу та вирішення організаційних питань.

До обов'язків заступника генерального директора входить: виконання поручень генерального директора та контролювання роботи менеджерів з продажу. Заступнику директора надаються повноваження на відповідальність за захист інформації

До обов'язків бухгалтера входить: підготовка звітів та нарахування заробітної плати.

До обов'язків менеджерів з продажу входить: пошук клієнтів, підготовка документів до укладання договорів та продаж продукції підприємства.

До обов'язків системного адміністратора входить: усунення технічних несправностей, технічна підтримка елементів 1С, забезпечення розмежування доступу співробітників до інформації згідно політики безпеки, підтримка працездатності системи, створення резервних копій даних, видалення шкідливого ПЗ та вірусів, оновлення системи.

Також задіяний обслуговуючий персонал власника будівлі:

- Прибиральниця
- Охоронник

За необхідністю, їм буде наданий доступ до ОІД.

Інформація на підприємстві зберігається у паперовому та електронному вигляді. Власник інформації – генеральний директор. На ОІД циркулює відкрита інформація та конфіденційна інформація з обмеженим доступом.

Інформаційна безпека складається з трьох основних вимог:

- Конфіденційність - властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом;
- Цілісність - властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом;
- Доступність - властивість ресурсу системи (КС, послуги, об'єкта КС, інформації), яка полягає в тому, що користувач і/або процес, який володіє

відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний

Таблиця 2. 2 – Класифікація інформації, що обробляється на ОІД

Вид інформації	Представлення в АС	Режим доступу	Правовий режим	Вимоги до власт. Інформ.		
				К	Ц	Д
Каталог	Електронний та паперовий	Відкрита	-	1	3	3
Графік роботи	Електронний та паперовий	Відкрита	-	1	2	3
Трудові договори	Електронний та паперовий	ІзОД	Конфіденційна	3	2	2
Інформація про співробітників	Електронний та паперовий	ІзОД	Конфіденційна	3	3	2
Інформація про клієнтів	Електронний та паперовий	ІзОД	Конфіденційна	3	2	2
Інформація про постачальників	Електронний та паперовий	ІзОД	Конфіденційна	3	2	2
База замовлень	Електронний	ІзОД	Конфіденційна	3	2	2
Паролі для доступу до системи	Електронний	ІзОД	Конфіденційна	3	3	3

Продовження таблиці 2.2

Вид інформації	Представлення в АС	Режим доступу	Правовий режим	Вимоги до власт. Інформ.		
				К	Ц	Д
Інформація про заробітню платню	Електронний та паперовий	ІзОД	Конфіденційна	3	2	1
Статистична інформація	Електронний	ІзОД	Відкрита	1	3	2
Накладні на товар	Електронний та паперовий	ІзОД	Конфіденційна	2	3	2
Інформація про складові ІТС	Електронний та паперовий	ІзОД	Конфіденційна	2	2	2
Установчі документи підприємства	Електронний та паперовий	ІзОД	Конфіденційна	1	3	2

К – вимоги до конфіденційності, 3- підвищена, 2- середня, 1- низька;

Ц – вимоги до цілісності, 3- підвищена, 2- середня, 1- низька;

Д- вимоги до доступності, 3- підвищена, 2- середня, 1- низька.

2.4 Опис обчислювальної системи ОІД

Обчислювальна система поєднує в собі технічні пристрої, що знаходяться в межах ОІД. Підключення до мережі Інтернет забезпечує Інтернет провайдер «Воля», який надає послуги відповідно договору.

Обладнання інформаційної системи складається з 6 комп'ютерів, 3 принтерів та Wi-Fi роутера. Перелік основних технічних засобів наведено у

таблиці 2.3. Розташування ОТЗ наведено на рисунку 2.3. Схема ІТС наведена на рисунку 2.4.

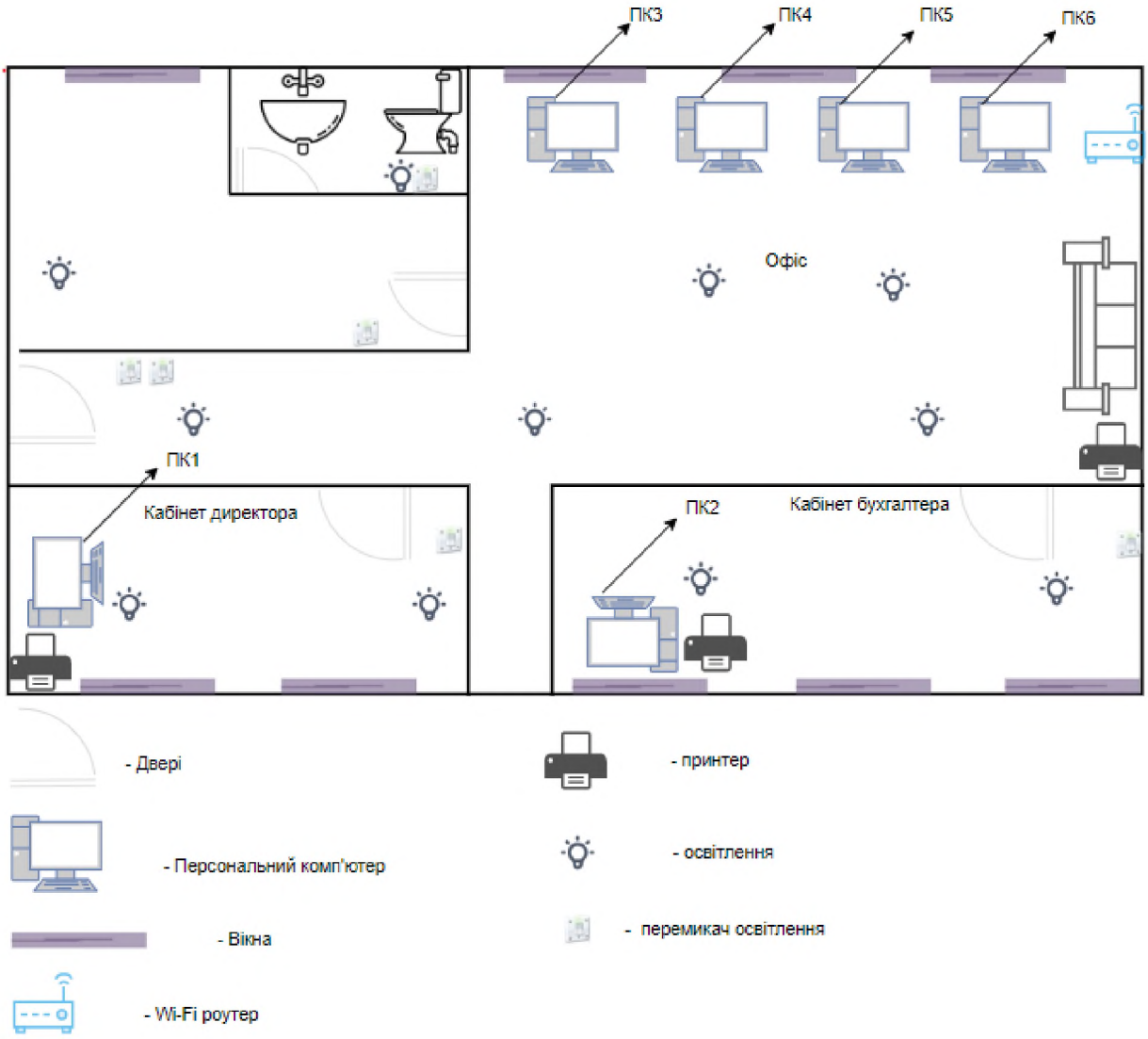


Рисунок 2.4.1 – Розташування складових ІТС

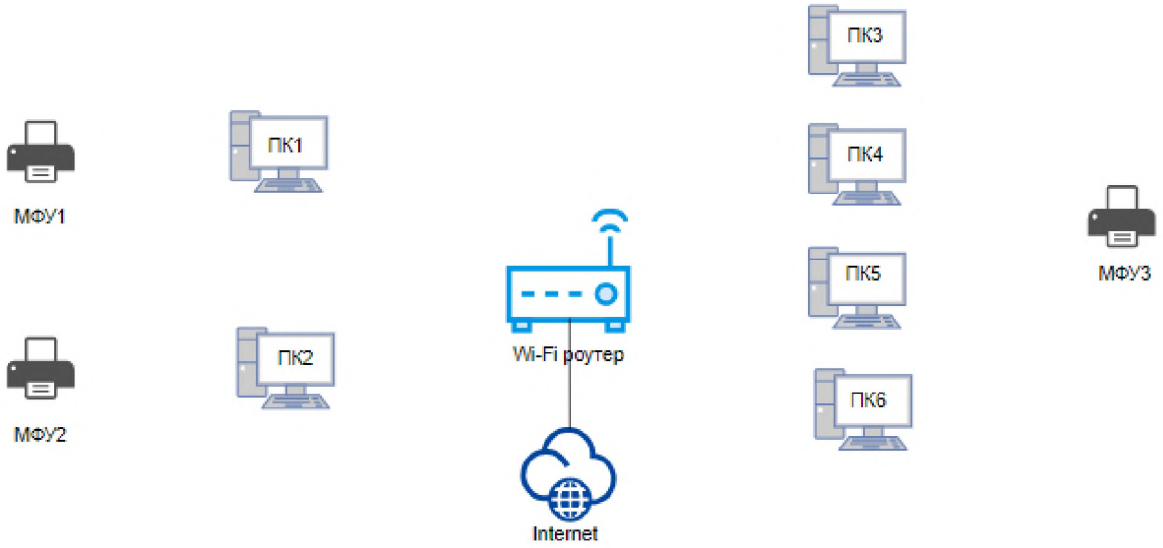


Рисунок 2.4.2 – Схема ІТС

Таблиця 2.4.1 Перелік основних технічних засобів

Назва у системі	Кількість	Назва обладнання	Системні характеристики	Місце розташування
ПК1, ПК2	2	Ноутбук ASUS Zenbook UX435EGL-KC051T	Дисплей – 14, 1920 x 1080 (Full HD) Процесор- Intel Core i5-1135G7 (Tiger Lake) 2,4- 4,2 ГГц Оперативна пам’ять- 16 ГБ, SSD- 1 ТБ, Відеокарта – NVIDIA GeForce MX450	Кабінет бухгалтерії, кабінет директора

Продовження таблиці 2.4.1

Назва у системі	Кількість	Назва обладнання	Системні характеристики	Місце розташування
ПК3, ПК4, ПК5, ПК6	4	Ноутбук HP ENVY x360 15-es1000ua	Дисплей – 15, 6, 1920x1080 (Full HD) Процесор- Intel Core i5-1155G7 (Tiger Lake), 2,5- 4,5 ГГц Оперативна пам'ять- 16 ГБ, SSD- 512 ГБ Відеокарта- Intel Iris Xe Graphics	Торгівельний зал
Принтер	3	МФУ лазерне Canon Ir2206	-	Торгівельний зал, кабінет генерального директора, кабінет бухгалтерії
Комп'ютерна миша	5	Миша HP Wireless Mouse X200	-	Торгівельний зал, кабінет генерального директора, кабінет бухгалтерії
Wi-Fi роутер		TP-LINK ARCHER C64 AC1200 4Xge LAN 1Xge WAN MU-MIMO	-	Торгівельний зал

2.5 Модель порушника

Якщо існує інформаційна система, у якій циркулює інформація з обмеженим доступом та конфіденційні дані, то знайдеться особа (порушник), метою якої буде ознайомлення з інформацією, її модифікація чи знищення. Для того, щоб розробити комплекс заходів по забезпеченню захищеності інформаційних ресурсів, необхідно побудувати модель можливого порушника. Ця модель може бути побудована з урахування різних критеріїв.

Модель порушника розробляється для того, щоб отримати відповіді на наступні питання:

- від кого захищати інформацію?
- яка мета порушника?
- якими знаннями володіє порушник?
- які повноваження в системі має потенційний порушник?
- якими методами і засобами користується порушник?
- яка обізнаність порушника щодо об'єкта інформаційної діяльності і системи охорони?

Модель порушника представляє собою опис можливих дій порушника, який складається на основі аналізу типу зловмисника, рівня його повноважень, знань, теоретичних та практичних можливостей. Порушників прийнято поділяти на зовнішніх і внутрішніх. До внутрішніх належать співробітники, користувачі інформаційної системи, які можуть наносити шкоду інформаційним ресурсам як ненавмисно, так і навмисно; технічний персонал, який обслуговує будівлі і приміщення (електрики, сантехніки, прибиральниці тощо); персонал, який обслуговує технічні засоби (інженери, техніки). Зовнішні порушники – це сторонні особи, які знаходяться поза контрольованою зоною організації або не авторизовані для використання даної комп'ютерної системи. Це означає, що вони не мають в системі облікового запису і згідно системної політики безпеки взагалі не можуть працювати в даній системі. Приклад зовнішніх порушників: відвідувачі, які можуть завдати шкоди навмисно або через незнання існуючих

обмежень; кваліфіковані хакери; особи, яких найняли конкуренти для отримання необхідної інформації; порушники пропускного режиму.

При розробці моделі порушника необхідно визначитись, що і у якій мірі має відображати отримана модель. Для цього необхідно визначитись з необхідним ступенем деталізації моделі порушника. [12]

Всі класифікатори порушника наведено у таблицях

Таблиця 2.5.1 Рейтингова оцінка рівня загроз:

Рейтингова оцінка	Опис
0	Не становить загрози
1	Незначний
2	Низький
3	Сердній
4	Високий
5	Критичний

Таблиця 2.5.2 Категорії порушників. Внутрішні по відношенню к ІТС.

Позначення	Визначення категорії	Рівень загроз
ПВ0	Генеральний директор	0
ПВ1	Заступник директора	4
ПВ2	Бухгалтер	3
ПВ3	Менеджери	2
ПВ4	Системний адміністратор	4

Таблиця 2.5.3 Категорії порушників. Зовнішні по відношенню к ІТС.

Позначення	Визначення категорії	Рівень загроз
ПЗ0	Клієнти	1
ПЗ1	Комунальні служби	1
ПЗ2	Охоронник, прибиральниця	2

Таблиця 2.5.4 Специфікація моделі порушника за мотивами порушення

Позначення	Мотив порушення	Рівень загроз
М1	Безвідповідальність	1
М2	Корисливий інтерес	2

Таблиця 2.5.5 Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС

Позначення	Рівень кваліфікації	Рівень загроз
К1	Низький рівень знань, вміння працювати з компонентами ІТС	1
К2	Середній рівень знань, має практичний досвід з роботи з компонентами ІТС та їх обслуговування	2

Таблиця 2.5.6 Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту

Позначення	Характеристика можливостей порушника	Рівень загроз
З0	Не має навичок	0
З1	Підслуховування, підглядання за робочим процесом	1
З2	Взлом, підбір паролю до облікових засобів	2

Таблиця 2.5.7 Специфікація моделі порушника за часом дії

Позначення	Характеристика можливостей порушника	Рівень загроз
Ч1	Під час повної бездіяльності ІТС з метою відновлення та ремонту	1
Ч2	Під час призупинки компонентів ІТС з метою технічного обслуговування та модернізації	2
Ч3	Під час функціонування ІТС (або компонентів системи)	3
Ч4	У будь-який час, маючи доступ до інформації у хмарному сховищі (до облікового запису)	4

Таблиця 2.5.8 Специфікація моделі порушника за місцем дії

Позначення	Характеристика місця дії порушника	Рівень загроз
МД1	На робочому місці	2
МД2	У приміщенні, де розташовані ІТС	2
МД3	Віддалено, маючи доступ до хмарного сховища (до облікового запису)	2

Таблиця 2.5.9 Модель внутрішнього порушника

Посада	Категорія	Мотив	Кваліфікація	Можливості	За часом дії	За місцем дії	Сума загроз
Директор	ПВ0	М1	К2	З0	Ч4	МД3	9
	0	1	2	0	4	2	
Заступник директора	ПВ1	М2	К2	З2	Ч3	МД1	15
	4	2	2	2	3	2	
Бухгалтер	ПВ2	М1	К2	З1	Ч3	МД1	12
	3	1	2	1	3	2	
Менеджери	ПВ3	М2	К2	З2	Ч3	МД1	13
	2	2	2	2	3	2	
Системний адміністратор	ПВ4	М2	К2	32	Ч4	МД3	18
	4	2	2	2	4	2	
Клієнти	ПЗ0	М2	К1	З1	Ч1	МД2	8
	1	2	1	1	1	2	
Прибиральниця	ПЗ2	М2	К1	З1	Ч3	МД2	11
	2	2	1	1	3	2	
Охоронник	ПЗ2	М2	К1	З1	Ч3	МД2	11
	2	2	1	1	3	2	
Комунальні служби	ПЗ1	М2	К1	З1	Ч3	МД2	10
	1	2	1	1	3	2	

Найбільшу загрозу несуть працівники організації: заступник директора та системний адміністратор, трохи меншу інші працівники, а саме: заступник директора та менеджери, оскільки вони мають доступ до системи ІТС та працюють з її компонентами. Відповідно це ставить додаткові вимоги до потреби розробки ефективної політики безпеки інформації

2.6 Модель загроз

Модель загроз – це абстрактний формалізований або неформалізований опис методів і способів здійснення загроз.[15]

Під загрозами слід розуміти шляхи реалізації дій, що вважаються небезпечними. Наприклад, загроза знімання інформації і перехоплення випромінювання з дисплею може привести до втрати таємності або конфіденційності, загроза пожежі може привести до порушення цілісності та доступності інформації, загроза розриву каналу передачі інформації може реалізувати втрату доступності.

Існує багато підходів щодо класифікації загроз, проте, як здається, найбільш придатною для аналізу є визначення та класифікація загроз за результатом їх дії на інформацію, а точніше, на її основні (фундаментальні) властивості – конфіденційність, цілісність, доступність.

Тоді з цієї точки зору в ІТС розрізняються наступні класи загроз інформації:

1)порушення конфіденційності;

2)порушення цілісності;

3)порушення доступності або відмова в обслуговуванні;

4)порушення спостереженості або керованості.

Загрози можуть бути природнього характеру, навмисними та випадковими. Вони можуть бути як внутрішніми, так і зовнішніми.

Таблиця 2.6.1 Загрози та можливості їх реалізації

Загроза	Реалізація	Джерело
Стихійні явища (аварії, пожежа)	-несправність обладнання	Зовнішнє

	- легкозаймисті матеріали	

Продовження таблиці 2.6.1

Загроза	Реалізація	Джерело
Відмови системи електроживлення	- стара чи неякісна електропроводка - відсутність електричних запобіжників	Внутрішнє
Несанкціоноване підключення до ТЗ	- недосконала охоронна система	Зовнішнє
Втрата чи пошкодження носіїв інформації	- відсутність хмарного сховища відсутність резервного копіювання	Зовнішнє
Зчитування даних на робочому екрані або залишення без нагляду робочих документів	- некомпетентність персоналу - відсутність політики безпеки	Зовнішнє
Несанкціоноване підключення до каналів зв'язку	- відсутність захисту або використання застарілих протоколів захисту Інтернет мереж - Використання слабких паролів - Некомпетентність персоналу	Зовнішнє
Втрата або розголошення паролів доступу до системи	- некомпетентність персоналу	Внутрішнє
Соціальна інженерія	- погано підібраний персонал - низька мотивація працівників - низький рівень знань працівників	Внутрішнє

Таблиця 2.6.2 Шкала ймовірності реалізації загроз

Оцінка ймовірності	Характеристика
1	Практично неможливо
2	Низька ймовірність
3	Середня ймовірність
4	Висока ймовірність
5	Критична ймовірність

Таблиця 2.6.3 Характеристика рівня загроз

Оцінка	Характеристика
0	Конфіденційність не порушується
1	Конфіденційність порушується
0	Цілісність не порушується
1	Цілісність порушується
0	Доступність не порушується
1	Доступність порушується
0	Спостережність не порушується
1	Спостережність порушується

Рівень загрози визначається= (К+Ц+Д+С) * ймовірність реалізації загрози

Таблиця 2.6.4 Виявлення рівнів загроз

Загроза	Ймовірність	Що порушує				Рівень загроз
		К	Ц	Д	С	
Стихійні явища (аварії, пожежа)	2	0	1	1	1	6
Відмови системи електроживлення	2	0	1	0	1	4
Несанкціоноване підключення до ТЗ	2	1	0	0	0	2

Продовження таблиці 2.6.4

Загроза	Ймовірність	Що порушує				Рівень загроз
		К	Ц	Д	С	
Втрата чи пошкодження носіїв інформації	2	0	1	1	0	4
Зчитування даних на робочому екрані або залишення без нагляду робочих документів	4	1	0	1	0	8
Несанкціоноване підключення до каналів зв'язку	4	1	1	1	1	16
Втрата або розголошення паролів доступу до системи	3	1	1	1	1	12
Зараження системи комп'ютерними вірусами	4	1	1	1	1	16
Вхід у систему третіх осіб	3	1	1	1	1	12
Несанкціоноване внесення змін у програмне забезпечення та технічні засоби	2	0	1	1	1	6

За результатами обчислення можна зробити висновок, що найбільшу загрозу завдає зараження системи комп'ютерними вірусами та несанкціоноване підключення до каналів зв'язку

Також, велику загрозу завдають:

- Зчитування даних на робочому екрані або залишення без нагляду робочих документів
- Втрата або розголошення паролів доступу до системи
- Вхід у систему третіх осіб
- Соціальна інженерія

2.7 Профіль захищеності

Відповідно до НД ТЗІ 2.5-005 -99 зі зміною №1, Затвердженою наказом Адміністрації Держспецзв'язку від 15.10.2008 № 172 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу»

АС підприємства – АС «3» класу. Клас «3»- розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу. Істотна відміна від попереднього класу — необхідність передачі інформації через незахищене середовище або, в загальному випадку, наявність вузлів, що реалізують різну політику безпеки.

За результатами аналізу складу ІТС моделі загроз та порушника для даної АС «3» класу було обрано наступний профіль захищеності:

3.КЦД.2 = { КД-2, КА-2, КО-1, КВ-2,
ЦД-1, ЦА-2, ЦО-1, ЦВ-2,
ДР-1, ДВ-1,
НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }

Таблиця 2.7.1 Профіль захищеності

№	Послуга	Назва	Опис
1	КД-2	Базова довірча конфіденційність	Ця послуга дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування. Політика довірчої конфіденційності, що реалізується КЗЗ,

Продовження таблиці 2.7.1

№	Послуга	Назва	Опис
			повинна визначати множину об’єктів КС, до яких вона відноситься. КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта. Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта. КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта. КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес. Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації. Як частина політики довірчої конфіденційності повинні бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту
2	КА-2	Базова адміністративна конфіденційність	Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від захищених об'єктів до користувачів. Рівні даної послуги ран жируються на підставі повноти захисту і вибірковості управління. Політика адміністративної конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта.
3	КО-1	Повторне використання об’єктів	Ця послуга дозволяє забезпечити коректність повторного використання розділюваних об’єктів, гарантуючи, що в разі, якщо розділюваний об’єкт виділяється новому користувачу або процесу, то він не містить інформації, яка залишилась від попереднього користувача або процесу. Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження. КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і

Продовження таблиці 2.7.1

№	Послуга	Назва	Опис
			об'єктів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта. КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного процесу через керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес. Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної конфіденційності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту
4	КВ-2	Базова конфід енційні сть при обміні	Ця послуга дозволяє забезпечити захист об’єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ран жируються на підставі повноти захисту і вибірковості керування. Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати множину об’єктів при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуються, і спроможність користувачів і/або процесів керувати рівнем захищеності. КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об’єкті, який передається: - Запити на призначення або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження - Запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу - Запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу

Продовження таблиці 2.7.1

№	Послуга	Назва	Опис
5	ЦД-1	Мінімальна довірча цілісність	Ця послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену. Рівні даної послуги ран жируються на підставі повноти захисту і вибірковості керування. Політика довірчої цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта. Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта. КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту
6	ЦА-2	Базова адміністратив на цілісність	Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від користувачів до захищених об'єктів. Рівні даної послуги ран жируються на підставі повноти захисту і вибірковості керування. Політика адміністративної цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу процесу і захищеного об'єкта. Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження. КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, 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 модифікувати об'єкт. КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного процесу

Продовження таблиці 2.7.1

№	Послуга	Назва	Опис
			шляхом керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес. Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту
7	ЦО-1	Обмежений відкат	Ця послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкатити) захищений об’єкт до попереднього стану. Рівні даної послуги ран жируються на підставі множини операцій, для яких забезпечується відкат. Політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити певний набір (множину) операцій, виконаних над захищеним об’єктом за певний проміжок часу
8	ЦВ-2	Базова цілісність при обміні	Ця послуга дозволяє забезпечити захист об’єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ран жируються на підставі повноти захисту і вибірковості керування. Політика цілісності при обміні, що реалізується КЗЗ, повинна визначати множину об’єктів КС і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовуваними механізмами, і спроможність користувачів і/або процесів керувати рівнем захищеності. КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об’єкті, який передається а також фактів його видалення або дублювання. Запити на експорт захищеного об’єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу. Запити на імпорт захищеного об'єкта повинні оброблятися

Продовження таблиці 2.7.1

№	Послуга	Назва	Опис
			приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу. Запити на присвоєння або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження
9	ДР-1	Квоти	Ця послуга дозволяє користувачам керувати використанням послуг і ресурсів. Рівні даної послуги ран жируються на підставі повноти захисту і вибірковості керування доступністю послуг КС. Політика використання ресурсів, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. Політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу. Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження
10	ДВ-1	Ручне відновлення	Ця послуга забезпечує повернення КС у відомий захищений стан після відмови або переривання обслуговування. Рівні даної послуги ран жируються на підставі міри автоматизації процесу відновлення. Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов КС і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція КС. Після відмови КС або переривання обслуговування КЗЗ повинен перевести КС до стану, із якого повернути її до нормального функціонування може відповідні повноваження. Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути КС до нормального функціонування
11	НР-2	Захищений журнал	Реєстрація дозволяє контролювати небезпечні для КС дії. Рівні даної послуги ран жируються залежно від повноти і вибірковості контролю, складності засобів аналізу даних журналів реєстрації і спроможності вияву потенційних порушень. Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються. КЗЗ повинен бути здатним здійснювати реєстрацію

Продовження таблиці 2.7.1

№	Послуга	Назва	Опис
			подій, що мають безпосереднє відношення до безпеки. Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події. КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування. Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації
12	НИ-2	Одиночна ідентифікація і автентифікація	Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до КС. Рівні даної послуги ран жируються залежно від числа задіяних механізмів автентифікації. Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ. Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен автентифікувати цього користувача з використанням захищеного механізму. КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування
13	НК-1	Однонаправлений достовірний канал	Ця послуга дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ. Рівні даної послуги ран жируються залежно від гнучкості надання можливості КЗЗ або користувачу ініціювати захищений обмін. Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв’язку між користувачем і КЗЗ. Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв’язок з використанням даного каналу повинен ініціюватися виключно користувачем

Продовження таблиці 2.7.1

№	Послуга	Назва	Опис
14	НО-2	Розподіл обов'язків адміністраторів	Ця послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Рівні даної послуги ран жируються на підставі вибірковості керування можливостями користувачів і адміністраторів. Політика розподілу обов’язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції. Політика розподілу обов’язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі. Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі
15	НЦ-2	КЗЗ з гарантованою цілісністю	Ця послуга визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами. Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів. КЗЗ повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування. Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об’єктів контролюються КЗЗ
16	НТ-2	Самотестування при старті	Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Рівні даної послуги ран жируються на підставі можливості виконання тестів у процесі запуску або штатної роботи. Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ

Продовження таблиці 2.7.1

№	Послуга	Назва	Опис
17	НВ-1	Автентифікація вузла	Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ран жируються на підставі повноти реалізації. Політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ. КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму.Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації

2.8 Розробка політики безпеки інформації

Політика безпеки інформації (information security policy) — сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок обробки інформації. [1]

Під час розробки політики безпеки повинні бути враховані технологія обробки інформації, моделі порушників і загроз, особливості ОС, фізичного середовища та інші чинники. В ІТС може бути реалізовано декілька різних політик безпеки, які істотно відрізняються.

Як складові частини загальної політики безпеки в ІТС мають існувати політики забезпечення конфіденційності, цілісності, доступності оброблюваної інформації.

Політика безпеки повинна стосуватись: інформації (рівня критичності ресурсів ІТС), взаємодії об’єктів (правил, відповідальності за захист інформації, гарантій захисту), області застосування (яких складових компонентів ІТС політика безпеки стосується, а яких – ні).

Політика безпеки має бути розроблена таким чином, що б вона не потребувала частої модифікації (потреба частої зміни вказує на надмірну конкретизацію, наприклад, не завжди доцільно вказувати конкретну назву чи версію програмного продукту).

Політика безпеки повинна передбачати використання всіх можливих заходів захисту інформації, як-то: правові та морально-етичні норми, організаційні (адміністративні), фізичні, технічні (апаратні і програмні) заходи і визначати правила та порядок застосування в ІТС кожного з цих видів.

Політика безпеки повинна базуватися на наступних основних принципах:

- системності;
- комплексності;
- неперервності захисту;
- достатності механізмів і заходів захисту та їхньої адекватності загрозам;
- гнучкості керування системою захисту, простоти і зручності її використання;
- відкритості алгоритмів і механізмів захисту, якщо інше не передбачено окремо.

Політика безпеки повинна доказово давати гарантії того, що:

- в ІТС (в кожній окремій складовій частині, в кожному функціональному завданні і т. ін.) забезпечується адекватність рівня захисту інформації рівню її критичності;
- реалізація заходів захисту інформації є рентабельною;
- в будь-якому середовищі функціонування ІТС забезпечується оцінюваність і перевіряємість захищеності інформації;
- забезпечується персоніфікація положень політики безпеки (стосовно суб'єктів ІТС), звітність (реєстрація, аудит) для всіх критичних з точки зору безпеки ресурсів, до яких здійснюється доступ в процесі функціонування ІТС;
- персонал і користувачі забезпечені достатньо повним комплектом документації стосовно порядку забезпечення захисту інформації;
- всі критичні з точки зору безпеки інформації технології (функції) ІТС мають відповідні плани забезпечення неперервної роботи та її поновлення у разі виникнення непередбачених ситуацій;

- враховані вимоги всіх документів, які регламентують порядок захисту інформації в ІТС, та забезпечується їхнє суворе дотримання.

Політика безпеки розробляється на підготовчому етапі (НД ТЗІ 3.7-001-99) створення КСЗІ [11]. Методологія розроблення політики безпеки включає в себе наступні роботи:

- розробка концепції безпеки інформації в ІТС;
- аналіз ризиків;
- визначення вимог до заходів, методів та засобів захисту;
- вибір основних рішень з забезпечення безпеки інформації;
- організація виконання відновлювальних робіт і забезпечення неперервного функціонування ІТС;
- документальне оформлення політики безпеки.
- Концепція безпеки інформації в ІТС викладає систему поглядів, основних принципів, розкриває основні напрями забезпечення безпеки інформації. Розроблення концепції здійснюється після вибору варіанту концепції створюваної ІТС і виконується на підставі аналізу наступних чинників:
- правових і (або) договірних засад;
- вимог до забезпечення безпеки інформації згідно з завданнями і функціями ІТС;
- загроз, яким зазнають впливу ресурси ІТС, що підлягають захисту.
- За результатами аналізу мають бути сформульовані загальні положення безпеки, які стосуються або впливають на технологію обробки інформації в ІТС:
- мета і пріоритети, яких необхідно дотримуватись в ІТС під час забезпечення безпеки інформації;
- загальні напрями діяльності, необхідні для досягнення цієї мети;
- аспекти діяльності у галузі безпеки інформації, які повинні вирішуватися на рівні організації в цілому;
- відповідальність посадових осіб та інших суб’єктів взаємовідносин в ІТС, їхні права і обов'язки щодо реалізації завдань безпеки інформації.

Спираючись на отриманні результати аналізу моделі загроз та порушників і дивлячись на вимоги профілю захищеності, було розроблено основні елементи організаційної складової захисту інформації, що відповідають найбільш суттєвим загрозам, зокрема:

- Політика «Чистого столу»;
- Політика антивірусного захисту;
- Політика контролю використання мережі Інтернет користувачами системи;
- Політика захисту паролів;
- Політика бездротової мережі.
- Політика віддаленого доступу

Політики безпеки мають наступну структуру:

1) Мета;
2) Область застосування;
3) Зміст політики;
4) Відповідальність;
5) Періодичність та порядок перегляду політики.

2.8.1 Політика «Чистого столу»

Мета:

Метою цієї політики є встановлення мінімальних вимог для підтримки «чистого столу» – де міститься конфіденційна/критична інформація про наших співробітників, нашу інтелектуальну власність, наших клієнтів і наших постачальників.

Область застосування:

Ця політика поширюється на всіх співробітників ТОВ «ЛевіДрім».

Політика:

- Працівники зобов’язані гарантувати, що вся конфіденційна інформація в паперовому або електронному вигляді захищена у кінці робочого дня, або, якщо працівник відходить від робочого місця на довгий час;

- ПК повинен бути заблокований, коли працівник не за робочим місцем;

- ПК повинен бути повністю вимкнений у кінці робочого дня;

- Будь-яка обмежена або конфіденційна інформація повинна бути прибрана зі столу і замкнена в шухляді, коли стіл незайнятий і в кінці робочого дня.

- Файлові шафи, що містять обмежену або конфіденційну інформацію, повинні зберігатися закритими і заблокованими, коли не використовуються або коли працівник не присутній за робочим місцем;

- Ключі, які використовуються для доступу до обмеженої або конфіденційної інформації, не повинні залишатися без нагляду;

- Ноутбуки повинні бути або заблоковані за допомогою замикаючого кабелю, або замкнені в шухляді;

- Паролі не можуть залишатися на липких нотатках, розміщених на комп'ютері або під ним, і вони не можуть бути записані в доступному місці;

- Роздруківки, що містять обмежену або конфіденційну інформацію, повинні бути негайно видалені з принтера;

Відповідальність:

Відповідні всі працівники підприємства.

Працівник, який порушив цю політику, може бути підданий дисциплінарному стягненню, аж до припинення трудових відносин.

Періодичність та порядок перегляду політики:

Політика безпеки повинна переглядатись щороку директором та системним адміністратором. У разі необхідності корективи можуть бути внесені раніше терміну перегляду.

2.8.2Політика антивірусного захисту

Мета:

Зменшення ризику зараження ІТС шкідливими програмними засобами

Область застосування:

Ця політика поширюється на всіх співробітників ТОВ «ЛевіДрім».

Політика:

- На кожному комп'ютері повинні бути встановлені антивірусні засоби;

- Дозволяється використовувати лише ліцензійне антивірусне програмне забезпечення, яке рекомендоване системним адміністратором;

- Налаштуванням та встановленням засобів антивірусного ПЗ займається лише системний адміністратор;

- Антивірусне ПЗ повинно завжди вчасно оновлюватись;

- Всі файли, які завантажуються із мережі Інтернет повинні бути перевірені антивірусним ПЗ перед відкриттям;

- У разі виникнення проблем із ПЗ працівники повинні негайно повідомити про це системного адміністратора

Відповідальність:

Відповідні всі працівники підприємства.

Працівник, який порушив цю політику, може бути підданий дисциплінарному стягненню, аж до припинення трудових відносин.

Періодичність та порядок перегляду політики:

Політика безпеки повинна переглядатись щороку директором та системним адміністратором. У разі необхідності корективи можуть бути внесені раніше терміну перегляду.

2.8.3 Політика контролю використання мережі Інтернет користувачами системи

Мета:

Метою цієї політики є визначення належного використання Інтернету співробітників ТОВ «ЛевіДрім».

Область застосування:

Ця політика поширюється на всіх співробітників ТОВ «ЛевіДрім».

Політика:

Інтернет повинен використовуватись лише для:

- Пошуку інформації, яка необхідна для виконання прямих обов'язків

- Приймання та обробка замовлень

- Збору інформації для вдосконалення продуктів компанії

- Оновлення сайту підприємства

Відповідальність:

Відповідні всі працівники підприємства.

Працівник, який порушив цю політику, може бути підданий дисциплінарному стягненню, аж до припинення трудових відносин.

Періодичність та порядок перегляду політики:

Політика безпеки повинна переглядатись щороку директором та системним адміністратором. У разі необхідності корективи можуть бути внесені раніше терміну перегляду.

2.8.4 Політика захисту паролів

Мета:

Метою цієї політики є встановлення стандарту для створення надійних паролів і захист цих паролів.

Область застосування:

Ця політика поширюється на всіх співробітників ТОВ «ЛевіДрім».

Політика:

- Усі паролі на рівні користувача та системи мають відповідати інструкції зі створення пароля;

- Користувачі повинні використовувати окремий унікальний пароль для кожного з робочих облікових записів;

- Користувачі не можуть використовувати будь-які робочі паролі для власних особистих облікових записів;

- Паролі слід змінювати лише тоді, коли є підстави вважати, що пароль був скомпрометований;

- Забороняється передавати паролі третім особам, включаючи керівників та колег;

- Всі паролі слід розглядати як конфіденційну інформацію ТОВ «ЛевіДрім»;

- Паролі не можна вставляти в повідомлення електронної пошти, казати комусь по телефону або передавати якимось іншим способом;

- Не використовуйте функцію «Запам’ятати пароль» у програмах (наприклад, web-браузери);

- Будь-який користувач, який підозрює, що його/її пароль міг бути зламаний, повинен повідомити про цей інцидент і змінити всі паролі;

- Багатофакторна аутентифікація дуже заохочується, і її слід використовувати, коли це можливо, не тільки для робочих облікових записів, а й особистих облікових записів.

Відповідальність:

Відповідні всі працівники підприємства.

Працівник, який порушив цю політику, може бути підданий дисциплінарному стягненню, аж до припинення трудових відносин.

Періодичність та порядок перегляду політики:

Політика безпеки повинна переглядатись щороку директором та системним адміністратором. У разі необхідності корективи можуть бути внесені раніше терміну перегляду

2.8.5 Політика бездротової мережі

Мета:

Метою цієї політики є захист і безпека інформаційних активів, що належать ТОВ «ЛевіДрім», що надають комп'ютерні пристрої, мережі та інші електронні інформаційні системи для виконання місій, цілей та ініціатив. ТОВ «ЛевіДрім» надає доступ до цих ресурсів і повинні відповідально керувати ними для збереження конфіденційності, цілісності та доступності усіх інформаційних активів.

Ця політика визначає умови, яким повинні задовольняти пристрої бездротової інфраструктури для підключення до мережі ТОВ «ЛевіДрім».

Область застосування:

Ця політика поширюється на всіх співробітників ТОВ «ЛевіДрім».

Політика:

Усі пристрої бездротової інфраструктури, які знаходяться на підприємстві ТОВ «ЛевіДрім» повинні:

- Дотримуватись стандартів, зазначених у стандарті бездротового зв'язку;

- Використовувати схвалені протоколи автентифікації та інфраструктури ТОВ «ЛевіДрім»;

- Використовувати схвалені протоколи шифрування ТОВ «ЛевіДрім»;

- Підтримувати апаратну адресу (MAC-адресу), яку можна зареєструвати та відстежити.

Відповідальність:

Відповідні всі працівники підприємства.

Працівник, який порушив цю політику, може бути підданий дисциплінарному стягненню, аж до припинення трудових відносин.

Періодичність та порядок перегляду політики:

Політика безпеки повинна переглядатись щороку директором та системним адміністратором. У разі необхідності корективи можуть бути внесені раніше терміну перегляду

2.8.6 Політика віддаленого доступу

Мета:

Метою цієї політики є визначення правил та вимог для підключення до ТОВ «ЛевіДрім» з будь-якого хоста. Ці правила та вимоги покликані звести до мінімуму потенційного впливу ТОВ «ЛевіДрім» від пошкоджень, які можуть виникнути в результаті несанкціонованого використання ресурсів ТОВ «ЛевіДрім».

Область застосування:

Ця політика поширюється на всіх співробітників ТОВ «ЛевіДрім».

Політика:

- Безпечний віддалений доступ має суворо контролюватись за допомогою шифрування (тобто віртуальної приватної мережі (VPN)) і повинен мати надійні паролі;

- Авторизовані користувачі повинні захищати свої логін і пароль навіть від членів сім'ї;

- Під час використання комп’ютера, що належить ТОВ «ЛевіДрім», для віддаленого підключення до корпоративної мережі, авторизовані користувачі

повинні переконатися, що віддалений хост не є одночасно підключений до будь-якої іншої мережі, за винятком персональних мереж, які знаходяться під їх повним контролем;

- Усі хости, які підключені до внутрішніх мереж ТОВ «ЛевіДрім» через віддалений доступ повинні використовувати найсучасніше антивірусне програмне забезпечення;

- Персональне обладнання, яке використовується для підключення до мереж ТОВ «ЛевіДрім», повинно відповідати вимогам до обладнання, що належить ТОВ «ЛевіДрім» для віддаленого доступу, як зазначено в стандартах конфігурації апаратного та програмного забезпечення для віддаленого доступу до мережі підприємства.

Відповідальність:

Відповідні всі працівники підприємства.

Працівник, який порушив цю політику, може бути підданий дисциплінарному стягненню, аж до припинення трудових відносин.

Періодичність та порядок перегляду політики:

Політика безпеки повинна переглядатись щороку директором та системним адміністратором. У разі необхідності корективи можуть бути внесені раніше терміну перегляду

2.9Висновок до другого розділу:

У даному розділі були наведені загальні відомості про підприємство «ЛевіДрім». Було проведено повне обстеження ОІД. Результатом обсеження став аналіз загроз та вразливостей ОІД. Була створена модель порушника, модель загроз та було створено політику безпеки, яка включає в себе:

- Політика «Чистого» столу
- Політика антивірусного захисту
- Політика контролю використання мережі Інтернет користувачами системи
- Політика захисту паролів
- Політика бездротової мережі
- Політика віддаленого доступу

3 ЕКОНОМІЧНА ЧАСТИНА

Метою виконання економічного розділу дипломного проекту є техніко-економічне обґрунтування доцільності запровадження політики безпеки підприємства ТОВ «ЛевіДрім»

3.1 Розрахунок витрат на впровадження політики безпеки

Трудомісткість розробки політики безпеки інформації визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного спеціаліста з інформаційної безпеки):

$$t= t_{тз}+t_{в}+t_{а}+t_{вз}+t_{озб}+t_{овр}+t_{д}, \text{ год.}, \quad (3.1)$$

де: $t_{тз}$- тривалість складання технічного завдання на розробку політики безпеки інформації;

$t_{в}$- тривалість розробки концепції безпеки інформації у організації;

$t_{а}$- тривалість процесу аналізу ризиків;

$t_{в}з$- тривалість визначення вимог до заходів, методів та засобів захисту;

$t_{озб}$- тривалість вибору основних рішень з забезпечення безпеки інформації;

$t_{овр}$- тривалість організації виконання відновлюваних робіт і забезпечення неперервного функціонування організації;

$t_{д}$- тривалість документального оформлення політики безпеки.

Згідно формули 2.1, трудомісткість розробки політики безпеки інформації дорівнює:

$$t= 5+4+6+4+3+4+2=28 \text{ год.}$$

Розрахунок витрат на створення політики безпеки:

$$К_{рп}=З_{зп}+З_{мч} \quad (3.2)$$

де: $К_{рп}$ – витрати на створення політики безпеки;

$З_{зп}$ – заробітна плата спеціаліста з інформаційної безпеки;

$З_{мч}$ – вартість витрат машинного часу, що необхідні для створення політики безпеки.

Витрати на заробітну плату спеціаліста ІБ розраховуються за формулою:

$$З_{зп} = t * З_{іб} \text{ грн.}, \quad (3.3)$$

де: t – загальна тривалість розробки політики безпеки, годин;

$З_{іб}$ – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

Средньогодинна заробітна плата спеціаліста з інформаційної безпеки становить – 109 грн/ годину.

Заробітня плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальні потреби та визначається за формулою 3.3 :

$$З_{зп} = 28 * 109 = 3052 \text{ грн};$$

Таким чином капітальні витрати на проектування та впровадження проектного варіанту системи ІБ за формулою:

$$К = К_{пр} + К_{зпз} + К_{рп} + К_{аз} + К_{навч} + К_{н} \quad (3.4)$$

де: $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення консультантів. Зовнішні консультанти не наймались, тому даний коефіцієнт не враховуємо

$К_{зпз}$ – вартість закупівель ліцензійного і основного і додаткового ПЗ. (Було обрано комплект Windows 10 Pro+ Office 2021+ WinRar+ Avast – 6 шт (5*2800=16800 грн)

$К_{рп}$ – вартість розробки політики безпеки інформації – 3640 грн;

$К_{аз}$- вартість закупівлі апаратного забезпечення та допоміжних матеріалів (Було обрано: «Датчик руху накладний 180° IP44 DE-22 WH» - 4 шт (399*4=1596 грн), «Бездротовий датчик детектування диму та чадного газу Ajax FireProtect Plus EU White» - 10 шт (2834*10=28340 грн)).

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

$К_{навч}$ – витрати на навчання технічних фахівців в обслуговуючого персоналу, витрати на навчання системного адміністратора 1500 грн;

К = 16800 +29936+3640+1500=51876 грн.

3.2 Розрахунок поточних витрат

Річні експлуатаційні витрати на систему ІБ складають:

$$С=С_в +С_к+С_{ак}, \text{ тис. грн} \quad (3.5)$$

де: $С_в$- це витрати на оновлення системи;

$С_{ак}$- витрати викликані активністю користувачів системи ІБ.

$С_к$- вартість на керування системою в цілому, рахується за формулою:

$$С_к= С_н+ С_а +С_з +С_{єв}+С_{ел}+С_о+С_{тос} \quad (3.6)$$

де: $С_н$- це витрати на навчання адміністративного персоналу і користувачів, проведення тренінгів, становить 1500 грн;

$С_а$ – це річний фонд амортизаційних відрахувань, що відзначається від суми капітальних інвестицій. ПЗ вийшло на 16800 грн, а апаратного забезпечення на 29936 грн.

Сумарно буде 46736 грн. Ліквідаційна вартість програмного забезпечення для 6 комп'ютерів 2800 грн, а для апаратного забезпечення - 2139 грн.

$С_{а1}$=16800/2=8400 грн;

$С_{а2}$=29936/5=5987.2 грн;

$С_а$=8400+5987.2=14387.2 грн.

$С_з$- це річний фонд заробітної плати інженерно-технічного персоналу, котрий обслуговує систему ІБ, вираховується за формулою:

$$С_з=З_{осн}+З_{дод}, \text{ грн} \quad (3.7)$$

де: $З_{осн}$ – основна заробітна плата, складає 12000 грн на місяць, на рік буде 144000 грн.

$З_{дод}$- додаткова заробітна плата, складає 960 грн на місяць, на рік буде 11520 грн.

В 2021 році ЄСВ є 22% від фонду заробітної плати і становить:

$$С_{ев} = 144000*22\% = 31680 \text{ грн}$$

$$С_{з} = 144000+11520+31680=187200 \text{ грн}$$

$С_{ел}$- це вартість електроенергії, що споживається апаратурою системи ІБ протягом року, вираховується за формулою:

$$С_{ел} = Р * F_р * Ц_е, \text{ грн} \quad (3.8)$$

де: Р- встановлена потужність апаратури інформаційної безпеки, 0.22кВт середня потужність одного комп'ютера;

$$Р = 0.22\text{кВт} * 6 \text{ комп'ютерів} = 1.32 \text{ кВт}.$$

$F_р$- це річний фонд робочого часу системи інформаційної безпеки, ОІД працює 5 днів на тиждень, по 9.5 годин (мінус перерва 60 хв – буде 8.5 годин)

$$F_р = 240 \text{ днів} * 8.5 \text{ годин} * 6 \text{ комп'ютерів} = 12240 \text{ год}.$$

$Ц_е$ – це тариф на електроенергію, 1,44грн/кВт годин.

$$С_{ел} = 1.32*12240*1,44=23265,8 \text{ грн};$$

$С_{тос}$ – це витрати на технічне та організаційне адміністрування та сервіс системи ІБ визначаються за даними організації. Або 1% від суми капітальних інвестицій – 518.76 грн.

$С_о$ –це витрати на залучення сторонніх організацій для виконання деяких видів обслуговування та сертифікацію обслуговування персоналу.

$$С_к = 1500 + 14387.2 + 187200 + 31680 +23265,8 +518.76= 258551,7 \text{ грн}.$$

Тепер ми можем розрахувати експлуатаційні витрати:

$$С = 258551,7 +2000+3150 =263701.7 \text{ грн}.$$

3.3 Розрахунок витрат при виникненні загроз

Таблиця 3.1 Заробітна плата робітників на місяць

Посада	Кількість працівників	Заробітна плата в місяць, грн	Заробітна плата помножена на кількість працівників, грн
Генеральний директор	1	29000	29000
Заступник директора	1	17000	17000
Системний адміністратор	1	12000	12000
Бухгалтер	1	15000	15000
Менеджер	2	10000	20000
Всього:		83000	93000

Упущена вигода від простою атакованого сегмента становить:

$$U = П_п + П_в + V \quad (3.9)$$

де: $П_п$ – це виплати за простої робітників та, якщо трапляються проблеми з корпоративною мережею;

$П_в$- це вартість відновлення працездатності корпоративної мережі;

V- витрати від зниження обсягу продажів під час простою, коли проблеми з мережею;

Місячний час робочого часу складає 170 годин. Час простою в наслідок атаки 5 годин:

$$П_п = (З_с/F)*t_в, \text{ грн} ; \quad (3.10)$$

де: $З_с$ – загальна кількість витрат на заробітну плату співробітників за місяць;

F- місячний фонд робочого часу;

$t_в$- відновлення після проблеми, що обслуговує мережу;

$$П_п= (93000/170)*5=2735.3 \text{ грн};$$

Витрати на відновлення працездатності складаються з декількох частин:

1) $П_{пв}$ – витрати на відновлення системи;

2)$П_{ви}$ –витрати на повторне введення інформації;

3) $П_{зч}$- вартість заміни частини системи;

Витрати на повторне введення інформаціх розраховуються за формулою:

$$П_{ви} = (З_с/F) * t_{ви}; \quad (3.11)$$

$t_{ви}$ –це час повторного введення загубленої інформації співробітниками під час проблеми.

$$П_{ви}= (93000/170)*10 =5470.6 \text{ грн};$$

Витрати на відновлення Ппв розраховуються за формулою:

$$Ппв=(З_о/ F)* tв; \quad (3.12)$$

де: $З_о$ – заробітна плата системного адміністратора;

$$П_{пв}= (12000/170)*5=352.9 \text{ грн};$$

$П_{зч}$- вартість для витрат на заміну частин складає 3000 грн.

$$П_в = П_{ви} +П_{пв}+П_{зч}; \quad (3.13)$$

$$П_в=5470.6+352.9+3000=8823.5 \text{ грн.}$$

Витрати від зниження працездатності під час проблеми(атаки):

$$V= (O/F_г) (t_п+t_в+t_{ви}); \quad (3.14)$$

де: $F_г$ – це річний фонд часу роботи компанії, 1920 годин;

О- це обсяг продажів аткованого вузла або сегмента мережі, 4900000 грн.

$t_п$ – 5 годин простою після атаки;

$t_в$ – 5 годин відновлення після атаки;

$t_{ви}$ – це 10 годин повторного введення загубленої інформації під час атаки;

$$V = (4900000/ 2040) (5+5+10) =2402*20=48040 \text{ грн};$$

Тепер ми можемо розрахувати упущену вигоду від атаки на ІТС організації:

$$U= П_п+П_в+V: \quad (3.15)$$

$$U =2735.3 +8823.5 +48040=59598.8 \text{ грн};$$

В такому випадку, загальний збиток від атаки на сегмент або вузол корпоративної мережи складає:

$$B= \sum i \sum n U; \quad (3.16)$$

де: і- число атакованих вузлів, 6 комп'ютерів;

n – середнє число атак на рік, 3 рази

$$B= 6*3*59598.8 =1072778.4 \text{ грн}$$

3.4 Визначення та аналіз показників економічної ефективності

Урахування ризиків порушення ІБ становить:

$$E =B*R-C; \quad (3.17)$$

де: R- це очікувана ймовірність атаки на вузол або сегмент корпоративної мережі

В- це загальний збиток від атаки на вузол або сегмент корпоративної мережі;

С- це щорічні витрати на експлуатацію системи інформаційної безпеки;

$$E=(1072778.4*0,75)- 261564.6 =543019.2 \text{ грн};$$

Аналіз показників економічної системи

$$ROSI=E/K \quad (3.18)$$

ROSI показує скільки грн додаткового прибутку приносить гривня капітальних інвестицій на впровадження системи ІБ.

ROSI це коефіцієнт повернення інвестицій.

Е – це загальний ефект від впровадження системи ІБ

К – це капітальні затрати, становлять 34233 грн.

$$ROSI = 543019.2/ 37876 =14.33$$

То це термін окупності капітальних інвестицій показує за скільки років капітальні інвестиції окупляться від впровадження системи ІБ:

$$T_o = К/Е = 1/ ROSI, років \quad (3.19)$$

$$T_o=1/ 14.33 = 0,06(1 місяць)$$

3.5 Висновок до третього розділу

Під час виконання економічної частини були проведені основні розрахунки капітальних витрат на внесення основних елементів політики безпеки інформації, для визначення доцільності їх впровадження.

Під час розрахунків було визначено:

1. Капітальні витрати на впровадження та експлуатацію політики безпеки інформації становить 51876 грн.
2. Повна вартість річних експлуатаційних витрат становить 263701.7 грн.
3. Загальний збиток від атаки складатиме 1072778.4 грн.
4. Загальний ефект від впровадження системи інформаційної безпеки становить 543019.2 грн.
5. Термін окупності капітальних інвестицій складає 0,06 року.

Дані, які були отримані у ході виконання економічної частини, вказують на доцільність впровадження розроблених елементів політики безпеки.

ВИСНОВКИ

У першому розділі кваліфікаційної роботи було зазначено стан питання та визначено необхідні умови для створення КСЗІ в ІТС, був проаналізований список нормативно-правових документів в сфері захисту інформації. У розділі була описана необхідність створення КСЗІ та виділені основні етапи, серед яких:

- Формування загальних вимог до КСЗІ в ІТС;
- Розробка політики безпеки інформації в ІТС;
- Розробка технічного завдання на створення КСЗІ;
- Розробка проекту КСЗІ;
- Введення КСЗІ в дію та оцінка захищеності інформації в ІТС.

У другому розділі кваліфікаційної роботи наведені загальні відомості про інформаційно-телекомунікаційну систему ТОВ «ЛевіДрім». Було розроблено модель порушника, модель загроз та елементи політики безпеки інформації, серед яких:

- Політика «Чистого» столу
- Політика антивірусного захисту
- Політика контролю використання мережі Інтернет користувачами системи
- Політика захисту паролів
- Політика бездротової мережі
- Політика віддаленого доступу

У третій частині кваліфікаційної роботи було підтверджено доцільність впровадження розроблених елементів політики безпеки через отримані дані. Під час розрахунків було визначено:

- Капітальні витрати на впровадження та експлуатацію політики безпеки інформації;
- Повна вартість річних експлуатаційних витрат;
- Загальний збиток від атаки;

- Загальний ефект від впровадження системи інформаційної безпеки;
- Термін окупності капітальних інвестицій

ПЕРЕЛІК ПОСИЛАНЬ

1. НД ТЗІ 1.1-003-99 - Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. [Чинний від 28.04.1999]- К. : ДСТСЗІ СБУ, 2005. - №22 - (Нормативний документ системи технічного захисту інформації).

2. НД ТЗІ 3.7-003 -2005 - Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. – [Чинний від 08.11.2005]- К. : ДССЗЗІ, 2005. - №125 - (Нормативний документ системи технічного захисту інформації).

3. Кіберзлочини в Україні: як бізнесу захиститися від хакерських атак [Електронний ресурс] – Режим доступу https://hub.kyivstar.ua/news/kiberzlochini-v-ukrayini-yak-biznesu-zahistitisya-vid-hakersikih-atak/.

4. Бізнес під загрозою кібератаки. Як захистити компанію? [Електронний ресурс] – Режим доступу https://biz.ligazakon.net/news/208297_bznes-pd-zagrozoyu-kberataki-yak-zakhistiti-kompanyu.

5. Закон України «Про інформацію» [Електронний ресурс] – Режим доступу https://zakon.rada.gov.ua/laws/show/2657-12#Text

6. Закон України «Про захист інформації в автоматизованих системах» [Електронний ресурс] – Режим доступу https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

7. НД ТЗІ 1.1-002-99 - Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. - [Чинний від 28.04.1999]- К. : ДСТСЗІ СБУ, 2005. - №22 - (Нормативний документ системи технічного захисту інформації).

8. НД ТЗІ 1.4-001-2000 - Типове положення про службу захисту інформації в автоматизованій системі. [Чинний від 04.12.2000]- К. : ДСТСЗІ СБУ, 2005. - №53 - (Нормативний документ системи технічного захисту інформації).

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

несанкціонованого доступу. [Чинний від 28.04.1999]- К. : ДСТСЗІ СБУ, 2005. - №22 - (Нормативний документ системи технічного захисту інформації).

10. НД ТЗІ 2.5-004-99 - Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. [Чинний від 28.04.1999]- К. : ДСТСЗІ СБУ, 2005. - №22 - (Нормативний документ системи технічного захисту інформації).

11. НД ТЗІ 3.7-001-99 - Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. [Чинний від 28.04.1999]- К. : ДСТСЗІ СБУ, 2005. - №22 - (Нормативний документ системи технічного захисту інформації).

12. НД ТЗІ 1.1-001-99 - Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення. [Чинний від 28.05.1999]- К. : ДСТСЗІ СБУ, 2005. - №26 - (Нормативний документ системи технічного захисту інформації).

13. Методичні рекомендації до виконання кваліфікаційних робіт бакалаврів спеціальності 124 Кібербезпека/ Упоряд.: О.В. Герасіна, Д.С. Тимофєєв, О.В. Кручінін, Ю.А. Мілінчук – Дніпро: НТУ «ДП», 2020. – 47 с.

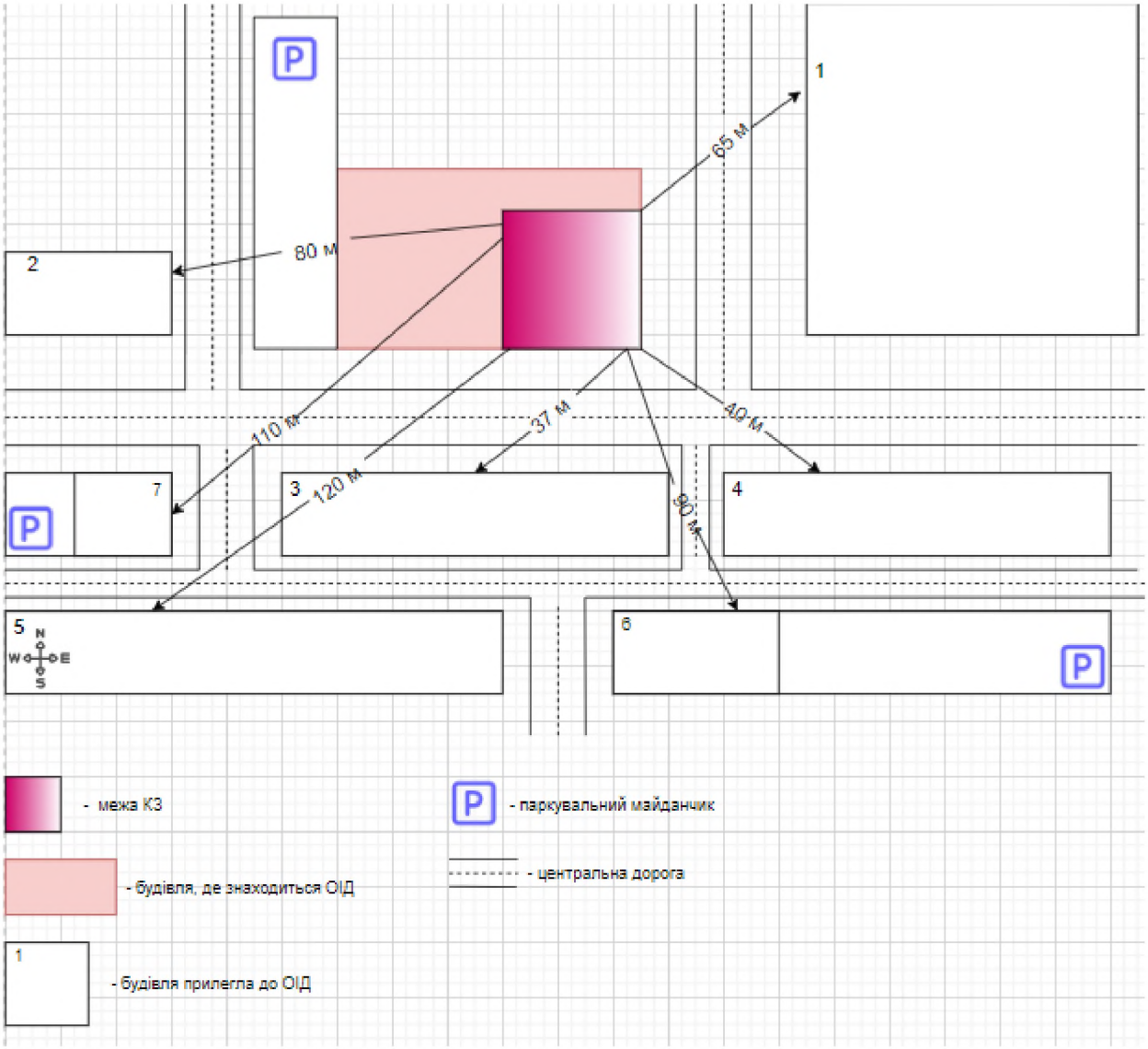
14. Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека / Упорядн.: Д.П. Пілова – Дніпро: Національний технічний університет «Дніпровська політехніка», 2019. – 16 с.

15. RANSOMWARE:THE TRUE COST TO BUSINESS [Електронний ресурс]- Режим доступу https://www.cybereason.com/hubfs/dam/collateral/ebooks/Cybereason_Ransomware_Research_2021.pdf

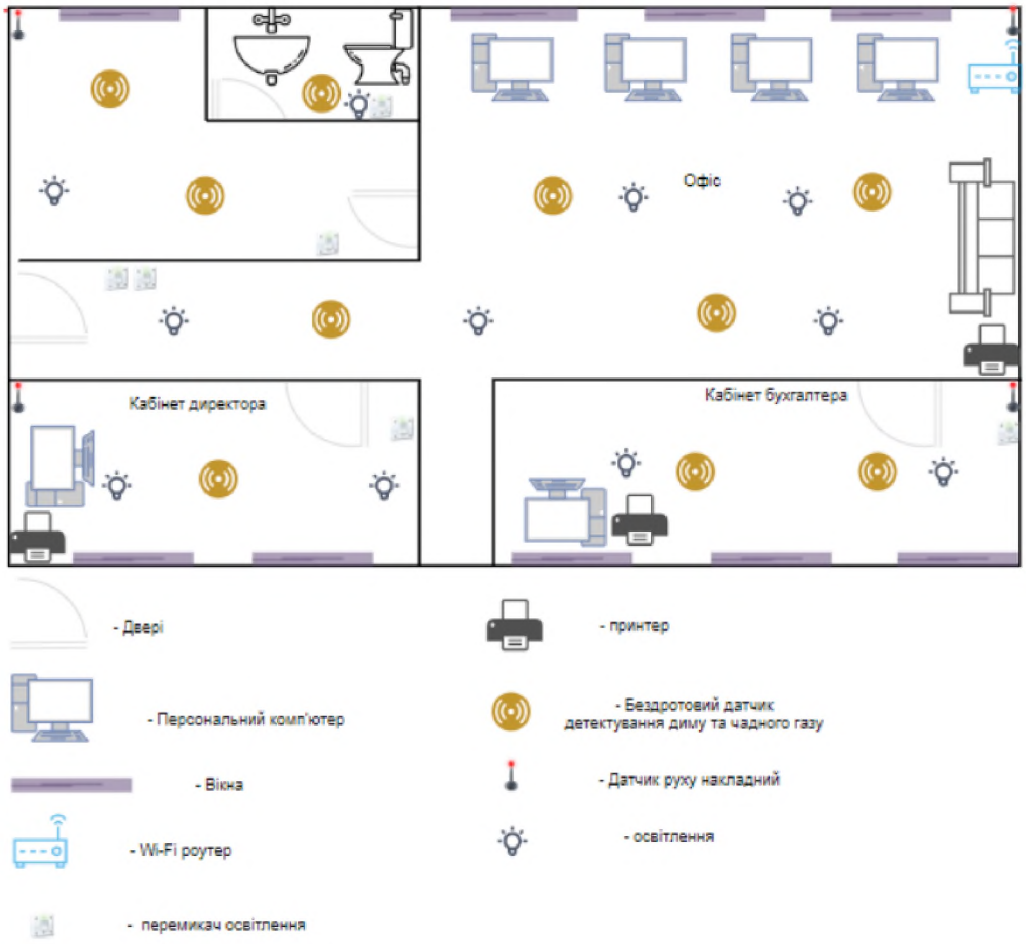
ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	1 Розділ	9	
5	А4	2 Розділ	36	
6	А4	3 Розділ	8	
7	А4	Висновки	2	
8	А4	Перелік посилань	2	
9	А4	Додаток А	1	
10	А4	Додаток Б	1	
11	А4	Додаток В	1	
12	А4	Додаток Г	1	
13	А4	Додаток Ґ	1	
14	А4	Додаток Д	1	
15	А4	Додаток Е	1	
16	А4	Додаток Є	1	
17	А4	Додаток Ж	1	

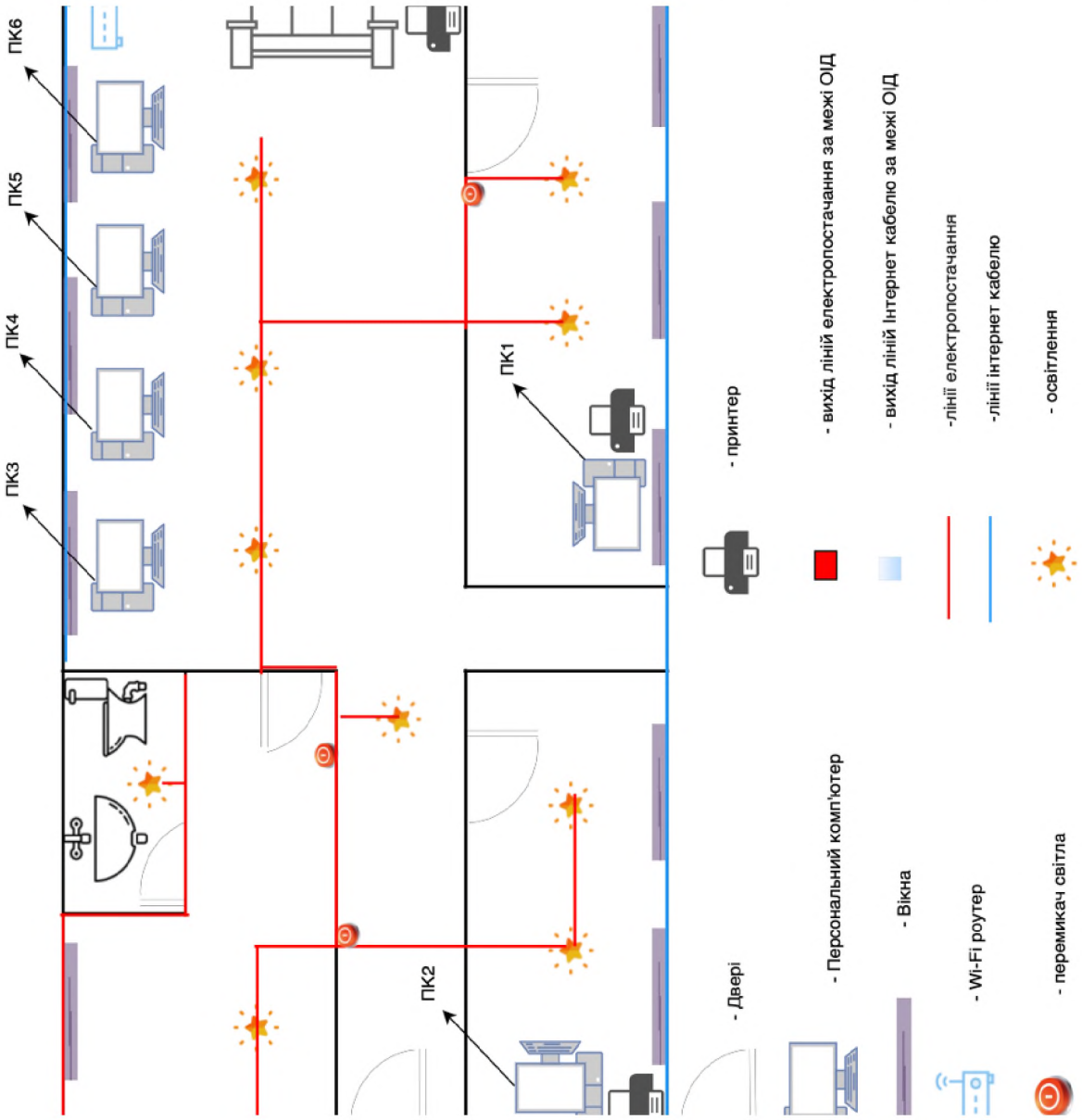
ДОДАТОК Б. Ситуаційний план ОІД



ДОДАТОК В. Генеральний план ОІД.



ДОДАТОК Г. Розташування ліній електромережі та Інтернет



ДОДАТОК Ґ. Наказ на створення КСЗІ

НАКАЗ

м. Дніпро

15.05.2022 №1

Про створення комплексної системи
захисту інформації в автоматизованій
системі класу «3» ІТС ТОВ «ЛевіДрім»

На виконання вимог статті 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» (зі змінами) та п.16 «Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», затверджених Постановою Кабінету Міністрів України від 26.03.2006 року №373 (зі змінами).

НАКАЗУЮ:

1. Створити комплексну систему захисту інформації в автоматизованій системі класу «3» для обробки інформації з обмеженим доступом.
2. Відповідальному за службу захисту інформації в автоматизованих системах Бондаренко С.В., забезпечити супроводження робіт зі створення комплексної системи захисту інформації.
3. Контроль за виконанням наказу покласти на заступника директора компанії Скляр М.О.

Директор Скляр О.В.

ДОДАТОК Д. Акт категоріювання

Гриф обмеження доступу

Прим. № ___

ЗАТВЕРДЖУЮ
Керівник установи-власника
(розпорядника, користувача) об’єкта
___директор_Скляр О.В._____
(посада, підпис, ініціали, прізвище)
____. ____. 20___

АКТ
категоріювання _____ТОВ «ЛевіДрім»_____
(найменування об’єкта категоріювання)

1. Підстава для категоріювання _____
(рішення про створення КСЗІ, закінчення терміну дії акта категоріювання,
_____
зміна ознаки, за якою була встановлена категорія об’єкта, тощо;
_____
посилання/реквізити на розпорядчий документ про призначення комісії з категоріювання)

2. Вид категоріювання _____первинне_____
(первинне, чергове, позачергове)
_____
(у разі чергового або позачергового категоріювання вказується категорія, що була встановлена до цього категоріювання; посилання/реквізити на документ, яким було встановлено цю категорію)

3. На ОІД здійснюється _____обробка інформації технічними засобами_____
(обробка інформації технічними засобами та/або озвучування інформації)

4. Ступінь обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на об’єкті
_____конфіденційна інформація_____
(передбачена законом таємниця (крім державної); службова інформація; конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України “Про доступ до публічної інформації”; інша конфіденційна інформація, вимога щодо захисту якої встановлена законом)

5. Встановлена категорія_____4 категорія, до четвертої категорії відносяться об’єкти, в яких циркулює службова та конфіденційна інформація, вимога щодо захисту якої встановлена законом_____

Голова комісії _____ _____
(підпис) (ініціали, прізвище)
Члени комісії: _____ _____
(підпис) (ініціали, прізвище)
____.____. 20___

ДОДАТОК Е. Перелік матеріалів на оптичному носії

Левітан_ОС_125_18_3_ПЗ.docx

Левітан_ОС_125_18_3_ДМ.pptx

Левітан_ОС_125_18_3_ПЗ.pdf

Левітан_ОС_125_18_3_ПЗ.pdf.p7s.p7s

ДОДАТОК Є. Відгук керівника економічного розділу

Відгук керівника економічного розділу:

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку _95_ б. («відмінно»).

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (ініціали, прізвище)

ДОДАТОК Ж. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студентки групи 125-18-3
Левітан Ольги Сергіївни
на тему: «Політика безпеки інформації інформаційно-телекомунікаційної системи ТОВ «ЛевіДрім»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 65 сторінках.

Метою кваліфікаційної роботи є забезпечення достатнього рівня захисту інформації у інформаційно- телекомунікаційній системі підприємства.

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: аналіз стану питання, аналіз нормативно-правової бази, виконання постановки задачі, виконання обстеження об'єкту інформаційної діяльності, розробка моделі порушника та загроз, розробка елементів політики безпеки інформації.

Практичне значення результатів кваліфікаційної роботи полягає у підвищенні рівня захищеності інформації на об'єкті інформаційної діяльності, за рахунок слабких місць та розробки політики безпеки

Оформлення пояснювальної записки до кваліфікаційної роботи виконано з незначними відхиленнями від стандартів.

За час дипломування Левітан О.С. проявила себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації бакалавра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека».

Рівень запозичень у кваліфікаційній роботі не перевищує вимог "Положення про систему виявлення та запобігання плагіату".

Кваліфікаційна робота заслуговує оцінки «90 (відмінно)».

Керівник кваліфікаційної роботи д.ф.-м.н., проф. Кагадій Т.С.

Керівник спец. розділу ст. викл Тимофєєв Д.С.