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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Михайленко Артема Андрійовича*

академічної групи *125-17-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплексна система захисту інформації інформаційно-телекомунікаційної системи готельно-ресторанного господарювання «Avenue 69»*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		Рейтинговою	інституційною	
кваліфікаційної роботи	доц. Горєв В.М.			
розділів:				
спеціальний	ас. Мілінчук Ю.А.			
економічний	доц. Пілова Д.П.			

Рецензент				

Нормконтролер	ст.викл. Тимофєєв Д.С.			

Дніпро
2021

ЗАТВЕРДЖЕНО:

завідувач кафедри

безпеки інформації та телекомунікацій

____________ д.т.н., проф. Корнієнко В.І.

« » 20 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студента *Михайленко Артема Андрійовича* *академічної групи 125-17-2*

спеціальності *125 Кібербезпека*

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплексна система захисту інформації інформаційно-телекомунікаційної системи готельно-ресторанного господарювання «Avenue 69»*

Затверджено наказом ректора НТУ «Дніпровська політехніка» від _07.06.2021_ № 317-с

Розділ	Зміст	Термін виконання
Розділ 1	Проаналізувати нормативно-правову базу в сфері захисту інформації в Україні, визначити актуальність проблеми захисту інформації в ІТС, виконати постановку задачі на розробку КСЗІ в ІТС.	20.05.2021 - 27.05.2021
Розділ 2	Провести обстеження ОІД, виконати категоріювання ОІД, провести аналіз загроз, обрати профіль захищеності, розробити комплексну-систему захисту інформації.	30.05.2021 - 05.06.2021
Розділ 3	Обґрунтувати економічну доцільність впровадження КСЗІ, розрахувати витрати та ефект впровадження КСЗІ в ІТС	07.06.2021 - 12.06.2021

Завдання видано ________________ ________________
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: _____11.01.2021________

Дата подання до екзаменаційної комісії: _____12.06.2021______

Прийнято до виконання: ________________ Михайленко А.А.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 59 с., 7 рис., 19 табл., 8 додатка, 14 джерел.

Об`єкт дослідження: готельно-ресторанне господарювання «Avenue 69».

Предмет дослідження: інформаційно-телекомунікаційна система готельно-ресторанного господарювання «Avenue 69».

Метою дипломної роботи є розробка комплексної-системи захисту інформації інформаційно-комунікаційної системи готельно-ресторанного господарювання «Avenue 69».

У перший розділ кваліфікаційної роботи описано стан питання, проаналізовано нормативно-правову базу у сфері захисту інформації України. Надано загальний аналіз проблем інформаційної безпеки світу та України, розглянуто стан інформаційної безпеки в малому та середньому бізнесах відповідно. Також у першому розділі було сформульовано постановку задачі для цієї кваліфікаційної роботи. Була сформульована актуальність проблеми захисту інформації в ІТС системах готельно-ресторанного бізнесу на основі обраного підприємства.

У другому розділі було описано підприємство готельно-ресторанного господарювання "Avenue 69", його організаційна структура. Було проаналізовано інформацію, що оброблюється на ІТС. Також у другому розділі кваліфікаційної роботи проведено акт обстеження об'єкту інформаційної діяльності та категоріювання ОІД. Наведено загальні відомості про об'єкт інформаційної діяльності, обрано профіль захищеності ІТС. Задля забезпечення захисту інформації, були запропоновані програмно-апаратні та організаційні методи щодо захисту інформації в ІТС.

У третьому розділі було розраховано витрати на створення комплексу засобів захисту та щорічні експлуатаційні витрати на його підтримку. Також було доведено економічну доцільність створення комплексу.

КОМПЛЕКСНА СИСТЕМА ЗАСОБІВ ЗАХИСТУ, ПОЛІТИКИ БЕЗПЕКИ, ОПЕРАЦІЙНІ СИСТЕМИ, МОДЕЛЬ ПОРУШНИКА

РЕФЕРАТ

Пояснительная записка: 59 стр., 7 рис., 19 табл., 7 прил., 14 ист.

Объект исследования: гостинично-ресторанное хозяйствования «Avenue 69».

Предмет исследования: информационно-телекоммуникационная система гостинично-ресторанного хозяйства «Avenue 69».

Целью работы является разработка комплексной-системы защиты информации информационно-коммуникационной системы гостинично-ресторанного хозяйства «Avenue 69».

В первом разделе квалификационной работы описывает состояние вопроса, анализируется нормативно-правовая база в сфере защиты информации Украины. Предоставлено общий анализ проблем информационной безопасности мира и Украины, рассмотрено состояние информационной безопасности в малом и среднем бизнесах соответственно. Также в первой главе были сформулированы постановку задачи для этой квалификационной работы. Была сформулирована актуальность проблемы защиты информации в ИТС системах гостинично-ресторанного бизнеса на основе выбранного предприятия.

Во втором разделе были описаны предприятие гостинично-ресторанного хозяйства "Avenue 69", его организационная структура. Также во второй главе квалификационной работы проведено акт обследования объекта информационной деятельности и категорирование ОИД. Приведены общие сведения об объекте информационной деятельности, избран профиль защищенности ИТС. Для обеспечения защиты информации, были предложены программно-аппаратные и организационные методы по защите информации в ИТС.

В третьем разделе было рассчитано затраты на создание комплекса средств защиты и ежегодные эксплуатационные расходы на его поддержку. Также было доказано экономическую целесообразность создания комплекса.

КОМПЛЕКС СРЕДСТВ ЗАЩИТЫ, УСЛУГИ БЕЗОПАСНОСТИ, УПРАВЛЕНИЕ ДОСТУПОМ, ОПЕРАЦИОННЫЕ СИСТЕМЫ, АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ

ABSTRACT

Explanatory note: _59_ p., _7_ fig., _19_ tab., _19_ additions, _14_ sources.

The object of the study: the hotel and restaurant economy "Avenue 69".

Subject of the study: information and telecommunications system of hotel and restaurant economy "Avenue 69".

The aim of the work is to develop an integrated information security system of information and communication system of hotel and restaurant enterprise "Avenue 69".

The first section of the qualification work describes the state of the issue, analyzes the normative-legal base in the field of information protection in Ukraine. Provided a general analysis of the problems of information security of the world and Ukraine, considered the state of information security in small and medium-sized businesses, respectively. Also in the first chapter the problem statement for this qualification work was formulated. The relevance of the problem of information security in the ITS systems of the hotel and restaurant business on the basis of the selected enterprise was formulated.

The second section described the hotel and restaurant enterprise "Avenue 69", its organizational structure. It was analyzed the information that is processed on the ITS. Also in the second chapter of the qualification work was the act of examining the object of information activities and categorization of the ITS. The general information about the object of information activity was given, the ITS security profile was chosen. To ensure the protection of information, were proposed software and hardware and organizational methods for the protection of information in ITS.

In the third section, the cost of creating a set of security features and annual operating costs to support it was calculated. It was also proved the economic feasibility of creating the complex.

The practical value of the project is to increase the level of information security in information processing in ITS.

INTEGRATED INFORMATION SECURITY SYSTEM, OPERATING SYSTEMS, INTRUDER MODEL, THREAT MODEL

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ДСТУ - державний стандарт України;

ІзОД – інформація з обмеженим доступом;

ІС – інформаційна система;

ТЗІ – технічний захист інформації;

ВП - внутрішній порушник;

КЗЗ - комплекс засобів захисту;

НСД — несанкціонований доступ;

ОІД – об’єкт інформаційної діяльності;

ПЗ – програмне забезпечення;

ВП - внутрішній порушник;

ІТ - інформаційні технології;

ПК – персональний комп’ютер;

ІТС – інформаційно-телекомунікаційна система;

КЗ– контрольована зона;

ДТЗ – допоміжні технічні засоби;

ОС - операційна система;

НД ТЗІ – нормативний документ із технічного захисту інформації;

ОС – обчислювальна система;

КСЗІ – Комплексна Система Захисту Інформації;

NCSI – National Cyber Security Index.

ISO - International Organization for Standardization (Міжнародна організація зі стандартизації);

ЗМІСТ

ВСТУП

Середня вартість збитків через витік інформації з компаній у світі зросла в цьому році на 6,4% і склала $ 3,86 млн. Про це свідчить дослідження, проведене Ponemon Institute і IBM Security[1]. При цьому згідно зі статистикою InfoWatch, велика частина витоків відбувається з вини співробітників. Найчастіше таких зловмисників цікавлять персональні дані, комерційні таємниці, відомості про нові розробки і платіжна інформація. На думку фахівців, компанії обов'язково повинні приділяти увагу контролю доступу до корпоративної інформації і аутентифікації користувачів. Це ж стосується шифрування всіх критичних даних і зберігання ключів шифрування.

Згідно з Міжнародним союзом електрозв'язку (ITU)[2], було проаналізовано національний індексі кібербезпеки (NCSI), Україна зайняла 25 місце у в рейтингу країн.

Основний удар кіберзлочинців направлений на малий та середній бізнес, так як інфраструктура таких підприємств менш розвинена і методи забезпечення безпеки є недостатньо ефективними або зовсім не розвинені/впроваджені. Також одним з основних чинників у виборі атак для кіберзлочинців є невелика кількість навченого персоналу та управління загрозами та реагування на них.

Фінансовий сектор малого та середнього бізнесу вразливий для кібератак. Фінансовий сектор є привабливим об'єктом для кіберзлочинців через його важливу роль у ролі підприємства. Пряма кібератака на підприємство може мати суттєві наслідки у виді фінансових збитків, а також втрати репутації.

Від кібератак малий та середній бізнеси страждають в найбільшій мірі. В таких організаціях зосереджується конфіденційна інформація про фінансову діяльність багатьох людей. Ці підприємства зберігають та оброблюють інформацію про співробітників та клієнтів, що розширює коло потенційних зловмисників, зацікавлених в крадіжці або псуванні такої інформації.

Типи кібератак на організації, що займаються готельно-ресторанним господарюванням, мало відрізняються від атак на організації/компанії, що працюють в інших сферах. Поширені загрози інформаційної безпеки

- крадіжка особистих даних і втрата конфіденційних даних. Ця інформація може бути особливо цінною для зловмисників, вони можуть використовувати здобуту інформацію в якості інструменту для шахрайства, здирництва та інших фінансових злочинів.

- автоматизовані загрози. Злом облікових даних, сканування вразливостей, відмова в обслуговуванні можуть потенційно загрожувати системі компанії.

- порушення бізнесу. Кібератаки можуть серйозно підірвати бізнес, наприклад стерти комп’ютерну інфраструктуру, яка включає: телефонні довідники, електронну пошту, ділові записи, шаблони договорів. Така атака на компанію може на деякий час перервати її роботу. Проблеми захисту інформації підприємств, що займаються схожим видом господарювання:

- Проблема збереженості цілісності даних;

- проблема захисту від комп'ютерних вірусів;

- проблема фізичного несанкціонованого доступу до інформації.

Об’єктом дослідження є готельно-ресторанне господарювання «Avenue 69».

Предметом дослідження є інформаційно-телекомунікаційна система готельно-ресторанне господарювання «Avenue 69».

Метою кваліфікаційної роботи є розробка комплексної-системи захисту інформації інформаційно-комунікаційної системи готельно-ресторанне господарювання «Avenue 69».

Так як у малих та середніх бізнесах, що займаються готельно-ресторанною діяльністю немає досить налагодженої комплексної системи захисту інформації з обмеженим доступом, то такі підприємства у першу чергу стають потенційними жертвами зловмисників. Як наслідок, конфіденційна інформація та ІзОД, яка обробляється в ІТС є недостатньо захищеною від атак зловмисників, що в свою чергу становить велику загрозу для репутації підприємства. Через це кваліфікаційна робота в якій пропонується створення комплексної системи захисту інформації є актуальною.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

Станом на кінець 2020 року, кіберспеціалісти Служби безпеки України задокументували несанкціоноване втручання в роботу інформаційно-телекомунікаційних систем малих та середніх бізнесів.

Несанкціонований доступ (НСД) - доступ до інформації з використанням засобів, включених до складу комп’ютерної системи, що порушує встановлені правила розмежування доступу (ПРД). НСД може здійснюватись як з використанням штатних засобів, тобто сукупності програмно-апаратного забезпечення, включеного до складу комп’ютерної системи розробником під час розробки або системним адміністратором в процесі експлуатації, що входять у затверджену конфігурацію комп’ютерної системи, так і з використанням програмно-апаратних засобів, включених до складу комп’ютерної системи зловмисника.

Під захистом від НСД слід розуміти діяльність, спрямовану на забезпечення додержання правил розмежування доступу шляхом створення і підтримки в дієздатному стані системи заходів із захисту інформації.

До основних способів НСД належать:

- безпосереднє звернення до об'єктів з метою одержання певного виду доступу;
- створення програмно-апаратних засобів, що виконують звертання до об'єктів в обхід засобів захисту;
- модифікація засобів захисту, що дозволяє здійснити НСД;
- впровадження в комп’ютерну систему програмних або апаратних механізмів, що порушують структуру і функції комп’ютерної системи і дають можливість здійснити НСД.

Малий та середній бізнеси в нашій країні – це одна з провідних галузей зростанні економіки країни. Для забезпечення працездатності малого та середнього бізнесів використовують великий об'єм інформаційних ресурсів, та велику кількість одиниць обчислювальної техніки.

Тому основною складовою нормальної роботи таких підприємств є впровадження правильної комплексної системи захисту інформації.

При створенні та впровадженні комплексної системи захисту інформації інформаційно-телекомунікаційної системи готельно-ресторанного бізнесу слід враховувати розміри підприємства, фінансовий стан підприємства, стан інформаційної безпеки на момент створення комплексної системи захисту інформації.

Реалізація комплексної системи захисту інформації повинна бути простою та зрозумілою, механізми реалізації комплексної системи захисту інформації не повинні вимагати особливих навичок від співробітників цього підприємства, не повинні виникати додаткові витрати при виконанні робіт на реалізацію комплексної системи захисту інформації, а також, не повинні ставити за мету виконувати співробітникам підприємства незрозумілих та/або малознайомих їм операцій.

1.2 Аналіз нормативно-правового забезпечення захисту інформації

Поняття нормативно-правового забезпечення національної безпеки -- це процес створення і підтримки функціональних характеристик системи національної безпеки за допомогою впорядковуючого впливу нормативно-правових засобів в необхідних межах організацій.

Забезпечення захисту інформації базується на нормативно-правових актах держави.

Закон України «Про Інформацію» визначає інформацію як документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому середовищі.

Згідно статті 1 Закону України «Про Інформацію», інформація - це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. У Законі України «Про Інформацію» докладно описується інформація; види інформації, серед яких слід виділити інформацію з обмеженим доступом.

Згідно статті 8 Закону України "Про захист інформації в ІТС", Державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності комплексної системи захисту інформації здійснюється за результатами державної експертизи, яка проводиться з урахуванням галузевих вимог та норм інформаційної безпеки у порядку, встановленому законодавством.

Згідно статті 9 Закону України "Про захист інформації в ІТС", відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

Власник системи, в якій обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним.

В НД ТЗІ 1.1-003-99 розглядається термінологія та визначення понять в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу. Терміни, що встановлюються 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 терміну не допускається.

Для довідки наведені іноземні еквіваленти термінів, що запроваджуються, а також алфавітні покажчики термінів.

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. №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”. НД ТЗІ призначений для суб’єктів відносин (власників або розпорядників АС, користувачів), діяльність яких пов’язана з обробкою в автоматизованих системах інформації, що підлягає захисту згідно з нормативно-правовими актами, а також для розробників комплексних систем захисту інформації в автоматизованих системах.

НД ТЗІ 2.5-004-99 встановлює критерії оцінки захищеності інформації, яка обробляється 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.

Стандарт ДСТУ ISO/IEC 27001:2015 визначає вимоги до проектування, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою з урахуванням обставин організації. Цей стандарт також містить вимоги для оцінювання та оброблення ризиків інформаційної безпеки, пов'язаних з потребами організації. Цей стандарт створений для визначення вимог для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та постійного вдосконалення системи управління інформаційною безпекою (СУІБ).

Стандарт ДСТУ ISO/IEC 27005:2015 забезпечує рекомендації для менеджменту ризиків інформаційної безпеки, які включають інформацію і менеджмент ризиків безпеки технологій телекомунікації.

Згідно з пунктом 5 НД ТЗІ 1.6-005-2013 об'єкти, на яких здійснюватиметься обробка технічними засобами та/або озвучуватиметься інформація з обмеженим доступом, що не становить державної таємниці, підлягають обов'язковому категоріюванню.

Категоріювання може бути первинним, черговим або позачерговим.

Категоріювання здійснюється для визначення необхідного (зі встановлених нормативно-правовими актами та нормативними документами системи технічного захисту інформації рівнів) рівня захисту інформації, що обробляється технічними засобами та/або озвучується на об'єкті.

Відповідальність за своєчасність категоріювання та правильність встановлення категорії об'єкта покладається на керівника установи - власника (розпорядника, користувача) об'єкта.

Об'єктами категоріювання є об'єкти інформаційної діяльності, в тому числі об'єкти ЕОТ.

Категоріювання здійснюється за ознакою: ступінь обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на ОІД.

Об'єктам, на яких обробляється технічними засобами та/або озвучується інформація з обмеженим доступом, що не становить державної таємниці, встановлюється четверта (IV) категорія.

За рішенням розпорядників (користувачів) інформації або за рішенням власників (розпорядників, користувачів) об'єктів, на яких обробляється технічними засобами та/або озвучується інформація з обмеженим доступом, що не становить державної таємниці, об'єктам може встановлюватися III категорія.

Об'єкти, яким встановлено відповідну категорію, вносяться до Переліку категорійованих об'єктів, який ведеться власником (розпорядником, користувачем) об'єктів інформаційної діяльності.

1.3 Постановка задачі

На основі проаналізованих проблем у пункті 1.1, у якому виявили типові проблеми готельно-ресторанного бізнесу, у якості задачі визначено необхідність розробки комплексної системи захисту інформації інформаційно-телекомунікаційної системи готельно-ресторанного господарювання.

Для більш коректної розробки комплексної системи захисту інформації (КСЗІ), потрібно дотримуватись таких пунктів:

- Ознайомлення з характерними особливостями конкретного підприємства;
- Аналіз характеристик об'єкту;
- Аналіз видів інформації, що циркулює на об'єкті;
- Аналіз особливостей взаємодії з інформацією;
- Обрання профілю захищеності;

Висновки першого розділу

У розділі 1 кваліфікаційної роботи було проаналізовано стан інформаційної безпеки в малому та середньому бізнесах України, наведена статистика кібератак. У розділі 1 були перелічені та проаналізовані нормативно-правові документи в сфері захисту інформації. Серед документів, що є правовою основою забезпечення безпеки інформації розглянуті НД ТЗІ та їх галузі використання, Закони України, положення та накази.

Обґрунтовано потребу у створенні та розробці комплексної системи захисту інформації інформаційно-телекомунікаційної системи готельно-ресторанного господарювання.

2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальні відомості про готельно-ресторанне господарювання “Avenue 69”.

У якості об’єкта дослідження було обрано інформаційно-телекомунікаційну систему готельно-ресторанного господарювання «Avenue 69». Всі деталі були частково змінені на вимогу керівництва підприємства в цілях забезпечення анонімності підприємства.

Заклад займається веденням готельно-ресторанного бізнесу, заклад громадського харчування.

Сьогодні підприємство розташоване у м. Кам’янське.

2.2 Обґрунтування необхідності створення КСЗІ

Підставою для необхідності створення КСЗІ є нормативно-правові акти, що розглянуті в Розділі 1, де вказані вимоги, які встановлюють обов’язковість обмеження доступу до певних видів інформації. Згідно з актом категоріювання об'єкту (Додаток А), інформація яка обробляється на підприємстві не потребує обов'язкового захисту, але на підставі проведеного аналізу власником інформації, яким виступає директор, прийняте рішення щодо створення КСЗІ та видано наказ «Про визначення відповідального за забезпечення технічного захисту інформації та створення КСЗІ ІТС готельно-ресторанного господарювання «Avenue 69» (Додаток Б).

Завданнями захисту інформації на підприємстві можна виділити:

- ідентифікація загроз та вразливостей інформації та подальше запобігання їх реалізації;
- створення комплексної системи захисту інформації для ефективного керування доступом користувачів до ресурсів, контроль за їхньою роботою та сповіщення про спроби НСД;
- реєстрація, збір, зберігання, обробка даних про всі події в системі, які мають відношення до безпеки інформації;
- реалізація захисту від потенційних внутрішніх та зовнішніх загроз.

2.3.1 Організаційна структура підприємства

Кількість співробітників компанії – 30 чоловік. Адміністративний відділ - центральний офіс, з якого йде регулювання процесами всієї компанії. Адміністративний відділ підрозділяється на:

- Основний торгівельний зал;
- Кухня
- Бухгалтерія
- Приміщення для проведення навчання;
- Технічні приміщення (склади, прибиральні).

Так як основний торговельний зал та бухгалтерія були обрані як ОІД, розглянемо їх більше детально

Основний торгівельний зал та бухгалтерія підприємства налічує 10 співробітників, які мають чітку ієрархію та розподілення обов’язків. Прямі обов’язки бухгалтерії:

- ведення роздрібної торгівлі;
- відображення у документах достовірної та у повному обсязі інформації про усі операції і результати діяльності, необхідної для оперативного управління бюджетними призначеннями та фінансовими і матеріальними (нематеріальними) ресурсами;
- ведення бухгалтерського обліку;
- складення на підставі даних бухгалтерського обліку фінансової та бюджетної звітності, а також державної статистичної, зведеної та іншої звітності в порядку, встановленому законодавством;
- своєчасне та у повному обсязі перерахування податків і зборів (обов'язкових платежів) до відповідних бюджетів;

2.3.2 Аналіз підприємства

Основний торговельному залі та бухгалтерії готельно-ресторанного бізнесу «Avenue 69» обробляється інформація з обмеженим доступом: персональні дані співробітників та клієнтів, трудові договори, інформація про документи підприємства, інформація про стан мережі та інші.

Вся документація підприємства існує у двох видах: паперовому та електронному. Електронний вид документації створюється працівниками підприємства на робочих комп'ютерах з інстальованим програмним забезпеченням. Копії паперових документів здійснюються завдяки: принтерам, ксероксам. Електронні копії документів зберігаються на робочих станціях директора та бухгалтерів.

Детальний перелік інформації, правовий режим, вид зберігання та потреби до К(Конфіденційність), Ц (Цілісність), Д (Доступність) наведено у таблиці 2.1.

К – вимоги до конфіденційності

Ц – вимога до цілісності

Д – вимога до доступності

Таблиця 2.1 Класифікація інформації, що обробляється на ОІД

№	Вид інформації	По режиму доступності	По режиму секретності	Вид представлення в інформаційній системі	Потреби до К,Ц,Д			
					К	Ц	Д	
2	Персональні дані співробітників, їх посадові інструкції	З обмеженим доступом	Персональні дані	Паперовий Електронний	3	2	2	0,4
3	Персональні дані клієнтів	З обмеженим доступом	Персональні дані	Паперовий Електронний	3	2	2	0,4
4	Інформація про діяльність підприємства	Відкрита	________	Паперовий Електронний	1	2	2	0,15

Продовження таблиці 2.1

№	Вид інформації	По режиму доступності	По режиму секретності	Вид представлення в інформаційній системі	Потреби до К,Ц,Д			
					К	Ц	Д	
5	Інформація про графік роботи підприємства	Відкрита	________	Паперовий Електронний	1	2	2	0,15
6	Статутні документи підприємства	Відкрита	________	Паперовий Електронний	1	3	2	0,15
7	Трудові договори	З обмеженим доступом	Конфіденційна	Паперовий	1	3	2	0,3
8	Інформація про документи підприємства (Службові записки, накладні, накази)	З обмеженим доступом	Конфіденційна	Паперовий Електронний	3	2	3	0,6
9	Звіти закупівель	З обмеженим доступом	Конфіденційна	Паперовий Електронний	3	2	3	0,6
10	Документи постачання	З обмеженим доступом	Конфіденційна	Паперовий Електронний	3	2	3	0,6
11	Інформація про фінансову діяльність підприємства	Відкрита	________	Паперовий Електронний	3	2	2	0,4
12	Інформація про стан мережі і її компонентів	З обмеженим доступом	Конфіденційна	Електронний	3	3	2	0,6

- К1 - рівень конфіденційності інформації, при якому компанія зазнає незначних збитків в разі розкриття інформації особам, які не мають допуску до неї;
- К2 - рівень конфіденційності інформації, при якому організація пізнає відчутних збитків в разі розкриття інформації особам, які не мають допуску до неї;
- К3 - рівень конфіденційності інформації, яка може призвести до значних матеріальних втрат у разі розкриття інформації особам, які не мають допуску до неї;
- Ц1 - рівень цілісності інформації, при якому компанія зазнає незначних збитків в разі втрати цілісності інформації;
- Ц2- рівень цілісності інформації, при якому організація відчуває від-чутних збитків в разі втрати цілісності інформації;
- Ц3 - рівень цілісності інформації, яка може призвести до значних матеріальних втрат у разі втрати цілісності інформації;
- Д1 - рівень доступності інформації, при якому компанія відчуває не-значні збитки в разі втрати доступності інформації;
- Д2 - рівень доступності інформації, при якому організація несе відчутних збитків в разі втрати доступності інформації;
- Д3 - рівень доступності інформації, яка може призвести до значних матеріальних втрат у разі втрати доступності інформації;

2.3.3 Обстеження об'єкту інформаційної діяльності

Назва підприємства – ресторан «Avenue 69». Основний торгівельний зал є об'єктом інформаційної діяльності, що досліджується в кваліфікаційній роботі. ОІД є складовою адміністративного відділу компанії

Адреса – м. Кам'янське, пр. Наддніпрянський, 1А.

Загальна площа – 330 м^2

Приміщення ОІД знаходиться на 3 поверсі Адміністративної будівлі, займає 4 приміщення.

Робочі години з 9:00 до 23:00

Робочі дні: понеділок – неділя

За фізичну охорону ОІД відповідає внутрішня охорона компані, а саме - Служба охорони, що забезпечує фізичну охорону на території всього закладу. До повноважень служби охорони входить:

- Адміністрування систем відеоспостереження;
- Контроль за активністю співробітників.

Місце розташування ОІД зображено в додатку Е.

Таблиця 2.2 Прилеглі споруди відносно ОІД

Номер на плані	Тип споруди	Назва	Місце розташування	Відстань до ОІД	Кількість поверхів
1	Житлова будівля	-	Південний Захід	55 м	9
2	Житлова будівля	-	Південний Захід	100 м	9

Прилеглі вулиці відносно КЗ вказані у таблиці 2.3.

Таблиця 2.3 Прилеглі вулиці відносно КЗ

Назва	Опис
Проспект Наддніпрянський	Відносно ОІД проспект розташований на півдні, Автомобільний трафік становить 30 - 60 машин на годину.

Комунікаційні системи КЗ вказані у таблиці 2.4.

Таблиця 2.4 Комунікаційні системи

Вид комунікації	Характеристика
Система електропостачання	Підключена до трансформаторної підстанції, знаходиться за межами КЗ

Продовження таблиці 2.4

Лінія Інтернету	Підключено до ІСП «Фрінет»
Вид комунікації	Характеристика
Кабелі комп'ютерної мережі	Кабель неекранованої мережі, вита пара
Система сигналізації	Складається з датчиків відкриття (магнітно-контактний датчик)
Система водопостачання	Підключена до мережі міста, знаходиться в межі КЗ
Система опалення	Проходить через будівлю та знаходиться в межах КЗ. Труби опалення зроблені з поліпропіленового матеріалу, що унеможливлює витік інформації по віброакустичному каналу
Система каналізації	Підключена до мережі міста, знаходиться в межах КЗ
Система вентиляції	Приточно-витяжна

Опис технічних засобів, що використовуються на підприємстві наведений у таблиці 2.5.

Таблиця 2.5 Технічні засоби

№	Тип засобу	Назва та марка	Інвентарний номер	Розташування	Мін.відстань до кордонів ОІД (см)
1	Ноутбук	MacBook Air MWTK2RU/A	96314	На столі	20
2	Ноутбук	MacBook Air MWTK2RU/A	96315	На столі	15

Продовження таблиці 2.5

№	Тип засобу	Назва та марка	Інвентарний номер	Розташування	Мін.відстань до кордонів ОІД (см)
3	Ноутбук	MacBook Air MWTK2RU/A	96316	На столі	20
4	Роутер	TP-Link CCR1036-8G-2S+EM	96317-1	У столі	20
5	Роутер	TP-Link CCR1036-8G-2S+EM	96317-2	У столі	15

Таблиця 2.6 Перелік ДТЗС

№	Назва	Марка	Модель	Серійний номер	Розміщення
1	Датчик диму	Ajax FireProtect Plus EU White (000005637)	13502013776	На стелі	20
2	Датчик диму	Ajax FireProtect Plus EU White (000005637)	13502013776	На стелі	20

Продовження таблиці 2.6

№	Назва	Марка	Модель	Серійний номер	Розміщення
3	Датчик диму	Ajax FireProtect Plus EU White (000005637)	13502013776	На стелі	20
4	Датчик диму	Ajax FireProtect Plus EU White (000005637)	13502013776	На стелі	20
5	Кондиціонер	LEBERG LBS-FRA06UA /LBU-FRA06UA	80908964086	На стіні	20
6	Кондиціонер	LEBERG LBS-FRA06UA /LBU-FRA06UA	80908964087	На стіні	20
7	Кондиціонер	LEBERG LBS-FRA06UA /LBU-FRA06UA	80908964088	На стіні	20
8	МФУ2	Canon PIXMA G3411 with Wi-Fi (2315C025)	73567363	На столі	80

Продовження таблиці 2.6

№	Назва	Марка	Модель	Серійний номер	Розміщення
9	МФУ3	HP LaserJet Pro M428fdn, fax,duplex, ethernet,DADF (W1A29A)	533634564563456	На столі	80
10	Датчик руху	Ajax CombiProtect White (000001134)	34563242	На стіні	12
11	Датчик руху	Ajax CombiProtect White (000001134)	643754564	На стіні	12
12	Датчик руху	Ajax CombiProtect White (000001134)	2566825462	На стіні	12
13	Відеокамера	Hikvision Turbo DS-2CE16D0T-IRF	564745674567	На стіні	12
14	Відеокамера	Hikvision Turbo DS-2CE16D0T-IRF	46547465	На стіні	12
15	Відеокамера	Hikvision Turbo DS-2CE16D0T-IRF	4535231663	На стіні	12

Продовження таблиці 2.6

№	Назва	Марка	Модель	Серійний номер	Розміщення
16	Відеокамера	Hikvision Turbo DS-2CE16D0 T-IRF	13456354535	На стіні	12
17	Фіскальний апарат	Datecs FP-101	38277742600	На столі	12

Таблиця 2.7 Встановлене програмне забезпечення

№	Призначення	Назва	Версія	Тип ліцензії
1	ОС	macOS Big Sur 11.4	17763.769	Commercial
2	Браузер	Google Chrome	90.0.4430.93	Commercial
3	Антивірусне ПЗ	Avast	14.4	Commercial
4	ПЗ для роботи з документами	Microsoft Office	2019	Commercial
6	Електронна пошта	Gmail	-	Commercial

Таблиця 2.8 Обстеження середовища користувачів

№	Користувач	Посада	Кількість працівникі в на посаді	Рівень кваліфікації
1	PC-1	Директор	1	Кваліфікований робітник
2	PC-2	Адміністратор	1	Кваліфікований робітник
3	PC-3	Бухгалтер	1	Висококваліфікований робітник
4	-	Системний адміністратор	1	Висококваліфікований робітник
4	-	Офіціант	1	Не кваліфікований робітник
5	-	Бармен	1	Не кваліфікований робітник

На певній зміні та на все підприємство знаходяться/працюють лише 1 офіціант, 1 бармен та 1 адміністратор. З настанням нової зміни, змінюються тільки люди на певній посаді, тому фактично, на зміні завжди є 1 офіціант, 1 бармен та 1 адміністратор.

Обов'язки робітників:

Директор – керівництво закладом, обробка важливих документів, підписання документів.

Адміністратор – керівництво працівниками закладу. обробка документів, складання звітності.

Бухгалтер – обробка інформації, підписання документів, ведення звітності.

Офіціант – обслуговування клієнтів закладу.

Бармен – обслуговування клієнтів закладу.

Відомості щодо інформаційної діяльності на ОІД та категорія ОІД:

На об'єкті інформаційної діяльності (ОІД) видом інформаційної діяльності є обробка технічними засобами та озвучення інформації з обмеженим доступом.

Об'єкту встановлена четверта (IV) категорія, на якому обробляється технічними засобами та озвучується інформація з обмеженим доступом, що не становить державної таємниці.

Характеристика ОІД:

Тип ОІД — заклад громадського харчування "Avenue 69".

Ситуаційний план зображено у додатку Є(див. додаток Є. Ситуаційний план) .

Територія контрольованої зони (КЗ) обмежена стіною, яка суміжна з будівлею поруч з КЗ. Будівля КЗ не обмежена парканом. Територія КЗ обмежена будівлею, в якій охорона ОІД покладається на охоронців. Трансформаторна підстанція розміщена поруч з будівлею підприємства.

Схема (Ситуаційний план ОІД) — Додаток Є (див. додаток Є. Ситуаційний план).

Суміжні будівлі № 9, №10, №11.

Архітектурно-будівельні особливості ОІД:

Розміри Об’єкту Інформаційної Діяльності: 14х8м. Висота стелі 2,55м. Поверх — 1ий.

Стеля (матеріал — бетон, товщина — 0,45м); підлога (матеріал — бетон+дошки (паркет, товщина — 0,7м); стіни (матеріал — бетон, товщина 0,5м).

Вікна (кількість — 3 шт, матеріал вікна — пластик, розміри — 2,6х1,7м). Вікно виходить на проспект Наддніпрянський. Сектору прямої видимості з будівель навпроти -немає.

Характеристика складових ОІД:

Відомості щодо ОТЗ наведені в таблиці 2.1 (див. Таблиця 2.1 Перелік ОТЗ). З допоміжних технічних засобів і систем зустрічаються датчики диму, МФУ, кондиціонери. датчики руху, відеокамери та фіскальний апарат. Усі ДТЗС знаходяться на території ОІД. Опис допоміжних технічних засобів і систем надано у таблиці 2.2 Перелік ДТЗС (див стор. 14).

Схема розташування ОТЗ та транзитних комунікацій зображено у Додатку Є. Рисунок 1.1.1 Транзитні комунікації.

Схема систем електроживлення зображено на Генеральному плані (Додаток Ж, Рисунок 1.1 Ситуаційний план.).

Схема заземлення зображена на Ситуаційному плані - Додаток Є, Рисунок 1.1 Ситуаційний план. Заземлення за КЗ. Підключення ДТЗС або інших технічних засобів сторонніх споживачів до заземлення відсутня. Наявність підключення до контуру заземлення ОТЗ відсутня. Розетки та інші ОТЗ і ДТЗС заземленню не підлягають.

Транзитні комунікації, які мають вихід за межі ОІД: система опалення, система каналізації та водопостачання, система електроживлення, Інтернет(комунікація ДТЗС).

Відомості про обладнання, що може впливати на показники захищеності інформації:

За межі КЗ мають вихід: електроживлення, водопостачання, оптоволоконний кабель Інтернету.

Система електроживлення проходить до КЗ повітрям, до ОІД проходить внутрішньо. Кабель інтернету також проходить до ОІД через перший поверх. Водопостачання проходить до КЗ через перший поверх. Система опалення проходить внутрішньо, по стіні будівлі через кімнати.

Виявлені характерні особливості ОІД, що впливають на вибір заходів та засобів ТЗІ: системи водопостачання, каналізації проходять дуже поруч з кімнатами ОІД. відсутність лінії телефонного зв’язку; перший поверх будівлі.

2.3.4 Опис обчислювальної системи

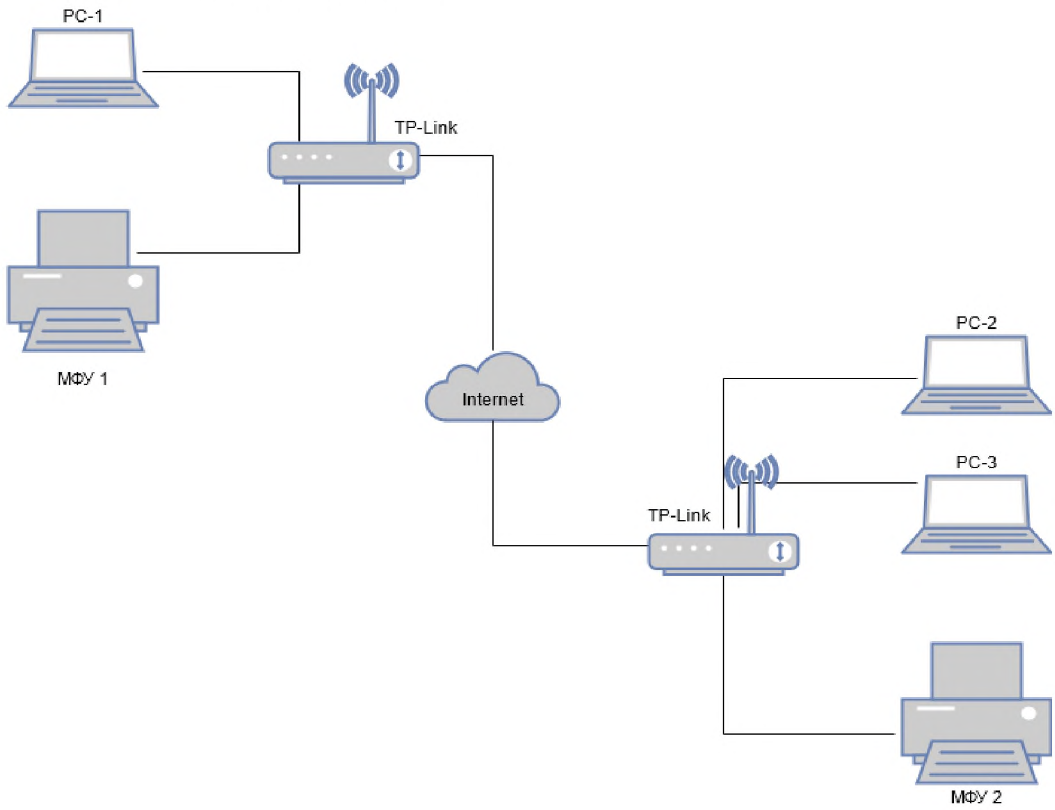


Рисунок 2.1 Схема ІТС

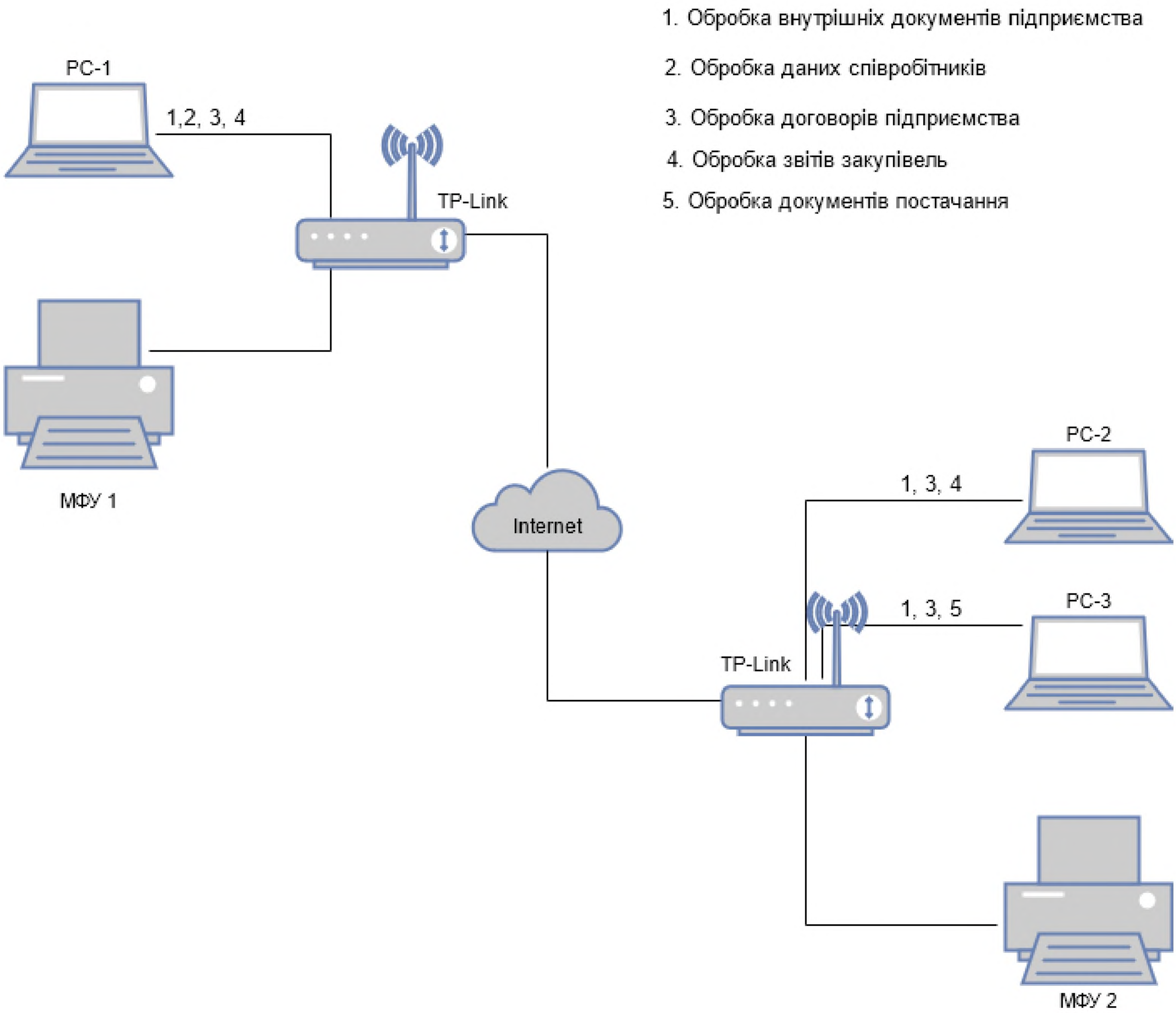


Рисунок 2.2 Схема інформаційних потоків

Порушником вважається особа, яка здійснює спробу несанкціонованого доступу до об'єктів захисту (ознайомлення, модифікація, знищення, зміна режимів використання чи функціонування тощо).

Потенційними порушниками можуть бути: особи, які знаходяться за межами ІТС, мають можливість фізичного підключення до каналів зв'язку або інших складових мережі передачі даних, користувачі АС, персонал, який безпосередньо пов'язан із забезпеченням функціонування ІТС, особи, яким не передбачено доступ до ІзОД, але які мають доступ до приміщень, де розміщено компоненти ІТС і можуть отримати доступ до ІзОД.

2.4 Модель порушника

У таблицях наведено специфікації моделі порушника за мотивами здійснення порушень, за рівнем кваліфікації та обізнаності щодо ІТС, за показником можливостей використання засобів ІТС для реалізації загроз, за часом та місцем дії. Сукупність цих характеристик визначає профіль порушника.

Таблиця 2.9 Категорії порушників

Позначення	Визначення категорії	Потенціальний рівень загроз
П1	Авторизовані користувачі ІС, яким надано право доступу до ІзОД	5
П2	Авторизовані користувачі, яким надано повноваження контролювати дії користувачів та персоналу та забезпечувати управління ІС	4
П3	Особи, які забезпечують працездатність ІС	2
П4	Особи, яким не передбачено доступ до ІзОД, але які мають доступ до приміщень, де розміщено ІС і потенційно можуть отримати доступ до ІзОД	2
П5	Особи, які знаходяться за межами ІС, мають можливість фізичного підключення до каналів зв’язку та можуть здійснити дії щодо порушення діючої в ІС	5

Таблиця 2.10 Специфікація моделі порушника за місцем дії

Позначення	Визначення категорії	Потенціальний рівень загроз
Д1	Усередині приміщення, але без доступу до технічних засобів ІС	3
Д2	З робочих місць користувачів та персоналу ІС, а також місць розміщення обладнання ІС, де обробляється інформація, яка підлягає захисту	4

Продовження таблиці 2.10

Позначення	Визначення категорії	Потенціальний рівень загроз
Д3	Без доступу до приміщень, в тому числі з зовнішніх каналів зв'язку, з можливістю застосування технічних засобів здобуття інформації оптичними, акустичними каналами.	2

Таблиця 2.11 Специфікація моделі порушника за рівнем кваліфікації та обізнаності

Позначення	Визначення категорії	Потенціальний рівень загроз
К1	Не володіє знаннями та інформацією про порядок функціонування ІС, не має навичок щодо користування штатними засобами обробки інформації системи та захисту інформації	1
К2	Має навички щодо користування ПК на рівні користувача	3
К3	Володіє базовими знаннями щодо функціонування програмного забезпечення і операційних систем, а також практичними навичками роботи з засобами обробки інформації	4
К4	Володіє знаннями щодо: функціонування засобів та механізмів обробки інформації та її захисту, що використовуються на ІС та їх недоліків.	5

Таблиця 2.12 Специфікація моделі порушника за показником можливостей використання засобів ІТС для реалізації загроз

Позначення	Визначення категорії	Потенціальний рівень загроз
З1	Має фізичний доступ до компонентів ІС, але не є авторизованим користувачем ІС	2
З2	Має можливість запуску програм, що реалізують функції обробки інформації	3
Позначення	Визначення категорії	Потенціальний рівень загроз
З3	Має можливість керування функціонуванням ІТС, тобто конфігурує програмне забезпечення ІС.	4

Таблиця 2.13 Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Визначення категорії	Потенціальний рівень загроз
М1	Безвідповідальність (недбалість, ненавмисне порушення)	3
М2	Корислива цілеспрямованість (зловмисне порушення)	5

Таблиця 2.14 Специфікація моделі порушника за часом дії

Позначення	Визначення категорії	Потенціальний рівень загроз
Ч1	Під час бездіяльності компонентів системи (під час планових перерв у роботі, неробочий час)	3
Ч2	Під час функціонування ІС	5
Ч3	Під час перерв у роботі для обслуговування та ремонту	2

1) внутрішній порушник «ПВ» -варіант мінімальних загроз з причини безвідповідального ставлення до виконання своїх посадових обов’язків;
2) зовнішній порушник «ПЗ» (агент конкурентів або закордонних спецслужб «під прикриттям») -варіант максимальних загроз з причини цілеспрямованих несанкціонованих дій з метою модифікації або викрадення інформації.

Після зведення усіх даних в одну таблицю отримаємо модель внутрішнього порушника безпеки інформації(Таблиця 2.15) та модель зовнішнього порушника(Таблиця 2.16) . Модель внутрішнього порушника політики безпеки інформації»:

Таблиця 2.15 Модель внутрішнього порушника безпеки інформації

Посада	Мо-тив пору-шень	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума заг-роз
Директор	M1	K4	З1	Ч1	Д2	9
Адміністратор	M1	K3	З1	Ч1	Д2	8
Бухгалтер	M1	K2	З1	Ч1	Д2	7

Директор, адміністратор та бухгалтер мають рівні права доступу до інформації, яка оброблюється в ІТС. Тому далі вони розглядаються як «Користувач».

Таблиця 2.16 Модель зовнішнього порушника

Посада	Мо-тив пору-шень	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи, захисту	Можливості за часом дії	Можливості за місцем дії	Сума заг-роз
Прибиральниця	M1	K1	З1	Ч1	Д2	6
Системний адміністратор	M1	K4	З1	Ч1	Д2	9
Електрик	M1	K1	З1	Ч1	Д2	6

Продовження таблиці 2.16

Посада	Мо-тив пору-шень	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума заг-роз
Конкурент	М2	К3	З1	Ч1	Д3	10

Висновок: з останньої таблиці видно, що найбільшу загрозу, що має відношення до проблеми захисту інформації, становить Конкурент, Директор та Головний бухгалтер. Тому організація роботи цих осіб повинна бути найбільш контрольованою, оскільки Конкурент, Директор та Головний бухгалтер є основними потенційними порушниками безпеки інформації.

2.5 Модель загроз

Таблиця 2.17 Модель загроз.

№	Вид загрози	Джерело загрози	Вразливості	Наслідки
Випадкові загрози				
1	Вірусне зараження	Користувач	Відсутність Антивірусних програмних засобів;	К, Ц
2	Вірусне зараження	Конкурент	Наявність неконтрольованих каналів витоку інформації.	Ц
3	Помилки	Користувач	Відсутність політики інформаційної безпеки	К, Ц
4	Ненавмисні дії користувачів	Користувач	Низький рівень кваліфікації користувачів;	К, Ц

Продовження таблиці 2.17

№	Вид загрози	Джерело загрози	Вразливості	Наслідки
5	Помилки захисту	Користувач	Відсутність політики інформаційної безпеки	К, Ц, Д
Навмисні загрози				
6	Крадіжка	Конкурент	Вразлива система охорони;	Д
7	Несанкціонований доступ	Конкурент	Вразлива система охорони, порушення правил використання КС, відсутність системи розмежування доступом	К, Ц, Д
8	Порушення правил розмежування доступу	Користувач	Помилки при розмежуванні доступу.	К, Ц, Д
9	Копіювання ІзОД	Конкурент	Відсутність політики безпеки, яка регулює використання дозволених ПЗ	К, Д
10	Крадіжка ІзОД шляхом використання електронної пошти, месенджерів, файлообмінювачів	Конкурент	Відсутність політики безпеки, яка регулює використання дозволених програмних засобів; Порушення правил встановлених політикою безпеки.	К, Д

Продовження таблиці 2.17

№	Вид загрози	Джерело загрози	Вразливості	Наслідки
11	Втручання та/або зміна ПЗ	Конкурент	Відсутність або вразливість системи розмежування прав користувачів; Піратське ПЗ; Недосконаліcть системи розмежування доступом.	К, Ц, Д
12	Порушенні цілісності інформації	Користувач	Відсутність резервного копіювання; Використання піратських ПЗ.	Ц, Д
Природні катаклізми				
11	Повінь	-	Старе приміщення, порушення фундаменту	Ц, Д

Висновок:

1. Ненавмисні помилки користувачів, вірусне зараження, помилки захисту, що призвели до зміни інформації на зовнішніх носіях та жорсткому диску. Це може бути можливим через низьку кваліфікацію працівника, його необізнаність та відсутності знань та навичок.

2. Порушення правил безпеки, що може призвести до пожежі. Це можливо внаслідок неакуратного використання робочого місця(вживання їжі, води, кави, чаю на робочому місці), відсутності вогнегасників, відсутності ознайомлення з технікою безпеки.

3. Порушення цілісності, конфіденційності, доступності інформації співробітниками шляхом установки стороннього ПЗ. Це може бути реалізоване,

тому що не має чіткої перевірки за встановленням ПЗ та відсутністю обмеження прав на установку ПЗ.

4. Порушення конфіденційності інформації шляхом копіювання інформації на зовнішні носії. Це можливо через відсутність контролю та обліку носіїв.

5. Порушення доступності інформації шляхом крадіжки носіїв інформації. Це можливо через відсутність контролю та обліку носіїв.

2.6 Профіль захищеності

На основі проведеного раніше аналізу загроз та вразливостей, обираємо клас системи згідно з НД ТЗІ 2.5-004-99, було обрано клас «3» — розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності.

Автоматизована система, в якій підвищені вимоги до — забезпечення конфіденційності, цілісності і доступності оброблюваної інформації (підкласи «х.КЦД»);

Стандартний функціональний профіль захищеності в КС, що входить до складу АС класу 3, з підвищеними вимогами до забезпечення конфіденційності, цілісності і доступності оброблюваної інформації:3.КЦД.1 = { КД-2, КО-1, КВ-1,ЦД-1, ЦО-1, ЦВ-1,ДР-1, ДВ-1,НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }

Таблиця 2.18 Опис послуг профілю захищеності

№	Послуга	Назва послуги	Опис послуги
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. Атрибути доступу об'єктів і користувачів повинні містити інформацію, що використовується КЗЗ для розмежування доступу до об'єктів з боку конкретного користувача.

Продовження таблиці 2.18

№	Послуга	Назва послуги	Опис послуги
2	КО-1	Повторне використання об’єктів	Реалізація даної послуги забезпечує коректність повторного використання поділюваних об'єктів, гарантуючи, що в разі, якщо розділяється об'єкт виділяється новому користувачеві або процесу, в ньому не міститься інформація, яка залишилася після використання його попереднім користувачем або процесом
3	КВ-1	Конфіденційність при обміні	Реалізація даної послуги забезпечує захист від несанкціонованого ознайомлення зі змістом інформаційних об'єктів (файлів), збережених в каталогах файлової системи захищених логічних дисків, розміщених на знімних і не знімних носіях, в разі вилучення даних носіїв з під контролю коштів захисту (наприклад, в результаті розкрадання).
4	ЦД-1	Довірча цілісність	Ця послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.
5	ЦО-1	Відкат	Реалізація даної послуги забезпечує можливість скасування послідовності визначених операцій і повернення (відкату) захищеного об'єкта в попереднє стан. Політика даної послуги поширюється на технологічну інформацію комплексу і на послідовність операцій, що виконуються комплексом при установці захисту на каталог.

Продовження таблиці 2.18

№	Послуга	Назва послуги	Опис послуги
6	ЦВ-1	Цілісність при обміні	Ця послуга забезпечує мінімальний захист. На включення даного рівня в свій рейтинг може претендувати система, що дозволить на підставі цифрового підпису перевіряти цілісність функціонуючого на ЕОМ ПЗ, або система електронної пошти, що забезпечує цифровий підпис повідомлень.
7	ДР-1	Квоти	Реалізація даної послуги забезпечує запобігання захоплення користувачами надмірного обсягу ресурсів
8	ДВ-1	Ручне 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
9	НР-2	Захищений журнал	Ця послуга дозволяє контролювати небезпечні для КС дії. Вибір фізичного носія, що використовується для зберігання даних реєстрації, повинен відповідати способу використання і обсягу даних. Будь-яке переміщення таких даних має виконуватись способом, що гарантує їх безпеку. Одним із найбезпечніших, хоч і досить дорогих рішень, є використання носіїв з одноразовим записом. В будь-якому випадку рівень захищеності даних реєстрації має бути не нижче, ніж рівень захищеності даних користувачів, яку забезпечують реалізовані послуги конфіденційності і цілісності. Повинні бути вироблені угоди щодо планування і ведення архівів даних реєстрації.
10	НИ-2	Одиночна ідентифікація і автентифікація	Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, який намагається одержати доступ до КС. Хоч поняття ідентифікація і автентифікація відрізняються, на практиці обидва ці процеси важко буває поділити.

Продовження таблиці 2.18

№	Послуга	Назва послуги	Опис послуги
11	НК-1	Однонаправлений достовірний канал	Дана послуга дозволяє гарантувати, що користувач взаємодіє безпосередньо з КЗЗ і ніякий інший користувач або процес не може втручатись у взаємодію (підслухати або модифікувати інформацію, що передається). Рівні даної послуги ранжируються в залежності від того, чи має КЗЗ можливість ініціювати захищений обмін, чи це є прерогативою користувача.
12	НО-2	Розподіл обов'язків 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 рол
13	НЦ-2	КЗЗ з гарантованою цілісністю	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
14	НТ-2	Самотестування при старті	Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ. КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження

Продовження таблиці 2.18

№	Послуга	Назва послуги	Опис послуги
15	НВ-1	Автентифікація вузла	Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ранжируються на підставі повноти реалізації.

КД-2. Базова довірча конфіденційність. Реалізована. Персональні фото, документи.

КО-1. Повторне використання об’єктів. Реалізована. Політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС.

КВ-1. Базова конфіденційність при обміні. Не реалізована.

ЦД-1. Довірча цілісність. Реалізована. Політика адміністративної цілісності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС.

ЦО-1. Обмежений відкат. Реалізований. У системі наявна можливість відміни останніх дій у Microsoft Office 2019 Pro Plus.

ЦВ-1: Базова цілісність при обміні. Не реалізована. Електронна пошта.

ДР-1. Квоти. Реалізовано організаційними методами захисту.

ДВ-1. Ручне відновлення. Реалізована. Інтерфейся КС дозволяють виконати ручне відновлення (параметри відновлення задаються вручну).

НР-2. Захищений журнал. Реалізована. У системі наявна можливість вибору фізичного носія, що використовується для зберігання даних реєстрації.

НИ-2. Одиночна ідентифікація та автентифікація. Реалізована. У системі наявний менеджер паролів, що задовольняє вимоги щодо захисту паролів. Реалізовано організаційними методами захисту.

НК-1. Однонаправлений достовірний канал. Реалізована.

НО-2. Розподіл обов'язків адміністраторів. Не реалізована.

НЦ-2. КЗЗ з гарантованою цілісністю. Реалізована. Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів

НТ-2. Самотестування при старті. Не реалізована

НВ-1. Автентифікація вузла. Не реалізована.

2.7 Розробка КСЗІ.

Так як серед інформації, що обробляється на ІТС, наявна інформація з обмеженим доступом та конфіденційна інформація, що знаходиться у власності власника ІТС, був обраний принцип досягнення допустимого рівня захищеності інформації за мінімальних витрат, що є найбільш доцільним.

Спираючись на таблицю 2.14 Модель загроз, де були описані основні загрози в ІТС, було створено заходи, що представлені в КСЗІ, направлені на зниження цих загроз. В першу чергу, потрібно ввести заходи для зниження критичних загроз. До цього відносяться: зараження антивірусним ПЗ, некомпетентність персоналу, інсталювання незнайомого ПЗ, несанкціоноване копіювання.

Для забезпечення безпеки, було обрано використання програмно-апаратних та організаційних методів захисту. Антивірусне програмне забезпечення "Avast Business". Відповідає вимогам нормативних документів системи технічного захисту інформації. Призначений для захисту комп'ютерів користувачів від вірусних програм та шкідливого ПЗ. Дійсний до кінця року. Вартість ліцензії на одну робочу станцію - 1291,5 грн. Не потребує навчання персоналу бо підтримка програми здійснюється розробниками в режимі онлайн. Оновлення не рідше 1 разу в рік.

На рішення щодо вибору вплинули такі фактори:

- вартість програмного засобу;
- Наявність технічної підтримки з боку розробників програми;
- Не потребує підвищення кваліфікації/навчання персоналу.

Організаційні методи та способи їх реалізації:

Так як у директора, адміністратора та бухгалтера рівні права доступу до ІзОд, то обрання засобів технічного захисту інформації вважаю недоцільним.

Для забезпечення вимог використання тільки ліцензійного ПЗ, було такі програмні продукти:

Microsoft Office 2019 Pro Plus. Призначений для Вартість ліцензії на одну робочу станцію - 1350 грн. Дійсний до кінця року. Потребує мінімального навчання персоналу задля нормального користування. Оновлення не рідше 1 разу в рік.

Так як на ІТС готельно-ресторанного господарювання «Avenue 69» було обрано впровадження інформаційного захисту, при якому головним пріоритетом є досягнення необхідного рівня захищеності інформації за мінімальних витрат. Необхідно зосередитися на організаційних методах захисту. Для цього розробляються наступні політики безпеки інформації:

- Політика антивірусного захисту;
- Політика використання Інтернету
- Політика паролів користувачів
- Політика резервного копіювання;

Політика антивірусного захисту

Мета політики: Створення вимог, яких повинні дотримуватися усі комп'ютери, які входять до ІТС готельно-ресторанного господарювання «Avenue 69».

Правила політики безпеки мають виконувати усі працівники закладу.

Зміст політики. Загальна частина – встановлює наступні загальні правила, які слід виконувати для вирішення проблеми вірусу:

- завжди підтримуйте корпоративні вимоги, підтримка антивірусного ПЗ є необхідною для корпоративного вузла. Завантажте і підтримуйте поточну версію; завантажте і встановіть модифікації антивірусного програмного забезпечення, як тільки вони стають доступними;

- ніколи не відкривайте будь-які файли або макрокоманду, що торкається електронної пошти від невідомого, підозрілого або ненадійного джерела. Видаліть ці повідомлення негайно, потім видаліть їх за допомогою спорожнення вашого сміття;
- видаліть Spam, ланцюг і іншу електронну пошту, які не мають атрибутів Вашої компанії відповідно до політики безпеки;
- ніколи не завантажуйте файли від невідомих або підозрілих джерел;
- уникайте прямого дискового доступу (читання/запис), за винятком того, що відповідає необхідним діловим вимогам;
- перед використанням завжди скануйте дискету від невідомого джерела на предмет вірусів;
- регулярно дублюйте критичні дані і системні конфігурації зберігайте їх в безпечному місці;
- якщо лабораторна перевірка встановлює конфлікт з антивірусним ПЗ, запустить антивірусну утиліту, що гарантує незабрудненість машини, блокуйте ПЗ, потім двинути лабораторну перевірку. Тільки після лабораторної перевірки дозволяйте використовувати антивірусне ПЗ. Під час блокування антивірусного ПЗ блоковано, ні в якому разі не завантажуйте будь-які додатки, які могли б перенести вірус.
- нові віруси відкриваються майже щодня. Періодично перевіряйте Антивірусну політику відділу і ці рекомендації для внесення змін.

Політика використання Інтернету

Підключення до Інтернету створює для компанії нові ризики, які необхідно усунути для захисту життєво важливих інформаційних активів підприємства. До цих ризиків відносяться: Доступ персоналу до Інтернету, який не відповідає потребам бізнесу, призводить до нецільового використання ресурсів. Така діяльність може негативно позначитися на продуктивності праці через часу, витраченого на використання або "серфінг" в Інтернеті. Крім того, компанія може зіткнутися з втратою репутації і можливими судовими позовами в результаті інших видів не цільового використання.

Вся інформація, знайдена в Інтернеті, повинна розглядатися як підозріла до тих пір, поки не буде підтверджена іншим надійним джерелом. В Інтернеті не існує процесу контролю якості, і значна частина інформації застаріла або неточна. Доступ до Інтернету буде надаватися користувачам для підтримки ділової діяльності і тільки в міру необхідності для виконання їхніх робочих і професійних обов'язків.

Метою даної політики є визначення належного використання Інтернету співробітниками і філіями “Avenue 69”.

4.1 Використання ресурсів

Доступ до Інтернету буде схвалений і надано тільки при наявності розумних ділових потреб. Послуги Інтернету будуть надаватися на підставі поточних посадових обов'язків співробітника.

Вимоги користувачів до доступу в Інтернет будуть періодично переглядатися відділами компанії, щоб переконатися в існуванні постійних потреб.

4.2 Дозволене використання

Доступ в Інтернет надається виключно для підтримки ділової активності, необхідної для виконання посадових обов'язків. Всі користувачі повинні слідувати корпоративним принципам використання ресурсів і проявляти розсудливість при використанні Інтернету. З питаннями можна звертатися до відділу інформаційних технологій.

Прийнятне використання Інтернету для виконання робочих функцій може включати в себе:

- Спілкування між співробітниками і не співробітниками в робочих цілях;

- перегляд веб-сайтів можливих постачальників для отримання інформації про продукцію;

- довідкова нормативна або технічна інформація.

4.3 Використання в особистих цілях

Використання комп'ютерних ресурсів компанії для доступу в Інтернет в особистих цілях без дозволу системного адміністратора може розглядатися як привід для дисциплінарного стягнення аж до звільнення.

Всі користувачі Інтернету повинні знати, що в мережі компанії створюється журнал аудиту, що відображає запити на обслуговування, як входять, так і вихідні адреси, і він періодично перевіряється.

Користувачі, які вирішили зберігати або передавати особисту інформацію, таку як закриті ключі, номери кредитних карт, сертифікати або використовувати "гаманці" в Інтернеті, роблять це на свій страх і ризик. Компанія не несе відповідальності за будь-яку втрату інформації, наприклад, інформації, що зберігається в гаманці, або будь-яку подальшу втрату особистого майна.

4.4 Заборонене використання

Інформація, що зберігається в гаманці, або будь-яка подальша втрата особистого майна.

Придбання, зберігання і поширення даних, які є незаконними, порнографічними або негативно відображають расу, стать або віросповідання, конкретно заборонено.

Компанія також забороняє ведення комерційної діяльності, політичної діяльності, участь в будь-якій формі збору розвідувальної інформації з наших об'єктів, участь в шахрайської діяльності, а також свідоме поширення неправдивих або наклепницьких матеріалів.

Інші види діяльності, які строго заборонені, включають, але не обмежуються ними:

- Доступ до інформації компанії, яка не входить в сферу діяльності співробітника. Це включає несанкціоноване читання інформації про рахунки клієнтів, несанкціонований доступ до інформації про особисті справи персоналу, а також доступ до інформації, яка не потрібна для належного виконання посадових обов'язків.

- Неправильне використання, розкриття без належного дозволу чи зміна інформації про клієнтів або персоналі. Це включає внесення несанкціонованих змін до особової справи або обмін електронними даними про клієнтів або персоналі з уповноваженою персоналом.

- Навмисне вказівку або гіперпосилання веб-сайтів компанії на інші сайти в Інтернеті / В Інтернеті, зміст яких може суперечити або порушувати мети або політику компанії.

- Будь-яка поведінка, що може являти собою або заохочувати кримінальний злочин, привести до громадянської відповідальності або іншим чином порушити будь-які нормативні акти, місцеві, державні, національні або міжнародні закони.

- Використання, передача, дублювання або добровільне отримання матеріалів, що порушують авторські права, торгові марки, комерційні таємниці або патентні права будь-якої особи або організації. Припускайте, що всі матеріали в Інтернеті захищені авторським правом і / або запатентовані, якщо в спеціальних повідомленнях не вказано інше.

- Передача будь-якої службової, конфіденційної або іншої важливої інформації без належного контролю.

- Створення, розміщення, передача або добровільне отримання будь-яких незаконних, образливих, наклепницьких, загрозливих, що домагаються матеріалів, включаючи, крім іншого, коментарі на основі раси, національного походження, статі, сексуальної орієнтації, віку, інвалідності, релігії або політичних переконань.

- Будь-яка форма азартних ігор.

Якщо немає спеціального дозволу відповідно до положень розділу 4.3, наступні види діяльності також строго заборонені:

- Несанкціоноване скачування будь-яких shareware-програм або файлів для використання без попереднього дозволу IT-департаменту і менеджера користувача.

- Будь-яке замовлення (купівля) товарів або послуг в Інтернеті.

- Грати в будь-які ігри.

- Пересилання листів щастя.

- Участь в будь-яких он-лайн конкурсах або акціях.

- Ухвалення рекламних подарунків.

Пропускна здатність як всередині компанії, так і при підключенні до Інтернету є загальним, обмеженим ресурсом. Користувачі повинні докладати розумні зусилля для використання цього ресурсу таким чином, щоб не чинити негативного впливу на інших співробітників. Окремі відділи можуть встановлювати рекомендації по використанню пропускної здатності і розподілу ресурсів, а також забороняти завантаження певних типів файлів.

4.5 Ліцензія на програмне забезпечення

Компанія виступає за суворе дотримання ліцензійних угод з постачальниками програмного забезпечення. На робочому місці або при використанні обчислювальних або мережевих ресурсів компанії копіювання програмного забезпечення, яке не відповідає ліцензії виробника, суворо заборонено. Питання, що стосуються законного і незаконного копіювання, слід направляти до відділу інформаційних технологій для розгляду або запитувати рішення юридичного відділу до початку копіювання.

Аналогічним чином, відтворення матеріалів, доступних через Інтернет, має здійснюватися тільки з письмового дозволу автора або власника документа. Якщо попередньо не отримано дозволу від власника (власників) авторських прав, робити копії матеріалів з журналів, щоденників, інформаційних бюлетенів, інших публікацій та документів в Інтернеті заборонено, якщо це не є розумним і звичайним. Поняття "добросовісного використання" відповідає міжнародним законам про авторське право.

Використання комп'ютерних ресурсів компанії для виходу в Інтернет в особистих цілях без узгодження з менеджером користувача і відділом інформаційних технологій може розглядатися як привід для дисциплінарного стягнення аж до звільнення.

Всі користувачі Інтернету повинні знати, що в мережі компанії створюється журнал аудиту, що відображає запити на обслуговування, як входять, так і вихідні адреси, і він періодично перевіряється.

Користувачі, які вирішили зберігати або передавати особисту інформацію, таку як закриті ключі, номери кредитних карт, сертифікати або використовувати "гаманці" в Інтернеті, роблять це на свій страх і ризик.

4.6 Огляд публічної інформації

Всі загальнодоступні каталоги на комп'ютерах, підключених до Інтернету, будуть переглядатися і очищатися щовечора. Цей процес необхідний для запобігання анонімного обміну інформацією, несумісною з діяльністю компанії. Прикладами несанкціонованої публічної інформації є піратська інформація, паролі, номери кредитних карт і порнографія.

4.7 Очікування конфіденційності

4.7.1 Моніторинг

Користувачі повинні розглядати свою діяльність в Інтернеті як періодично відстежуємо і відповідним чином обмежувати свою діяльність.

Керівництво залишає за собою право в будь-який час і без попередження перевіряти електронну пошту, особисті каталоги файлів, доступ в Інтернет і іншу інформацію, що зберігається на комп'ютерах компанії. Така перевірка забезпечує дотримання внутрішньої політики та допомагає в управлінні інформаційними системами компанії.

4.7.2 Конфіденційність електронної пошти

Користувачі повинні знати, що електронна пошта з відкритим текстом не є конфіденційним засобом зв'язку. Компанія не може гарантувати, що електронні повідомлення будуть конфіденційними. Співробітники повинні знати, що електронні повідомлення, в залежності від технології, можуть бути переслані, перехоплені, роздруковані і збережені іншими особами. Користувачі також повинні знати, що після передачі електронного повідомлення воно може бути змінено. Видалення електронної пошти з окремої робочої станції не призведе до її видалення з різних систем, через які вона була передана.

4.8 Підтримка корпоративного іміджу

4.8.1 Представництво

При використанні ресурсів компанії для доступу і роботи в Інтернеті користувачі повинні розуміти, що вони представляють компанію. Кожен раз, коли співробітники заявляють про свою приналежність до компанії, вони також повинні чітко вказати, що "висловлені думки є моїми власними і не обов'язково збігаються з думкою компанії". З питаннями можна звертатися до відділу інформаційних технологій.

4.8.2 Матеріали компанії

Користувачі не повинні розміщувати матеріали компанії (приклади: внутрішні службові записки, прес-релізи, інформація про продукцію або використанні, документація і т.д.) в списках розсилки, публічних групах новин або подібних службах. Будь-яке розміщення матеріалів має бути схвалено менеджером співробітника і відділом по зв'язках з громадськістю і має бути розміщено уповноваженою особою.

4.8.3 Створення веб-сайтів

Всі особи та / або структурні підрозділи, які бажають створити домашню сторінку або сайт в WWW, повинні спочатку розробити плани по організації, впровадження та обслуговування. Це дозволить підтримувати стандарти публікації і змісту, необхідні для забезпечення послідовності і доречності.

Крім того, зміст матеріалів, що надаються громадськості через Інтернет, має бути офіційно розглянуто і схвалено перед публікацією. Всі матеріали повинні бути представлені директорам з корпоративних комунікацій для початкового схвалення, щоб продовжити публікацію. Всі сторінки компанії належать і є кінцевою відповідальністю директорів з корпоративних комунікацій.

Всі веб-сайти компанії повинні бути захищені від небажаного вторгнення за допомогою офіційних заходів безпеки, які можна отримати у відділі інформаційних технологій.

4.9 Періодичні перевірки

4.9.1 Огляди відповідності використання

Для забезпечення відповідності цій політиці будуть проводитися періодичні перевірки. Ці перевірки будуть включати в себе тестування ступеня відповідності політиці використання.

4.9.2 Перевірки дотримання політики

Періодичні перевірки будуть проводитися для забезпечення доречності та ефективності політики використання. Ці перевірки можуть привести до зміни, додаванню або видалення політик використання для кращої відповідності інформаційним потребам компанії.

Політика паролів користувачів

Паролі є важливим аспектом комп'ютерної безпеки. Неправильно підібраний пароль може призвести до несанкціонованого доступу і / або експлуатації наших ресурсів. Всі співробітники, включаючи підрядників і постачальників, що мають доступ до систем готельно-ресторанного бізнесу “Avenue 69”, несуть відповідальність за прийняття відповідних заходів, описаних нижче, для вибору і захисту своїх паролів.

Мета цієї політики - встановити стандарт для створення надійних паролів і захисту цих паролів.

Зміст політики безпеки:

1. Створення паролів
   - Всі паролі на рівні користувача і на рівні системи повинні відповідати Керівництву по створенню паролів.
   - Користувачі повинні використовувати окремий, унікальний пароль для кожної зі своїх облікових записів, пов'язаних з роботою. Користувачі не повинні використовувати паролі, пов'язані з роботою, для своїх власних, особистих облікових записів.
   - Облікові записи користувачів, які мають привілеї системного рівня, що надаються через членство в групах або програми, такі як sudo, повинні мати унікальний пароль від всіх інших облікових записів, що належать цьому користувачу, для доступу до привілеїв системного рівня. Крім того, настійно рекомендується використовувати будь-яку форму багатофакторної аутентифікації для будь-яких привілейованих облікових записів.
2. Зміна пароля

- Паролі слід міняти тільки в тому випадку, якщо є підстави вважати, що пароль був скомпрометований.
- Злом або вгадування пароля може проводитися періодично або випадково командою Infosec або її представниками. Якщо пароль буде вгаданий або зламаний під час однієї з таких перевірок, користувач повинен буде змінити його відповідно до Керівництва по створенню паролів.

3. Захист паролів
   - Паролі не повинні передаватися нікому, включаючи керівників і колег. Всі паролі повинні розглядатися як конфіденційна, конфіденційна інформація дитячо-юнацької спортивної школи. Корпоративна інформаційна безпека визнає, що застарілі програми не підтримують існуючі проксі-системи. Будь ласка, зверніться до технічної довідці для отримання додаткової інформації.
   - Паролі можна вставляти в повідомлення електронної пошти, ящики Alliance або інші форми електронного спілкування, а також повідомляти їх кому-небудь по телефону.
   - Паролі можуть зберігатися тільки в авторизованих організацією "менеджерах паролів".
   - Не використовуйте функцію "Запам'ятати пароль" в додатках (наприклад, в веб-браузерах).
   - Будь-який користувач, що підозрює, що його / її пароль міг бути зламаний, повинен повідомити про це і змінити всі паролі.

4. Розробка додатків

Розробники додатків повинні переконатися, що їх програми містять такі запобіжні заходи:

- Додатки повинні підтримувати аутентифікацію окремих користувачів, а не груп.
- Додатки не повинні зберігати паролі відкритим текстом або в будь-який легко оборотної формі.

- Додатки не повинні передавати паролі відкритим текстом по мережі.
- У додатках має бути передбачено управління ролями, щоб один користувач міг взяти на себе функції іншої без необхідності знати його пароль.

5. Багатофакторна аутентифікація

Багатофакторна аутентифікація дуже рекомендується і повинна використовуватися завжди, коли це можливо, не тільки для робітників, але і для особистих акаунтів.

Політика резервного копіювання

Оскільки катастрофи трапляються так рідко, керівництво часто ігнорує процес планування аварійного відновлення. Дана політика вимагає від керівництва фінансової підтримки і ретельного виконання заходів з планування на випадок стихійних лих. Лиха не обмежуються несприятливими погодними умовами. Будь-яка подія, яка може призвести до тривалої затримки обслуговування, має бути розглянуто. План аварійного відновлення часто є частиною плану забезпечення безперервності бізнесу.

Дана політика визначає вимоги до базового плану аварійного відновлення, який повинен бути розроблений і впроваджений в дитячо-юнацьку спортивну школу і описує процес відновлення IT-систем, додатків і даних після будь-якого типу лиха, що викликає серйозний збій в роботі.

Зміст політики безпеки:

- План реагування на комп'ютерні надзвичайні ситуації: З ким, коли і як слід зв'язатися? Які негайні дії повинні бути зроблені в разі певних подій?
- План наступності: Опишіть порядок передачі відповідальності, коли звичайний персонал не може виконувати свої обов'язки.
- Дослідження даних: Детально опишіть дані, що зберігаються в системах, їх критичність і конфіденційність.

- Список критичних послуг: Перерахуйте всі надані послуги та порядок їх важливості.
- Тут також пояснюється порядок відновлення в короткостроковому і довгостроковому періодах.
- План резервного копіювання та відновлення даних: Детально опишіть, які дані резервуються, на який носій вони зберігаються, де зберігаються і як часто можна створювати резервні копії. У ньому також має бути описано, як ці дані можуть бути відновлені.
- План заміни обладнання: Опишіть, яке обладнання необхідно для початку надання послуг, вкажіть, в якому порядку воно необхідне, і вкажіть, де його можна придбати.
- Управління засобами масової інформації: Хто відповідає за надання інформації засобам масової інформації?
- Також надайте деякі рекомендації щодо того, які дані слід надавати.

Після створення планів важливо, наскільки це можливо, відпрацювати їх на практиці. Керівництво повинно виділити час для перевірки виконання плану аварійного відновлення. Щорічно слід проводити тренування з використанням настільних систем. В ході цих випробувань можна виявити і усунути проблеми, які можуть призвести до збою плану, в умовах, що не мають значних наслідків.

Висновки другого розділу.

У другій частині кваліфікаційної роботи було наведено загальні відомості про підприємство та необхідність розробки та впровадження комплексної системи захисту інформації, організаційна структура і проведений аналіз оброблюваної інформаціиї. На основі цього проведений акт обстеження підприємства. Результатом обстеження ОІД став аналіз загроз та було обрано профіль захищеності. На основі обраного профілю захищеності були розроблено комплексну систему захисту інформації в ІТС.

За рахунок впровадження програмних та організаційних методів захисту інформації було зменшено рівень актуальних загроз в ІТС.

ЕКОНОМІЧНА ЧАСТИНА

3.1 Економічне обґрунтування доцільності впровадження політики безпеки інформації

Метою розрахунків впровадження політики безпеки інформації є економічне обґрунтування доцільності впровадження політики безпеки інформації. Для цього визначена економічна ефективність використання основних впроваджень та розрахунків, що були отримані у ході виконання роботи.

Економічна доцільність визначається завдяки:

- Капітальних витрат
- Експлуатаційних витрат
- Річного економічного ефекту від впровадження інформаційної безпеки

Визначення витрат на розробку ПБІ:

3.1.1 Визначення трудомісткості розробки політики безпеки інформації

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):

$$t = t_{тз} + t_{в} + t_{а} + t_{вз} + t_{озб} + t_{овр} + t_{д}$$, годин,

де

$t_{тз}$ - тривалість складання ТЗ на розробку ПБІ = 96 години;

$t_{в}$ - тривалість розробки концепції безпеки інформації у організації = 24 години;

$t_{а}$ - тривалість процесу аналізу ризиків = 72 години;

$t_{вз}$ - тривалість визначення вимог заходів, методів та засобів захисту = 32 години

$t_{озб}$ - тривалість виробу основних рішень з забезпечення БІ = 104 години;

$t_{овр}$ - тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організацій = 184 години;

$t_{д}$ - тривалість документального оформлення ПБ = 40 години;

t = 96+24+72+32+104+184+40= 552 години

3.1.2 Розрахунок витрат на створення КСЗІ

Витрати на розробку політики безпеки інформації Крп складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки Ззп і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації Змч.

$К_{рп} = З_{зп} + З_{мч}$.

$К_{рп} = З_{зп} + З_{мч}$ = 85 008 + 2092,08= 87 100,08 грн.

$З_{мч} = t * З_{пр}$ = 552*154 = 85 008 грн.

де t – загальна тривалість розробки політики безпеки, годин;

Зіб – середньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

$З_{мч} = t* С_{мч}$ =552*3,79= 2092,08 грн.

де $t_д$ – трудомісткість підготовки документації на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$С_{мч}$ = 0,6* 4 * 0,9 + ((7290*0,4)/1920) + ((2300*0,1)/1920) = 2,16+1,5187+0,1197=3,79 грн

Вартість ПК = 24300 грн, термін корисної служби = 42 місяці.

Мінімальний термін корисної служби = 24 місяці.

Накопичена амортизація = (24300 *42)/5*12 = 17010 грн

Залишкова вартість = 24300 – 17010 = 7290

Таким чином, капітальні (фіксовані) витрати на створення політики безпеки інформації:

$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н}$ = 20 114 + 20 000 + 0 + 0 + 4200 + 6000 = 50 314 грн.

де $К_{рп}$ – вартість розробки політики інформаційної безпеки та залучення для цього зовнішніх консультантів, 20 114 грн;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), 20 тис. грн:

Таблиця 2.19 Перелік програмних засобів

Програмний засіб	Вартість, грн.
POS “Poster”	2700
Microsoft Office 2019 Pro Plus	1725
Ajax Translator	950,17
Avast Business	1291,5
Кількість ПК	3
Всього	(2700+1725+950,17+1291,5)*3=20000

$К_{ПЗ}$ – вартість створення основного й додаткового програмного забезпечення, 0 грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, 0 грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, 4200 грн

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, 6000 грн.

Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$С = С_{в} + С_{к} + С_{ак}$, грн.

де $С_{в}$ - вартість відновлення й модернізації системи Св = 0;

$С_{к}$ - витрати на керування системою в цілому;

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки = Сак = 0 грн.

Витрати на керування системою інформаційної безпеки ($С_{к}$) складають:

$С_{к} = С_{н} + С_{а} + С_{з} + С_{ел} + С_{о} + С_{тос}$, грн

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються = $С_{н}$ = 10000 грн.

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_{з}$), складає:

$С_{з} = З_{осн} + З_{дод}$, грн.

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 16800 грн. Додаткова заробітна плата – 10% від основної заробітної плати. Виконання роботи щодо налаштувань інфраструктури безпечних підключень мобільних користувачів до інтрамережі підприємства потребує залучення спеціаліста інформаційної безпеки на 0,25 ставки. Отже,

$С_з$ = (16800*12 + 16800*12*0,1)*0,25= 55440 грн.

З 01.01.2019 р. Ставка ЄСВ для всіх категорій платників складає 22%.

$С_{єв}$ = 55440 *0,22 = 12 196,8 грн.

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$С_{ел} = Р \cdot F_р \cdot Ц_е$, грн.,

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=0,6 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки (Fр = 1920 год.);

$Ц_е$ – тариф на електроенергію, (Це = 1,68 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$С_{ел}$ = 0,6*1920*1,68 = 1935,36 грн.

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат - 1%

$С_{тос}$ = 50 314 *0,01=503,14 грн

Річний фонд амортизаційних відрахувань:

$С_а$ = 20 000 / 2

$С_а$ = 10 000 грн

Витрати на керування системою інформаційної безпеки визначаються:

$С_к$ = 10000+55 440+12196,8+1935,36+503,14 + 10 000 = 90 075,3 грн.

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають 90 075,3 грн.

3.2. Оцінка можливого збитку від атаки на вузол або сегмент мережі

3.2.1 Оцінка величини збитку:

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки для умовного підприємства.

Необхідні вихідні дані для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 3 години;

$t_{ви}$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 2 години;

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

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 7500 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 11000 грн./міс.;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 1 особи;

$П_{зч}$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 12 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 6150 грн. у рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин, грн;

I – число атакованих сегментів корпоративної мережі, 1;

N – середнє число атак на рік, 15.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$U = П_п + П_в + V$,

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

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

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

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

$П_п = ((11000 * 12)/176) * 3 = 2250$ грн,

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

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

$$П_{в} = П_{ви} + П_{пв} + П_{зч}$$

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

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації Пви розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі Зс, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу tви:

$П_{ви}$ = ((9500 *12)/176)*2 = 1295,45 грн.

Витрати на відновлення сегмента корпоративної мережі Ппв визначаються часом відновлення після атаки tв і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$П_{вп}$ = ((11750 *1)/176)*3 = 200,28 грн.

Витрати на заміни встаткування або запасних частин можуть скласти 2320,50 грн.

Тоді витрати на відновлення працездатності вузла або сегмента корпоративної мережі складуть:

$П_{в}$ = 1295,45 + 200,28 + 2320,50 = 3816,23 грн.

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

$$V = \frac{O}{F_Г} \cdot (t_{П} + t_{В} + t_{ВИ})$$

V = (2300000/2080)* (2+3+2) = 7740,38 грн.

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

U = 2250 + 3816,23 + 7740,38 = 13 806,61 грн.

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

B = 1 * 15 * 13 806,61 = 207 099,15 грн.

3.2.2 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B \cdot R - C$$ грн.,

де B – загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці = 57%;

C – щорічні витрати на експлуатацію системи інформаційної безпеки.

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

E = 207 099,15*0,57 – 90 075,3 = 27 972,22 грн.

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

$$ROSI = \frac{E}{K},$$ частки одиниці,

де – загальний ефект від впровадження системи інформаційної безпеки грн.

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

Коефіцієнт повернення інвестицій ROSI:

ROSI = 27 972,22 / 50 314 = 0,56 частки одиниці,

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$ROSI > (N_{деп} – N_{інф})/100),$$

де $N_{деп}$ – річна депозитна ставка, (23%);

$N_{інф}$ – річний рівень інфляції, (14%).

Розрахункове значення коефіцієнта повернення інвестицій:

0,56 > (23 – 14)/100 = 0,56 > 0,09.

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

$$T = 1/0{,}56 = 1{,}8\ ,\ \text{років.}$$

3.4 Висновок:

Розробка та впровадження політики інформаційної безпеки для є економічно доцільним, оскільки коефіцієнт повернення інвестицій ROSI складає 0,56 грн./грн., що означає отримання 0,56 грн. економічного ефекту на кожну гривню капітальних вкладень на розробку політики інформаційної безпеки підприємства. Отримане значення коефіцієнту повернення інвестицій значно вище дохідності альтернативного вкладення коштів. Термін окупності при цьому складатиме 1,8 років (біля 19,6 місяців). Капітальні витрати складають 50 314 грн.

ВИСНОВКИ

У першому розділі кваліфікаційної роботи було проаналізовано загальний стан інформаційної захищеності. В розділі також було наведено та перелічено основні нормативно-правові документи в сфері захисту інформації, було зазначено основні положення захисту інформації. Серед нормативно-правових документів були розглянуті документі що є правовою основою забезпечення безпеки інформації України: НД ТЗІ та їх галузі використання, Закони України, головні положення.

Обґрунтовано потребу у створенні політики безпеки на підприємстві для запобігання НСД до важливих інформаційних ресурсів розглянутої інформаційно-телекомунікаційної системи, обґрунтування необхідності створення, обстеження на ОІД, аналіз та оцінка інформаційних загроз та розробка політики безпеки, що враховує загрози найвищого рівня.

У другій частині кваліфікаційної роботи було наведено загальні відомості про підприємство та необхідність розробки та впровадження комплексної системи захисту інформації, організаційна структура і проведений аналіз оброблюваної інформації. На основі цього проведено акт обстеження підприємства. Результатом обстеження ОІД став аналіз загроз та вразливостей підприємства. На основі рівня загроз ОІД був обраний профіль захищеності.

Розробка та впровадження комплексної системи захисту інформації для “Avenue 69” є економічно доцільним, оскільки коефіцієнт повернення інвестицій ROSI складає 0,55 грн./грн., що означає отримання 0,55 грн. економічного ефекту на кожну гривню капітальних вкладень на розробку політики інформаційної безпеки підприємства. Отримане значення коефіцієнту повернення інвестицій значно вище дохідності альтернативного вкладення коштів. Термін окупності при цьому складатиме 1,8 років (біля 19,6 місяців). Капітальні витрати складають 50 341 грн.

ПЕРЕЛІК ПОСИЛАНЬ

1. Дослідження Ponemon Institute і IBM Security: https://www.google.com.ua/amp/s/iz.ru/export/google/amp/828235
2. Національний індекс кібербезпеки: https://ncsi.ega.ee/ncsi-index/
3. Закон України «Про інформацію» від 02.10.1992 No2657-XII // Відомості Верховної Ради України. - 1992. - No 48. [Електронний ресурс]. - Режим доступу https://zakon.rada.gov.ua/laws/show/2657-12 Класифікація "інформації в законодавстві України".
4. ДСТУ ISO/IEC27002:2015 [Електроннийресурс] // ДСТУ. -2015. - Режимдоступудоресурсу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66911.
5. Етапи створення КСЗІ [Електронний ресурс] - Режим доступу до ресурсу:http://www.vaas.gov.ua/news/zaxist-informacijnix-sistem-vazhlive-zavdannya-sogodennya/.
6. Закон України "Про захист інформації в інформаційно- телекомунікаційних системах" від 05.07.1994 No80-VI // Відомості Верховної Ради України. - 1994. - No 80. [Електронний ресурс]. - Режим доступу http://zakon4.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
7. Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека/Упорядн. Д. П. Пілова. – Дніпро: Національний технічний університет «Дніпровська політехніка», 2019.
8. Методичні рекомендації до виконання кваліфікаційних робіт бакалаврів спеціальності 125 Кібербезпека/ Упоряд.: О.В. Герас іна, Д.С. Тимофєєв, О.В. Кручінін , Ю.А. Мілінчук – Дніпро: НТУ «ДП», 2020. –47 с
9. НД ТЗІ 2.5-004 - Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. - [Чинний від 28.04.1999] - К. : ДСТСЗІ СБУ, 1999. - No22 - (Нормативний документ системи технічного захисту інформації).
10. НД ТЗІ 2.5-005 - Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від

несанкціонованого доступу. - [Чинний від 28.04.2000] - К. : ДСТСЗІ СБУ, 2000. - No22- (Нормативний документ системи технічного захисту інформації).

11. ДСТУ ISO/IEC 27002:2015 [Електронний ресурс] // ДСТУ. - 2015. - Режим доступу до ресурсу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66911.
12. ДСТУ ISO/IEC 27005:2017 [Електронний ресурс] // ДСТУ. - 2017. - Режим доступу до ресурсу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66912.
13. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.2–004–99. – Київ: ДСТСЗІ СБ України, 1999. – 55 с.
14. НД ТЗІ 1.6-005 - Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці. - [Чинний від 15.04.2013] - К. : ДССЗЗІ, 2013. - No125 - (Нормативний документ системи технічного захисту інформації)

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	1 Розділ	7	
6	А4	2 Розділ	42	
7	А4	3 Розділ	7	
8	А4	Висновки	1	
9	А4	Список літератури	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	
14	А4	Додаток Ґ	2	
15	А4	Додаток Д	5	
16	А4	Додаток Е	1	
17	А4	Додаток Є	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Михайленко_диплом.doc

2. Михайленко_диплом pdf

3 Михайленко_презентація.pptx

Додаток В

Гриф обмеження доступу
Прим. № ___
ЗАТВЕРДЖУЮ
Керівник установи-власника
(розпорядника,
користувача) об’єкта
_директор Бєлова Д.С.
(посада, підпис, ініціали, прізвище)
12. 05. 2021
М.П.

АКТ
категоріювання __готельно-ресторанного бізнесу “Avenue 69”__
(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 ___________ Листопад А.В.___________
(підпис) (ініціали, прізвище)
Члени комісії: ___________ Ужва Ю.А.______________
(підпис) (ініціали, прізвище)
____.____. 20___

Додаток Г

Н А К А З

м. Дніпро

09.05.21
№ 101

Про створення комплексної системи захисту інформації в автоматизованій системі класу «4» ІТС готельно-ресторанного бізнесу "Avenue 69"

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 «4» для обробки інформації з обмеженим доступом.

2. Відповідальному за службу захисту інформації в автоматизованих системах Сонічєва А.С., забезпечити супроводження робіт зі створення комплексної системи захисту інформації.

3. Контроль за виконанням наказу покласти на працівника – Ужва Ю.А.

Директор

Бєлова Д.С.

____
(ініціали, підпис)

Додаток Ґ. Ситуаційний план

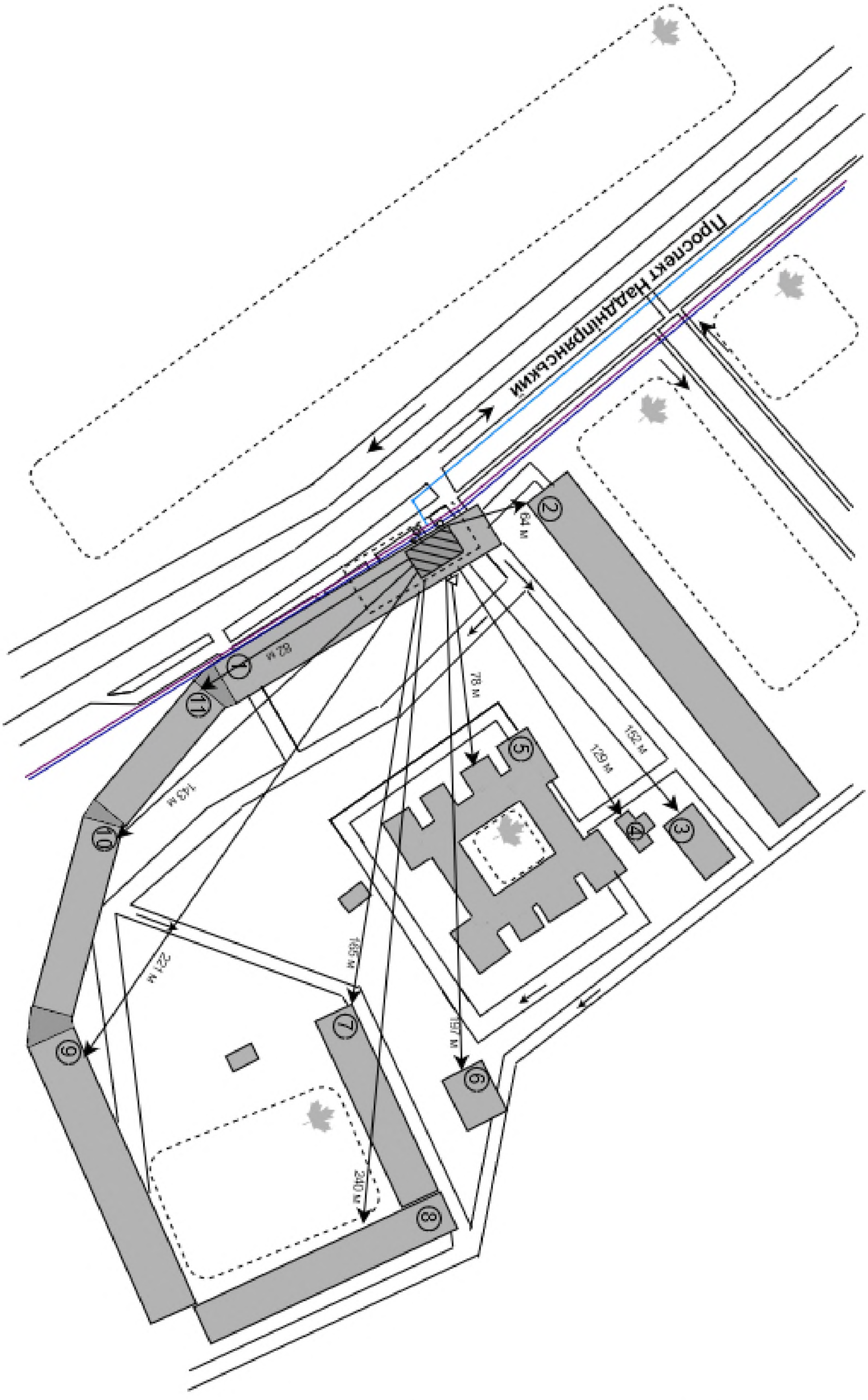


Рисунок 1 Ситуаційний план

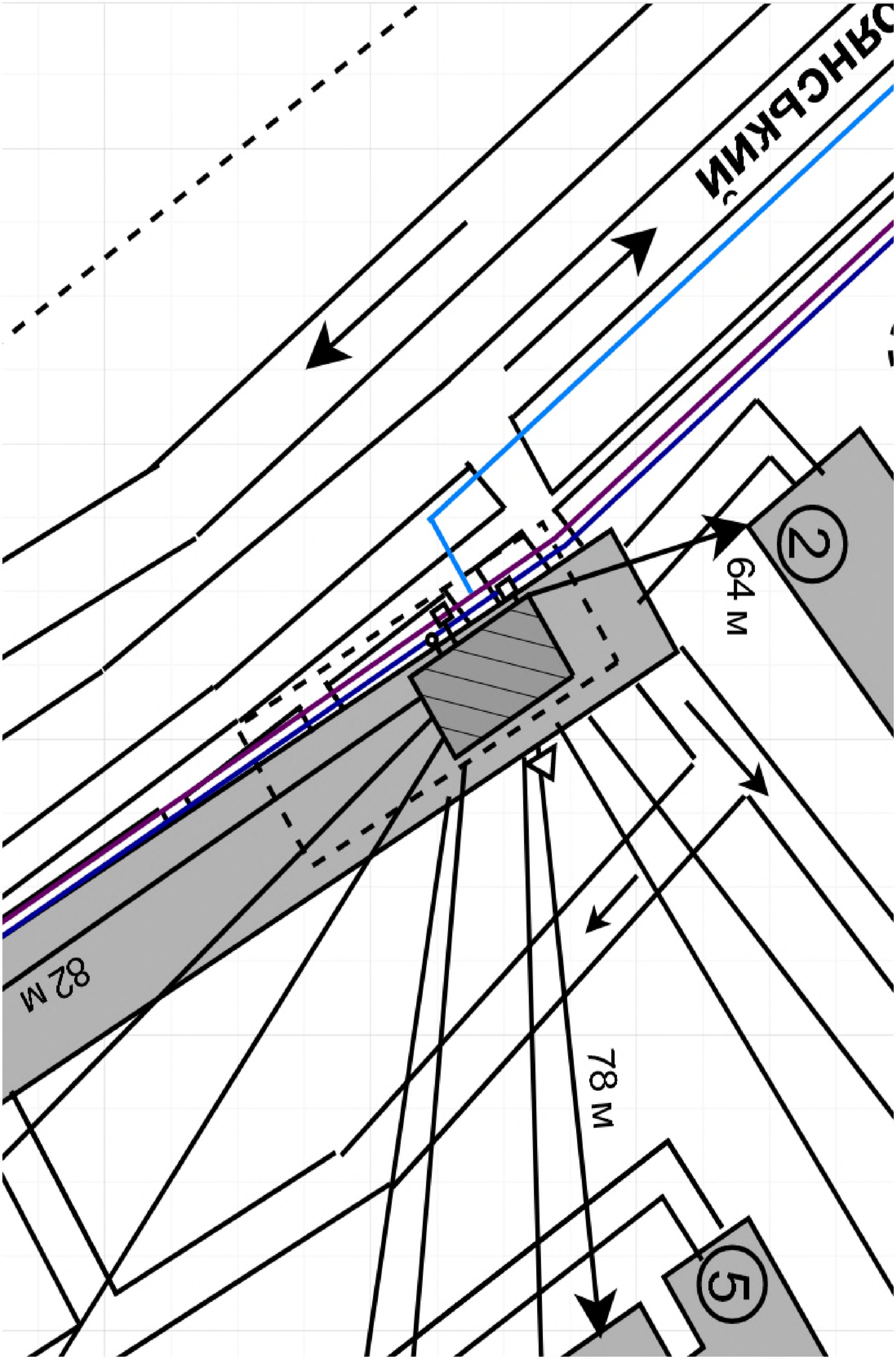
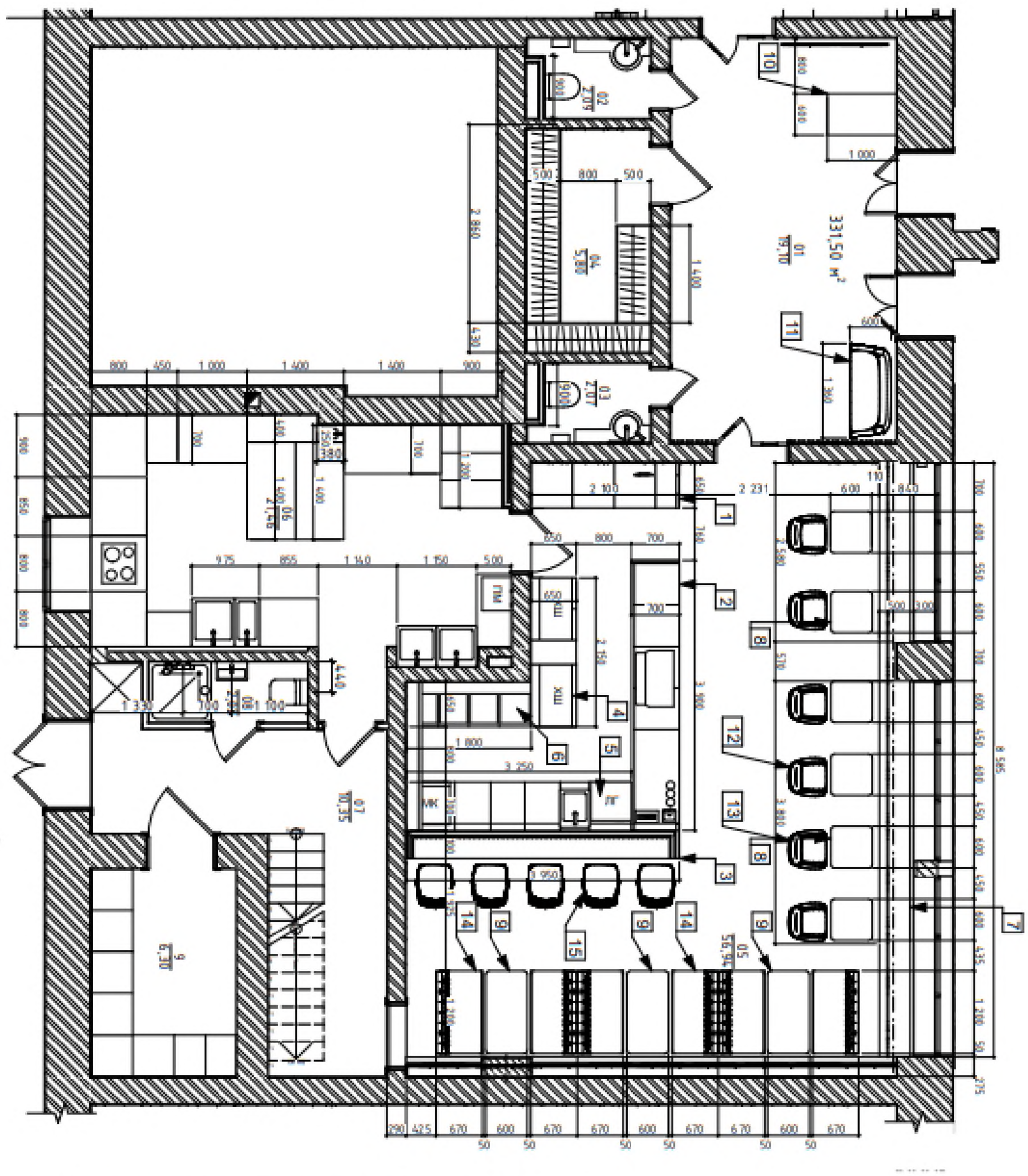


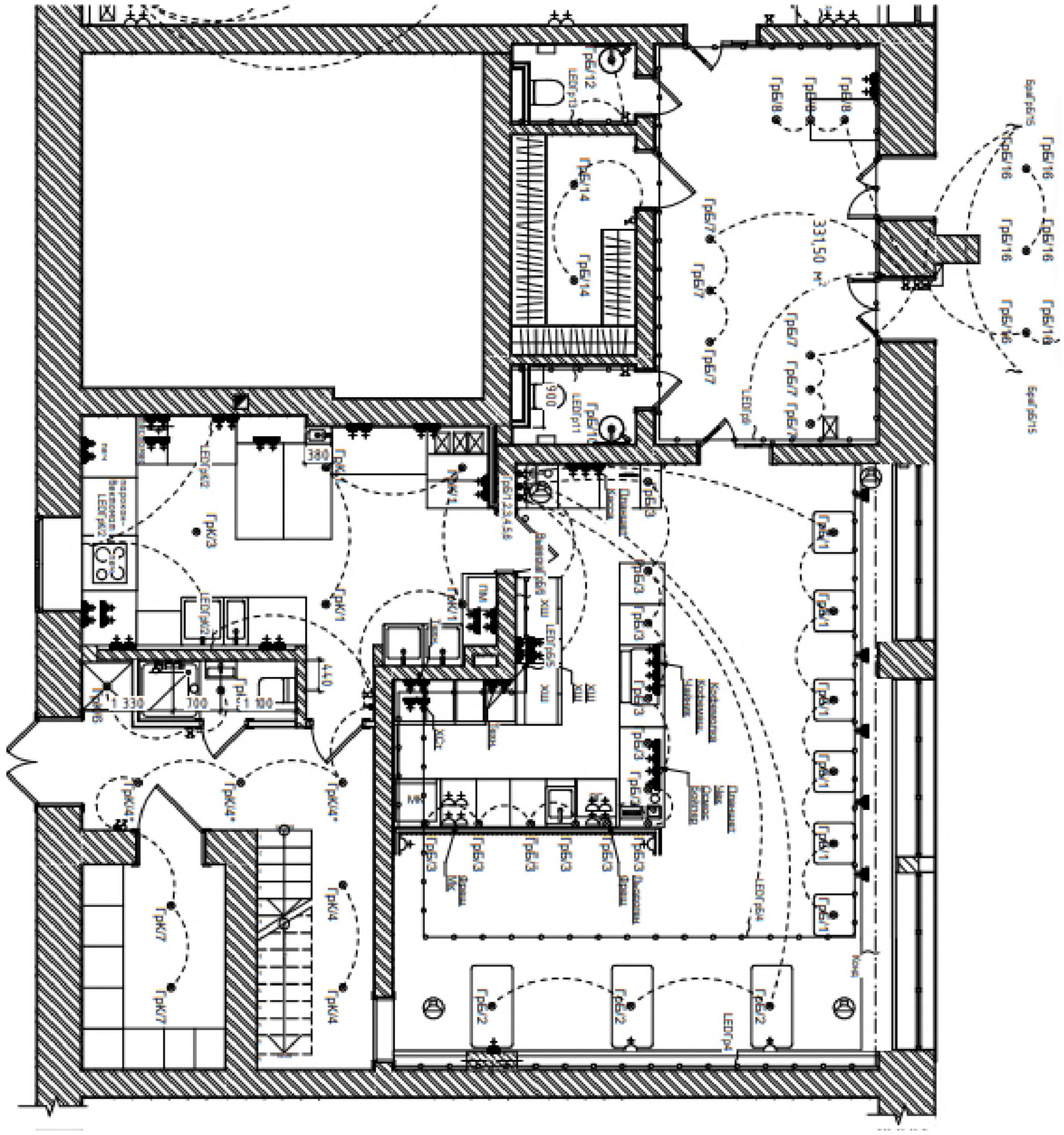
Рисунок 1.1.1 Транзитні комунікації

Додаток Д. Генеральний план



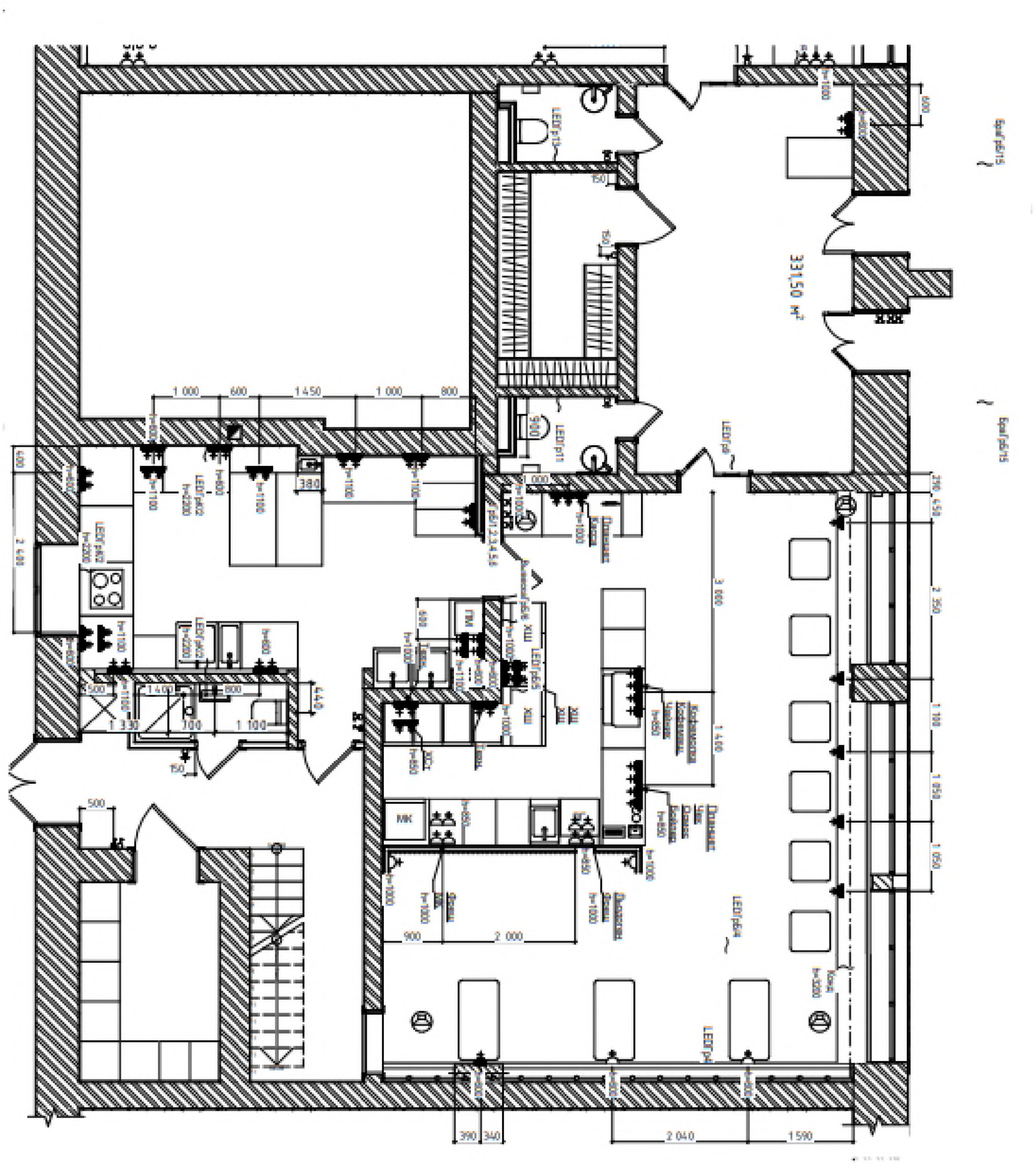
Назва	Розмір	Кол-во
1.Рабочая стойка	2100*600*900	
2.Рабочая стойка	3900*700*900	
3.Барная стойка	3950*400*1100	
4.Рабочая стойка	2150*650*900 (нержавейка)	
5.Рабочая стойка	3250*700*900 (нержавейка)	
6.Рабочая стойка	1800*650*900 (нержавейка)	
7.Деревян. лавка	8590*500*350	
8.Стол	600*600*750	6
9.Стол	600*1200*750	3
10. Ресепшн	1000*600*900	1
11.Диван	1400*670*900	1 шт.
12.Кресло (красный)	500*500*800	3 шт.
13.Кресло (зеленый)	500*500*800	3 шт.
14.Диван	1200*670*850	6 шт.
15.Стул барный	400*400*750	5 шт.

Рисунок 2. Генеральний план



№	Название,мм	шт
	Розетка	60
	Розетка накладная	60
	Выключатель	60
	Выключатель двойной	12
	Выключатель 2 накладной	3
	Выключатель проходной	2
К~	Вывод под кондиционер	
	Блок сигнализации	
	Блок автоматов	
	Wi-fi	
	Акустика	4
ГрБ/1	Группа кофейни	
ГрК/1	Группа кухни	
ГрЗ/1	Группа зала	
LED/Гр	LED лента	

Рисунок 2. Генеральний план. План живлення



№	Название,мм	шт
	Розетка	60
	Розетка накладная	60
	Выключатель	60
	Выключатель двойной	12
	Выключатель 2 накладной	3
	Выключатель проходной	2
К~	Вывод под кондиционер	
	Блок сигнализации	
	Блок автоматов	
	Wi-fi	
	Аккустика	4
ГрБ1	Группа кофейни	
ГрК1	Группа кухни	
ГрЗ1	Группа зала	
LEDГр	LED лента	

Рисунок 2. Генеральний план. Елекрoживлення.

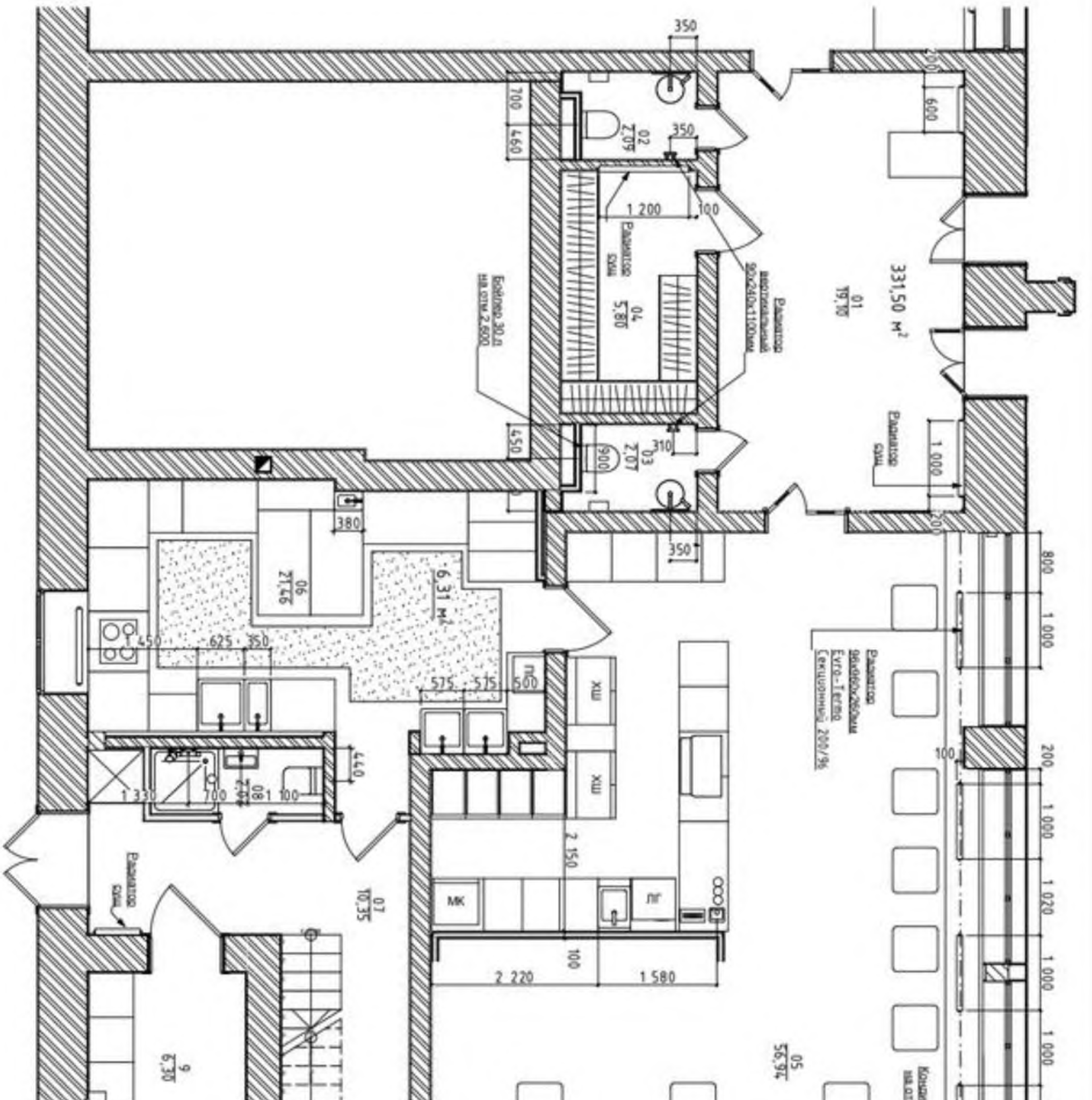
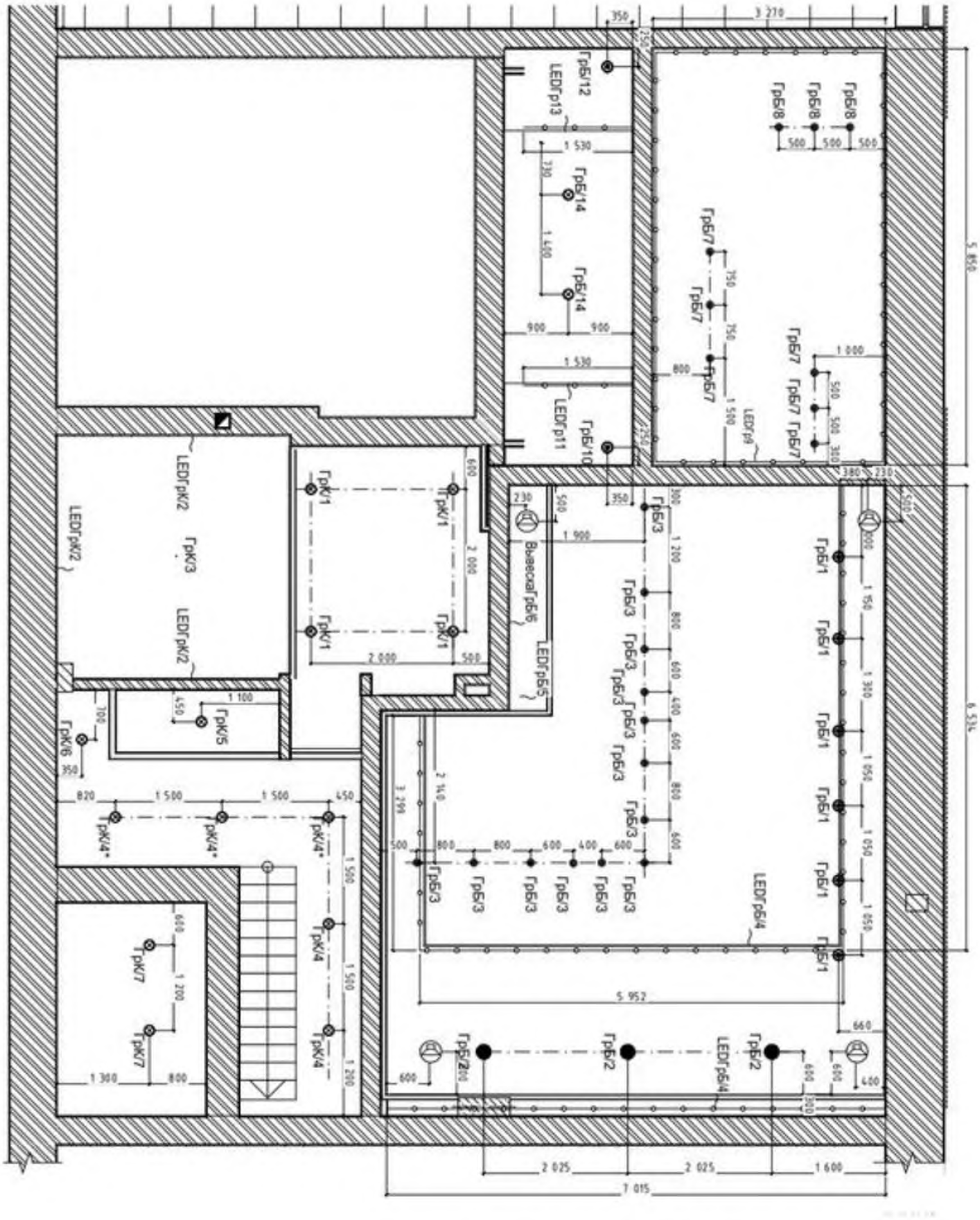


Рисунок 2. Генеральний план. Опалення



Об.ГР№	Название	Колво
ГрБ/1 ГрБ/10	Подвесной светильник	8 шт
ГрБ/2	Подвесной светильник	3 шт
ГрБ/3,7	Подвесной светильник	22 шт
ГрБ/4,5 9,11,13	LED лента	50 мп
ГрК/1	Врезной светильник	4 шт
ГрК/2	Настенный линейный LED светильник	3 шт
ГрК/4, 6,7	Врезной светильник	8 шт
ГрК/5	Врезной светильник влагостойкий	1 шт

Рисунок 2. Генеральний план. План освітлення

ДОДАТОК Е. Відгуки керівників розділів

Відгук керівника економічного розділу:

____
____
____
____
____
____
____
____
____
____
____
____
____

Керівник розділу ________________ ____________________

(підпис) (ініціали, прізвище)

ДОДАТОК Є. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125-17-2

Михайленко Артема Андрійовича

тему: «__комплексна система захисту інформації інформаційно-телекомунікаційної _системи ___ готельно-ресторанного господарювання «Avenue 69»______________

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на __59__ сторінках.

Метою кваліфікаційної роботи є розробка комплексної системи захисту інформації інформаційно-телекомунікаційної готельно-ресторанного господарювання «Avenue 69».

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 нормативно-правової бази у сфері забезпечення кібербезпеки; аналіз інформаційного середовища підприємства; аналіз моделі порушника та загроз.

На основі моделі разгроз було розроблено комплексну систему захисту інформації .

За час дипломування Михайленко А.А. проявив 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 «_____________».

Керівник кваліфікаційної роботи

Керівник спец. розділу