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 *Половченко Віталій Владиславович*

академічної групи *125-17-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплексна система захисту інформації інформаційно-телекомунікаційної системи ТОВ "GoldenCity"*

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

студенту ***Половченко Віталію Владиславовичу*** **академічної групи** ***125-17-2***
(прізвище ім'я по-батькові) (шифр)

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

на тему ***Комплексна система захисту інформації інформаційно-телекомунікаційної системи ТОВ "GoldenCity"***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 07.06.2021 № 317-с

Розділ	Зміст	Термін виконання
Розділ 1	Стан питання. Аналіз нормативно-правової бази. Обстеження ОІД, аналіз інформаційно-телекомунікаційної системи підприємства	05.05.2021 - 16.05.2021
Розділ 2	Розробка моделі загроз та моделі порушника. Оцінка існуючого стану захисту, проектні рішення, аналіз загроз після впровадження комплексу заходів	17.05.2021 – 30.05.2021
Розділ 3	Розрахунок економічної доцільності впровадження комплексу заходів	31.05.2021 -. 03.06.2021

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

Дата видачі: 18.01.2021р.

Дата подання до екзаменаційної комісії: 15.06.2021р.

Прийнято до виконання _____ Половченко В.В.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 79 с., 10 рис., 19табл., 5 додатків, 13 джерел.

Об’єкт розробки: інформаційно-телекомунікаційна система ТОВ "GoldenCity".

Предмет розробки: система забезпечення захисту інформації інформаційно-телекомунікаційної системи ТОВ "GoldenCity".

Мета роботи: підвищити рівень захисту ресурсів інформаційно-телекомунікаційної системи ТОВ "GoldenCity".

Методи розробки: спостереження, порівняння, аналіз, опис.

В першому розділі кваліфікаційної роботи надано загальний аналіз проблем забезпечення безпеки інформації України, розглянуто стан інформаційної безпеки на торгівельних підприємствах. Надано загальний опис підприємства "GoldenCity", його організаційна структура, проведено аналіз нормативно-правової бази, проаналізована інформаційно-обчислювальна системи підприємства.

В спеціальній частині кваліфікаційної роботи розроблено модель загроз та модель порушника, проаналізовані актуальні загрози та вразливості, обрано профіль захищеності та розроблені програмно-організаційні рішення для захисту інформації на підприємстві "GoldenCity".

В економічному розділі кваліфікаційної роботи розраховано капітальні та поточні витрати, проведено оцінку можливого збитку від атаки та виконано аналіз економічної доцільності запропонованих рішень.

Практичне значення роботи полягає у підвищенні рівня захисту інформації в інформаційно-телекомунікаційній системі ТОВ "GoldenCity", за рахунок розробки рекомендацій щодо захисту інформації на підприємстві.

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ОБ’ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, МОДЕЛЬ ЗАГРОЗ, ВРАЗЛИВОСТІ, МОДЕЛЬ ПОРУШНИКА, АКТ ОБСТЕЖЕННЯ, ЕКОНОМІЧНА ДОЦІЛЬНІСТЬ

РЕФЕРАТ

Пояснительная записка: 79 стр., 11 рис., 19 табл., 5 приложений, 13 источников.

Объект разработки: информационно-телекомуникационная система ООО "GoldenCity".

Предмет разработки: система обеспечения защиты информації информационно-телекомуникационной системы ООО "GoldenCity".

Цель работы: повысить уровень защищенности информационно-телекоммуникационной системы.

Методы разработки: наблюдение, сравнение, анализ, описание.

В первом разделе квалификационной работы проведен анализ проблем информационной безопасности на торговых предприятиях. Приведено общее описание предприятия "GoldenCity", его организационная структура, проведен анализ нормативно-правовой базы, проанализирована информационно-вычислительная система предприятия.

В специальной части квалификационной работы разработана модель угроз и модель нарушителя, проанализированы актуальные угрозы и уязвимости, выбран профиль защищенности и представлены программно-организационные решения для защиты информации на предприятии "GoldenCity".

В экономическом разделе квалификационной работы рассчитаны капитальные и текущие расходы, проведена оценка возможного ущерба от атаки и выполнен анализ экономической целесообразности предлагаемых решений.

Практическое значение работы состоит в повышении уровня информационной безопастности в информационно-телекоммуникационной системе ООО "GoldenCity", за счет разработки рекомендаций по защите информации на предприятии.

КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ, ОБЪЕКТ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ, МОДЕЛЬ УГРОЗ, УЯЗВИМОСТЬ,

МОДЕЛЬ НАРУШИТЕЛЯ, АКТ ОБСЛЕДОВАНИЯ, ЭКОНОМИЧЕСКАЯ ЦЕЛЕСООБРАЗНОСТЬ

ABSTRACT

Explanatory note: 79 p., 11 draw., 19 table, 5 appendices, 13 sources.

Object of research: Information and telecommunication system LLC "GoldenCity".

Object of development: information and telecommunication system of GoldenCity LLC.

Subject of development: information protection system of information and telecommunication system of LLC "GoldenCity".

Development methods: observation, comparison, analysis, description.

In the first section of the qualification work, an analysis of information security problems at trade enterprises is carried out. The general description of the enterprise "GoldenCity", its organizational structure is given, the analysis of the regulatory and legal framework is carried out, the information and computing system of the enterprise is analyzed.

In a special part of the qualification work, a threat model and an intruder model were developed, actual threats and vulnerabilities were analyzed, a security profile was selected, and software and organizational solutions for information protection at the GoldenCity enterprise were presented.

In the economic section of the qualification work, the capital and operating costs were calculated, the possible damage from the attack was assessed and the analysis of the economic feasibility of the proposed solutions was carried out.

The practical significance of the work is to increase the level of information security in the information and telecommunication system of "GoldenCity" LLC, through the development of recommendations for the protection of information at the enterprise.

COMPREHENSIVE INFORMATION PROTECTION SYSTEM, OBJECT OF INFORMATION ACTIVITY, MODEL OF THREATS, VULNERABILITY, MODEL OF THE VIOLENT, ACT OF INSPECTION, ECONOMIC PERFORMANCE

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

КСЗІ – комплексна система захисту інформації;

ТО – технічне обслуговування;

КСІБ – комп'ютерної системи інформаційної безпеки;

КЗ – контрольована зона;

ОІД – об’єкт інформаційної діяльності;

ІТС – інформаційна-телекомунікаційна система;

ІОД – інформація з обмеженим доступом;

ІБ – інформаційна безпека;

НД ТЗІ – нормативний документ технічного захисту інформації.

ЗМІСТ

С.

ВСТУП

Інформаційні технології відіграють важливу роль у сучасному світі. Їх застосування дає нові можливості для розвитку і оптимізації бізнесу, сприяють розширенню ринків збуту, продуктивності праці, ефективному використанню ресурсів, підвищенню якості управління бізнесом і надання послуг. Сьогодні, гостра конкуренція розвивається у багатьох галузях ринку, одні компанії намагаються відповідати цінам і характеристиками продукції інших, покупці дістають можливість вибирати серед маси конкуруючих товарів, що не розрізняються за якістю. У такій ситуації будь-яка компанія, що ставить основною задачею питання про задоволення актуальних потреб покупців, пропонує клієнтові високий рівень обслуговування, має безперечну перевагу, що дозволяє створювати довготривалі стосунки.

Сучасні тенденції розвитку торгівлі призводять до укрупнення компаній за рахунок збільшення чисельності підприємств в їх складі, консолідації активів різних операторів, проведення угод злиття і поглинань, створення мережевих розподільних центрів. В результаті ростуть вимоги до інформаційних технологій і їх значущість в організації торгівлі. Обробка інформаційних потоків у будь-якій компанії вимагає високих темпів і абсолютної точності.

Під інформаційною безпекою об’єкта торгівлі розуміються всі елементи системи управління підприємством, пов’язані з визначенням, досягненням конфіденційності, цілісності, доступності, неспростовності, підзвітності, автентичності та достовірності інформації або засобів її обробки. Для забезпечення ефективного функціонування всіх вище визначених елементів необхідно використання комплексного підходу.

Задля запобігання зловживанням інформацією, що циркулює в інформаційній системі або передається по каналах зв'язку, для забезпечення її захисту потрібна реалізація системного підходу, що включає комплекс взаємопов'язаних заходів (використання спеціальних технічних і програмних засобів, організаційних заходів, нормативно-правових актів, морально-етичних заходів протидії і т. д.). Комплексний

характер захисту виникає з комплексних дій зловмисників, які намагаються будь-якими засобами добути важливу для них інформацію.

Актуальність теми даної кваліфікаційної роботи визначається збільшенням інформаційних та технічних вразливостей підприємства та необхідністю створення комплексної системи захисту для забезпечення інформаційної безпеки.

Об’єкт дослідження: інформаційно-телекомунікаційна система "GoldenCity".

Предмет дослідження: система захисту інформаційно-телекомунікаційної системи "GoldenCity".

Мета роботи: підвищити рівень захисту ресурсів інформаційно-телекомунікаційної системи "GoldenCity".

Для досягнення поставленої мети у кваліфікаційній роботі необхідно вирішити наступні завдання:

– дослідити ОІД з точки зору безпеки;
– виконати аналіз вразливостей інформації з обмеженим доступом;
– побудувати модель порушника;
– зробити аналіз загроз для оброблювальної інформації;
– розробити вимоги з інформаційної безпеки;
– розробити програмно-організаційні заходи для підвищення рівня інформаційної безпеки підприємства.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

Комп'ютерні та інформаційні технології сьогодні охопили всі галузі економіки. Для будь-якої сучасної компанії інформація стає одним з головних ресурсів, збереження і правильне розпорядження яким має ключове значення для розвитку бізнесу і зниження рівня різноманітних ризиків. Актуальною проблемою для підприємства стає забезпечення інформаційної безпеки.

Управління сучасним магазином і торговельною мережею передбачає використання автоматизованих систем комплексного торговельного, складського і бухгалтерського обліку. Сьогодні керівники приймають управлінські рішення, рунтуючись на даних, отриманих з інформаційних систем. Таким чином, якою б не була структура фірми, ведення обліку договорів, руху товарно-матеріальних цінностей, грошових коштів і бухгалтерського обліку повинні здійснюватися в єдиному інформаційному просторі.

З метою автоматизації управління торговим процесом на підприємстві створюється інформаційна система, яка може включати:

- внутрішню систему обліку і звітності (містить дані про обсяг, структуру і швидкості товарного виробництва і обігу, витратах і втратах підприємства, валові доходи, чистого прибутку, рентабельності і т.д.);
- систему маркетингової інформації (дозволяє відстежувати поточний стан, тенденції та перспективи розвитку ринку). Дану інформаційну систему можна визначити і як розвідувальну, тому що вона забезпечує збір, обробку та аналіз даних про діяльність конкурентів.

Дані в інформаційну систему надходять від персоналу компанії і з офісних систем дистриб'юторів. Надалі вони використовуються для оперативного управління підприємством, контролю та аналізу діяльності компанії в цілому, регіональних представництв і дистриб'юторів. Споживачами даних інформаційної мережі є

менеджери і керівники компанії, і фірм- дистриб'юторів. На рисунку 1.1 наведені основні інформаційні потоки, що циркулюють в системі управління торговим підприємством (торговельною мережею), показані їх основні джерела і споживачі [1].

Керівнику підприємства, фінансовому директору, головному бухгалтеру, старшим менеджерам для прийняття стратегічних управлінських рішень вкрай необхідно представляти повну картину стану підприємства і тенденцій його розвитку.

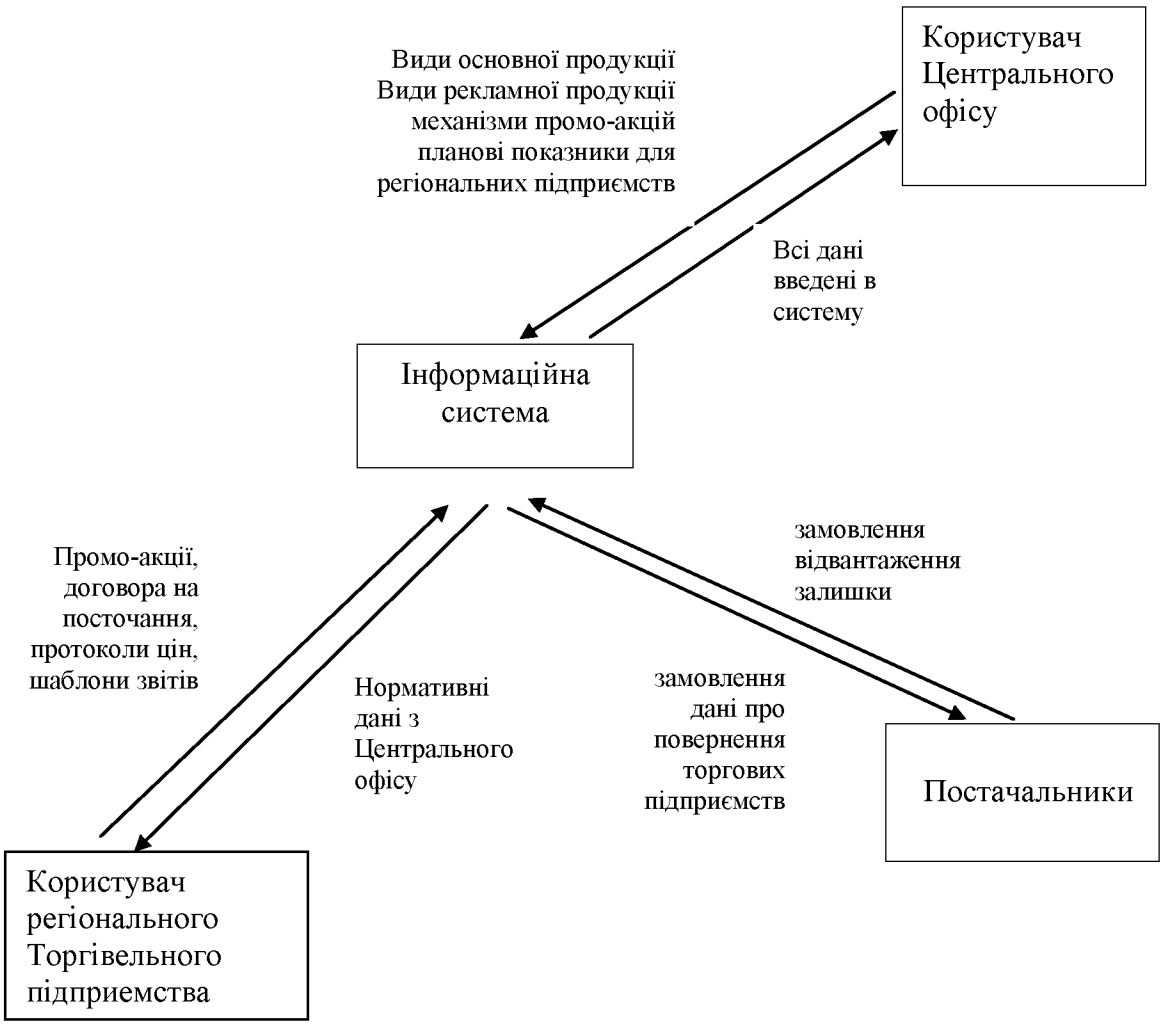

Рисунок 1.1 – Основні інформаційні потоки, що циркулюють в системі управління мережевої торгівельної компанії

На робочих місцях в бухгалтерії, в торговому залі, на складі працівники мають справу лише з окремими фрагментами загального інформаційного потоку. Їх завдання і функції, як правило, зводяться до оформлення та обліку приходу і витрати товарів, виписці рахунків, роботі на касовому апараті і т.п.

З огляду на ризики торговельних підприємств і вразливість інформаційних систем випливає, що в компанії повинна бути створена система інформаційної безпеки, вона є одним з основних елементів системи управління.

Зупинка роботи інформаційної системи може викликати незворотні наслідки для бізнесу. Так, за даними страхової компанії Atradius, при повній зупинці інформаційної системи торговельні компанії можуть проіснувати лише 2,5 дня, а для виробничих підприємств без безперервного виробничого циклу цей показник становить 5 днів.

Таким чином, керівники компаній повинні усвідомити важливість інформаційної безпеки, навчитися передбачати майбутні тенденції і управляти ними. Ефективна робота систем безпеки повинна стати першочерговим завданням для всього підприємства в цілому [2].

Основні напрямки захисту інформації:

- правовий захист включає: Законодавство України, власні нормативно-правові документи, в тому числі: положення про збереження конфіденційної інформації, перелік відомостей, що становлять комерційну таємницю, інструкція про порядок допуску працівників до конфіденційної інформації, положення про діловодство і документообіг, зобов'язання співробітника про нерозголошення конфіденційної інформації, пам'ятка співробітнику про збереження комерційної таємниці та ін .;
- організаційний захист включає режимно-адміністративні та організаційні заходи. До них відносяться: організація служби безпеки, організація внутрішньо об'єктного і пропускного режимів, організація роботи з співробітниками щодо нерозголошення відомостей, що становлять комерційну

та службову таємницю, організація роботи з документами, організація роботи з аналізу зовнішніх і внутрішніх загроз та ін.

- програмно-технічний захист - передбачає застосування різних технічних, електронних і програмних засобів, призначених для захисту інформації.

Реалізація програми захисту інформації повинна здійснюватися на основі комплексного використання систем і засобів безпеки виходячи з передумови, що неможливо забезпечити необхідний рівень захищеності тільки за допомогою одного окремого засобу або заходу, або їх простій сукупності. Необхідно їх системне узгодження. У цьому випадку реалізація будь-якої загрози може впливати на об'єкт, що захищається тільки в разі подолання всіх рівнів захисту.

Вихідними даними для створення ефективної системи інформаційної безпеки повинні бути чіткі уявлення про її цілі і структуру, про види загроз і їх джерелах, про можливі способи протидії [3].

1.2 Аналіз нормативно-правової бази

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

Закони України, нормативні документи в галузі технічного захисту інформації (НД ТЗІ) та державні стандарти України (ДСТУ) стосовно створення і функціонування КСЗІ:

- Закон України "Про захист персональних даних";
- Закон України “Про інформацію”;
- Закон України “Про захист інформації в інформаційно-телекомунікаційних системах”;

- НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу;
- НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу;
- НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі;
- НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації захисту інформації в комп'ютерних системах від несанкціонованого доступу;
- НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу;
- НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі;
- НД ТЗІ 1.6-005-2013 - Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці

1.3 Загальні відомості про організацію

ТОВ "GoldenCity" — мережа супермаркетів електроніки та побутової техніки. Заснована 1999 року, як підрозділ однойменної російської мережі. З 2013 року юридично є українською компанією.

Наприкінці 2016 компанія зробила ребрендинг, змінила написання назви компанії як, а також був запущений новий формат магазинів. Станом на кінець 2020 року мережа налічувала понад 120 магазинів по всій Україні.

Об'єктом інформаційної діяльності в кваліфікаційній роботі є супермаркет електроніки та побутової техніки "GoldenCity" в місті Кам'янському, що розташован за адресою вул. Сировця 9.

На рисунку 1.2 зображено організаційну структуру підприємства.

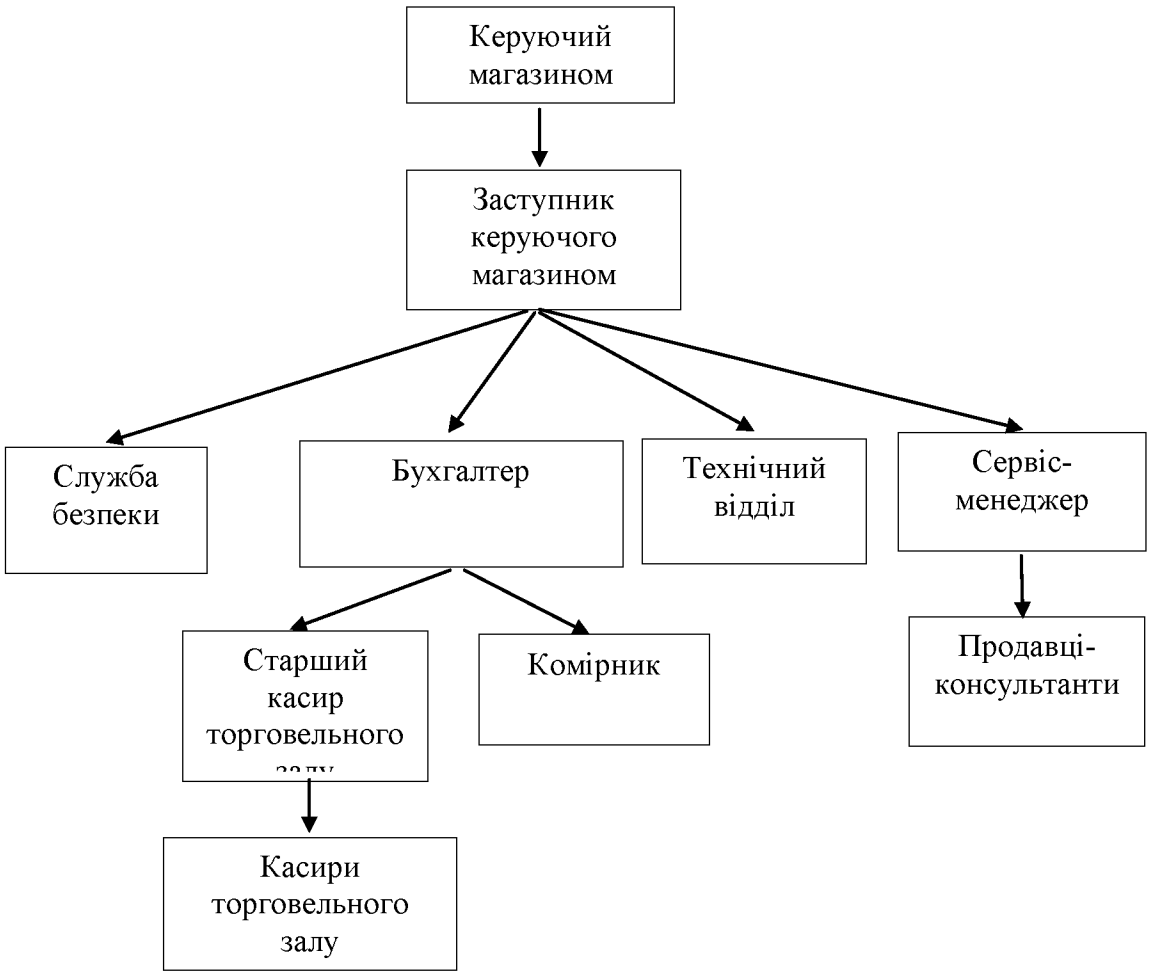

Рисунок 1.2 – Схема організаційної структури супермаркету електроніки та побутової техніки "GoldenCity" у м. Кам'янскому

Штат працівників та службові обов'язки:

- Керуючий магазином – організує вивчення попиту на види товарів та послуг, впроваджує прогресивні форми торгівлі та методи продажу товарів, вносить пропозиції щодо цінової політики магазину, веде обліково-звітну, статистичну документацію, розробляє заходи щодо поліпшення комерційної та фінансово-господарської діяльності, готує заявки на поставку товарів, контролює ритмічність надходження товарів та їх відповідність поданим заявкам.
- Заступник керуючого магазином – визначає критерії вимог до кандидатів на працевлаштування, забезпечує взаємозв'язок підлеглих йому працівників з

іншими відділами товариства, складає графік роботи працівників магазину з урахуванням раціонального розподілу праці, складає та оформлює табель обліку робочого часу працівників, в разі необхідності виконує обов'язки інших працівників магазину.

- Бухгалтер – здійснює оформлення бухгалтерських документів, розрахунків і платіжних зобов'язань, витрат фонду заробітної плати, за встановленням посадових окладів працівникам підприємства, проведенням інвентаризацій основних засобів, товарно-матеріальних цінностей і коштів, забезпечує складання балансу й оперативних зведених звітів про доходи і витрати коштів та іншої бухгалтерської і статистичної звітності, подання їх у встановленому порядку у відповідні органи.
- Комірник – здійснює роботу з приймання та відвантаження товарно-матеріальних цінностей, організовує зберігання матеріалів та продукції з метою запобігання їх псуванню та втратам, веде облік наявних на складі цінностей і звітну документацію про їх рух, забезпечує дотримання правил оформлення і здачі прибутково-видаткових документів.
- Сервіс менеджер – виконує обов'язки фахівця з якості, що пов'язані зі збереженням, обробкою, продажам (відпуском), перевезенням та застосуванням в процесі роботи товарно-матеріальних цінностей, подає данні для подальшого формування претензій постачальникам та сервісним партнерам по фактам постачання неякісного товару, приймає звернення покупців на обмін та повернення товарів та послуг.
- Старший касир торговельного залу – оформлює касові операції магазину в межах та у спосіб відповідно до вимог законодавства України про ведення касових операцій у національній валюті в Україні, оформлює документи тай одержує кошти і цінні папери в установах банку для виплат робітником заробітної плати, премій і інших виплат, контролює роботу касирів

торговельного залу, проводить інкасації, готує відомості інкасації, бере участь в інвентаризації грошових коштів.

- Касири(2) торговельного залу – веде косовий журнал, складає касову звітність, оформлює касові операції магазину в межах та у спосіб відповідно до вимог законодавства України про ведення касових операцій у національній валюті в Україні.
- Співробітник служби безпеки – здійснює охорону об'єкта від противоправних посягань, здійснює контроль справності засобів захисту товару, контрольно-спостережних приладів та освітлення.
- Техніки з налагоджування та випробувань(2) – підтримка торгово-технологічного обладнання, проведення ремонтних чи налагоджуваних робіт, надання сервісних послуг з підключення приладів та обладнання покупцям, в разі необхідності виконує обов'язки касира.
- Продавці-консультанти(10) – обслуговує покупців, консультує щодо конструктивних особливостей окремих видів товарів, їх призначення, властивостей, якості, правил догляду, цін, інформує покупців про наявність у продажу супутніх товарів і запасних частин, в разі необхідності виконує обов'язки касира.

1.4 Обґрунтування необхідності створення КСЗІ

На підприємстві наявна інформації, яка підлягає автоматизованій обробці та потребує захисту і забезпечення конфіденційності, цілісності та доступності відповідно до вимог нормативно-правових актів, розглянутих у підрозділі 1.2, що є підставою для необхідності створення КСЗІ. Власником інформації, прийняте рішення щодо створення КСЗІ та видано наказ «Про визначення відповідального за забезпечення технічного захисту інформації та створення КСЗІ на підприємстві ТОВ "GoldenCity" (Додаток Б).

1.5 Обстеження ОІД

1.5.1 Обстеження фізичного середовища

Інформація щодо об’єкта інформаційної діяльності (ОІД) була змінена на вимогу власника інформаційної системи з метою забезпечення конфіденційності інформації.

Об’єкт інформаційної діяльності знаходиться в ТРЦ ЦУМ, що розташовано за адресою вул. вул. Сировця, 9, м. Кам’янське, Дніпровська обл. Стіни будинку цегля. Перед будівлею знаходиться проїжджа частина.

До будинку в якому знаходиться ОІД підключені такі комунікації:

- Електропостачання від трансформаторної підстанції, що знаходиться на північному сході від ОІД, через підземні комунікації.
- Водопостачання підключене до міської магістралі.
- Система опалення – централізована, труби стояку йдуть з 0 поверху до КЗ, а потім до приміщень вище.

Усі комунікації виходять за межі контрольованої зони (КЗ), яка обмежена зовнішними стінами зі східної та північної сторони. Режим КЗ забезпечується таким чином:

- У робочий час забезпечується співробітниками охоронної організації, ролетами, металопластиковими дверми з механічним замком;
- У неробочий час забезпечується співробітниками охоронної організації, ролетами та дверима. Охоронна сигналізація КЗ підключенна окремо від сигналізації ТРЦ.

При проведені робіт використовувалася схема ОІД разом з його оточенням з географічної карти. Вона була використана, щоб отримати детальне розташування будівель, зелених насаджень та інших об’єктів навколо ОІД та вимірювання точних відстаней до них. Схема с ситуаційним планом наведена на рисунку 1.3.

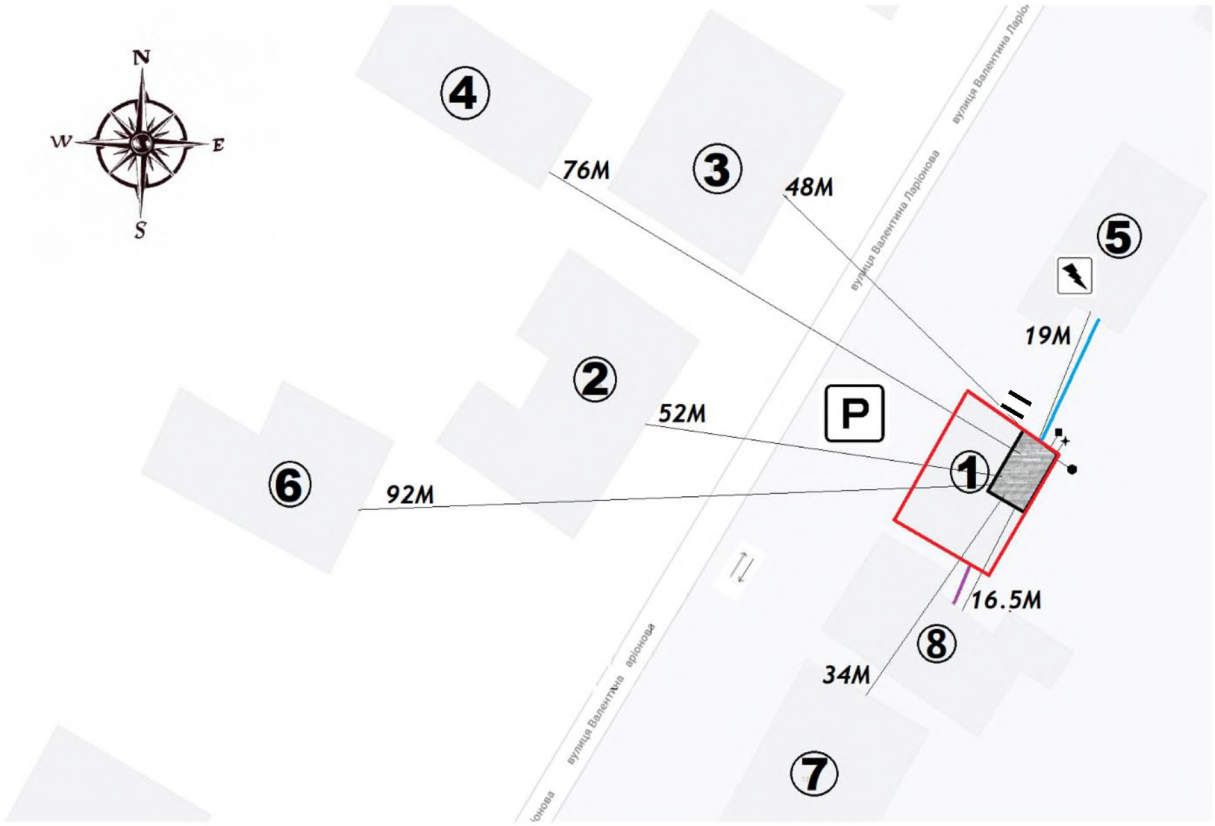

Рисунок 1.3 – Схема ситуаційного плану ОІД

У таблиці 1.1наведені характеристики прилеглих споруд.

Таблиця 1.1 – Характеристика прилеглих споруд

Найменування	Кіл-ть поверхів	Адреса	Відстань до КЗ, м
Офісний будинок(місце ОІД)	10	Вул. Валентина Ларионова, 13	0
Колегіум	2	Вул. Валентина Ларионова, 15	52
Магазин	9	Вул. Валентина Ларионова, 26	48
Магазин	9	Вул. Валентина Ларионова, 32	76
Трансформаторна підстанція №88	1	Вул. Валентина Ларионова, 11	19

Уся територія будівлі охороняється засобами охоронної сигналізації, яка встановлена на всіх дверях та вікнах. Усі дані з детекторів охоронної сигналізації в автоматичному режимі відправляються на пульт охорони, що знаходиться у будівлі на нульовому поверсі.

Об’єкт розташований на другому поверсі чотирьох поверхового будинку. До складу об’єкта інформаційної діяльності (ОІД) входить: торговельний зал, серверна, санвузол та коридор. Генеральний план зображено на рисунку 1.4.

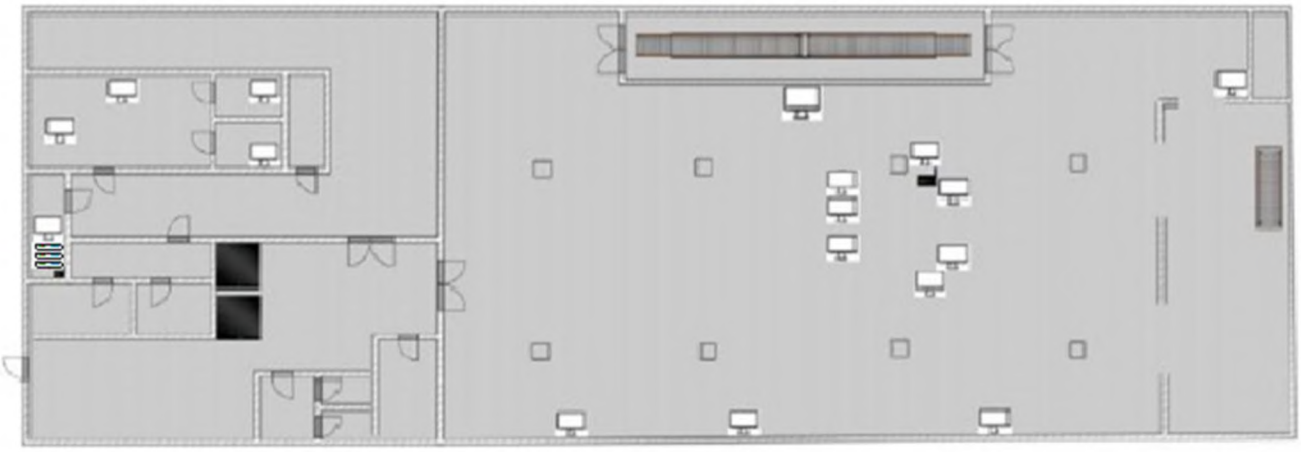

Рисунок 1.4 – Генеральний план

Площа ОІД – 9000 м².

Висота стелі – 2.5 м.

Стеля (матеріал – бетонні плити, товщина – 0.8 м), підлога (матеріал – бетон та ламінат, товщина – 1 м), стіни (матеріал – бетон та гіпсокартон, товщина 0,5 м)

Вікна (кількість- 3 шт, матеріал – пластик (полівінілхлорид або ПВХ), розміром 2,2 м на1,4 м. Жалюзі та штори на вікнах відсутні.

Лінія електропостачання – від розподільного щитка №1 на поверсі (рисунок 1.5).

Лінія комп'ютерної мережі — вита пара, Wi-Fi роутер підключений до мережевого обладнання провайдеру (рисунок 1.5).

Рисунок 1.5 – Схема електропостачання та освітлення

Сигналізація підключена до ПКП-5, що розташовано на одному поверсі з ОІД. Схему підключення зображено на рисунку 1.5.

Системи каналізації та водопостачання підключені до міської системи каналізації.

Система електропостачання підключена до трансформаторної, що знаходиться за межами КЗ і підтримує ще інших споживачів.

В таблиці 1.2 наведена інформація про системи комунікацій, та життєзабезпечення.

Таблиця 1.2 – Системи комунікацій, та життєзабезпечення

Система комунікацій	Спосіб підключення
Система опалення	Підключено до міської мережі опалення, знаходиться за межами КЗ
Електроживлення	Підключено до трансформаторної підстанції, котра обслуговує сторонніх споживачів і виходить за межі КЗ
Система водопостачання	Підключено до міського водоканалу, котрий виходить за межі КЗ
Система каналізації	Підключена до міської мережі каналізації, котра виходить за межі КЗ
Заземлення	Всі прилади заземлені на спільний контур заземлення, котрий є замкненим і виходить за межі КЗ
Система вентиляції	Приточно-витяжна
Протипожежна сигналізація	Всі прилади, комп'ютери заземлені на спільний контур заземлення, котрий є замкненим і виходить за межі КЗ
Кабелі комп'ютерної мережі	Всі прилади, комп'ютери заземлені на спільний контур заземлення, котрий є замкненим і виходить за межі КЗ

Схема вентиляції ОІД водопостачання, опалення, вентиляції та відеоспостереження наведена на рисунках 1.6 - 1.9.

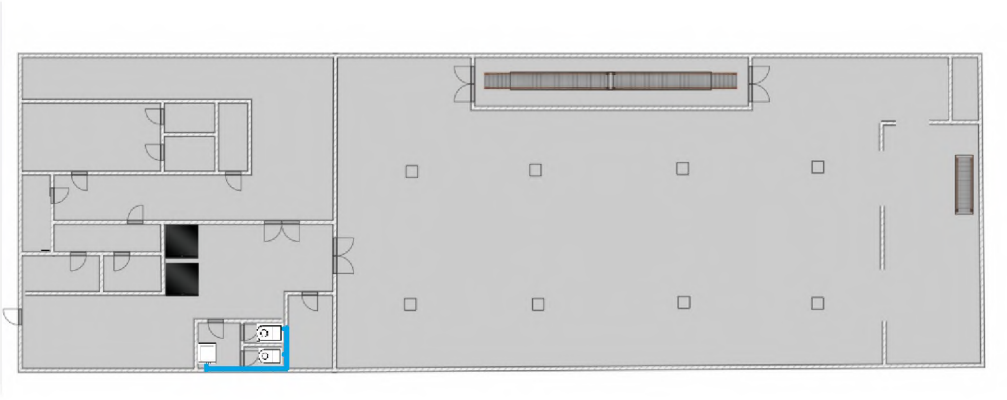

Рисунок 1.6 – Схема водопостачання на ОІД

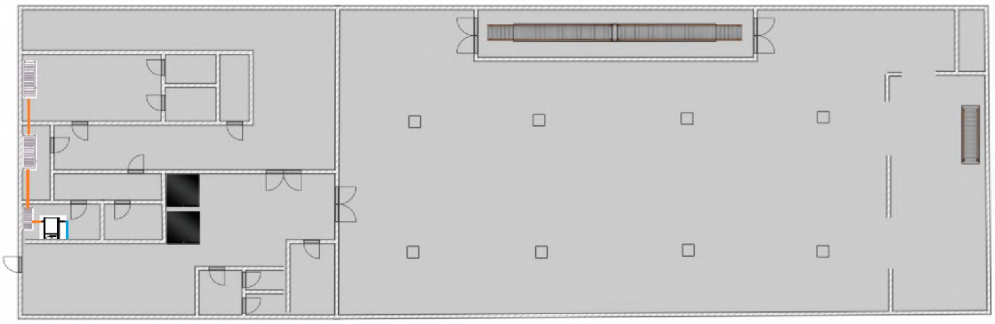

Рисунок 1.7 – Схема опалення на ОІД

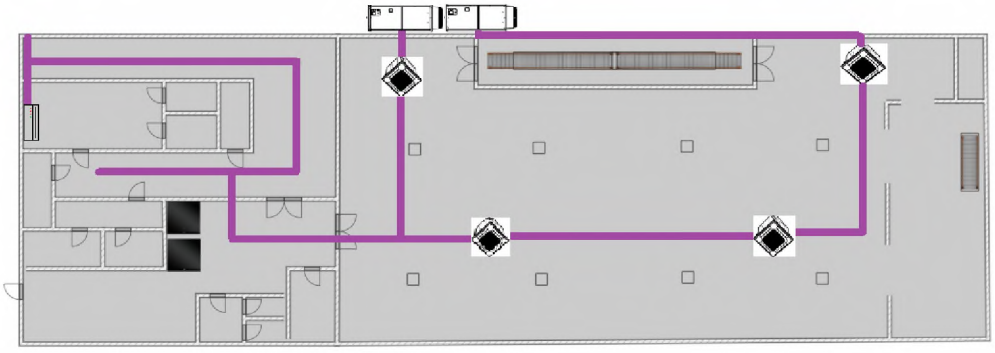

Рисунок 1.8 – Схема вентиляції на ОІД

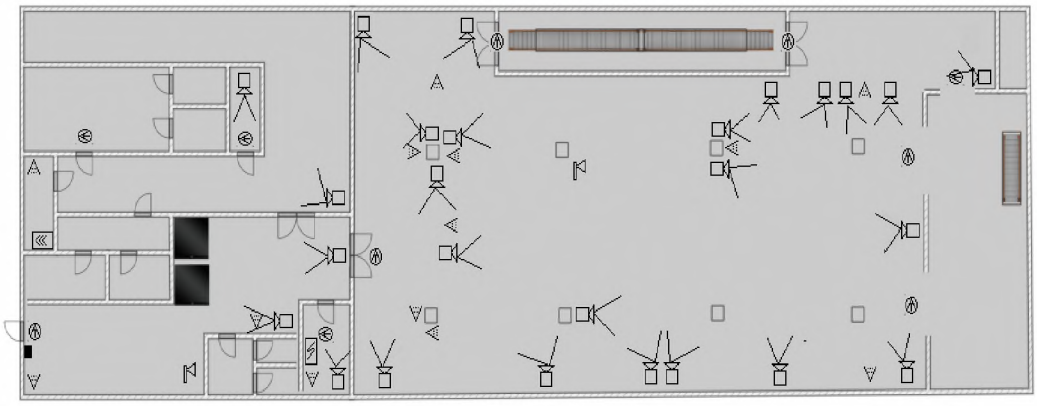

Рисунок 1.9 – Схема відеоспостереження на ОІД

1.5.2 Обстеження обчислювальної системи

ІТС ОІД являє собою мережу типу «пасивна зірка», побудовану з використанням одного комутатору. Являє собою багатомашинний багатокористувацький комплекс, а також має доступ до мережі Інтернет. Виходячи з наведеного вище, ІТС відноситься до АС 3 класу - розподілений багатомашинний, багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу.

На рисунку 1.10 представлена структурна схема ІТС.

Обчислювальна система налічує шістнадцять ПЕОМ з ОС Microsoft Windows 10.

Мережеве обладнання:

- коммутатор Cisco Catalyst 2960-X;
- Wi-Fi роутер ASUS CRS112-8G-4S-IN.

Інформація про основні та додаткові технічні засоби, які використовуються на підприємстві наведено в таблиці 1.3 та 1.4 відповідно.

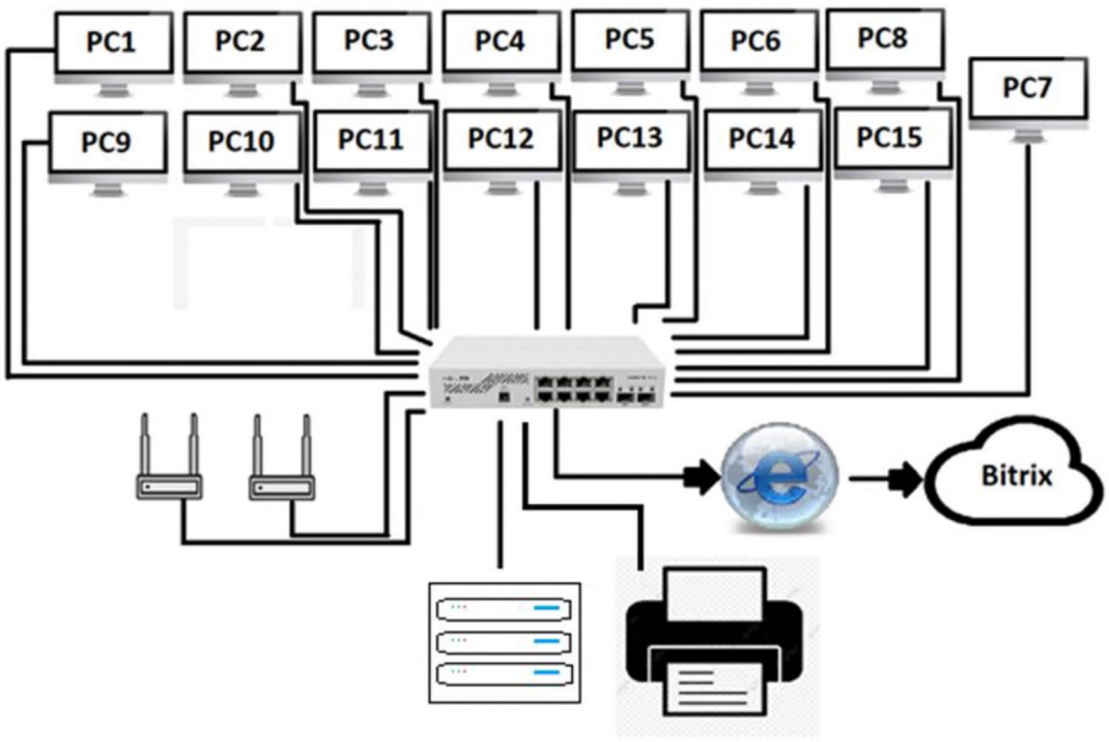

Рисунок 1.10 – Структурна схема ІТС

Таблиця 1.3 – Основні технічні засоби на підприємстві

Ім'я в системі	Тип	Марка	Модель	Розміщення	Серійний номер	Відстань до границі КЗ, м
ПК-1	Компьютер	Impression	IN5211	На стійці	Q5B7NTDA	1
ПК-2	Компьютер	Impression	IN5211	На стійці	EFKEY433	1
ПК-3	Компьютер	Impression	IN5211	На стійці	8NT3W4A7	1
ПК-4	Компьютер	Impression	IN5211	На стійці	64SKGQQR	1
ПК-5	Компьютер	Impression	IN5211	На стійці	YAT6EAKT	1
ПК-6	Компьютер	Impression	IN5211	На столі	IS6SSD964D	3
ПК-7	Компьютер	Impression	IN5211	На столі	SD98SD6SD	8

Продовження таблиці 1.3

Ім’я в системі	Тип	Марка	Модель	Розміщення	Серійний номер	Відстань до границі КЗ, м
ПК-8	Компьютер	Impression	IN5211	На столі	SDF88DFG7	7
ПК-9	Компьютер	Impression	IN5211	На столі	Y8R835T3R	7
ПК-10	Компьютер	Impression	IN5211	На столі	JHMB78F6Y	8
ПК-11	Компьютер	Impression	IN7500	На столі	6VB76VY8Y	2
ПК-12	Компьютер	Impression	IN7500	На столі	VJ43VD3DY	2
ПК-13	Компьютер	Impression	IN7500	На столі	A3S5F43FG3	2
ПК-14	Компьютер	Impression	IN7500	На столі	S3A6WR4R2	7
ПК-15	Компьютер	Impression	IN7500	На столі	A34F13A5E	7
Wi-Fi роутер (2шт)	Wi-Fi роутер	ASUS	CRS112-8G-4S-IN	На стіні	436MF4GN	8
Принтер	Принтер	HP	I-SENSYS M420X	На столі	436MF8NL	9
Сервер	Север	Cisco	UCS-SPR-C240M4-E2	На підлозі	5827qqwd8	5
Клавіатура (15)	Клавіатура	Logitech	K380	на столі	DCdiBVY	-
Комп’ютерна миша (15)	Комп’ютерна миша	Logitech	B100	на столі	FsdQ8EH	-

Таблиця 1.4 – Додаткові технічні засоби на підприємстві

Назва	Модель	Розміщення	Серійний номер
Люстри з діодними лампами (48)	L-225	на стелі	xfymLQS
Датчик диму (7)	Nomi SSW005	на стелі	K7JTbPE
ІЧ датчик	GP2Y0A02 YK0	на стіні	Jq3XKUc

Характеристика персональних комп'ютерів розташованих в торговельному залі Impression IN5211 (ім'я в системі ПК1 – ПК5):

- CPU: Intel Celeron G3900;
- RAM: 4 GB 1866 MHz DDR3;
- HDD: Barracuda 500 GB;
- GPU: Intel UHD Graphics;
- Материнская плата Asus H110M-R.

Характеристика персональних комп'ютерів розташованих в кабінете директора та відповідальних (ім'я в системі ПК6 – ПК15):

- CPU: Intel Pentium G5400;
- RAM: 4 GB 1866 MHz DDR3;
- HDD: Barracuda 500 GB;
- GPU: Intel UHD Graphics;
- Материнская плата Asus H110M-R.

Сервер (ПК16):

- HDD: WD Gold 2 TB;
- CPU: Intel Xeon E5-2620 v3;
- RAM: 64 GB 2666 MHz DDR4.

В таблиці 1.5 перераховане програмне забезпечення, встановлене на всіх ПК, які використовують співробітники ТОВ "GoldenCity".

Таблиця 1.5 – Програмне забезпечення на ПК ОІД

ПО	Версія	Де встановлено	Ліцензія
Windows 10	20H2	ПК-1-16	Придбана
1С:ERP	2020.3.3	ПК-1-16	Придбана
1С:Каса	20.10.5	ПК-10-11	Придбана
Антивірус(Windows defender)	4.18.2102.4	ПК-1-16	Придбана
1С:Бухгалтерия	8.3.1.7	ПК-11-12, 14	Придбана
Google Chrome	89.0.4389	ПК-1-16	Придбана
Office 365	2.31.1	ПК-1-16	Придбана
Outlook	8.1.0	ПК-1-16	Придбана

1.5.3 Обстеження інформаційного середовища

На підприємстві циркулює відкрита інформація та інформація з обмеженим доступом. Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням(згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом [4].

Паперові документи зберігаються в кабінеті директора в ящику стола с замком і ключем. Після втрати чинності документи знищуються. Облік місця та режим зберігання електронних носіїв інформації, а також їх переміщення на підприємстві не відстежується.

Роль адміністратора мережі покладена на керуючого магазином. Співробітники служби безпеки, являють собою охоронців, які слідкують за порядком у магазині по зображенню з камер відеоспостереження, що транслюється на моніторі ПК9. Роль адміністратора служби безпеки на підприємстві не передбачена.

Цифрові копії документів зберігаються на хмарному сервісі(Bitrix).

Продавці мають доступ тільки до комп'ютерів у торговому залі авторизуючись під обліковим записом "Продавець", обмеження доступу до робочого місця забезпечується паролем (всі продавців мають однаковий пароль).

В ІТС підприємства циркулює наступна інформація:

- організаційно-розпорядча інформація;
- інформація про закупочну, продажну вартість товарів та послуг;
- інформація про промо-акції;
- інформація о реалізації товарів;
- фінансова інформація;
- інформація про бухгалтерські звіти;
- інформація про співробітників (персональна, трудові договори);
- інформація про закази товару;
- інформація на веб-сайті.

В таблиці 1.6 наведена характеристика інформації, що обробляється на підприємстві.

Таблиця 1.6 – Характеристика інформації, що циркулює на підприємстві

Інформація	Режим доступу	Правовий режим	Вид зберігання	Вимоги до захисту		
				К	Ц	Д
організаційно-розпорядча	ІЗоД	Конфіденційна інформація	Електронний, паперовий	К2	Ц3	Д2
про промо-акції	ІЗоД	Комерційна таємниця	Електрон-ний, паперовий	К4	Ц4	Д4

Продовження таблиці 1.6

Інформація	Режим доступу	Правовий режим	Вид зберігання	Вимоги до захисту		
про продажі	ІЗоД	Конфіденційна інформація	Електронний, паперовий	К4	Ц4	Д3
фінансова	Відкрита	–	Електронний, паперовий	К1	Ц4	Д3
бухгалтерська	ІЗоД	Комерційна таємниця	Електронний, паперовий	К3	Ц4	Д4
про співробітників (персональна)	ІЗоД	Конфіденційна інформація	Електронний, паперовий	К4	Ц4	Д2
про закази товару	ІЗоД	Конфіденційна інформація	Електронний, паперовий	К2	Ц4	Д3

Рівні конфіденційності:

- К1 – рівень конфіденційності інформації, при якому можна знехтувати збитками у разі розкриття інформації особам, що не мають допуску до неї, або при якому інформація не є конфіденційною;
- К2 – рівень конфіденційності інформації, при якому компанія зазнає незначних збитків у разі розкриття інформації особам, що не мають допуску до неї;
- К3 – рівень конфіденційності інформації, при якому організація зазнає відчутних збитків у разі розкриття інформації особам, що не мають допуску до неї;
- К4 – рівень конфіденційності інформації, що може призвести до значних матеріальних втрат у разі розкриття інформації особам, що не мають допуску до неї;
- К5 – критичний рівень конфіденційності інформації, що може призвести до краха компанії у разі втрати конфіденційності інформації.

Рівні цілісності:

- Ц1– рівень цілісності інформації, при якому можна знехтувати втратою цілісності інформації;

- Ц2 – рівень цілісності інформації, при якому компанія зазнає незначних збитків у разі втрати цілісності інформації;
- Ц3 – рівень цілісності інформації, при якому організація зазнає відчутних збитків у разі втрати цілісності інформації;
- Ц4 – рівень цілісності інформації, що може призвести до значних матеріальних втрат у разі втрати цілісності інформації;
- Ц5 – критичний рівень цілісності інформації, що може призвести до краху компанії у разі втрати цілісності інформації.

Рівні доступності:

- Д1– рівень доступності інформації, при якому можна знехтувати втратою доступності інформації;
- Д2 – рівень доступності інформації, при якому компанія зазнає незначних збитків у разі втрати доступності інформації;
- Д3 – рівень доступності інформації, при якому організація зазнає відчутних збитків у разі втрати доступності інформації;
- Д4 – рівень доступності інформації, що може призвести до значних матеріальних втрат у разі втрати доступності інформації;
- Д5 – критичний рівень доступності інформації, що може призвести до краху компанії у разі втрати доступності інформації.

Технологія обробки інформації на підприємстві наступна:

Керуючий магазином або заступник отримує інформацію від куруючої компанії за допомогою поштового сервісу (Outlook), за потреби вона друкується. Паперові документи зберігаються у кабінеті керуючого.

В кінці місяця відпрацьований час співробітників заноситься до 1С:ERP керуючий магазином. У базі 1С:ERP зберігається інформація о продажах (саме з нею працюють продавці), а також інформація о знижках магазину (оновлюються завдяки ІТ відділу головного офісу).

Наприкінці кожного дня касир виводить гроші с каси, вносить їх до бази 1С:Бухгалтерія та закриває зміну.

Зважаючи на технологію обробки інформації на підприємстві можна виділити такі інформаційні потоки:

- Обробка організаційно-розпорядчої інформації (1);
- Обробка інформації про працівників (2);
- Обробка бухгалтерської та фінансової інформації (3);
- Обробка інформації о продажах (4);
- Обробка інформації о заказах (5);
- Обробка інформації о промо-акціях (6).

Схема інформаційних потоків зображена на рисунку 1.12

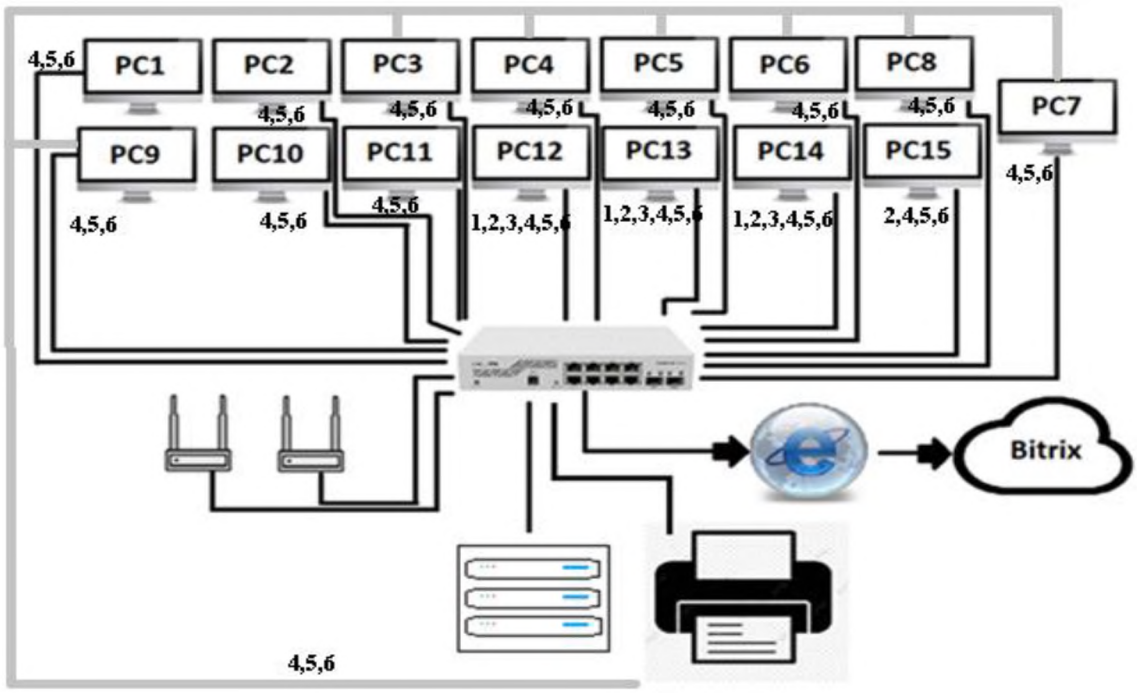

Рисунок 1.12 – Схема інформаційних потоків

В таблиці 1.7 надана матриця розмежування доступу до інформації, згідно з посадовими обов'язками співробітників ТОВ "GoldenCity".

Таблиця 1.7 – Матриця розмежування доступу

	КМ	ЗК	Б	К	СМ	СК	КС	СБ	ТН	П
організаційно-розпорядча	RWDC	RWDC	RWDC	R	R	RDW	R	R	RDW	R
про промо-акції	RWD	RWD	R	R	R	RDW	R	R	RDW	R
про продажі	RWDC	RWDC	R	R	–	RDWC	RCW	R	RDWC	RWDC
фінансова	RWDC	RWDC	RWDC	–	–	RDW	R	R	R	–
бухгалтерська	RWDC	RWDC	RWDC	–	–	RDW	R	R	R	–
про співробітників (персональна)	RWDC	RWDC	RWDC	–	–	RDW	R	R	RDW	–
про закази товару	RWDC	RWDC	–	RDWC	–	RWDC	RWDC	–	RDWC	RWDC
Повноваження інсталювання ПО	+	–	–	–	–	–	–	–	–	–
Ресурси	ПК16(сервер)	ПК15	ПК14	ПК13	ПК6	ПК12	ПК11-ПК10	ПК9	ПК8-ПК7	ПК1-ПК5

Умовні скорочення:

КМ – керуючий магазином;

ЗК – заступник керуючого;

Б – бухгалтер;

К – комірник;

СМ – сервіс менеджери;

СК – старший касир;

КС – касири;

СБ – співробітники служби безпеки;

ТН – техніки з налагоджування;

П – продавці.

R – читання;

C – створення нових файлів;

W – запис;

D – видалення.

1.6 Постановка задачі

Проаналізувавши проблеми кібербезпеки торговельних підприємств, що були розглянуті у пункті 1.1 та дослідивши особливості функціонування ТОВ "GoldenCity", ставимо задачу розробити комплексну систему захисту інформації (КСЗІ). Розробку КСЗІ необхідно проводити спираючись на аналіз фізичного, обчислювального, інформаційного середовища ТОВ "GoldenCity" та особливості обробки потоків інформації, що було виконано в пункті 1.5.

У другому розділі необхідно:

- розробити модель загроз;
- модель порушника;
- обрати профіль захищеності;
- розробити методи захисту.

1.7 Висновок

Торговельні підприємства є об'єктами, які мають свої особливості функціонування та, відповідно, вимагають особливого підходу до забезпечення їх інформаційної безпеки.

У першому розділі було досліджено стан та особливості інформаційної безпеки на торгівельних підприємствах, проаналізована нормативно-правова база, що регулює відносини у сфері захисту інформації, поставлена задача для розробки комплексної системи захисту інформації ТОВ "GoldenCity".

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Модель порушника

Стрімке проникнення інформаційно-комунікаційних технологій в усі сфери життєдіяльності людини і суспільства спричинило як позитивні, так і негативні наслідки. Комп'ютеризація різних організацій дозволила прискорити взаємодію між службовцями, а також оптимізувати їх роботу. Однак поряд зі збільшенням швидкості роботи з'явилися нові можливості і для недобросовісних співробітників. Тепер вони можуть швидко і просто, не покидаючи свого робочого місця, передати конфіденційну інформацію третій особі. Загроза, яка представляє собою виток інформації, актуальна і для сфери торгівлі.

Забезпечення безпеки підприємств торгівлі вимагає комплексу заходів, спрямованих на попередження, припинення і усунення загроз і небезпечних ситуацій. Цей комплекс повинен будуватися за принципом системного підходу і включати в себе сукупність організаційних заходів, технічних засобів безпеки та фізичної охорони.

Порушником є особа, яка здійснює спробу несанкціонованого доступу до об’єктів захисту (ознайомлення, модифікація, знищення, зміна режимів використання чи функціонування тощо). Потенційними порушниками є:

- 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.

Модель порушника - абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії тощо.

Зовнішній порушник (ЗП) - це порушник, що діє із зовнішнього, відносно ІТС, боку. У цій моделі розглядається як особа, що має доступ до приміщень, у яких розташовані засоби обчислювальної техніки, але не є авторизованим користувачем.

Категорії осіб, які можуть бути зовнішніми порушниками:

- Технічний персонал;
- Покупці;
- Сторонні особи, що знаходяться за межами контрольованої території.

Внутрішній порушник (ВП) - це порушник, що діє зсередини ІТС. У цій моделі розглядається як особа, що має доступ до приміщень, у яких розташовані засоби обчислювальної техніки та є авторизованим користувачем ІТС.

Внутрішнім порушником може бути особа з наступних категорій персоналу:

- Системний адміністратор;
- Співробітники магазину.

У таблиці 2.1. наведені категорії порушників, що будуть використовуються при створенні моделі.

Таблиця 2.1 – Категорії порушників, що визначені в моделі

Позначення	Визначення категорії	Потенційний рівень загрози
П1	Системний адміністратор	5
П2	Співробітники магазину	4
П3	Тех. персонал	3
П4	Покупці	2
П5	Сторонні особи, що знаходяться за межами контрольованої території	5

У таблицях 2.2-2.6 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 2.2 – Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив порушення	Ефективний рівень загрози
М1	Безвідповідальність/недбалість	5
М2	Корислива цілеспрямованість	4

Рівні кваліфікації порушників, які можуть становити загрозу інформаційній системі магазину наведені в таблиці 2.3.

Таблиця 2.3 – Специфікація моделі порушника за рівнем обізнаності щодо ІТС та кваліфікації

Позначення	Основні кваліфікаційні ознаки порушника	Ефективний рівень загрози
К1	Не володіє знаннями та інформацією щодо порядку функціонування ІТС, не має навичок щодо користування штатними засобами системи	1
К2	Має навички щодо користування ПК на рівні користувача	3
К3	Володіє базовими знаннями щодо функціонування програмного забезпечення та операційних систем і практичними навичками роботи із засобами, що реалізовані в ІТС	4
К4	Володіє знаннями щодо функціонування засобів/механізмів захисту, що використовується в ІТС та знає недоліки	5

Можливості для реалізації загроз порушниками, які можуть становити загрозу інформаційній системі наведені в таблиці 2.4.

Часові проміжки, під час яких порушники можуть реалізувати загрози інформаційній системі наведені в таблиці 2.5.

Таблиця 2.4 – Специфікація моделі порушника за показником можливостей використання засобів ІТС для реалізації загроз

Позначення	Характеристика можливостей порушника	Ефективний рівень загрози
З1	Має фізичний доступ до автоматизованого робочого місця, але не є авторизованим користувачем ІТС	3
З2	Має можливість запуску фіксованого набору завдань, що реалізують заздалегідь передбачені функції обробки інформації	4
З3	Має можливість керування функціонуванням елементів ІТС (конфігурує ПЗ)	5
З4	Не має фізичного доступу	1

Таблиця 2.5 – Специфікація моделі порушника за часом дії

Позначення	Характеристика можливостей порушника	Ефективний рівень загрози
Ч1	Під час бездіяльності компонентів ІТС	4
Ч2	Під час функціонування ІТС	5
Ч3	Під час перерв у роботі для обслуговування та ремонту	4

Можливі місця реалізації порушниками загроз інформаційно-телекомунікаційній системі магазину наведені в таблиці 2.6.

Таблиця 2.6 – Специфікація моделі порушника за місцем дії

Позначення	Характеристика місця дії порушника	Ефективний рівень загрози
Д1	Всередині будівлі та приміщення (без фізичного доступу до технічних засобів ІТС)	3
Д2	З робочих місць користувачів	4
Д3	З інших об’єктів ІТС, у тому числі каналів зв’язку	5

У графі «Рівень загроз» зазначених таблиць наведені у вигляді відносного ранжування оцінки можливих збитків, які може заподіяти порушник за умови наявності відповідних характеристик. Рівень збитків відповідно НД ТЗІ 1.4-001-2000 може характеризуватись наступними категоріями:

1 – незначний або відсутній;

2 – нижчий за середній;

3 – середній;

4 – вищий за середній;

5 – значний (високий).

Профілі можливостей порушників, які можуть становити загрозу інформаційно-телекомунікаційній системі магазину наведені в таблиці 2.7.

Таблиця 2.7 – Профілі можливостей порушників

Порушник	Категорія	Характер дій порушника					
		Мотив порушення	Кваліфікація	Можливості	Час дії	Місце дії	Сумарний рівень загрози
Внутрішні порушники (ВП)							
КМ	П1/5	М2/4	К4/5	З3/5	Ч2/5	Д2/4	28
ЗК	П2/4	М2/4	К4/5	З2/4	Ч2/5	Д2/4	26
Б	П2/4	М2/4	К3/4	З2/4	Ч2/5	Д2/4	25
К	П2/4	М2/4	К3/4	З2/4	Ч2/5	Д2/4	25
СМ	П2/4	М2/4	К4/5	З2/4	Ч2/5	Д2/4	26
СК	П2/4	М2/4	К3/4	З2/4	Ч2/5	Д2/4	25
КС	П2/4	М2/4	К3/4	З2/4	Ч2/5	Д2/4	25
СБ	П2/4	М2/4	К3/4	З2/4	Ч2/5	Д2/4	25
ТН	П2/4	М2/4	К3/4	З2/4	Ч2/5	Д2/4	25
П	П2/4	М2/4	К3/4	З2/4	Ч2/5	Д2/4	25

Продовження таблиці 2.7

Зовнішні порушники (ЗП)							
Хакери	П5/5	М2/4	К3/4	З1/3	Ч2/5	Д2/4	25
Конкуренти	П5/5	М2/4	К3/4	З1/3	Ч2/5	Д2/4	25
Обслуговуючий тех. персонал будівлі	П3/3	М2/4	К2/3	З1/3	Ч3/4	Д3/5	22

Проаналізувавши побудовану модель порушника, треба зазначити наступне:

По-перше, конкуруючі організації в торгівельній галузі завжди зацікавлені у володінні інформаційними активами конкурентів, бо володіння такою інформацією - це розуміння стратегії конкурентів. Звідси і випливає важливість контролю дій внутрішнього порушника, адже саме внутрішні співробітники мають доступ до цінних даних.

По-друге, враховуючи, що у більшості користувачів (співробітників магазину) досить обмежені можливості передачі великих обсягів критичної для бізнесу інформації, то ризики витоку за рахунок дій звичайних користувачів досить низькі. Тому особливу увагу треба звернути на зловмисні дії або недбалість адміністратора інформаційної системи. Привілейовані права доступу дозволяють йому нанести максимально критичний збиток організації.

При розробці КСЗІ ТОВ "GoldenCity" необхідно проаналізувати побудовану модель порушника та врахувати її особливості.

2.2 Виявлення актуальних загроз

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

А – обумовлені діями суб'єкта (антропогенні джерела загроз);

Т – обумовлені технічними засобами (техногенні джерела загроз);

С – обумовлені стихійними джерелами.

Антропогенними джерелами загроз безпеці інформації виступають суб'єкти, дії яких можуть бути кваліфіковані як умисні або випадкові злочини.

Як антропогенного джерела загроз можна розглядати суб'єкта, що має доступ (санкціонований або несанкціонований) до роботи зі штатними засобами об’єкта, що захищається. Суб'єкти (джерела), дії яких можуть призвести до порушення безпеки інформації можуть бути як зовнішні (А.З), так і внутрішні (А.В).

Зовнішні джерела можуть бути випадковими або навмисними і мати різний рівень кваліфікації. До них відносяться:

А.З.1 – конкуренти;

А.З.2 – представники організацій, обслуговуючі технічні системи;

А.З.3 – хакери.

До внутрішніх відносяться:

А.В.1 – системний адміністратор;

А.В.2 – персонал (співробітники).

Для ранжування антропогенних джерел загроз використовуються наступні коефіцієнти:

К1 – визначає ступінь доступності до об’єкта, що захищається;

К2 – визначає рівень кваліфікації;

К3 – визначає ступінь фатальності.

Для визначення ступеня доступності до об’єкта К1 використовують ранги:

5 – джерело має повний доступ до технічних засобів;

4 – джерело має можливість опосередкованого доступу до системи та її компонентів за необхідності;

3 – джерело має обмежену можливість доступу до системи та її компонентів;

2 – джерело дуже обмежено у можливостях;

1 – повна відсутність доступу.

Для визначення рівня кваліфікації К2:

5 – максимальний рівень прав;

4 – може вносити зміни;

3 – середній рівень прав;

2 – обмежені права;

1– повна відсутність прав.

Для визначення ступеня фатальності К3:

5 – велика проблема, для вирішення якої треба призупиняти функціонування системи або її компонентів;

4 – проблема, яка потребує негайного вирішення;

3 – проблема, яка не потребує негайного вирішення;

2 – незначні проблеми;

1 – проблеми не виникали.

Техногенними джерелами виступають технічні засоби, які так само можуть бути зовнішніми (Т.З) та внутрішніми (Т.В):

Т.З.1 – телекомунікаційні мережі;

Т.З.2 – мережі інженерних комунікацій (водопостачання, каналізації);

Т.В.1 – технічні засоби обробки інформації;

Т.В.2 – програмні засоби обробки інформації;

Т.В.3 – допоміжні засоби (охорони, сигналізації).

Для ранжування техногенних джерел загроз використовуються наступні коефіцієнти:

К1 – визначає ступінь віддаленості джерела загрози від об’єкту;

К2 – необхідні умови готовності джерела загрози;

К3 – визначає ступінь фатальності.

Для визначення ступеня віддаленості джерела загрози від об’єкту, що захищається використовують наступні значення:

5 – співпадаючі об’єкти;

4 – джерело знаходиться поруч;

3 – джерело знаходиться на деякій невеликій відстані;

2 – джерело знаходиться на деякій великій відстані;

1 – джерело знаходиться дуже далеко.

Для визначення необхідних умов готовності джерела загрози використовують значення:

5 – загроза може бути успішно реалізована;

4 – загроза може бути реалізована;

3 – загроза може бути помірно реалізована;

2 – загроза слабко реалізується;

1 – загроза не може бути реалізована.

Ступінь фатальності визначають слідуючим чином:

5 – велика проблема, для вирішення якої треба призупиняти функціонування системи або її компонентів;

4 – проблема, яка потребує негайного вирішення;

3 – проблема, яка не потребує негайного вирішення;

2 – незначні проблеми;

1 – проблеми не виникали.

Стихійні лиха, як джерела загроз інформаційній безпеці, як правило, є зовнішніми по відношенню до об'єкту, що захищається і під ними розуміються насамперед природні катаклізми (С.З):

С.З.1 – пожежі;

С.З.2 – землетруси, повені, урагани;

С.З.3 – епідемії;

С.З.4 – масові заворушення.

Для ранжування стихійних лих, як джерел загроз використовуються наступні коефіцієнти:

К1 – визначає особливості місцезнаходження об'єкту, що захищається;

К2 – необхідні умови готовності джерела;

К3 – визначає ступінь фатальності.

Для визначення особливостей місцезнаходження об'єкту, що захищається К1 використовують наступні значення:

5 – зона захисту знаходиться у зоні стихійного лиха;

4 – стихійне лихо часто відбувається у зоні захисту;

3 – інколи трапляється стихійне лихо у зоні захисту;

2 – мала ймовірність виникнення стихійного лиха у зоні захисту;

1 – виникнення стихійного лиха у зоні захисту майже неможливо.

Необхідні умови готовності джерела К2 визначаються виходячи з можливості реалізації загрози в конкретних умовах розташування об'єкта:

5 – загроза може бути успішно реалізована;

4 – загроза може бути реалізована;

3 – загроза може бути помірно реалізована;

2 – загроза слабко реалізується;

1 – загроза не може бути реалізована.

Ступінь фатальності визначається слідуючими рангами

5 – велика проблема, для вирішення якої треба призупиняти функціонування системи або її компонентів;

4 – проблема, яка потребує негайного вирішення;

3 – проблема, яка не потребує негайного вирішення;

2 – незначні проблеми;

1 – проблеми не виникали.

За допомогою ранжування усіх джерел загроз, можна провести їх кількісну оцінку використовуючи формулу:

$$К_н = \frac{К1 \cdot К2 \cdot К3}{125}, \quad (2.1)$$

де Кн – загальний коефіцієнт небезпеки;

К1, К2, К3 – коефіцієнти для ранжування джерел загроз.

Враховуючи проведене ранжування розрахуємо загальний коефіцієнт небезпеки для кожного з визначених джерел (таблиця 2.8).

Таблиця 2.8 – Джерела загроз

Умовне позначення	К1	К2	К3	Кн
А.З.1	3	3	5	0,36
А.З.2	2	3	3	0,14
А.З.3	4	2	4	0,26
А.В.1	5	4	4	0,64
А.В.2	4	3	4	0,38
Т.З.1	4	3	4	0,38
Т.З.2	4	3	4	0,38
Т.В.1	5	3	4	0,64
Т.В.2	5	4	4	0,64
Т.В.3	4	3	4	0,38
С.З.1	2	2	5	0,16
С.З.2	3	2	3	0,14
С.З.3	2	2	3	0,1
С.З.4	2	2	2	0,06

Найбільш небезпечними можна назвати джерела загроз, загальні коефіцієнти небезпеки яких більше за 0,3.

Згідно проведеного аналізу це:

А.З.1 – конкуренти (0,36);

А.В.1 – системний адміністратор (0,64);

А.В.2 – персонал (співробітники) (0,38);

Т.З.1 – телекомунікаційні мережі (0,38);

Т.З.2 – мережі інженерних комунікацій (водопостачання, каналізації) (0,38);

Т.В.1 – технічні засоби обробки інформації (0,64);

Т.В.2 – програмні засоби обробки інформації (0,64);

Т.В.3 – допоміжні засоби (охорони, сигналізації) (0,38).

Зважаючи на результати ранжування джерел загроз, визначимо загрози безпеці інформації для ІТС ТОВ "GoldenCity" та вразливості які вони використовують. Побудована модель загроз представлена в таблиці 2.9.

Таблиця 2.9 – Модель загроз ТОВ "GoldenCity"

Джерело загроз	Вразливість	Загроза	Значення наслідків	Йомо-сть реалізації загрози	Показник ризику	К	Ц	Д
Конкуренти	Неконтро-льоване копіювання	Перехоплення конкурентами інформації	5	3	15	x		
Конкуренти	Встановлення апаратних закладок у приміщенні		5	2	10	x		
Системний адміністратор (керуючий магазином)	Неправильний розподіл прав доступу	Зловживання правами	5	3	15	x	x	x
	Відсутність регулярних аудитів		5	3	15	x	x	x
Основний персонал	Помилки при експлуатації програмного забезпечення	Зараження комп'ютерів вірусами	4	5	20	x	x	x
	Відсутня обережність під час розміщення	Читання/викрадення документів	4	3	12	x		
	Неналежна обізнаність щодо питань безпеки	Помилки під час використання	4	5	20	x	x	
	Відсутність механізма моніторінга	Незаконне оброблення даних	4	4	16	x	x	x
Телекому-нікаційні мережі	Одна точка відмови	Аварія теле-комунікацій-ного обладнання	4	3	12			x
Мережі інженерних комунікацій	Ушкодження електро-, водо-, газо-, теплопостачання, каналізації	Призупинення роботи на деякий час через аварію інженерних систем	2	3	6			x
Технічні засоби обробки інформації	Чутливість до змін напруги	Втрата електро-живлення	2	3	6			x
	Відсутній ефективний контроль змін конфігурації	Помилки під час використання	3	5	15			x

Продовження таблиці 2.9

Джерело загроз	Вразливість	Загроза	Значення наслідків	Йомо-сть реалізації загрози	Показник ризику	К	Ц	Д
Програмні засоби обробки інформації	Доступність зайвих сервісів	Незаконне оброблення даних	4	5	20	х	х	х
	Відсутній журнал подій	Зловживання правами	4	4	16	х	х	х
Допоміжні засоби (охорони, сигналізації)	Ушкодження системи охорони та/або сигналізації	Призупинення роботи на деякий час	2	3	6			х

Значення наслідків:

1 – незначний (дуже низький)

2 – низький

3 – середній

4 – вищий за середній

5 – значний (дуже високий).

Імовірність реалізації загрози:

1 – дуже низька (зовсім малоймовірно)

2 – низька(малоймовірно)

3 – середня (можливо)

4 – висока (можлива)

5 – дуже висока (часто).

Побудована модель загроз пов’язує чинники наслідків та імовірності реалізації загрози (враховуючи аспекти вразливостей).Таким чином, остаточно загрози можуть бути ранжовані в порядку їх пов’язаного показника ризику.

В подальшому, для розробки заходів безпеки до урахування будемо брати загрози показник ризику яких більше, або дорівнює 15, а саме:

- Зараження комп’ютерів вірусами;
- Помилки під час використання;
- Незаконне оброблення даних;
- Зловживання правами;
- Перехоплення конкурентами інформації.

Статистика основних загроз і джерел втрат торгового підприємства виглядає наступним чином: 70% загроз виходить від персоналу: офісних і технічних працівників, контролерів, касирів, продавців, постачальників. 25% загроз - від покупців, і тільки 5% - техногенні і форс-мажорні загрози. Отримані моделі загроз та порушника повністю це підтверджують. Основні загрози для інформації ТОВ "GoldenCity". — це в першу чергу порушення технології роботи, а по другу — порушення доступності і конфіденційності. У зв'язку з цим до комплексних засобів захисту (КЗЗ) обчислювальних систем (ОС), що входять до складу торгівельних АС, пред'являються вимоги щодо забезпечення захисту від зазначених загроз. Тому рекомендується використовувати ОС, КЗЗ яких реалізують профілі 3.КЦД.х.

Проаналізувавши середовища функціонування інформаційно-телекомунікаційної системи на ОІД, розробивши модель загроз та модель порушника, було обрано стандартний функціональний профіль захищеності 3.КЦД.1, призначений для АС 3 класу з підвищеними вимогами до конфіденційності, цілісності та доступності:

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} [9]

КД-2. Базова довірча конфіденційність:

- політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься;
- КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта;
- запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта;
- КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта;

- КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес.

КО-1. Повторне використання об'єктів:

- політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС;
- перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані;
- перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною.

КВ-1. Мінімальна конфіденційність при обміні:

- політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів і інтерфейсних процесів, до яких вона відноситься;
- політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуються, і спроможність користувачів і/або процесів керувати рівнем захищеності;
- КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається.

ЦД-1. Мінімальна довірча цілісність:

- політика довірчої цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься;
- КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта;

- запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта;
- КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт;
- права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту.

ЦО-1. Обмежений відкат:

- політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься;
- повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу.

ЦВ-1: Мінімальна цілісність при обміні:

- політика цілісності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів КС і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовуваними механізмами, і спроможність користувачів і/або процесів керувати рівнем захищеності;
- КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається, а також фактів його видалення або дублювання.

ДР-1. Квоти:

- політика використання ресурсів, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься;

- політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу;
- запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження.

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;
- після відмови КС або переривання обслуговування КЗЗ повинен перевести КС до стану, із якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження;
- повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути КС до нормального функціонування.

НР-2. Захищений журнал:

- політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються;
- КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки;
- журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події;

- КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування;
- адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації.

НИ-2. Одиночна ідентифікація і автентифікація:

- політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ;
- перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен автентифікувати цього користувача з використанням захищеного механізму;
- КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування.

НК-1. Однонаправлений достовірний канал:

- політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ;
- достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем.

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 функції, які необхідні для виконання даної ролі;

- користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі.

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;
- повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

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, при ініціалізації КЗЗ.

НВ-1: Автентифікація вузла:

- політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ;
- КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму;
- підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації.

2.3 Визначення методів та засобів захисту

Основним критерієм вибору методів захисту було:

- використовувати методи захисту відповідно до п. 17 Положення про технічний захист інформації в Україні, затвердженого Указом Президента України від 27 вересня 1999 р. № 1229. Перелік призначений для використання суб'єктами системи технічного захисту інформації (ТЗІ) під час розроблення, модернізації та впровадження комплексів ТЗІ на об’єктах інформаційної діяльності (ОІД) та комплексних систем захисту інформації (КСЗІ) в автоматизованих системах (АС);
- використовувати економічно обґрунтовані методи захисту;
- дотримуватись принципів логічності.

Проаналізувавши основні загрози та вразливості ТОВ "GoldenCity", що надані в таблиці 2.9, було запропоновано наступне:

1. Вимоги з інформаційної безпеки, які під час роботи забороняють:

- користуватись мобільними пристроями зв’язку (телефон, смартфон тощо) в торгівельному залі;
- підключати до комп’ютерів, що знаходяться в торгівельному залі будь-які зовнішні накопичувачі інформації (USB Flash, SD-карти, телефони/смартфони тощо);
- приносити та підключати до робочих комп’ютерів та/або локальної комп’ютерної мережі будь-яке стороннє обладнання/пристрої
- використовувати для входу в інформаційну систему облікові дані іншого співробітника;
- ремонтувати робочий комп’ютер, вносити зміни у склад його апаратних та програмних засобів (завантажувати інтерфейс керування системним ПЗ BIOS, вносити зміни або знищувати системні/конфігураційні файли операційної системи/мережевих пристроїв, самостійно встановлювати програмне

забезпечення, самостійно підключати або відключати периферійне обладнання, порушувати цілісність корпусу робочого комп'ютера (крім випадків обумовлених виконанням посадових/договірних обов'язків);

- залишати на робочому місці робочі записи/чернетки після закінчення робочого часу (в електронному вигляді - видаляти, в паперовому - знищувати у пристроях утилізації паперу);
- залишати ввімкненим робочий комп'ютер по закінченню робочого часу, за винятком випадків коли його подальша робота викликана технологічними вимогами;
- намагатись та/або вчиняти дії щодо отримання несанкціонованого доступу до робочих комп'ютерів, мережевого обладнання та сервера, а також втручатись в роботу системи антивірусного захисту;
- використовувати Інтернет для обміну інформацією розважального характеру, зокрема відвідувати файл обмінні сервіси, соціальні мережі, сайти знайомств, чати, відео-/аудіо-ресурси та ін.
- відправляти повідомлення електронною поштою, особам, які не мають відношення до інформації, що пересилається (спам в електронній пошті);
- поширювати електронні повідомлення, що містять підозрілі вкладення, посилання на сторонні ресурси. Намагатись переглянути вкладення підозрілих електронних повідомлень;
- завантажувати з мережі Інтернет зберігати та/або використовувати на робочому комп'ютері програмне забезпечення та/або інформацію, що не має відношення до виконання посадових обов'язків.
- використовувати мережеві та обчислювальні ресурси ТОВ "GoldenCity" для отримання або спроби отримання несанкціонованого доступу, участі у мережевих атаках та будь-яких деструктивних діях по відношенню до будь-якої мережі через Інтернет.

2. Впровадити технологію DLP

Технологія DLP (Data Leak Prevention) запобігає витоку конфіденційної інформації з інформаційної системи. DLP-системи будуються на аналізі потоків даних, які перетинають периметр інформаційної системи. Якщо була знайдена після аналізу потоків конфіденційна інформація - спрацьовує активна компонента системи, і передача повідомлення (пакета, потоку, сесії) блокується.

Для запровадження була обрана DLP-система з переліку засобів ТЗІ, які мають експертний висновок про відповідність до вимог технічного захисту інформації, що сформовано відповідно до п. 17 Положення про технічний захист інформації в Україні, а саме Safetica Full DLP версії 9.x, виробництва компанії Safetica Technologies (Чехія), експертний висновок №1082 (дійсний з 24.01.2020 до 24.01.2023).

Safetica Full DLP є комплексним засобом захисту від внутрішнього порушника, яке дозволяє закрити канали витоку інформації і врегулювати ризики, пов'язані з людським фактором. За допомогою моніторингу діяльності співробітників Safetica Full DLP виявляє їх нелегітимну поведінку, блокує нестандартні операції і захищає підприємство від наслідків небажаної активності персоналу.

Safetica Full DLP дозволить закрити основні канали витоку інформації, що дозволить захистити конфіденційні дані компанії не тільки від несанкціонованого доступу, а й від потенційно шкідливої активності співробітників, наділених правом працювати з такими відомостями. Завдання розпізнавання нестандартної діяльності співробітників вирішується завдяки звітам з діяльності співробітника, а саме:

- підрахунку згенерованого і одержаного мережевого трафіку;
- контролю використання додатків і пристроїв;
- відвідування веб-сайтів;
- контроль друку, роботи з файлами і електронною поштою.

3. Впровадити новий програмний продукт антивірусного захисту, що обрано з переліку засобів ТЗІ, які мають експертний висновок про відповідність до вимог

технічного захисту інформації, що сформовано відповідно до п. 17 Положення про технічний захист інформації в Україні, а саме ESET Endpoint Security для Windows (EES) з системою централізованого керування ESET Remote Administrator, виробництва компанії ESET (Словаччина), експертний висновок №1075 (дійсний з 24.01.2020 до 24.01.2023).

Endpoint Security виявляє та знешкоджує загрози, спрямовані на операційну систему Windows, забезпечує управління змінними носіями, запобігає вторгненням (HIPS), дозволяє створювати завантажувальний образ операційної системи з встановленим антивірусним сканером для очищення заражених ПК.

4. Провести розмежування ролі адміністратора мережі та адміністратора безпеки ТОВ "GoldenCity".

Основним припущенням, що зроблене під час аналізу потенційного порушника для ТОВ "GoldenCity" є те, що системний адміністратор має найвищий рівень довіри з погляду забезпечення захисту інформації і розглядається як особа, відповідальна за стан захищеності інформації, що обробляється в межах об'єкта. Тому є доцільним, з метою забезпечення контролю його дій, розділити ролі адміністраторів мережі та безпеки з мінімізацією функцій кожного так, щоб включати тільки ті функції, які необхідні для виконання даної ролі, та передати роль адміністратора безпеки довіреному персоналу. Наказ на суміщення відповідальності приведено в ДОДАТКУ В.

5. Створення політики або впровадження в існуючу політику розділів, щодо розмежування доступу та ведення журнала реєстрації подій.

В таблиці 2.10 наведені основні положення, що повинні включати запропоновані політики безпеки.

Таблиця 2.10 – Основні положення політик безпеки

Назва	Опис
Політика	Політика розмежування прав доступу регламентує правила доступу користувачів і процесів до пасивних об'єктів.

Назва	Опис
розмежування прав доступу	Відповідно до НД ТЗІ 1.4-001.2000, мають виконуватися наступні дії: кожне робоче місце повинно мати свого користувача, який несе відповідальність за його працездатність;

Продовження таблиці 2.10

Назва	Опис
	- для попередження неавторизованого доступу до даних, ПЗ, інших ресурсів, керування механізмами захисту здійснюється адміністратором системи; - за всі зміни ПЗ, створення резервних та архівних копій несе відповідальність адміністратор системи; - кожний користувач має свій ідентифікатор та пароль. Атрибути для адміністратора системи надає адміністратор безпеки. Видача атрибуті доступу дозволяється тільки після документальної реєстрації користувача; - користувачі проходять процедуру автентифікації для отримання доступу до ресурсів ІТС; - атрибути користувачів змінюються двічі на рік, а невикористовуванні і скомпрометовані – видаляються.
Політика ведення журнала реєстрації подій	Журнал реєстрації призначений для зберігання подій, що виникають в процесі роботи користувачів з інформаційною базою. Усі системи, які обробляють конфіденційну інформацію, мають підключення до мережі або приймають рішення щодо контролю доступу (автентифікація та авторизація), повинні фіксувати та зберігати інформацію про реєстрацію події, достатню для відповіді на наступні запитання: - Яку діяльність виконували? - Хто або що виконував діяльність, включаючи те, звідки чи за якою системою діяльність здійснювалась (суб'єкт)? - З якою діяльністю виконувались (об'єкт)? - Коли виконувалася діяльність?

Продовження таблиці 2.10

Назва	Опис
	- Яким інструментом (інструментами) виконувалась діяльність? - Яким був статус (наприклад, успіх проти невдачі), результат чи результат діяльності? Журнал повинен створюватися щоразу, коли система вимагає виконання будь-якої з наступних дій: - створювати, читати, оновлювати або видаляти конфіденційну інформацію, включаючи конфіденційну інформацію про автентифікацію, таку як паролі; - створювати, оновлювати або видаляти інформацію, не висвітлену в №1; - ініціювати підключення до мережі; - прийняти підключення до мережі; - аутентифікація та авторизація користувачів для дій, описаних в №1 або №2, таких як вхід та вихід користувача; - надати, змінити або скасувати права доступу, включаючи додавання нового користувача або групи, зміну рівнів привілеїв користувача, зміну дозволів файлів, зміну дозволів об'єктів бази даних, зміну правил брандмауера та зміну пароля користувача; - зміни конфігурації системи, мережі чи послуг, включаючи встановлення виправлень та оновлень програмного забезпечення, або інші встановлені зміни програмного забезпечення; - запуск, призупинення або перезапуск процесу застосування;

Продовження таблиці 2.10

	- переривання, відмова або аномальне завершення процесу програми, особливо через вичерпання ресурсів або досягнення обмеження або порогу ресурсу відмови мережі послуги, такі як DHCP або DNS, або несправність обладнання; - виявлення підозрілих / шкідливих дій, таких як система виявлення або запобігання вторгненню (IDS / IPS), антивірусна система чи система захисту від шпигунського програмного забезпечення.

6. Запровадити організаційні методи, що направлені на підвищення обізнаності щодо інформаційної безпеки у співробітників.

Основною метою підвищення обізнаності працівників організації з питань інформаційної безпеки є зменшення втрат (матеріальних, фінансових, іміджевих), що виникають внаслідок загроз, пов'язаних з недостатнім знанням працівників або нерозумінням основних принципів інформаційної безпеки, у тому числі при роботі в інформаційній системі організації.

Таким чином необхідно:

- розробити зобов'язання про нерозголошення конфіденційної інформації, яке співробітник повинен підписувати до того, як йому буде повідомлено склад конфіденційних відомостей;
- інформувати працівників про існуючі загрози (вразливості) та питання безпеки, які можуть виникнути під час їх повсякденної роботи;
- забезпечити працівників основними вимогами, обмеженнями та правилами політики інформаційної безпеки організації.
- проводити регулярні тренінги, спрямовані на підвищення обізнаності користувачів в питаннях інформаційної безпеки.

2.4 Аналіз загроз після впровадження програмно-організаційних рішень

В таблиці 2.11 наведено перелік загроз з визначенням порушень властивостей інформації ІТС після впровадження запропонованих програмно-організаційних рішень ТОВ "GoldenCity".

Таблиця 2.11 – Перелік загроз з визначенням порушень властивостей інформації ІТС після впровадження програмно-організаційних рішень

Джерело загроз	Вразливість	Загроза	Значення наслідків	Імовірність реалізації загрози	Показник ризику	К	Ц	Д
Конкуренти	Неконтро-льоване копіювання	Перехоплення конкурентами інформації	5	5	10	х		
	Встановлення апаратних закладок у приміщенні		5	2	10	х		
Системний адміністратор (керуючий магазином)	Неправильний розподіл прав доступу	Зловживання правами	5	2	10	х	х	х
	Відсутність регулярних аудитів		5	2	10	х	х	х
Основний персонал	Помилки при експлуатації програмного забезпечення	Зараження комп'ютерів вірусами	4	3	12	х	х	х
	Відсутня обережність під час розміщення	Читання/викрадення документів	4	3	12	х		
	Неналежна обізнаність щодо питань безпеки	Помилки під час використання	4	3	12	х	х	
	Відсутність механізма моніторінга	Незаконне оброблення даних	4	2	8	х	х	х

Продовження таблиці 2.11

Телекомунікаційні мережі	Одна точка відмови	Аварія телекомунікаційного обладнання	4	3	12			X
Мережі інженерних комунікацій	Ушкодження електро-, водо, газо-, теплопостачання, каналізації	Призупинення роботи на деякий час через аварію інженерних систем	2	3	6			x
Технічні засоби обробки інформації	Чутливість до змін напруги	Втрата електроживлення	2	3	6			x
	Відсутній ефективний контроль змін конфігурації	Помилки під час використання	3	4	12			x
Програмні засоби обробки інформації	Доступність зайвих сервісів	Незаконне оброблення даних	4	3	12	x	x	x
	Відсутній журнал подій	Зловживання правами	4	3	12	x	x	
Допоміжні засоби (охорони, сигналізації)	Ушкодження системи охорони та/або сигналізації	Призупинення роботи на деякий час	2	3	6			x

Проаналізувавши таблицю 2.11, можна визначити, що після запровадження рекомендацій показник ризику зменшився до прийнятого рівня (менше 15), а саме:

- ризик зараження комп'ютерів вірусами через помилки при експлуатації програмного забезпечення знизився з 20 до 12;
- ризик помилки під час використання через неналежну обізнаність щодо питань безпеки знизився з 20 до 12;
- ризик незаконного оброблення даних через відсутність механізму моніторингу знизився з 20/16 до 8;
- ризик зловживання правами через відсутній журнал подій знизився з 16 до 12;
- ризик перехоплення конкурентами інформації через неконтрольоване копіювання знизився з 15 до 10.

2.5 Висновки до спеціальної частини

Ігнорування загроз та вразливостей інформаційно-телекомунікаційної системи може призвести до значних фінансових втрат та витоку інформації ТОВ "GoldenCity".

В ході виконання другого розділу розроблено модель порушника та модель загроз ТОВ "GoldenCity", обрано стандартний профіль захищеності, який використовується на підприємстві. Виявлено найбільш актуальні загрози, запропоновані організаційні та програмні рішення для їх мінімізації для підприємства:

- сформульовані вимоги з інформаційної безпеки;
- впроваджено Safetica Full DLP версії 9.x, виробництва компанії Safetica Technologies (Чехія), експертний висновок №1082 (дійсний з 24.01.2020 до 24.01.2023);
- впроваджено новий програмний продукт антивірусного захисту ESET Endpoint Security для Windows (EES) з системою централізованого керування ESET Remote Administrator, виробництва компанії ESET (Словаччина), експертний висновок №1075 (дійсний з 24.01.2020 до 24.01.2023);
- проведено розмежування ролі адміністратора мережі та адміністратора безпеки ТОВ "GoldenCity";
- розроблено елементи політики, щодо розмежування доступу та ведення журнала реєстрації подій;
- запровадити організаційні методи, що направлені на підвищення обізнаності щодо інформаційної безпеки у співробітників.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Обґрунтування витрат на розробку політики безпеки інформації

Метою обґрунтування витрат на розробку комплексної системи захисту інформації ТОВ «GoldenCity» є розрахунок капітальних та експлуатаційних витрат, оцінка величини можливого збитку від атаки, визначення та аналіз показників економічної ефективності [12].

3.2 Розрахунки витрат на розробку комплексної системи безпеки інформації

При розробці та експлуатації політики безпеки інформації необхідно розрахувати витрати ТОВ «GoldenCity » .

3.2.1 Розрахунок капітальних (фіксованих) витрат

Капітальні (фіксовані) витрати на розробку та впровадження політики безпеки інформації складають:

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

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

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

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

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

Вихідні дані ТОВ «GoldenCity» становлять:

$К_{пр}$ = 34056 грн.(Розроблення політики безпеки – 7056 грн., залучення зовнішніх консультантів – 27000 грн);

$К_{аз}$ = 0 грн;

Кзпз = 47600 грн.(29000 грн. – ліцензійна система(windows), 17600 грн. - ліцензійне ПО, 1000 ЕЦП)

$К_{н}$ = 26020 грн (витрати на встановлення обладнання та налагодження системи інформаційної безпеки).

Трудомісткість розробки політики безпеки:

$$t = t_{тз} + t_{в} + t_{а} + t_{вз} + t_{озб} + t_{овр} + t_{д}, \quad (3.2)$$

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

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

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

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

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

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

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

Таким чином:

$$t = t_{тз} + t_{в} + t_{а} + t_{вз} + t_{озб} + t_{овр} + t_{д} = 20 + 6 + 18 + 12 + 3 + 1 = 60 \text{ год} \quad (3.3)$$

Витрати на створення політики безпеки становлять:

$$К_{пр} = З_{зп} + З_{мч}, \quad (3.4)$$

де $К_{рп}$ – витрати на створення ПБ;

$З_{зп}$ - заробітна плата спеціаліста с ІБ;

$З_{мч}$ - вартість витрат машинного часу, що необхідні для створення ПБ.

Витрати на заробітну плату адміністратору інформаційної безпеки:

$$З_{зп} = t \cdot P_{аб}, \tag{3.5}$$

де t – загальна тривалість розробки ПБ, годин;

$З_{іб}$ – середньогодинна ЗП спеціаліста с ІБ, грн/годину.

Середньогодинна ЗП адміністратора з ІБ становить 35 грн/год. Таким чином заробітна плата адміністратора з ІБ буде становить:

$$З_{зп} = t \cdot P_{аб} = 60 \cdot 35 = 2100 \text{ грн.} \tag{3.6}$$

Витрати машинного часу:

$$З_{мч} = t \cdot С_{мч}, \tag{3.7}$$

де t – трудомісткість розробки ПБ на ПК, годин;

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

$$С_{мч} = P \cdot t_{нал} \cdot С_{е} + \left(\frac{Ф_{зал} \cdot Н_{а}}{Fp} + \frac{К_{лпз} + Н_{апз}}{Fp}\right). \tag{3.9}$$

$$С_{мч} = 1.26 \cdot 1 \cdot 1.68 + 80 + 0.5 = 82.6 \text{ грн.} \tag{3.8}$$

$$З_{мч} = t \cdot С_{мч} = 82.6 \cdot 60 = 4956 \text{ грн.} \tag{3.10}$$

Отже:

$$К_{пр} = З_{зп} + З_{мч} = 2100 + 4956 = 7056 \text{ грн.} \tag{3.11}$$

Визначимо капітальні витрати:

$$К = К_{пр} + К_{аз} + К_{зпз} + К_{н} = 34056 + 0 + 2620 + 47600 = 107676 \text{ грн.} \quad (3.12)$$

3.2.2 Розрахунок річних поточних (експлуатаційних) витрат

Річні поточні витрати складаються:

$$С = С_{а} + С_{ел} + С_{о} + С_{тос}, \quad (3.13)$$

де $С_{а}$ – річний фонд амортизаційних відрахувань;

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

$$С_{ел} = P \cdot F_{р} \cdot Ц_{е}, \quad (3.14)$$

де P – встановлена потужність апаратури інформаційної безпеки, кВт;

$F_{р}$ – річний фонд робочого часу системи інформаційної безпеки;

$Ц_{е}$ – тариф на електроенергію, грн/кВт·годин;

$С_{о}$ – витрати на залучення сторонніх організацій для виконання деяких видів обслуговування, навчання та сертифікацію обслуговуючого персоналу;

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

Річний фонд амортизаційних відрахувань становить:

$$С_{а} = \frac{Ф_{п}}{Т} = \frac{68359}{5} = 13671.8 \text{ грн.}, \quad (3.15)$$

де $Ф_{п}$ – первісна вартість придбаного ПО, грн;

Т - мінімальний строк корисного використання.

Програмне забезпечення - Eset Endpoint Security на 17 ПК – 2699 грн·17=45883 грн;

Впровадження DLP – 12476 грн;

Розмежування ролі адміністратора мережі та адміністратора безпеки, виплата заробітної плати працівнику ІТ відділу за впровадження – 12000 грн.

Потужність (Р) комп'ютерів та ноутбуків становить 1,26 кВт.

За 40-годинного робочого тижня річний фонд робочого часу системи інформаційної безпеки (Fр) становить 1920 годин.

Тариф на електроенергію складає 1,68 грн/кВт·годин. Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року становить:

$$С_{ел} = P \cdot F_p \cdot Ц_е = 1.26 \cdot 1920 \cdot 1.68 = 4064.26 \text{ грн.} \quad (3.16)$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки (Со) складають 18000 грн.

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки (Стос) визначаються ТОВ «GoldenCity» і складають 3% від вартості капітальних витрат.

$$С_{тос} = 107676 \cdot 0.03 = 3230.28 \text{ грн.} \quad (3.17)$$

Визначаємо річні поточні витрати:

$$С = С_а + С_{ел} + С_о + С_{тос} =$$
$$= 13671.8 + 4064.26 + 18000 + 3230.28 = 38933.34 \text{ грн.} \quad (3.18)$$

3.3 Оцінка можливого збитку від атаки

Загалом можливо виділити такі види збитку, що можуть вплинути на ефективність системи інформаційної безпеки (СІБ):

- порушення конфіденційності ресурсів СІБ (тобто неможливість доступу до них неавторизованих суб'єктів або несанкціонованого використання каналів зв'язку);
- порушення доступності ресурсів СІБ (тобто можливість доступу до них авторизованих суб'єктів (завжди, коли їм це потрібно);
- порушення цілісності ресурсів СІБ (тобто їхня неушкодженість);
- порушення автентичності ресурсів КСІБ (тобто їхньої дійсності, непідробленості).

Можна виділити й деякі універсальні форми нанесення збитку, наприклад, порушення конфіденційності, доступності, цілісності або автентичності ресурсу можно характеризувати як компрометацію ресурсу, тобто втрату довіри до нього користувачів (це може мати прямий збиток, зв'язаний, наприклад, з переустановленням програмного забезпечення або проведенням розслідування).

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

Необхідні вихідні дані для розрахунку:

- tп – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин;
- tв – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин;
- tви – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин;
- Зо – місячна заробітна плата обслуговуючого персоналу (адміністраторів та ін.) з нарахуванням єдиного соціального внеску, грн на місяць;

- Зс – місячна заробітна плата співробітника атакованого вузла або сегмента корпоративної мережі з нарахуванням єдиного соціального внеску, грн на місяць.

Заробітна плата не повинна бути нижче мінімальної заробітної плати на 01 січня поточного року. Ставка єдиного соціального внеску 22% и більше згідно класу професійного ризику підприємства, на якому проводиться захист інформації.

Чо – чисельність обслуговуючого персоналу (адміністраторів та програмних інженерів), осіб.;

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

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

Пзч – вартість заміни встаткування або запасних частин, грн;

I – число атакованих вузлів або сегментів корпоративної мережі;

N – середнє число можливих атак на рік.

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

$$U = П_п + П_в + V, \tag{3.19}$$

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

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

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

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

$$П_п = \frac{\sum З_с}{F} \cdot t_п = \frac{394200}{176} \cdot 4 = 8959.1 \text{ грн.}, \quad (3.20)$$

де $\sum З_с$ – заробітна платня співробітників, грн/міс;

F – місячний фонд робочого часу, год;

$t_п$ – час простою.

В таблиці 3.1 наведені виплати на заробітну плату співробітників з урахуванням ЄСВ.

Таблиця 3.1 – Виплати на заробітну плату співробітників

Посада	Кількість співробітників, осіб	Місячна заробітна плата, грн	Витрати на заробітну плату, грн	Єдиний соціальний внесок, грн	Витрати на заробітну плату з урахуванням ЄСВ, грн
Керуючий магазином	1	23000	23000	4600	27600
Заступник керуючого магазином	1	18000	18000	3600	21600
Служба безпеки	1	16000	16000	3200	19200
Бухгалтер	1	15000	15000	3000	18000
Старший касир торговельного залу	1	14500	14500	2900	17400
Касири Торговельного залу	2	12000	12000	2400	14400
Комірник	1	13500	13500	2700	16200
Технічний відділ	2	15000	15000	3000	18000
Сервіс-менеджер	1	13500	13500	2700	16200
Продавець-консультант	10	15000	15000	3000	18000
Всього					394200

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

$$П_в = П_{ви} + П_{пв} + П_{зп}, \quad (3.21)$$

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

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

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

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

$$П_{ви} = \frac{\sum З_с}{F} \cdot t_{ви} = \frac{394200}{176} \cdot 3 = 6719.1 \text{ грн.} \quad (3.22)$$

Витрати на відновлення вузла або сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньо годинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum З_с}{F} \cdot t_в = \frac{18000}{176} \cdot 3 = 306.8 \text{ грн.} \quad (3.23)$$

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

$$П_в = П_{ви} + П_{пв} + П_{зп} = 6719.1 + 306.8 + 0 = 7025.9 \text{ грн.} \quad (3.24)$$

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

$$V = \frac{O}{F_r} \cdot (t_в + t_{ви} + t_в) = \frac{120000000}{4320} \cdot (4 + 3 + 3) = 277777.9 \text{ грн.}, \quad (3.25)$$

де F_r – річний фонд часу роботи організації (організація працює 12 годин в добу, 1 січня - вихідний) становить близько 4320 ч.

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

$$U = П_п + П_в + V = 8959.1 + 7025.9 + 277777.9 = 293762.9 \text{ грн.} \quad (3.26)$$

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

$$В = \sum i \cdot \sum n \cdot U = 293762.9 \cdot 2 \cdot 1 = 587525.8 \text{ грн.} \quad (3.27)$$

3.4 Загальний ефект від впровадження КСЗІ

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

$$E = B \cdot R - C = (587525.8 \cdot 0.5) - 38966{,}34 = 254796.56 \text{ грн.}, \quad (3.28)$$

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

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

С – щорічні витрати на експлуатацію всіх заходів, грн.

3.5 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Оцінка економічної ефективності системи захисту інформації, розглянутої у. спеціальній частині кваліфікаційній роботі, здійснюється на основні визначення та аналізу наступних показників:

- сукупна вартість володіння (ТСО);
- коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI (Return on Investment for Security);
- термін окупності капітальних інвестицій.

Ключовою перевагою показника ТСО є те, що він дозволяє зробити висновки про доцільність реалізації проекту в області інформаційної безпеки на підставі оцінки одних тільки витрат. ТСО використовується, якщо величину відверненого збитку від атаки на вузол або сегмент корпоративної мережі важко або неможливо визначити у вартісній формі. У цьому випадку необхідно порівняти сукупну вартість володіння, щодо удосконалення системи інформаційної безпеки.

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

Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі, а отже:

$$ROSI = \frac{E}{K} = \frac{254796.56}{107676} = 3.37, \quad (3.29)$$

де Е – загальний ефект від впровадження системи інформаційної безпеки;

K – капітальні інвестиції.

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

$$T_o = \frac{K}{E} = \frac{1}{ROSI} = \frac{107676}{254796.56} = 0.42. \quad (3.30)$$

Виходячи з зроблених розрахунків $T_o = 0.42$, а це приблизно становитомить 5 місяців.

3.6 Висновок

В економічному розділі була визначена економічна ефективність розробки та впровадження політики безпеки інформації в ТОВ "GoldenCity". Було розраховано капітальні витрати, які склали 107676 грн. Оцінено величину можливого збитку від реалізованої атаки через упущену вигоду – 38966,34 грн. Визначений термін окупності капітальних інвестицій становить 5 місяців. Таким чином можна вважати, що впровадження комплексної системи захисту інформації на підприємство є економічно доцільним рішенням, яке ефективно захистить інформаційні активи від негативних зовнішніх та внутрішніх впливів.

ВИСНОВКИ

Інформаційні технології сьогодні охопили всі галузі економіки. Для будь-якої сучасної компанії інформація стає одним з головних ресурсів, збереження і правильне розпорядження яким має ключове значення для розвитку бізнесу і зниження рівня різноманітних ризиків. Актуальною проблемою для підприємства стає забезпечення інформаційної безпеки.

Під інформаційною безпекою підприємства або компанії розуміють комплекс заходів організаційного та технічного характеру, спрямованих на збереження і захист інформації та її ключових елементів, а також обладнання та системи, які використовуються для роботи з інформацією, її зберігання і передачі. Згідно з законодавством України, інформація з обмеженим доступом підлягає обов'язковому захисту, вимоги до якого встановлені законом.

В кваліфікаційній роботі було проаналізовано стан інформаційної захищеності в торгівельній галузі, проаналізована нормативно-правова база, що регулює відносини в інформаційній сфері. Проведено обстеження ТОВ "GoldenCity" та обґрунтовано створення комплексної системи захисту інформації, виконана постановка задачі.

В рамках другого розділу було розроблено модель порушника, модель загроз та проведено оцінку ризиків інформації, що можуть призвести до завдання збитків ТОВ "GoldenCity". Згідно з проведеним аналізом, запропоновані до впровадження методи та засоби захисту інформації для забезпечення ефективної роботи всіх складових інформаційно-телекомунікаційної системи підприємства.

В економічному розділі, отримали данні щодо підтвердження економічної доцільності запропонованих проектних рішень.

ПЕРЕЛІК ПОСИЛАННЬ

1. Information Security [Електроний ресурс] Режим доступу до ресурсу: http://lib.itsec.ru/articles2/Inf_security/infosec-torg

2. Утечки информации в розничных торговых сетях: специфика и методы борьбы | Компания "Аладдин Р.Д." [Електроний ресурс] Режим доступу до ресурсу https://www.aladdin-rd.ru/company/pressroom/articles/utecki_informacii_v_roznicnyh_torgovyh_setah_specifika_i_metody_borby

3. Створення комплексних систем захисту інформації [Електронний ресурс] Режим доступу до ресурсу: https://tzi.com.ua/stvorennya-kompleksnix-sistem-zaxistu-nformacz.html.

4. Закон України «Про інформацію» від 02.10.1992 No2657-XII // Відомості Верховної Ради України-1992-No 48. [Електронний ресурс] Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2657-12.

5. Закон України «Про захист персональних даних» від 01.06.2010 No 2297-VI // Відомості Верховної Ради України-2010-No 5. [Електронний ресурс] Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2297-17.

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 до ресурсу: http://zakon4.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.

7. НД ТЗІ 3.7-003-2005 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. [Чинний від 08.11.2005] - К.: ДССЗЗІ, 2005- No125(Нормативний документ системи технічного захисту інформації).

8. 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).

9. 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).

10. НД ТЗІ 1.4–001-2000 - 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).

12. Методичні вказівки до виконання економічної частини дипломного проекту /Упорядн. Д. П. Пілова. – Дніпро: Національний технічний університет «Дніпровська політехніка», 2019.

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

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
Документація				
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	Стан питання. Постановка задачі.	25	
6	А4	Спеціальна частина	30	
7	А4	Економічний розділ	12	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	
14	А4	Додаток Д	1	

ДОДАТОК Б. Наказ на створення КСЗІ

Товариство з обмеженною відповідальністю "GoldenCity".

НАКАЗ

«___»_____ Дніпро №_____

Про створення КСЗІ
у товаристві з обмеженною відповідальністю
"GoldenCity".

З метою виконання вимог законів України «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист персональних даних», Положення про технічний захист інформації в Україні, затверджений від 27.09.1999 № 1229/99, Правил забезпечення захисту інформації в інформаційно-телекомунікаційних системах, затверджених постановою Кабінету Міністрів України від 29.03.2006 № 373,
НАКАЗУЮ:

1. Провести обстеження складових інформаційно-телекомунікаційної системи товариства з обмеженною відповідалністю "GoldenCity" (далі – підприємство).
2. Створити комплексну систему захисту інформації підприємства.
3. Затвердити політики безпеки інформації інформаційно-телекомунікаційної системи підприємства.
4. Відповідальність за виконання наказу покладаю на себе.

Директор товариства _____ Петров А.І.

ДОДАТОК В. Наказ на суміщення відповідальності

Товариство з обмеженною відповідальністю "GoldenCity"

НАКАЗ

«___»_____ Дніпро №_____

Про запровадження
суміщення відповідальності
у товаристві з обмеженною відповідальністю
"GoldenCity"

ДОРУЧИТИ:

Павлову Дмитру Івановичу, сервіс-менеджеру, без увільнення його від основної роботи обумовленної трудовим договором, виконання додаткової роботи на умовах суміщення за посадою адміністратора безпеки зі щомісячною доплатою в розмірі 50% посадового окладу, з дати підписання наказу.

Директор товариства _____ Петров А.І.

ДОДАТОК Г. Перелік документів на оптичному носії

1 Пояснювальна_записка_Половченко.doc

2 Пояснювальна_записка_Половченко.pdf

3 Презентація_Половченко.pptx

ДОДАТОК Д. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____
(підпис) (ініціали, прізвище)

ДОДАТОК Е. Відгук керівника кваліфікаційної роботи

ВІДГУК
на кваліфікаційну роботу студента групи 125-17-2
Половченко Віталія Владиславовича
на тему: «Комплексна система захисту інформації інформаційно-телекомунікаційної системи ТОВ «GoldenCity»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 79 сторінках.

Метою кваліфікаційної роботи є підвищити рівень захисту інформації в інформаційно-телекомунікаційній системі ТОВ «GoldenCity».

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека».

В кваліфікаційній роботі було проаналізовано стан інформаційної захищеності в торгівельній галузі, нормативно-правова база, що регулює відносини в інформаційній сфері. Проведено обстеження ТОВ «GoldenCity» та обґрунтовано створення комплексної системи захисту інформації.

В рамках другого розділу було розроблено модель порушника, модель загроз та проведено оцінку ризиків інформації, що можуть призвести до завдання збитків ТОВ «GoldenCity». Згідно з проведеним аналізом, запропоновані до впровадження методи та засоби захисту інформації для забезпечення ефективної роботи всіх складових інформаційно-телекомунікаційної системи підприємства.

Практичне значення результатів кваліфікаційної роботи полягає у підвищенні рівня захищеності властивостей інформації з обмеженим доступом в інформаційно-телекомунікаційній системі «GoldenCity».

До недоліків кваліфікаційної роботи потрібно віднести незначні відхилення від стандартів оформлення.

За час дипломування Половченко В.В. проявив себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації бакалавра за спеціальністю 125 Кібербезпека, освітньо-професійної програми «Кібербезпека».

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

Кваліфікаційна робота заслуговує оцінки «_____».

Керівник кваліфікаційної роботи: доц. Сафаров О.О.