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 *Трегубова Микити Дмитровича*

академічної групи *125-20-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплексна система захисту інформації інформаційно - комунікаційної системи ПрАТ "Інтеркорн"*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	доц. Герасіна О.В			
розділів:				
спеціальний	ст.вкл. Герасіна О.В			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту *Трегубова Микити Дмитровича* **академічної групи** *125-20-2*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Комплексна система захисту інформації інформаційно - Комунікаційної системи ПрАТ "Інтеркорн"***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 23.05.24 № 469-с

Розділ	Зміст	Термін виконання
Розділ 1	Розгляд компонентів комплексної системи захисту інформації	04.06.2024
Розділ 2	Впровадження комплексної системи захисної інформації підприємства	17.06.2024
Розділ 3	Розглянути економічну доцільність впровадження комплексної системи захисту інформації	18.06.2024

Завдання видано _____ Олександра Герасіна
(підпис керівника) (ім'я, прізвище)

Дата видачі: 15.01.2024р.

Дата подання до екзаменаційної комісії: 28.06.2024р.

Прийнято до виконання _____ Микита Трегубов
(підпис студента) (ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 73 с., 7 рис., 10 табл., 4 додатка, 7 джерел.

Об’єкт розробки: підприємство ПрАТ "Інтеркорн"

Предмет розробки: комплексна система захисту іфнормації підприємства

Мета роботи: Розробка, впровадження та покращення системи КСЗІ на підприємстві "Інтерконр", що спрямована на забезпечення надійного захисту інформації від несанкціонованого доступу, витоку даних та інших загроз інформаційній безпеці підприємства.

У першому розділі було розглянуто загрози та вразливості інформаційної безпеки, які включають як зовнішні, так і внутрішні фактори, що можуть вплинути на безпеку інформаційних систем. Описано основні компоненти комплексної системи захисту інформації (КСЗІ), їхні функції та важливість для захисту даних. Розглянуто роль управління ризиками в КСЗІ, підкреслюючи важливість ідентифікації та оцінки ризиків для забезпечення ефективного захисту інформації.

У другому розділі розглянуто спеціальні аспекти інформаційної безпеки ПрАТ "Інтеркорн", включаючи загальні відомості про організацію, її організаційну структуру, обстеження об’єкта інформаційної діяльності, інформаційного середовища та обчислювальної системи підприємства. Також було проведено аналіз існуючого стану інформаційної безпеки, описано модель порушника, проведено аналіз ризиків, розроблено політику інформаційної безпеки та розглянуто вибір і встановлення технічних засобів захисту.

У третьому розділі економічної частини проведено ретельний розрахунок фіксованих (капітальних) витрат на впровадження комплексної системи захисту інформації. Також були оцінені поточні витрати, пов'язані з експлуатацією системи, і проведена оцінка можливого збитку в разі інциденту інформаційної безпеки. Була приділена увага визначенню та аналізу показників економічної ефективності розробки політики інформаційної безпеки, що підтверджується низькими витратами на впровадження і швидким терміном окупності проекту.

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ПІДПРИЄМСТВО, ІНФОРМАЦІЙНА БЕЗПЕКА, ІНТЕРКОРН.

ABSTRACT

Explanatory note: 73 pp., 7 pic., 10 table, 4 app, 7 sources.

Object of development: enterprise PJSC "Interkorn"

Subject of study: a comprehensive system of protection and information norms for enterprises

Meta-works: Development, promotion and enhancement of the KSZI system at the Interconr enterprise, which is aimed at ensuring reliable protection of information from unauthorized access, the flow of data and other threats to information security of the enterprise.

The first section examined the threats to information security, which included both external and internal factors that could affect the security of information systems. The main components of an integrated information protection system (ISIS), their functions and importance for data protection are described. The role of risk management in the CCIS is reviewed, emphasizing the importance of identifying and assessing risks to ensure effective security of information.

Another section examines special aspects of information security of Interkorn PJSC, including behind-the-scenes information about the organization, its organizational structure, the subject of information activities, information middle and payment system of business. An analysis of the current information security system was also carried out, a burglar model was described, a risk analysis was carried out, the information security policy was analyzed, and the selection and installation of technical security measures was reviewed.

In the third section of the economic department, a detailed breakdown of fixed (capital) expenditures was carried out to promote a comprehensive information security system. The current costs associated with the operation of the system were also assessed, and the potential for disruption in each information security incident was assessed. Respect was given to the careful analysis of indicators of the cost-effectiveness of developing an information security policy, which is confirmed by the low costs of implementation and the rapid return on investment for the project.

INTEGRATED INFORMATION PROTECTION SYSTEM, ENTERPRISE, INFORMATION SECURITY, INTERCORN.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

КСЗІ - Комплексна система захисту інформації

МН – Машине навчання

ШІ - Штучний інтелект

ІКС – інформаційно-комунікаційна система

ПЗ – програмне забезпечення

АС - автоматизовані системи

ОІД - Об'єкт інформатизації держави

ПрАТ - Публічне акціонерне товариство

COBIT - Control Objectives for Information and Related Technologies

ITIL - Information Technology Infrastructure Library

NIST - National Institute of Standards and Technology

ЗМІСТ

с.

ВСТУП.....7
РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ.....9
1.1 Загрози та вразливості інформаційної безпеки.....9
1.2 Основні компоненти комплексної системи захисту інформації (КСЗІ).....11
1.3 Роль управління ризиками в КСЗІ.....12
1.4 Огляд сучасних тенденцій та викликів у сфері захисту інформації.....14
1.5 Правові та нормативні вимоги у сфері інформаційної безпеки.....15
1.6 Огляд методологій та стандартів розробки КСЗІ.....17
1.7 Аналіз існуючих рішень та технологій для захисту інформації.....18
1.8 Виклики та перспективи впровадження КСЗІ в Україні.....19
1.9 Постановка задачі.....20
1.10 Висновок до першого розділу.....20
РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА.....22
2.1 Загальні відомості про організацію.....22
2.2 Організаційна структура підприємства.....23
2.3 Обстеження об’єкта інформаційної діяльності.....23
2.4 Обстеження інформаційного середовища ПрАТ "Інтеркорн".....24
2.5 Обстеження обчислювальної системи ПрАТ "Інтеркорн".....24
2.6 Аналіз існуючого стану інформаційної безпеки ПрАТ "Інтеркорн".....27
2.7 Модель порушника.....31
2.8 Аналіз ризиків.....35
2.9 Розробка політики інформаційної безепеки.....37
2.10 Вибір і встановлення технічних засобів захисту.....41
2.11 Тестування і оцінка ефективності після впровадження КСЗІ.....48
Висновок до другого розділу.....51

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ.....53
3.1 Розрахунок фіксованих (капітальних) витрат.....53
3.2 Розрахунок поточних витрат.....57
3.3 Оцінка можливого збитку.....60
3.4 Загальний ефект від впровадження системи комплексної системи захисту інформації.....63
Висновок до третього розділу.....66
ВИСНОВОК.....67
ПЕРЕЛІК ПОСИЛАНЬ.....69
ДОДАТОК А. відомість матеріалів кваліфікаційної роботи.....70
ДОДАТОК Б. Перелік документів на оптичному носії.....71
ДОДАТОК В. Відгук керівника кваліфікаційної роботи.....72
ДОДАТОК Г. Відгук керівника кваліфікаційної роботи.....73

ВСТУП

У сучасному цифровому світі безпека інформації є однією з найважливіших складових успішної діяльності будь-якого підприємства. З кожним роком кількість кіберзагроз зростає, інформаційні технології стають все складнішими, що вимагає від організацій ефективних заходів захисту. Реалізація комплексних систем захисту інформації набуває вельми актуального значення для забезпечення стійкості підприємства до внутрішніх і зовнішніх загроз.

Об'єктом розробки є інформаційно-комунікаційна система ПрАТ "Інтеркорн", яка включає в себе широкий спектр інформаційних технологій та мережевих інфраструктур.

Предметом розробки є комплексна система захисту інформації цієї інформаційно-комунікаційної системи (ІКС), спрямована на забезпечення конфіденційності, цілісності та доступності інформації.

Метою даної дипломної роботи є розробка та обґрунтування комплексної системи захисту інформації для інформаційно-комунікаційної системи ПрАТ "Інтеркорн", спрямованої на підвищення рівня безпеки обробки, зберігання та передачі інформації, відповідно до специфіки підприємства та вимог щодо захисту конфіденційної інформації.

Практичне значення роботи полягає у одержанні конкретних рекомендацій та розробці стратегії захисту інформації, які дозволять підприємству ефективно реагувати на сучасні кіберзагрози та забезпечити надійний захист конфіденційної інформації.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Загрози та вразливості інформаційної безпеки

Інформаційна безпека в сучасному світі є критично важливою складовою функціонування будь-якого підприємства чи організації. Загрози та вразливості, пов'язані з інформаційною безпекою, можуть мати різні джерела і прояви. Їх розуміння та ефективне управління ними є ключем до захисту інформаційних активів. У цьому тексті розглянемо основні загрози та вразливості, що впливають на інформаційну безпеку.

Зовнішні загрози походять від джерел за межами організації та можуть включати хакерські атаки, шкідливе програмне забезпечення та фішингові атаки. Хакерські атаки спрямовані на порушення конфіденційності, цілісності або доступності інформації шляхом несанкціонованого доступу до системи. Шкідливе програмне забезпечення, таке як віруси, трояни та черви, може проникати в системи і завдавати шкоди даним або програмам. Фішингові атаки використовують соціальну інженерію для обману користувачів з метою отримання конфіденційної інформації, наприклад, паролів або фінансових даних.

Внутрішні загрози пов'язані з діяльністю співробітників або інших осіб, які мають доступ до внутрішніх ресурсів організації. Це можуть бути ненавмисні дії, такі як помилки або недотримання політик безпеки, а також зловмисні дії, спрямовані на завдання шкоди або отримання вигоди. Ненавмисні помилки можуть включати випадкове видалення або зміну даних, неправильне налаштування систем безпеки або неналежне поводження з конфіденційною інформацією. Зловмисні дії, як правило, включають крадіжку даних, саботаж або продаж конфіденційної інформації конкурентам.

Технічні вразливості виникають через недоліки або помилки у програмному забезпеченні, апаратному забезпеченні або мережевій інфраструктурі. Це можуть бути незахищені порти, слабкі паролі, відсутність оновлень безпеки або вразливості у програмному коді. Вразливості у програмному забезпеченні можуть

бути використані хакерами для виконання шкідливих дій, таких як виконання віддаленого коду або отримання несанкціонованого доступу до системи. Відсутність регулярних оновлень безпеки збільшує ризик експлуатації відомих вразливостей.

Фізичні загрози включають ризики, пов'язані з фізичним доступом до інформаційних ресурсів. Це можуть бути крадіжка обладнання, вандалізм або природні катастрофи, такі як пожежі або повені. Крадіжка обладнання, такого як ноутбуки або мобільні пристрої, може призвести до втрати конфіденційної інформації або компрометації систем безпеки. Вандалізм може включати навмисне пошкодження обладнання або інфраструктури, що може спричинити втрату даних або зупинку роботи систем.

Людські фактори є однією з найважливіших категорій вразливостей. Це включає недостатню підготовку або обізнаність співробітників, недотримання політик безпеки, а також недостатнє управління доступом та моніторинг дій користувачів. Недостатня обізнаність може призвести до неусвідомленого виконання шкідливих дій, таких як відкриття фішингових листів або завантаження небезпечних програм. Недотримання політик безпеки, наприклад, використання слабких паролів або спільний доступ до облікових записів, також збільшує ризик несанкціонованого доступу до інформації. Організаційні вразливості включають недоліки в управлінні інформаційною безпекою, відсутність політик та процедур безпеки, а також недостатню підтримку з боку керівництва. Відсутність чітких політик та процедур може призвести до неконтрольованого доступу до інформації, неналежного управління інцидентами безпеки або відсутності резервного копіювання даних. Недостатня підтримка з боку керівництва може виявлятися у відсутності фінансування на заходи безпеки або недостатньому контролі за виконанням політик безпеки.

Загрози з боку постачальників та партнерів включають ризики, пов'язані з обробкою та зберіганням інформації третіми сторонами. Це можуть бути ненадійні постачальники програмного забезпечення, неналежний захист інформації у партнерів або недостатній контроль за доступом до інформаційних ресурсів з боку

третіх сторін. Використання програмного забезпечення з ненадійних джерел або партнерів з низьким рівнем безпеки може призвести до компрометації систем або втрати конфіденційної інформації.

1.2 Основні компоненти комплексної системи захисту інформації (КСЗІ)

Комплексна система захисту інформації (КСЗІ) складається з трьох основних компонентів: організаційних, технічних та фізичних заходів.

Організаційні заходи спрямовані на створення правил, процедур та політик, що забезпечують ефективне управління інформаційною безпекою. Це включає розробку політик безпеки, які регулюють доступ до інформаційних систем, використання паролів, управління даними та реагування на інциденти. Важливо також проводити регулярні тренінги для підвищення обізнаності співробітників щодо загроз та методів захисту, а також впроваджувати системи контролю доступу, які обмежують доступ до інформаційних ресурсів на основі ролей та повноважень. Управління інцидентами включає розробку планів реагування на інциденти та створення команди реагування, яка буде відповідати за моніторинг, аналіз та реагування на інциденти.

Технічні заходи включають використання різноманітних технологій та інструментів для захисту інформаційних систем від внутрішніх та зовнішніх загроз. Основними технічними засобами є міжмережеві екрани (фаєрволи), які контролюють та обмежують доступ до мережі підприємства, та системи виявлення та запобігання вторгнень (IDS/IPS), які моніторять мережевий трафік для виявлення підозрілої активності. Антивірусне програмне забезпечення захищає комп'ютерні системи від шкідливих програм, а криптографічні засоби забезпечують шифрування даних для їх конфіденційності. Системи резервного копіювання дозволяють відновити інформацію у разі її втрати, а системи управління подіями та інформацією безпеки (SIEM) централізовано збирають та аналізують дані про події безпеки.

Фізичні заходи спрямовані на захист інформаційних ресурсів від фізичних загроз, таких як крадіжка, пошкодження або знищення обладнання. Вони включають контроль доступу до приміщень за допомогою магнітних карток, біометричних ідентифікаторів та інших засобів, а також використання відеоспостереження та охоронних систем. Захист обладнання передбачає розміщення серверів у захищених приміщеннях, використання засобів захисту від електромагнітних впливів та пожежної безпеки. Крім того, важливо встановити автоматичні системи пожежогасіння та розробити плани дій у разі природних катастроф.

1.3 Роль управління ризиками в КСЗІ

Управління ризиками є одним з ключових елементів комплексної системи захисту інформації (КСЗІ) на підприємстві. Воно забезпечує ідентифікацію, оцінку, управління та моніторинг ризиків, пов'язаних із захистом інформаційних ресурсів. Розглянемо основні аспекти цього процесу детальніше.
Ідентифікація ризиків

Першим етапом ідентифікація ризиків є управління ризиками та їх ідентифікація. Цей процес включає визначення потенційних загроз та вразливостей, які можуть вплинути на інформаційні ресурси підприємства. Загрози можуть бути зовнішніми (кіберзлочинці, хакери, природні катастрофи) та внутрішніми (інсайдерські загрози, помилки співробітників). Вразливості можуть виникати через недоліки в програмному забезпеченні, неправильне налаштування систем або недостатню обізнаність співробітників щодо правил інформаційної безпеки. Ідентифікація ризиків є безперервним процесом, що вимагає постійного моніторингу та аналізу нових загроз і вразливостей.

Після ідентифікації ризиків наступним кроком є їх оцінка. Оцінка ризиків включає визначення ймовірності реалізації кожної загрози та потенційних наслідків для підприємства. Цей процес дозволяє пріоритизувати ризики за ступенем їхньої небезпеки та впливу на інформаційні ресурси. Оцінка ризиків може

проводитися за допомогою різних методів, таких як якісний та кількісний аналіз ризиків. Якісний аналіз включає експертну оцінку ризиків, тоді як кількісний аналіз базується на статистичних даних і математичних моделях.

Управління ризиками включає розробку та впровадження заходів, спрямованих на зниження ймовірності реалізації загроз або зменшення їх наслідків. Це може включати як технічні, так і організаційні заходи. Технічні заходи можуть включати впровадження антивірусного програмного забезпечення, міжмережевих екранів, систем виявлення та запобігання вторгнень, а також шифрування даних. Організаційні заходи включають розробку політик та процедур безпеки, проведення регулярних тренінгів для співробітників та створення команд реагування на інциденти. Важливо також передбачити резервне копіювання даних та розробку планів відновлення після інцидентів.

Моніторинг та перегляд ризиків є важливим елементом управління ризиками, який забезпечує постійний контроль за станом інформаційної безпеки та адаптацію до нових загроз. Моніторинг включає регулярний перегляд і оновлення оцінки ризиків, а також аналіз ефективності впроваджених заходів безпеки. Це дозволяє своєчасно виявляти нові ризики та коригувати стратегії управління ризиками. Перегляд ризиків також включає оновлення планів реагування на інциденти та резервного копіювання даних відповідно до змін у загрозах та вразливостях.

1.4 Огляд сучасних тенденцій та викликів у сфері захисту інформації

У сучасному світі, де інформаційні технології відіграють ключову роль у функціонуванні підприємств, захист інформації стає все більш складним та багатогранним завданням. Розвиток технологій, поява нових загроз та зміни у бізнес-середовищі постійно впливають на підходи до захисту інформації. Розглянемо основні сучасні тенденції та виклики у цій сфері. Однією з головних тенденцій у сфері інформаційних технологій є перехід на хмарні сервіси.

Хмарні технології дозволяють підприємствам зберігати дані та використовувати обчислювальні ресурси на віддалених серверах, що забезпечує

гнучкість та економію коштів. Однак використання хмарних сервісів також створює нові виклики для захисту інформації. Основні загрози включають можливість несанкціонованого доступу до даних, компрометацію облікових записів та вразливості у хмарних платформах. Щоб забезпечити безпеку даних у хмарі, необхідно впроваджувати такі заходи, як шифрування даних, контроль доступу, багатофакторна аутентифікація та регулярний аудит безпеки. Зростання використання мобільних пристроїв, таких як смартфони та планшети, створює додаткові вразливості для інформаційної безпеки. Мобільні пристрої часто використовуються для доступу до корпоративних даних та систем, що робить їх привабливою ціллю для зловмисників. Основні ризики включають крадіжку або втрату пристроїв, несанкціонований доступ до даних через незахищені мережі та встановлення шкідливих програм. Для захисту мобільних пристроїв необхідно впроваджувати політики безпеки, що включають використання шифрування, управління мобільними пристроями (MDM), контроль доступу та навчання користувачів правилам безпеки. Інтернет речей (IoT) є ще однією значущою тенденцією, яка створює нові виклики для захисту інформації. Підключення до мережі великої кількості пристроїв, таких як сенсори, побутові прилади та промислове обладнання, збільшує площу атаки та ускладнює управління безпекою. Основні загрози включають вразливості в прошивках пристроїв, недостатню аутентифікацію та можливість здійснення DDoS-атак через IoT-пристрої. Для забезпечення безпеки IoT необхідно впроваджувати заходи, такі як регулярне оновлення прошивки, використання сильних паролів, шифрування даних та ізоляція IoT-пристроїв від основної мережі.

Соціальна інженерія залишається однією з найбільш поширених та ефективних методів атак на інформаційні системи. Зловмисники використовують методи соціальної інженерії для маніпуляції людьми та отримання доступу до конфіденційної інформації. Це можуть бути фішингові атаки, де зловмисники надсилають підроблені електронні листи, які виглядають як повідомлення від легітимних джерел, або атаки через соціальні мережі. Для захисту від соціальної інженерії необхідно проводити регулярні тренінги для співробітників,

впроваджувати політики безпеки щодо обробки електронних листів та повідомлень, а також використовувати технічні засоби для виявлення та блокування фішингових атак.

Штучний інтелект (ШІ) та машинне навчання (МН) починають відігравати все більшу роль у захисті інформації. Ці технології можуть використовуватися для автоматичного виявлення та реагування на загрози, аналізу великих обсягів даних та прогнозування можливих атак. Наприклад, системи на базі ШІ можуть аналізувати мережевий трафік для виявлення аномалій або аналізувати поведінку користувачів для виявлення підозрілої активності. Однак зловмисники також можуть використовувати ШІ для розробки нових методів атак, що вимагає постійного вдосконалення захисних заходів.

1.5 Правові та нормативні вимоги у сфері інформаційної безпеки

Правові та нормативні вимоги у сфері інформаційної безпеки є важливим аспектом для забезпечення захисту інформаційних ресурсів підприємства. Вони встановлюють стандарти та правила, яких необхідно дотримуватися для мінімізації ризиків та забезпечення відповідності законодавчим вимогам.

В Україні основним документом, що регулює питання інформаційної безпеки, є Закон України "Про захист інформації в інформаційно-телекомунікаційних системах". Крім того, існують інші нормативно-правові акти, такі як закони про персональні дані, електронний цифровий підпис, державну таємницю тощо. Наприклад, Закон України "Про захист персональних даних" встановлює правила обробки та зберігання персональних даних, забезпечуючи захист приватності громадян.

Важливим є також дотримання міжнародних стандартів, таких як ISO/IEC 27001, який визначає вимоги до систем управління інформаційною безпекою. Цей стандарт допомагає організаціям створити, впровадити, підтримувати та постійно покращувати систему управління інформаційною безпекою (СУІБ). Інші

міжнародні стандарти, такі як ISO/IEC 27002, надають рекомендації щодо практичної реалізації заходів безпеки.

Крім національних і міжнародних стандартів, підприємства можуть також слідувати галузевим нормативам. Наприклад, для банківського сектора важливими є вимоги PCI DSS (Payment Card Industry Data Security Standard), що забезпечують захист даних платіжних карток. Для підприємств, що працюють у сфері охорони здоров'я, актуальними є вимоги HIPAA (Health Insurance Portability and Accountability Act), які регулюють захист медичних даних.

Дотримання правових та нормативних вимог не лише забезпечує захист інформаційних ресурсів, але й допомагає уникнути юридичних проблем та штрафів. Впровадження відповідних політик та процедур дозволяє підприємству відповідати вимогам регуляторів та клієнтів, забезпечуючи тим самим свою репутацію та конкурентоспроможність.

1.6 Огляд методологій та стандартів розробки КСЗІ

Існує багато методологій та стандартів, які можна використовувати для розробки та впровадження комплексних систем захисту інформації (КСЗІ). Вибір конкретної методології залежить від специфіки підприємства, його розміру, галузі діяльності та інших факторів.

Один із найпоширеніших стандартів у цій сфері є ISO/IEC 27001. Цей міжнародний стандарт визначає вимоги до систем управління інформаційною безпекою, спрямовані на захист інформаційних активів від різних загроз, забезпечення конфіденційності, цілісності та доступності інформації. Впровадження ISO/IEC 27001 дозволяє підприємствам систематично підходити до управління ризиками і забезпечувати високий рівень захисту інформації.

Методологія NIST (National Institute of Standards and Technology) є ще однією з популярних рамкових моделей для розробки КСЗІ. Вона включає п'ять основних функцій: ідентифікація, захист, виявлення, реагування та відновлення. Ці функції сприяють створенню комплексного підходу до управління ризиками інформаційної

безпеки, що дозволяє ефективно виявляти, уникати та відновлюватися після кіберзагроз.

Крім того, методології COBIT (Control Objectives for Information and Related Technologies) та ITIL (Information Technology Infrastructure Library) також мають вагому роль у розробці КСЗІ. COBIT надає набір стандартів для управління технологіями та інформаційною безпекою, тоді як ITIL зосереджується на керуванні інформаційними технологіями та сервісами. Використання цих методологій допомагає підприємствам створити систему управління інформаційною безпекою, що відповідає їхнім потребам і забезпечує стійкість до сучасних кіберзагроз.

1.7 Аналіз існуючих рішень та технологій для захисту інформації

Сучасний ринок інформаційної безпеки пропонує різноманітні рішення та технології, спрямовані на захист корпоративних ресурсів від кіберзагроз. Однією з ключових технологій є міжмережеві екрани (фаєрволи), які контролюють трафік мережі та фільтрують його з метою захисту від несанкціонованого доступу.

Системи виявлення та запобігання вторгнень (IDS/IPS) забезпечують нагляд за мережевим трафіком і вчасне виявлення підозрілих активностей, що дозволяє швидко реагувати на потенційні загрози.

Антивірусне програмне забезпечення використовується для захисту комп'ютерних систем від шкідливих програм, зокрема вірусів, троянів та червів, що можуть завдати значних збитків інформаційним ресурсам підприємства.

Криптографічні засоби гарантують конфіденційність і цілісність даних шляхом їх шифрування, що є важливим аспектом у забезпеченні безпеки інформаційних активів.

Системи управління подіями та інформацією безпеки (SIEM) забезпечують централізований збір і аналіз даних про події безпеки, що дозволяє ефективно виявляти та реагувати на потенційні загрози в реальному часі.

Технології резервного копіювання відновлюють доступ до даних у випадку їх втрати або пошкодження, забезпечуючи безперервну роботу підприємства та захист важливої інформації.

Хмарні технології забезпечують високий рівень захисту та доступності даних, що стає все більш популярним у відгуках нарощуванням масштабів діяльності підприємств та необхідністю зменшення витрат на IT-інфраструктуру та обслуговування.

Ці рішення та технології представляють собою комплексний підхід до захисту інформаційних ресурсів підприємства, що дозволяє забезпечити їх ефективний захист від сучасних кіберзагроз.

1.8 Виклики та перспективи впровадження КСЗІ в Україні

Впровадження комплексних систем захисту інформації (КСЗІ) в Україні стикається з низкою викликів, але має й перспективи для розвитку.

Одним з основних викликів є недостатнє фінансування та обмежені ресурси. Багато підприємств не мають достатніх коштів для впровадження сучасних технологій та рішень у сфері інформаційної безпеки. Це призводить до використання застарілих систем та методів захисту, що збільшує ризики.

Ще одним викликом є низький рівень обізнаності та підготовки кадрів. Відсутність кваліфікованих спеціалістів у сфері інформаційної безпеки ускладнює впровадження та підтримку КСЗІ на належному рівні.

Правова та нормативна база також потребує вдосконалення. Незважаючи на існування законодавчих актів у сфері інформаційної безпеки, їх виконання та контроль за дотриманням залишаються на недостатньому рівні.

Перспективи впровадження КСЗІ в Україні включають розвиток державних програм та ініціатив, спрямованих на підтримку інформаційної безпеки. Це може включати фінансову підтримку підприємств, проведення навчальних програм для підготовки кадрів та вдосконалення нормативно-правової бази.

Крім того, важливо розвивати співпрацю між державою, бізнесом та академічною спільнотою для створення ефективних рішень та підвищення рівня інформаційної безпеки на національному рівні. Це дозволить забезпечити захист інформаційних ресурсів підприємств та підвищити їх конкурентоспроможність на міжнародному ринку.

1.9 Постановка задачі

Для того щоб провести Комплексна система захисту інформації інформаційно -Комунікаційної системи ПрАТ "Інтеркорн" необхідно виконати наступні завдання:

- Зібрати дані про підприємство, виконати обстеження ОІД, обстеження інформаційного середовища та обстеження обчислювальної системи;
- Провести аналіз існуючого стану інформаційної безпеки;
- На підставі зібраних даних про об’єкт розробити модель загроз та модель порушника;
- Провести аналіз ризиків;
- Розробка політики інформаційної безпеки;
- Вибір і встановлення технічних засобів захисту:
- Тестування і оцінка ефективності після впровадження

Висновок до першого розділу

У цьому розділі ми детально розглянули основні аспекти інформаційної безпеки, які є критично важливими для функціонування будь-якого підприємства чи організації. Проаналізовано загрози та вразливості інформаційної безпеки, що можуть мати різні джерела та прояви, включаючи зовнішні, внутрішні, технічні, фізичні та організаційні фактори. Зокрема, ми зосередили увагу на хакерських атаках, шкідливому програмному забезпеченні, фішингових атаках, людських помилках, технічних вразливостях та фізичних загрозах.

Також було описано основні компоненти комплексної системи захисту інформації (КСЗІ), яка складається з організаційних, технічних та фізичних заходів. Організаційні заходи включають створення політик та процедур безпеки, проведення тренінгів для співробітників та управління інцидентами. Технічні заходи охоплюють використання міжмережевих екранів, систем виявлення та запобігання вторгнень, антивірусного програмного забезпечення, криптографічних засобів, резервного копіювання та систем управління подіями безпеки. Фізичні заходи забезпечують захист інформаційних ресурсів від фізичних загроз через контроль доступу, відеоспостереження, пожежну безпеку та захист обладнання.

Особливу увагу приділено ролі управління ризиками в КСЗІ. Управління ризиками включає ідентифікацію, оцінку, управління та моніторинг ризиків. Цей процес забезпечує визначення потенційних загроз та вразливостей, оцінку ймовірності їх реалізації та наслідків для підприємства, розробку та впровадження заходів для зниження ризиків, а також постійний моніторинг та адаптацію до нових загроз.

Таким чином, забезпечення інформаційної безпеки є складним і багатогранним процесом, який вимагає інтегрованого підходу з урахуванням різноманітних загроз та вразливостей. Ефективне управління інформаційною безпекою можливе лише за умови поєднання організаційних, технічних та фізичних заходів, а також постійного управління ризиками та моніторингу ситуації. Тільки таким чином підприємства зможуть забезпечити захист своїх інформаційних активів і стабільну роботу в умовах сучасних загроз інформаційної безпеки.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальні відомості про організацію

Назва підприємства: Приватне акціонерне товариство "Інтеркорн" (ПрАТ "Інтеркорн")

Основна діяльність: Виробництво кукурудзяних сиропів

Історія

ПрАТ "Інтеркорн" було засноване у 2003 році з метою забезпечення високоякісних кукурудзяних сиропів для харчової промисловості України та міжнародногоринку.

Опис діяльності та сновні продукти:

Кукурудзяний сироп з високим вмістом фруктози: Використовується у виробництві безалкогольних напоїв, випічки та кондитерських виробів.

Мальтозний кукурудзяний сироп: Застосовується у виготовленні пива, медових продуктів та цукерок.

Глюкозний сироп: Використовується у виробництві джемів, желе, морозива та соусів.

Розташування та інфраструктура

Адреса: вул. Маршала Малиновського, 120, м. Дніпро, Україна

Площа виробничих приміщень: 600 кв. м

Кількість співробітників: 15 Осіб

2.2 Організаційна структура підприємства

Підприємство працює кожен день з 08.00 – 17.00.

Графік роботи співробітників:

Директор, бухгалтери, енергетик, логісти, інженер, системний адміністратор, механік – 08.00 – 17.00 у будні дні. Перерва з 12.00 – 13.00.

Охоронці підприємства (3 на зміні) - 08.00-16.00, 16.00-24.00, 24.00-08.00.

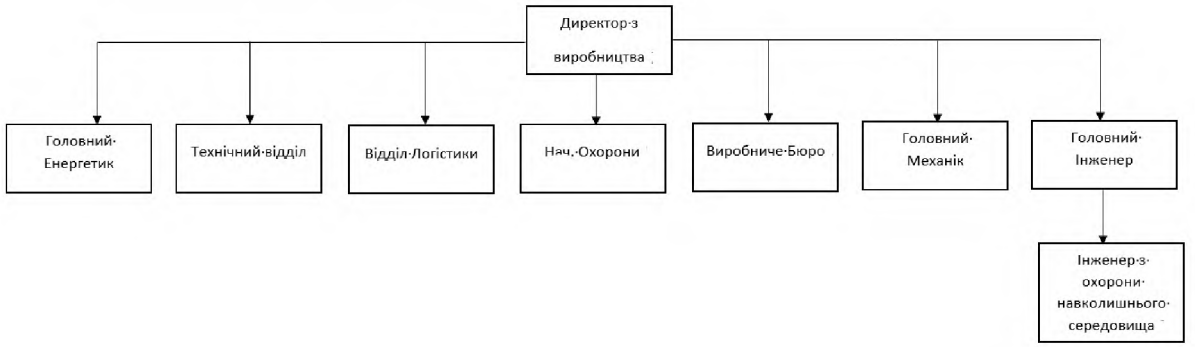


Рисунок 2.1 – Організаційна структура підприємства "ІНТЕРКОРН".

2.3 Обстеження об’єкта інформаційної діяльності

Об'єктом запровадження Комплексної системи захисту інформації є двоповерхова офісна будівля, розташування якої знаходиться в промзоні із високим рівнем руху транспортних засобів.

На першому поверсі знаходиться: КПП, Комора, Санвузол, Кімната охорони, Побутові приміщення, Кімната прибиральниць та водіїв.

На другому поверсі: Виробниче бюро, Головний інженер, Головний механік, Технічний відділ, Відділ логістики, Директор з виробництва.

2.4 Обстеження інформаційного середовища ПрАТ "Інтеркорн"

Згідно з НД ТЗІ 1.6-005-2013, на підприємстві ПрАТ "Інтеркорн" здійснюється обробка інформації з обмеженим доступом, яка включає технологічні дані про виробництво глюкозно-фруктозних сиропів, мальтозних сиропів та інші важливі дані про виробничі процеси. Ця інформація класифікується як конфіденційна згідно з вимогами НД ТЗІ, оскільки вона містить важливі дані про технологічні процеси та фінансовий стан підприємства.

Додатково, фінансові відомості, також класифіковані як конфіденційна інформація, включають в себе дані про фінансовий стан підприємства та бюджетні плани. Вони підлягають захисту від несанкціонованого доступу згідно з визначенням конфіденційності за НД ТЗІ 1.1-003-99.

ПрАТ "Інтеркорн" забезпечує дотримання встановлених вимог щодо захисту конфіденційної інформації шляхом впровадження відповідних технічних і організаційних заходів безпеки. Відповідно до вимог законодавства України, підприємство також підтверджує відсутність інформації, що є державною таємницею.

Додатково, підприємство підтверджує відсутність інформації, яка є державною таємницею, згідно з чинним законодавством України.

2.5 Обстеження обчислювальної системи ПрАТ "Інтеркорн"

На території об’єкту знаходиться 10 комп’ютерів, також в офісі знаходяться принтери, роутери, комутатори та серверна.

На усіх пристоях на підприємстві встановлено ліцензоване програмне забезпечення.

У кожного працівника підприємства є свій обліковий запис, доступ до якого має лише він. Забезпеченням роботи комп’ютерної техніки, комп’ютерної мережі і програмного забезпечення в організації займається системний адміністратор.

Використовувати зовнішні носії мають право лише директор з виробництва, та системний адміністратор. Усі співробітники мають доступ до Інтернету, але з обмеженням доступу до соціальних мереж.

Вихід комп'ютерів до мережі Інтернет забезпечується через кабель. На рисунку 2.2 зображена схема мережі інформаційно-комунікаційної системи ПрАТ "Інтеркорн"

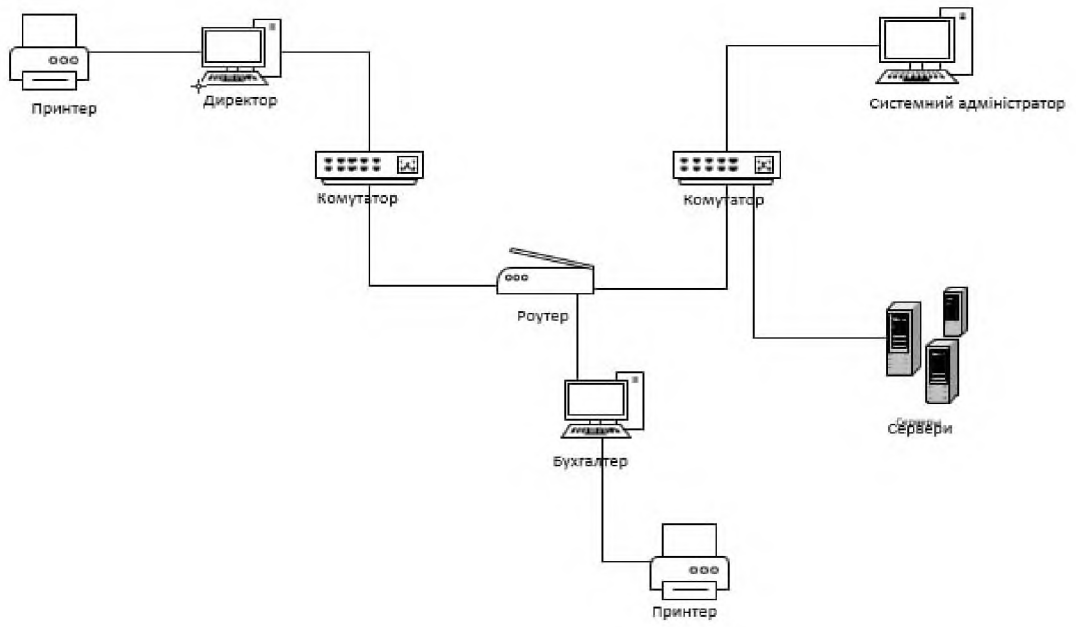


Рисунок 2.2 – Структурна схема мережі інформаційно- комунікаційної системи ПрАТ "Інтеркорн"

Також Згідно з вимогами НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу", ПрАТ "Інтеркорн" використовує автоматизовану систему третього класу. Ця система включає в себе розподілений багатомашинний багатокористувацький комплекс, призначений для обробки інформації різних категорій конфіденційності. Вона забезпечує ефективне управління і захист інформації, що обробляється, зокрема за допомогою відповідних технічних і організаційних заходів. Такий підхід дозволяє забезпечити високий рівень безпеки та захисту конфіденційної інформації, що є критичним для діяльності ПрАТ "Інтеркорн" в умовах сучасного інформаційного середовища.

У таблицях 2.1 і 2.2 представлений перелік апаратного і програмного забезпечення мережі ПрАТ "Інтеркорн"

Таблиця 2.1 – Апаратне забезпечення системи

№	Найменування	Характеристика	Кількість
1	Wi-Fi роутер	AX180 Dual Band WiFi 6 Router	2
2	Комутатор	Cisco CBS220-24P-4G-EU	2
3	Принтер	Canon i-SENSYS MF3010	3
4	Сервер	Patriot Tower E3-1220V3: Intel 1 Xeon Quad-Core E3-1220 v3 (3.1 ГГц)/ 8 ГБ/ 2 x Seagate ST500NM0011 500 ГБ, 64 МБ, Constellation ES, Serial ATA 6 Гбіт/с	1
5	Клавіатура	Logitech MK120	10
6	Робоча станція		10
7	Мишка	Logitech M220	10

Таблиця 2.2 – Програмне забезпечення системи

№	Тип програмного забезпечення	Найменування
1	Операційна система	Windows 10
2	Прикладне ПЗ	Microsoft Office 2021

Продовження таблиці 2.2

		Kaspersky Anti-Virus (антівірус)
		WinRaR (архіватор)
3	Операційна система (сервіс)	Microsoft Windows Server 2019

2.6 Аналіз існуючого стану інформаційної безпеки ПрАТ "Інтеркорн"

Аналіз існуючого стану інформаційної безпеки на підприємстві ПрАТ "Інтеркорн"

виявив кілька критичних аспектів, які потребують уваги. Офісне приміщення, розташоване на двох поверхах, має обмежені заходи контролю доступу. Вхід до офісу здійснюється через головний вхід з механічними замками, а доступ до окремих офісних кімнат також контролюється лише механічними замками. Серверна кімната, де розміщені сервери та мережеве обладнання, обладнана лише простим механічним замком, що створює ризик несанкціонованого доступу. IT-інфраструктура потребує покращення, оскільки сервери розміщені у виділеній серверній кімнаті без належної системи охолодження та контролю мікроклімату. Мережеве обладнання, таке як маршрутизатори і комутатори, розміщене без додаткового захисту. Комп'ютери співробітників не мають належного програмного захисту, зокрема антивірусних програм та міжмережевих екранів, а також відсутня централізована система оновлення програмного забезпечення.

Політика безпеки та управління доступом на підприємстві має значні прогалини. Більшість співробітників мають доступ до загальних ресурсів мережі без належного розподілу прав доступу. Не використовується двофакторна автентифікація для доступу до важливих систем, а паролі співробітників не відповідають вимогам складності і немає політики їх регулярної зміни. Фізична

безпека також потребує покращення. Відеоспостереження охоплює лише зовнішній периметр будівлі, тоді як внутрішні приміщення, включаючи серверну кімнату, не охоплені відеоспостереженням. Офісні приміщення не мають сучасної системи виявлення пожеж, відсутні датчики диму та системи автоматичного пожежогасіння.

На підставі проведеного аналізу було визначено, що для забезпечення належного рівня інформаційної безпеки на підприємстві необхідно вжити низку заходів. Рекомендується встановити електронні системи контролю доступу до всіх приміщень, включаючи серверну кімнату, з використанням карткового доступу або біометричної автентифікації. Необхідно впровадити антивірусне програмне забезпечення та міжмережеві екрани на всіх робочих станціях, а також встановити централізовану систему оновлення програмного забезпечення.

Важливо посилити фізичну безпеку шляхом встановлення систем відеоспостереження у внутрішніх приміщеннях та обладнати офісні приміщення сучасними системами виявлення пожеж і автоматичного пожежогасіння. Оновлення політик безпеки включатиме впровадження розподілу прав доступу до мережевих ресурсів, встановлення вимог до складності паролів та політики їх регулярної зміни, а також впровадження двофакторної автентифікації для доступу до критичних систем.

Ці заходи допоможуть забезпечити належний рівень захисту інформації на підприємстві ПрАТ "Інтеркорн" і відповідатимуть вимогам стандартів інформаційної безпеки.

На генеральному плані підприємства (рисунок 2.3) та (рисунок 2.4) показане розміщення основних офісних приміщень на підприємстві та обчислювальної системи.

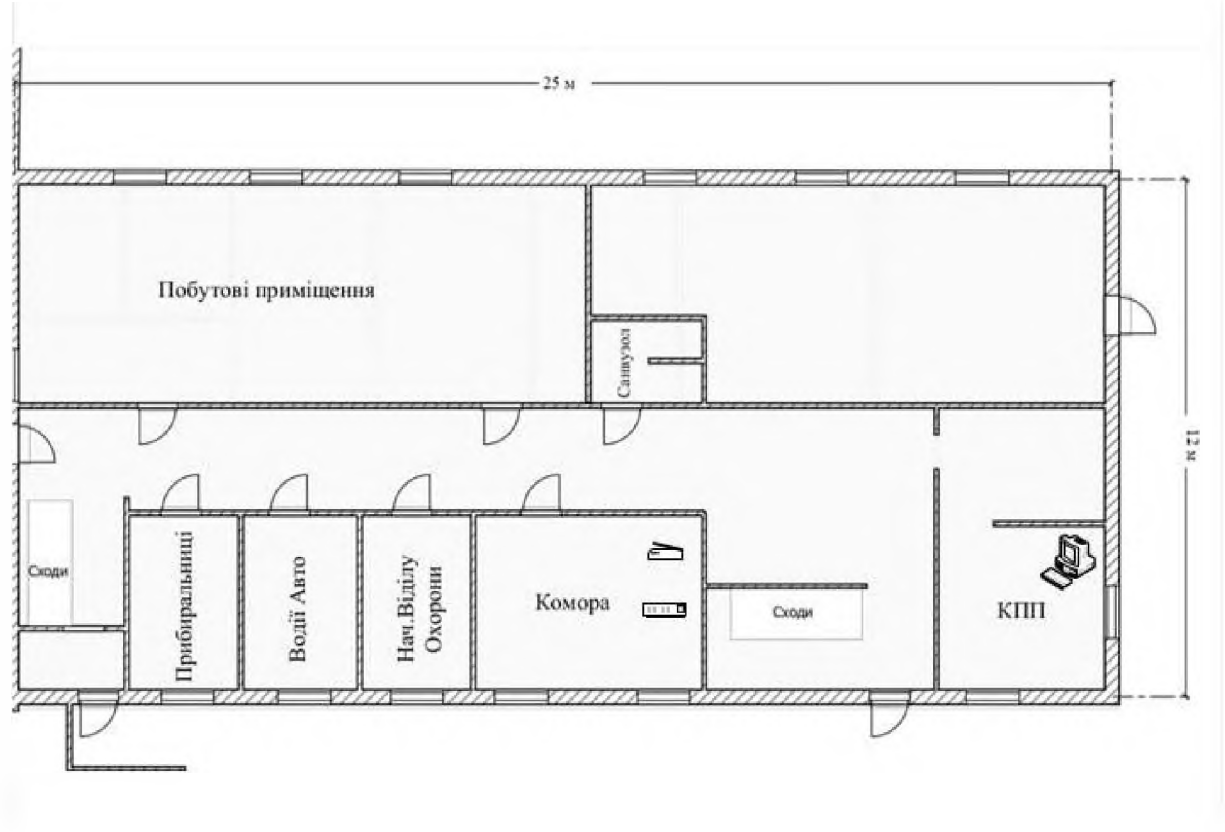


Рисунок 2.3 Генеральний план ПрАТ "Інтеркорн"1 поверх

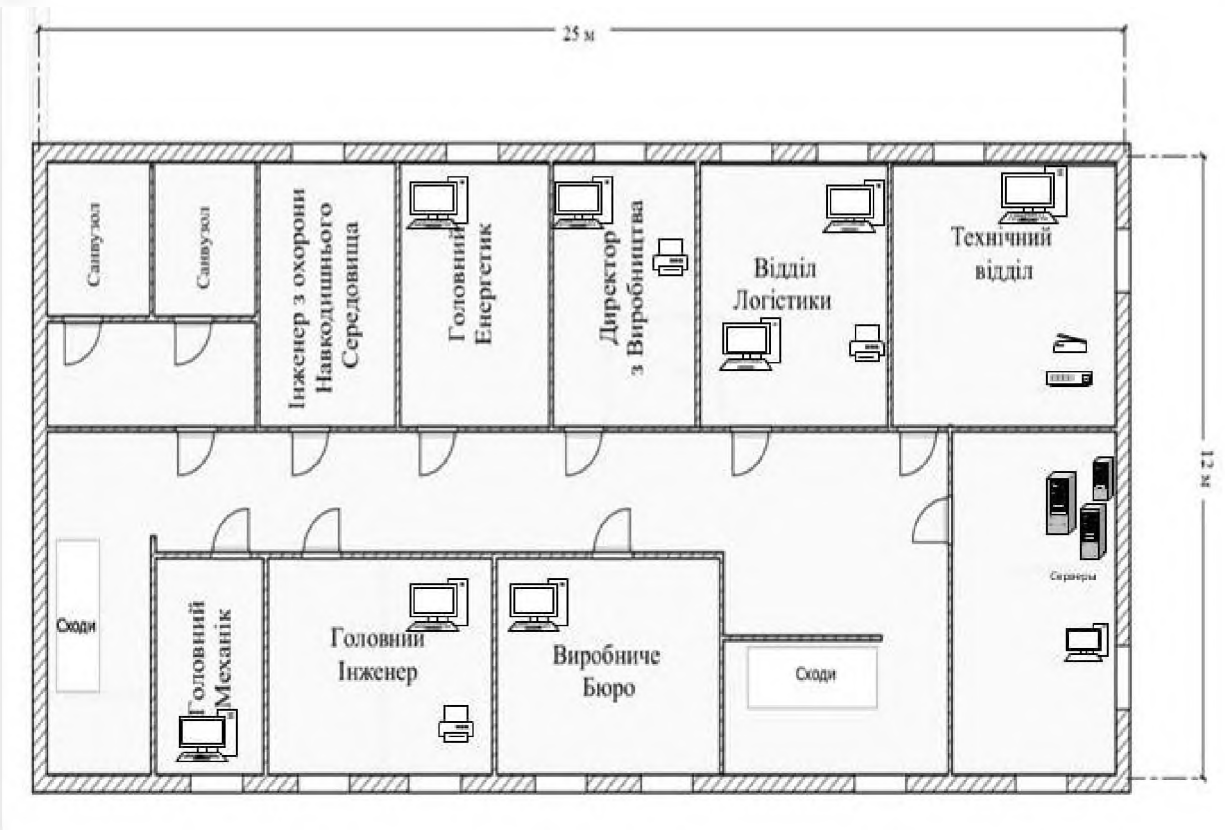


Рисунок 2.4 Генеральний план ПрАТ "Інтеркорн" 2 поверх

Фізична характеристика об’єкта інформаційної діяльності:

- товщина несучих стін - 0,45 м;
- товщина перекритя - 125 мм;
- стеля - залізобетонна монолітна заливна товщиною 155 мм;
- склад стін - залізобетонні конструкції, висота перекриттів 2,8 м
- склад перегородок – цегла;
- підлога - монолітна бетонна стяжка товщиною 105 мм;
- покриття підлоги – ламінат 12 мм;
- вікна 1 поверх – 13 штук, зроблені з металопластику, розмірами 1300мм*1500мм, з 2-камерним склопакетом;
- вікна 2 поверх – 15 штук, зроблені з металопластику, розмірами 1300мм*1500мм, з 2-камерним склопакетоп.
- внутрішні двері 1 поверх – 7 штук, зроблені з дерева зі шпоном, розміром 800 мм * 2000мм;
- внутрішні двері 2 поверх – 12 штук, зроблені з дерева зі шпоном, розміром 800 мм * 2000мм;
- зовнішні двері – 5 штук, зроблені із алюмінію з використанням теплого профілю, оздоблені двосистемним замок, розміром 1000 мм * 2000мм;

Електропостачання здійснюється через підключення до трансформаторної підстанції, виходить за межі контрольованої зони, на об’єкті є Інтернет і телефонний зв'язок.

Підприємство обладнано системою контролю доступу. Режим доступу здійснюється через контрольно-пропускний пункт (тобто вхід в будівлю здійснюється за пропусками та через охорону).

2.7 Модель порушника

Порушники бувають двох видів, внутрішні (ті, що працюють в організації) та зовнішні (наприклад, водії чи кліенти).

Порушниками можуть бути:

- персонал підприємства;
- водії що привозять продукцію;
- клієнти, партнери;
- конкуренти;
- кримінальні організації;
- персонал керуючої компанії котра обслуговує комунікації (наприклад, Internet, водопостачання, мобільний зв'язок).

Відповідно до НД ТЗІ 1.4-001-200, порушники класифікуються за кількома критеріями, такими як рівень можливостей, знання, методи і способи, а також місце здійснення дій.

На найнижчому рівні можливостей користувачі можуть лише використовувати систему та запускати задані програми для обробки інформації.

На середніх рівнях вони можуть створювати власні програми, що розширюють функціонал обробки даних.

У високих рівнях можливостей користувачі можуть керувати програмним забезпеченням системи, включаючи проектування, реалізацію, впровадження та підтримку програмно-апаратного забезпечення з новими функціями обробки інформації.

Порушники систем класифікуються за рівнем знань на декілька категорій.

Найнижчий рівень знань відображає тих, хто не має достатньої інформації про автоматизовані системи.(АС)

Середній рівень знань описує осіб, які знають функціональні особливості системи та базові аспекти управління даними і можуть користуватися стандартними засобами.

Високий рівень знань характеризує тих, хто має значний досвід у роботі з технічними засобами, глибокі знання в області обчислювальної техніки та програмування, а також розуміння захисних засобів та їх функціональних можливостей.

Порушники класифікуються за використовуваними методами і способами на кілька категорій.

Найнижчий рівень включає тих, хто використовує лише агентурні методи для отримання інформації.

На середньому рівні знаходяться особи, що використовують технічні засоби для перехоплення інформаційних сигналів. Далі йдуть ті, хто використовує недоліки в проектуванні КСЗІ або стандартні засоби АС для спроб несанкціонованого доступу.

Найвищий рівень знань описує осіб, які активно впливають на систему, змінюючи її конфігурацію через підключення додаткового обладнання, модифікацію штатних засобів, а також використання спеціалізованого програмного забезпечення. добавь ще трохи інформації сюди

Згідно з класифікацією за місцем дії, порушники можуть бути розділені на наступні категорії:

Не мають доступу на контрольовану територію та не мають доступу до автоматизованих систем підприємства.

Володіють доступом на контрольовану територію, але не мають можливості доступу до автоматизованих систем.

Володіють доступом до робочих місць користувачів автоматизованих систем.

Володіють доступом до місць накопичення та зберігання даних.

Володіють доступом до засобів керування комплексною системою захисту інформації та до засобів адміністрування автоматизованих систем.

Внаслідок проведення аналізу можливих порушників складено модель порушника, яка наведена у таблиці 2.7

Таблиця 2.3 – Модель порушника

№	Порушник	За рівнем можливостей	За рівнем знань	За використовуваними Методами і способами
		Внутрішні		
1	Директор	Високий	Високий	Адміністративні, організаційні
2	Інженер	Високий	Високий	Технічні, інженерні
3	Логіст	Середній	Середній	Організаційні, логістичні
4	Енергетик	Середній	Середній	Технічні
5	Механік	Середній	Середній	Технічні
6	Охорона	Середній	Середній	Фізичні, контрольні
7	Бухгалтер	Високий	Високий	Адміністративні, фінансові
8	Системний адміністратор	Високий	Високий	Технічні, IT
9	Прибиральниці	Низький	Низький	Фізичні, господарські
		Зовнішні		
10	Водії	Низький	Низький	Логістичні, транспортні
11	Партнери	Середній	Середній	Бізнесові, партнерські

Продовження таблиці 2.3

12	Кримінальні організації;	Високий	Високий	Злочинні, силові, хакерські
13	Персонал керуючої компанії комунікацій	Середній	Середній	Технічні, організаційні

2.8 Аналіз ризиків

У цьому розділі проведено комплексний аналіз потенційних загроз і вразливостей інформаційної безпеки на підприємстві. Основні аспекти аналізу включають виявлення та оцінку різних видів ризиків, що можуть вплинути на нормальну роботу організації та безпеку її інформаційних активів.

Віповідно до ISO/IEC 27000 аналіз ризику це - процес розуміння характеру ризику і визначення рівня ризику.

Для проведення аналізу ризику необхідно:

- визначити види інформації, які можуть бути пошкоджені;
- оцінити ймовірність реалізації загрози;
- оцінити величину збитків;
- визначити ймовірні наслідки;
- фінансові втрати;
- зниження продуктивності праці;
- неприємності для підприємства (які впливають на рівень суспільної довіри)

Таблиця 2.4 – Аналіз ризиків

№	Загроза	Інформація, що може бути пошкоджена	Ймовірність реалізації загрози	Величина збитків	Ризик	Імовірні наслідки
1	Кібератака на систему управління виробництвом	Дані про процеси виробництва	Висока	Висока	Високий	Перерва в виробництві, втрати даних
2	Витік конфіденційної технологічної інформації	Інноваційні розробки, технології	Середня	Висока	Високий	Втрата конкурентоспроможності, зниження прибутковості
3	Неавторизований доступ до обладнання для обробки продуктів	Якість харчових продуктів	Висока	Висока	Високий	Порушення стандартів безпеки, втрата довіри клієнтів
4	Втрата ключового персоналу знань	Експертні знання та навички	Середня	Висока	Високий	Зниження продуктивності, затримки в розробці нових продуктів
5	Пожежа в офісних приміщеннях	Важливі документи та обладнання	Середня	Висока	Високий	Втрата матеріальних цінностей, затримки в роботі

6	Фізичне вторгнення в офісні приміщення	Конфіденційні документи та обладнання	Низька	Висока	Середній	Втрата конфіденційності, виток інформації
7	Екологічна аварія (викиди, забруднення)	Екологічні стандарти та дозволи	Середня	Висока	Високий	Закриття виробництва, штрафи, втрата репутації
8	Соціальні конфлікти (страйки, соціальні протести)	Порушення виробничих процесів	Низька	Висока	Середній	Втрата часу, зниження продуктивності
9	Крадіжка інформації або носіїв інформації	Конфіденційна інформація, документи	Середня	Висока	Високий	Витік конфіденційної інформації, втрата довіри клієнтів

Продовження таблиці 2.4

У представленій таблиці 2.4 досліджені ймовірності реалізації загроз і величини збитків, та вказані ймовірні наслідки, які можуть виникнути. Найвищий рівень ризику мають такі загрози:

- Кібератака на систему управління виробництвом;
- Неавторизований доступ до обладнання для обробки продуктів

2.9 Розробка політики інформаційної безпеки

Політика інформаційної безпеки ПрАТ "Інтеркорн" має на меті забезпечити захист конфіденційної та внутрішньої інформації підприємства, а також відповідність законодавчим та нормативним вимогам. Основними цілями цієї політики є запобігання витоку даних, забезпечення їх цілісності та доступності. Політика поширюється на всіх співробітників, підрядників і партнерів ПрАТ "Інтеркорн" і охоплює всі інформаційні системи, мережі, пристрої та дані компанії.

Відповідальність за розробку, впровадження та підтримку політики інформаційної безпеки покладається на CISO (Chief Information Security Officer), який також контролює виконання політики та проведення аудиту. Комітет з інформаційної безпеки, що складається з представників IT-відділу, відділу кадрів та юридичного відділу, підтримує CISO у прийнятті рішень щодо безпеки. IT-відділ відповідає за технічну реалізацію заходів безпеки, здійснює моніторинг та підтримку інформаційних систем. Користувачі зобов'язані дотримуватися політики та правил інформаційної безпеки, а також брати участь у тренінгах та навчаннях з інформаційної безпеки.

В рамках оцінки ризиків проводиться ідентифікація загроз, таких як кібератаки на систему управління виробництвом, витік конфіденційної технологічної інформації, неавторизований доступ до обладнання для обробки продуктів, пожежа в офісних приміщеннях, крадіжка інформації або носіїв інформації. Оцінка ймовірності реалізації загроз показує, що кібератаки та неавторизований доступ мають високу ймовірність, витік технологічної інформації, пожежа та крадіжка інформації – середню. Визначення потенційного впливу загроз на бізнес включає втрату конфіденційності, зниження продуктивності, втрати даних, матеріальні збитки та втрату довіри клієнтів.

Політика та процедури управління доступом передбачають встановлення прав доступу до інформації на основі ролей і обов'язків співробітників, використання багатофакторної аутентифікації для критичних систем. Дані класифікуються за рівнями конфіденційності (конфіденційна, внутрішня,

загальнодоступна) та захищаються відповідно до їх класифікації. Управління інцидентами включає процедури повідомлення про інциденти безпеки, план реагування на інциденти та відновлення після них. Навчання персоналу передбачає регулярні тренінги з інформаційної безпеки для всіх співробітників та оновлення знань про нові загрози та методи захисту.

Технічні та організаційні заходи включають використання шифрування для захисту даних під час передачі та зберігання, встановлення антивірусного програмного забезпечення на всі пристрої та його регулярне оновлення, відстеження та запис дій користувачів і систем для виявлення порушень, а також захист фізичних місць зберігання інформації за допомогою систем контролю доступу та відеоспостереження.

Впровадження політики здійснюється через інформування всіх співробітників про політику інформаційної безпеки, розсилку внутрішніх документів та інструкцій, проведення регулярних тренінгів для співробітників щодо правил інформаційної безпеки, оцінку знань співробітників та їх готовності дотримуватися політики, включення політики в усі бізнес-процеси компанії та забезпечення відповідності політики при зміні процесів або впровадженні нових технологій.

Регулярні перевірки передбачають періодичні перевірки дотримання політики, проведення внутрішніх перевірок для оцінки ефективності заходів безпеки. Аудити, включаючи внутрішні та зовнішні, допомагають оцінити ефективність політики та підготувати рекомендації для вдосконалення заходів безпеки. Звіти про стан інформаційної безпеки готуються для керівництва, включаючи результати аудитів та перевірок.

Політика передбачає регулярне оновлення відповідно до нових загроз та технологій, аналіз інцидентів для вдосконалення заходів безпеки, збирання зворотного зв'язку від користувачів для вдосконалення політики, врахування пропозицій співробітників при оновленні політики.

Таким чином, політика інформаційної безпеки ПрАТ "Інтеркорн" спрямована на забезпечення надійного захисту інформаційних активів компанії та підтримку високого рівня інформаційної безпеки.

Таблиця 2.5 Таблиця відповідальних осіб та ролей

Роль	Відповідальність
CISO	Розробка, впровадження та підтримка політики, проведення аудиту
Комітет з інформаційної безпеки	Підтримка CISO, прийняття рішень щодо безпеки
IT-відділ	Технічна реалізація заходів безпеки, моніторинг систем
Користувачі	Дотримання політики, участь у тренінгах

Таблиця 2.6 класифікації даних

Рівень конфіденційності	Типи даних	Заходи захисту
Конфіденційна	Технологічна інформація, фінансові дані	Шифрування, обмежений доступ
Внутрішня	Операційні дані, внутрішня кореспонденція	Захист паролем, обмежений доступ
Загальнодоступна	Публічні звіти, маркетингові матеріали	Захист від неавторизованих змін

2.10 Вибір і встановлення технічних засобів захисту.

На основі проведеного аналізу існуючого стану інформаційної безпеки на підприємстві та аналізу ризиків буде впроваджено технічні засоби захисту в ПрАТ "Інтеркорн", що сприятиме мінімізації ризиків та забезпечить надійний захист інформаційних ресурсів підприємства.

Використання сучасних технічних засобів захисту, таких як системи контролю доступу, відеоспостереження, картридери та інші, вимагає комплексного підходу та детального аналізу потреб інформаційної безпеки компанії. Будуть впроваджені та інтегровані вибрані технічні засоби захисту, а також їхні переваги і можливі обмеження в контексті унікальних потреб ПрАТ "Інтеркорн".

Для забезпечення безпеки та захисту інформаційних ресурсів на підприємстві заплановано впровадити комплекс заходів. На першому та другому поверсі офісних приміщень буде встановлено камери відеоспостереження з функцією запису відео в реальному часі, нічним режимом і обробкою образу для забезпечення візуального моніторингу. Також будуть встановлені датчики руху для виявлення активності в зоні покриття, датчики пожежі для раннього виявлення диму та вогню, а також датчики відкриття вікон для моніторингу доступу через віконні конструкції.

Для забезпечення фізичної безпеки та обмеження доступу до об'єктів впроваджується картридерний контроль доступу до входу в офіс та до серверної кімнати. Це дозволить точно ідентифікувати та авторизувати користувачів за допомогою карток доступу, забезпечуючи обмежений фізичний доступ.

Інтеграція системи контролю доступу з антивірусним програмним забезпеченням та системами виявлення та запобігання вторгнень (IDS/IPS) забезпечить повний спектр захисту інформаційних ресурсів компанії. Система контролю доступу регулюватиме фізичний доступ до серверних приміщень, забезпечуючи лише авторизований доступ. Антивірусне ПЗ забезпечить надійний захист від вірусів та інших загроз на робочих станціях, з автоматичними оновленнями вірусних баз даних і проактивним виявленням нових загроз. IDS/IPS буде моніторити мережевий трафік для виявлення аномальної активності та негайного реагування на потенційні вторгнення, що забезпечить високий рівень інформаційної безпеки компанії.

Мережу поділено на мережеві (робочі) групи – директор, заступник директора, системний адміністратор, бухгалтер, інші користувачі. Кожна з цих мережевих груп має доступ лише до певної інформації та програм.

На оновленому генеральному плані підприємства (рисунок 2.1) показане розміщення основних технічних засобів, а також обладнання нового Комплексу Системи Захисту Інформації ПрАТ "Інтеркорн". Умовні позначення цих об'єктів наведені в таблиці 2.1.

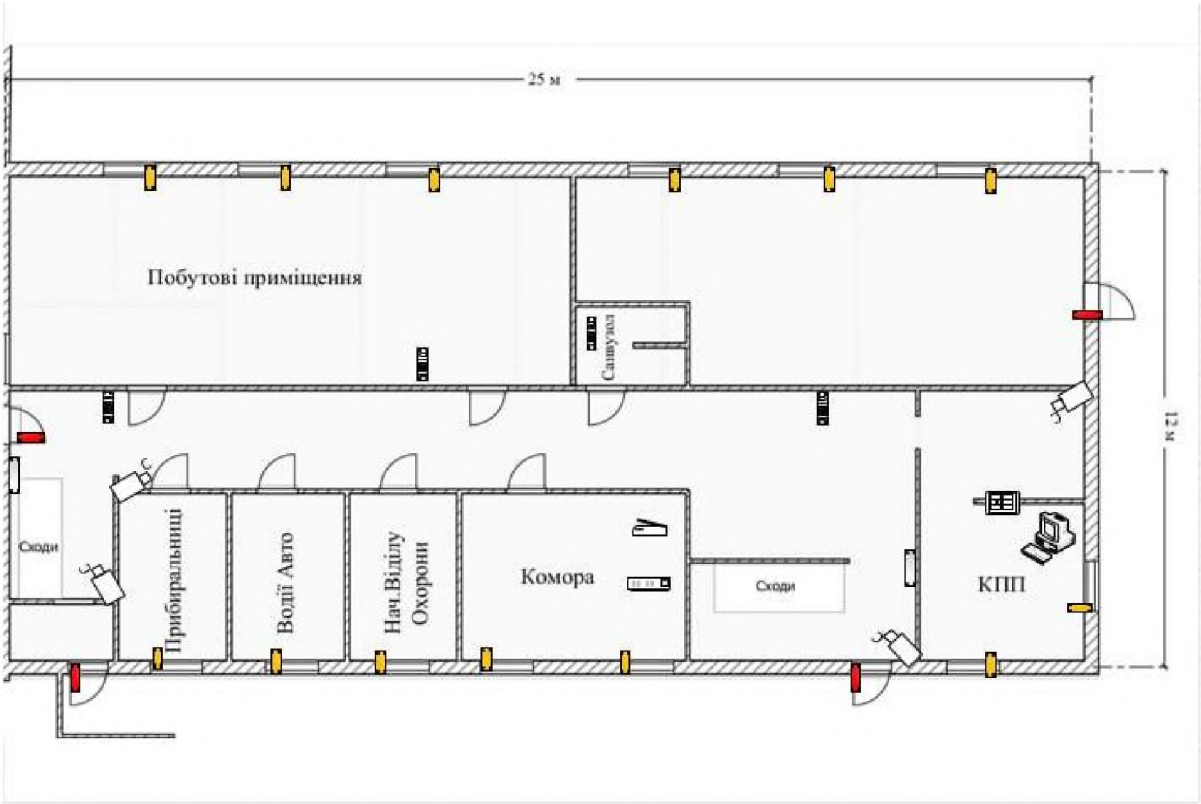


Рисунок 2.5 Генеральний план ПрАТ "Інтеркорн" 1 поверх після впровадження КСЗІ.

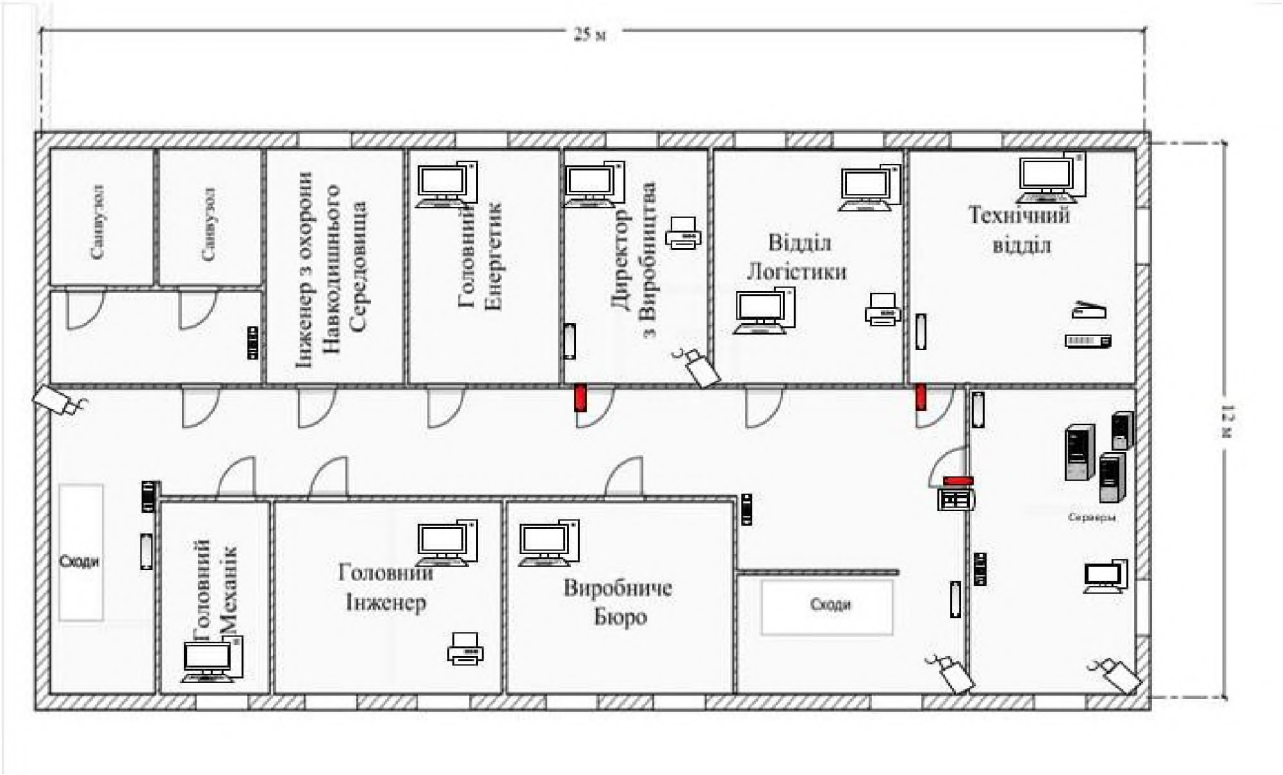
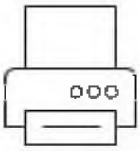
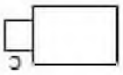
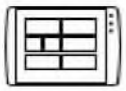


Рисунок 2.6 Генеральний план ПрАТ "Інтеркорн" 2 поверх після впровадження КСЗІ.

Таблиця 2.7 – Умовні позначення

№	Позначка на плані	Значення
1		Комп’ютер
2		Принетер
3		Камера

Продовження таблиці 2.7

4		Сервери
5		Картрідер
6		Датчик руху
7		Пожежний датчик
8		Датчик відкриття вікон
9		Датчик відкриття дверей
10		Комутатор
11		Роутер

Таблиця 2.8 – Апаратне забезпечення системи після впровадження КСЗІ

№	Найменування	Характеристика	Кількість
1	Камера	Hikvision DS-2CD1021-I(F)	8
2	Картрідер	Manhattan Smart Card N USB 2.0	2
3	Датчик руху	Crow Swan PGB	7
4	Пожежний датчик	Артон СПД-3.10	8
5	Датчик відкриття вікон	CoVi Security MC-25	13
6	Датчик відкриття дверей	CoVi Security MC-25	7

Після інтегрування нового апаратного забезпечення у вже наявну обчислювальну систему у комплексі системи захисту інформації (КСЗІ) на підприємстві ПрАТ "Інтеркорн" встановлено ряд нових програмних рішень, які сприятимуть підвищенню рівня безпеки та ефективності інформаційної інфраструктури. Одним із ключових кроків є встановлення системи управління інформаційною безпекою (ISMS). Наприклад, сертифікаційні програми, такі як ISO/IEC 27001, що пропонуються BSI Group або LRQA, допоможуть контролювати та вдосконалювати процеси інформаційної безпеки, забезпечуючи відповідність міжнародним стандартам.

Далі необхідно розглянути системи управління подіями та інформацією безпеки (SIEM). Програмні рішення, такі як Splunk, IBM QRadar або ArcSight, дозволяють централізовано збирати, аналізувати та реагувати на події безпеки в режимі реального часу. Це забезпечує швидке виявлення та усунення загроз, мінімізуючи потенційні ризики для підприємства.

Системи виявлення та запобігання вторгнень (IDS/IPS), такі як Snort, Suricata або Cisco Firepower, є важливим елементом захисту мережі від несанкціонованих вторгнень. Вони постійно моніторять мережевий трафік та

виявляють підозрілу активність, що дозволяє своєчасно реагувати на потенційні загрози.

Антивірусне та антималварне програмне забезпечення, наприклад, Symantec Endpoint Protection, McAfee Total Protection або Kaspersky Anti-Virus, забезпечує захист комп'ютерних систем від шкідливих програм, таких як віруси, трояни та черви. Це програмне забезпечення виконує регулярні сканування системи, забезпечуючи її чистоту та безпеку.

Криптографічні засоби, такі як VeraCrypt, BitLocker або PGP (Pretty Good Privacy), забезпечують шифрування даних, що є важливим для захисту конфіденційної інформації. Шифрування гарантує, що навіть у разі несанкціонованого доступу до даних вони залишатимуться недоступними для зловмисників.

Системи управління подіями та інформацією безпеки (SIEM), такі як Veeam Backup & Replication, Acronis Backup або Commvault, забезпечують резервне копіювання та відновлення даних у випадку їх втрати або пошкодження. Це дозволяє зберегти важливу інформацію та швидко відновити роботу після інциденту.

Хмарні технології, які стають все більш популярними для зберігання та обробки даних, забезпечують високий рівень захисту та доступності інформації, а також дозволяють знизити витрати на інфраструктуру та обслуговування. Використання хмарних сервісів дозволяє підприємству зосередитися на своїй основній діяльності, не турбуючись про підтримку складної IT-інфраструктури.

Крім того, системи моніторингу мережевого трафіку та управління, такі як Nagios, Zabbix або SolarWinds Network Performance Monitor, допомагають відстежувати мережевий трафік та виявляти аномальні дії, що може свідчити про потенційні загрози. Це дозволяє своєчасно реагувати на інциденти та запобігати їх розвитку.

Програмне забезпечення для управління ризиками, наприклад, RSA Archer, LogicGate або RiskWatch, дозволяє оцінювати та керувати ризиками, пов'язаними з інформаційною безпекою. Це забезпечує систематичний підхід до виявлення,

оцінки та мінімізації ризиків, що сприяє підвищенню загального рівня безпеки підприємства.

Окрему увагу варто приділити платформам для проведення навчань з інформаційної безпеки, таким як KnowBe4, PhishMe або SANS Security Awareness. Ці платформи допомагають підвищити обізнаність співробітників щодо сучасних загроз та методів захисту, що є критично важливим для запобігання інцидентам, пов'язаним із людським фактором.

Встановлення цих систем та програмного забезпечення дозволить значно підвищити рівень захисту інформаційних активів підприємства ПрАТ "Інтеркорн" та забезпечити відповідність нормативним вимогам у сфері інформаційної безпеки. Це сприятиме зміцненню довіри клієнтів та партнерів, а також підвищить конкурентоспроможність підприємства на ринку.

Таблиця 2.9 – Програмне забезпечення системи після впровадження КСЗІ на підприємстві

№	Тип програмного забезпечення	Найменування
1	Система управління інформаційною безпекою (ISMS)	ISO/IEC 27001
2	Система управління подіями та інформацією безпеки (SIEM)	IBM QRadar,
3	Системи виявлення та запобігання вторгнень (IDS/IPS)	Cisco Firepower
4	Антивірусне та антималварне програмне забезпечення	Kaspersky Anti-Virus
5	Криптографічні засоби	BitLocker,

Продовження таблиці 2.9

6	Системи резервного копіювання та відновлення даних	Acronis Backup,
7	Системи моніторингу мережевого трафіку та управління	Nagios,
8	Програмне забезпечення для управління ризиками	LogicGate,
9	Платформи для проведення навчань з інформаційної безпеки	SANS Security Awareness

2.11 Тестування і оцінка ефективності після впровадження КСЗІ

На підприємстві ПрАТ "Інтеркорн" було проведено тестування ефективності впровадженого Комплексного Захисту Інформації (КСЗІ) з метою оцінки заходів безпеки та їх відповідності вимогам безпеки і стандартам. Основні етапи тестування включали перевірку фізичного захисту та програмного забезпечення.

Щодо фізичного захисту, було протестовано картрідери для контролю доступу, датчики руху, вікна та двері, відеокамери і пожежні датчики. Всі системи продемонстрували надійність і вчасність реагування на події, що відбуваються.

У рамках тестування програмного забезпечення перевірялися системи управління інформаційною безпекою (ISMS), система управління подіями та інформацією безпеки (SIEM), системи виявлення та запобігання вторгнень (IDS/IPS), антивірусне та антималварне програмне забезпечення, криптографічні засоби, системи резервного копіювання та відновлення даних, системи моніторингу мережевого трафіку та управління, програмне забезпечення для управління ризиками та платформи для навчання з інформаційної безпеки.

Після завершення тестування було зроблено оцінку ефективності впровадженого КСЗІ. Фізичний захист та програмне забезпечення показали

високий рівень працездатності та відповідності вимогам безпеки. Системи виявлення вторгнень були успішними у виявленні та блокуванні потенційних загроз, а системи управління ризиками і моніторингу мережевого трафіку забезпечили ефективне управління безпекою. Виявлені в ході тестування вразливості були оперативно усунуті, що підвищило загальний рівень захисту інформації на підприємстві.

Загальна оцінка показала, що Комплексний Захист Інформації успішно зменшив загрози та покращив рівень безпеки інформації на ПрАТ "Інтеркорн", відповідаючи сучасним вимогам і стандартам безпеки.

Для більш детального розуміння та наочної демонстрації змін у ризиках інформаційної безпеки до і після впровадження Комплексної Системи Захисту Інформації (КСЗІ) було проведено додатковий аналіз ризиків. Цей аналіз включав ідентифікацію основних загроз, оцінку ймовірності їх виникнення та можливого впливу на інформаційні активи підприємства ПрАТ "Інтеркорн".

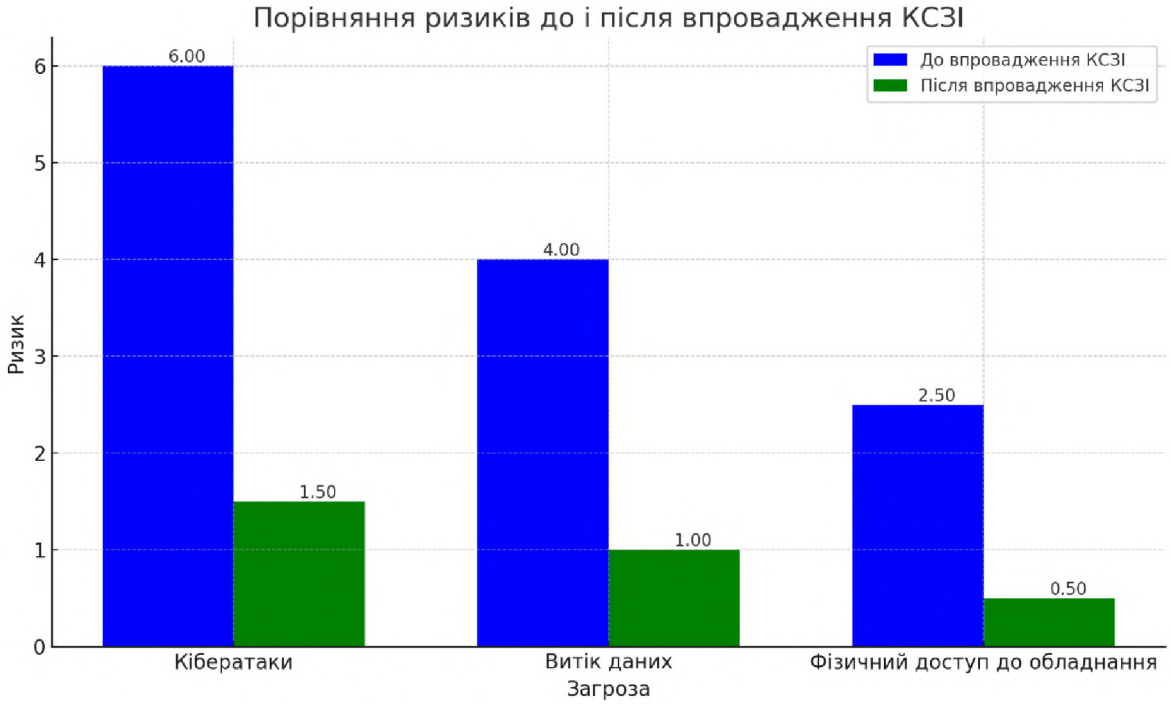


Рисунок 2.7 - Діаграма ризиків

Висновок до другого розділу

У даному розділі проведено всебічний аналіз та оцінку різних аспектів інформаційної безпеки на підприємстві ПрАТ "Інтеркорн". Проведена робота

включала обстеження організаційної структури, інформаційного середовища, обчислювальної системи та існуючого стану інформаційної безпеки підприємства. Також було розроблено модель порушника, проведено аналіз ризиків та розроблено політику інформаційної безпеки.

Загальні відомості про організацію та її організаційну структуру допомогли визначити ключові підрозділи та ролі, відповідальні за інформаційну безпеку. Це створило основу для подальших обстежень та аналізів, які забезпечили глибоке розуміння специфіки інформаційної діяльності підприємства.

Обстеження об'єкта інформаційної діяльності та інформаційного середовища ПрАТ "Інтеркорн" дозволило ідентифікувати критичні інформаційні активи, визначити місця їх розміщення та способи доступу до них. Це стало важливим етапом у виявленні потенційних вразливостей та загроз для інформаційної безпеки.

Аналіз обчислювальної системи ПрАТ "Інтеркорн" дав змогу оцінити існуючий стан технічної інфраструктури, виявити можливі проблеми та визначити напрями для покращення. На основі цього аналізу було зроблено висновки щодо необхідності впровадження додаткових заходів захисту.

У результаті аналізу існуючого стану інформаційної безпеки було визначено основні загрози та вразливості, з якими стикається підприємство. Це дало змогу розробити модель порушника, що враховує потенційні сценарії атак та їх ймовірність.

Аналіз ризиків включав ідентифікацію загроз, оцінку їх ймовірності та впливу на інформаційні активи підприємства. На основі цього аналізу було розроблено політику інформаційної безпеки, що включає заходи для мінімізації ризиків та підвищення загального рівня захисту.

Після вибору і встановлення технічних засобів захисту було проведено їх тестування та оцінку ефективності. Результати показали, що впроваджені заходи значно зменшили ризики та підвищили рівень безпеки інформації на підприємстві. Комплексний Захист Інформації (КСЗІ) успішно виконує свої функції, забезпечуючи відповідність сучасним вимогам і стандартам безпеки.

Таким чином, проведений аналіз та впроваджені заходи дозволили суттєво покращити стан інформаційної безпеки на ПрАТ "Інтеркорн", що сприяє стабільному та безпечному функціонуванню підприємства.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Метою виконання економічного розділу є техніко-економічне обґрунтування політики безпеки інформації приватного акціонерного товариства ПрАТ "Інтеркорн", яке займається виробництвом глюкозно-фруктозних сиропів, паток мальтозних, що замінюють цукор для виробництва кондитерських виробів, напоїв та пива; кукурудзяних зародишів для виробництва кукурудзяної олії; сухих кормів для відгодівлі великої рогатої худоби та птиці (клітковина і протеїн).

Основою для визначення витрат на розробку політики безпеки інформації є концепція сукупної вартості володіння (Total Cost of Ownership), запропонована Gartner Group, де розраховуються фіксовані (капітальні) вкладення і поточні витрати, а також величини можливих збитків, які може отримати підприємство.

3.1 Розрахунок фіксованих (капітальних) витрат

Капітальні (фіксовані) витрати на проектування та впровадження комплексної системи захисту інформації включають:

$$К = Кпр + Кзпз + Кпз + Каз + Кнавч + Кн , \qquad (3.1)$$

де Кпр – вартість розробки проекту комплексної системи захисту інформації та залучення для цього зовнішніх консультантів, тис. грн;

Кзпз – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн;

Крп – вартість розробки комплексної системи захисту інформації, тис. грн;

Каз – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

Кнавч – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн;

Кн – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн.

Розробку комплексної системи захисту інформації для приватного акціонерного товариства "Інтеркорн" планується здійснювати із залученням зовнішнього спеціаліста, отже Кпр=20000 грн.

Також планується закупівля додаткового апаратного забезпечення у вигляді датчиків руху, дверей, вікон, пожежі, картридерів та камер.

Загальна сума всього обладнання буде коштувати Каз= 48200 грн. Заплановано застосування ліцензійного програмного забезпечення, вартість якого визначається на рік користування, крім того ці витрати
відображатимуться в експлуатаційних витратах.

Витрати на навчання всіх співробітників і обслуговуючого персоналу (Кнавч) складуть 8 тис.

Витрати на встановлення обладнання та налагодження системи інформаційної безпеки становлять (Кн) 6 тис. грн.

Витрати на розробку політики безпеки інформації Крп складають додаткові витрат на заробітну плату зовнішнього спеціаліста, тому Крп=3000 грн.

Затрати праці на розробку політики безпеки інформації визначаються тривалістю кожної робочої операції, починаючи зі складання технічного завдання і закінчуючи оформленням документації (за умови роботи залученого спеціаліста з інформаційної безпеки).

$$t= t_{mn} + t_{m} + t_{m} + t_{mn} + t_{mmm} + t_{mmn} + t \text{ , годин,} \qquad (3.2)$$

де t_{mm} – тривалість складання технічного завдання на розробку політики безпеки інформації, $t_{тз}$=4 години;

t_m – тривалість розробки концепції безпеки інформації у організації, $t_в$=4 годин;

t_m – тривалість процесу аналізу ризиків, ta=10 годин;

t_{mn} – тривалість визначення вимог до заходів, методів та засобів захисту, $t_{вз}$=10 годин;

t_{mmm} – тривалість вибору основних рішень з забезпечення безпеки інформації, $t_{озб}$=6 годин;

t_{mmn} – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації, $t_{овр}$=6 годин

tд– тривалість документального оформлення політики безпеки, tд=6 годин.

Отже,

$$t = 4 + 4 + 10 + 10 + 6 + 6 + 6 = 46 \text{ годин.}$$

Витрати на заробітну плату спеціаліста з інформаційної безпеки Ззп дорівнюватимуть Ззп = 46 * 115 = 5290 грн.

Середньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями складає 115 грн/годину, виходячи із заробітної плати 20000 грн/міс.

Вартість 1 години машинного часу ПК визначається за формулою:

$$C_{година} = \frac{C_{амортизація} + C_{електроенергія} + C_{обслуговування} + C_{ремонт} + C_{інше}}{T_{річний}}$$

Річна вартість амортизації ПК: $C_{амортизація}$ =12,000 грн,

Річні витрати на електроенергію: $C_{електроенергія}$ =42,000 грн,

Річні витрати на обслуговування: $C_{обслуговування}$ =10,000 грн,

Річні витрати на ремонт: $C_{ремонт}$ =10,000 грн,

Інші річні витрати: $C_{інше}$ =10,000 грн,

Загальна кількість робочих годин на рік: $T_{річний}$ =2,000 годин (припустимо, що ПК працює 8 годин на день протягом 250 робочих днів на рік).

$$C_{\text{година}} \frac{12000 + 42000 + 10000 + 10000 + 10000}{200} = 42$$

Вартість машинного часу для розробки політики безпеки інформації на ПК становить:

$$З_{мч} = t * С_{мч} = 46 * 42 = 1932 \text{ грн.}$$

Отже,

$$К_{рп} = 5290 + 1932 = 7222 \text{ грн.}$$

Таким чином, капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта комплексної системи захисту іфнормації будуть складати:

К = 20000 + 48200 + 8000+ 6000 + 3000 + 7222 = 86422 грн.

3.2 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи комплексної системи захисту інформації складають:

$$С = Св + Ск + Сак \text{ , грн} \qquad (3.3)$$

де $С_в$ - вартість відновлення й модернізації системи;

$С_к$ - витрати на керування системою в цілому;

$С_{ак}$ - витрати, викликані активністю користувачів системи комплексної системи захисту інформації ($С_{ак}$ = 0 грн.).

Витрати на річне використання ліцензійного програмного забезпечення (див. таблицю 3.1) включають в себе витрати на оновлення та модернізацію системи інформаційної безпеки (Св).

Таблиця 3.1 - Вартість ліцензійного програмного забезпечення грн/рік

№	Найменування	Виробник	Ціна
1	Система управління інформаційною безпекою (ISMS)	IBM	15000 грн.
2	Система управління подіями та інформацією безпеки (SIEM)	Splunk	12000 грн.
3	Системи виявлення та запобігання вторгнень (IDS/IPS)	Cisco	10000 грн.
4	Антивірусне та програмне забезпечення	Kaspersky	8000 грн.
5	Системи резервного копіювання та відновлення даних	Veeam	10000 грн.
6	Системи моніторингу мережевого трафіку та управління	SolarWinds	10000 грн.
Всього = mm			65000 грн

Витрати на керування системою комплексної системи захисту інформації (Ск) складають:

$$С_к = С_н + С_а + С_з + С_{ел} + С_о + С_{тос}, \text{ грн.} \quad (3.4)$$

Витрати на навчання всіх співробітників і обслуговуючого персоналу складуть 8 тис.

Річна заробітня плата зовнішнього працівника, що обслуговує систему комплексної системи захисту інформації ($С_з$), складає:

$$С_з = Зосн + Здод, грн. \quad (3.5$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 5% від основної заробітної плати. Тож,

$$С_з = 20000*12 + 20000*12*0,05= 252000 грн.$$

Ставка ЄСВ (єдиного соціального внеску) для всіх категорій платників в Україні станом на 2024 рік становить 22%.

$$С_{єв} = 252000*0,22 = 55440 грн.$$

Ціна електроенергії, що споживається апаратурою комплексної системи захисту інформації протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р * F_m * Ц_е , грн., \quad (3.6)$$

де Р – встановлена потужність апаратури комплексної системи захисту інформації, (Р=8,9 кВт);

Fр – річний фонд робочого часу системи комплексної системи захисту інформації (Fр = 7980 год.);

Це – тариф на електроенергію, (Це = 4,32 грн./кВт за годину).

$$С_{ел} = 8,9*5080*4,32 = 164674.56 грн.$$

Витрати на технічне й організаційне адміністрування та сервіс системи комплексної системи захисту інформації визначаються у відсотках від вартості капітальних витрат - 2% (Стос = 86422*0,02= 1728,44 грн).

Витрати на керування системою інформаційної безпеки (Ск) визначаються:

$$С_к = 8000 + 252000 + 55440 + 164674.56 + 1728,44 = 481842 \text{ грн.}$$

Отже, загальні річні витрати на підтримку функціонування системи комплексної системи захисту інформації становлять:

$$С = 65000 + 481842= 546,842 \text{ грн.}$$

3.3 Оцінка можливого збитку

Для оцінки вартості такого збитку можна скористатися наступною спрощеною моделлю оцінки.

Необхідні дані для розрахунку:

t_n – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 6 години;

t_m – час відновлення після атаки спеціалістом, що обслуговує корпоративну мережу, 2 години;

t_{mn} – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 7 годин;

Зо – заробітна плата спеціаліста з обслуговування комплексної системи захисту інформації 20000 грн./міс.;

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

Чо – чисельність обслуговуючого персоналу комплексної системи захисту інформації 2 осіб.;

Чс – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 20 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 2 млн. грн. у рік;

Пзч – вартість заміни встаткування або запасних частин, грн;

I – число атакованих сегментів корпоративної мережі, 6;

N – середнє число атак на рік, 25.

Втрата прибутку внаслідок недоступності атакованого сегмента корпоративної мережі складається з:

$$U = Пп + Пв + V, \quad (3.7)$$

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

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

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

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі включають в себе збитки в заробітній платі за час, коли працівники не можуть працювати через атаку, і проводять час у непродуктивний режим:

$$П_П = \frac{\sum Зс}{F} \cdot t \ \frac{20000 \cdot 20}{176} \cdot 6 = 40909$$

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

Витрати на відновлення робочої здатності вузла або сегмента корпоративної мережі включають кілька частин:

Витрати на відновлення робочої здатності вузла або сегмента корпоративної мережі включають кілька частин:

$$Пв = Пви + Ппв + Пзч,$$

$П_{ви}$ – витрати на повторне уведення інформації, грн.;
$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;
$П_{зч}$ – вартість заміни устаткування або запасних частин, грн
Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі Зс, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви} \frac{\sum Зс}{F} t_{mn} = \frac{20000 \cdot 20}{176} \cdot 7 = 47727$$

Витрати на відновлення сегмента корпоративної мережі Ппв визначаються часом відновлення після атаки tв і розміром середньогодинної заробітної плати обслуговуючого спеціаліста:

$$П_{ви} \frac{\sum Зс}{F} t_{m} = \frac{11000 \cdot 2}{176} \cdot 2 = 250$$

$$Пв = 47727 + 250 = 47{,}977 \text{ грн.}$$

Втрати від зниження очікуваного обсягу прибутків за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із

середньогодинного обсягу прибутку і сумарного часу простою сегмента корпоративної мережі:

$$V = \frac{\text{U}}{F\text{г}} \cdot (t_n + t_m + t_{mn})$$

$$V = \frac{2000000}{2080} \cdot (6 + 2 + 7) = 14423$$

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

U = 40909 + 47977 + 14423 = 103309.грн.

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

$$B = \sum l \sum n = \sum 6 \sum 25\ 103309 = 32083090.$$

3.4 Загальний ефект від впровадження системи комплексної системи захисту інформації.

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

E = B · R - C грн.,

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

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці (19,6%);

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

Ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки:

Е = 32083090*0,196 – 546,842 = 6284442.558.грн.

3.5 Визначення та аналіз показників економічної ефективності розробки політики інформаційної безпеки

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

К– капітальні інвестиції за варіантами, що забезпечили цей ефект, грн. Коефіцієнт повернення інвестицій ROSI:\

$$\text{ROSI} = \frac{6284442.558}{86422} = 72.71, \text{частки одиниці,}$$

Проект вважається економічно доцільним, якщо внутрішньоекономічна норма доходності перевищує річну депозитну ставку, скориговану на інфляційні очікування.:

ROSI (Nдеп – Nінф)/100),

де Nдеп – річна депозитна ставка, (17 %);

Nінф – річний рівень інфляції, (10%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$72,71 > (17 - 10)/100 = 72,71 > 0.07$$

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

$$T_m = \frac{\mathrm{K}}{\mathrm{m}} = \frac{1}{ROSI} = \frac{1}{72,71} = 0.01375.$$

Висновок до третього розділу

Розділ присвячений оцінці економічних аспектів впровадження комплексної системи захисту інформації в ПрАТ "Інтеркорн". Проведені розрахунки фіксованих (капітальних) витрат дозволяють зрозуміти потреби підприємства у вкладеннях на початковому етапі проекту. Розрахунок поточних витрат відображає очікувані оперативні витрати, пов'язані з підтримкою та експлуатацією системи в майбутньому.

Оцінка можливого збитку дозволяє ідентифікувати потенційні ризики та їх вплив на фінансовий стан підприємства в разі виникнення інцидентів інформаційної безпеки. Загальний ефект від впровадження системи комплексної захисту інформації включає не лише економічні аспекти, а й підвищення рівня безпеки та довіри стейкхолдерів до підприємства.

Визначення та аналіз показників економічної ефективності розробки політики інформаційної безпеки свідчать про важливість правильного вибору стратегій та інструментів для досягнення оптимальних результатів.

Таким чином, економічний аналіз в цьому розділі надає обґрунтовану базу для прийняття управлінських рішень щодо впровадження комплексної системи захисту інформації в ПрАТ "Інтеркорн", сприяючи збалансованому підходу до інвестицій у інформаційну безпеку.

ВИСНОВОК

Підсумовуючи результати впровадження, можна стверджувати, що комплексна система захисту інформації надає значні переваги для підприємств з точки зору безпеки та ефективності. Завдяки використанню сучасних методів захисту, таких як нове апаратне забезпечення та спеціалізоване програмне забезпечення, ризик несанкціонованого доступу та шкідливих атак значно знижується.

Комплексний підхід до захисту інформації включає не лише технічні засоби, але й організаційні заходи, спрямовані на підвищення обізнаності персоналу щодо кібербезпеки. Впровадження новітніх технологій дозволяє ефективніше виявляти та реагувати на потенційні загрози в реальному часі.

Перед впровадженням комплексної системи захисту інформації було проведено детальний аналіз існуючого стану апаратного забезпечення підприємства. На основі цього аналізу був здійснений аналіз ризиків та розроблена політика безпеки. Після цього було впроваджено нове апаратне забезпечення та спеціалізоване програмне забезпечення, яке відповідає сучасним вимогам безпеки.

Інтегрування комплексної системи захисту інформації демонструє,що економічна ефективність використання такої системи перевищує початкові інвестиції, оскільки компанії отримують значну рентабельність інвестицій завдяки зниженню втрат від кіберзлочинів та підвищенню продуктивності праці.

Таким чином, впровадження комплексної системи захисту інформації є критично важливим кроком для сучасного бізнесу, який прагне забезпечити свою конкурентоспроможність на ринку та захистити свої компанії від кіберзагроз. Інвестиції в безпеку інформації виправдовують себе завдяки зниженню ризиків, підвищенню продуктивності та зміцненню довіри клієнтів і партнерів.

ПЕРЕЛІК ПОСИЛАНЬ

1 Information about the company Interkorn URL: https://intercorn-corn-processing-industry.biz-gid.com/ (дата звернення: 30.05.2024)

2 Threats and spills of information sicutity URL: https://datami.ua/informatsijna-bezpeka-vidi-zagroz-i-metodi-yih-usunennya/ (дата звернення: 30.05.2024)

3 A look at current trends and clicks in the information security industry URL: http://www.pdu-journal.kpu.zp.ua/archive/4_2023/48.pdf (дата звернення: 30.05.2024)

4 Analysis of existing solutions and technologies for information security URL: http://znp-cvsd.nuou.org.ua/article/view/126048/120738 (дата звернення: 30.05.2024)

5 Cybersecurity Statistics and Trends: веб-сайт. URL: https://www.varonis.com/blog/cybersecurity-statistics (дата звернення: 30.05.2024)

6 Information security policy overview URL: https://www.irbis-nbuv.gov.ua/cgibin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Vldubzh_2017_16_5

7 Select and install technical features for protection URL: https://tor-safety.com/tehnichni-zasobi-bezpeki-shho-tse-take-i-navishho-potribno/

ДОДАТОК А. відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	1 Розділ	13	
6	А4	2 Розділ	30	
7	А4	3 Розділ	12	
8	А4	Висновки	2	
9	А4	Перелік посилань	1	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

ТрегубовМД_125-20-2_Кр.docx

ТрегубовМД _125-20-2_Кр.Pdf

Презентація.pptx

ТрегубовМД _125-20-2_Кр. p7s

ДОДАТОК В. Відгук керівника економічного розділу

Відгук керівника економічного розділу:

_____

_____

_____

_____

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (ініціали, прізвище)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125-20-2

Трегубова Микити Дмитровича

на тему: Комплексна система захисту інформації інформаційно - комунікаційної системи ПрАТ "Інтеркорн"

Метою кваліфікаційної роботи є Розробка, впровадження та покращення системи КСЗІ на підприємстві, що спрямована на забезпечення надійного захисту інформації від несанкціонованого доступу, витоку даних та інших загроз інформаційній безпеці підприємства.

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: Проведення аналізу існуючого стану, на основі зібраних даних про об'єкт розробити модель загроз і модель порушника. Розробка політики інформаційної безпеки. Вибір і встановлення технічних засобів захисту після впровадження, а також їх тестування.

Практичне значення результатів кваліфікаційної роботи полягає у розробці комплексної системи захисту іфнормації, за допомогою яких організація зможе мінімізувати ризики кіберзагроз та зменшити потенційні економічні збитки від атак на підприємство.

За час дипломування Трегубов М.Д. проявив себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації бакалавра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека».

Кваліфікаційна робота заслуговує оцінки «_____».

Керівник кваліфікаційної роботи доц. Герасіна О.В.

Керівник спец. розділу ст викл. Герасіна О.В.