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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студентки *Умнякової Ірини Сергіївни*

академічної групи *125-18-3*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Політика безпеки інформації інформаційно-телекомунікаційної системи комунального підприємства "CapitalS"*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	доц. Герасіна О.В.	80	Добре	
розділів:				
спеціальний	ас. Мілінчук Ю.А.	80	Добре	
економічний	к.е.н., доц. Пілова Д.П.	90	Відмінно	

Рецензент				

Нормоконтролер	ст. викл. Тимофєєв Д.С.			

Дніпро
2022

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студентці *Умняковій І.С.* **академічної групи** *125-18-3*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації _____

за освітньо-професійною програмою *Кібербезпека*

на тему *Політика безпеки інформації інформаційно-телекомунікаційної системи комунального підприємства "CapitalS"*

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

Розділ	Зміст	Термін виконання
Розділ 1	Стан питання, постановка задачі	20.05.2022
Розділ 2	Відомості про підприємство, розробка моделі порушника та загроз. Розробка політики безпеки	30.05.2022
Розділ 3	Економічні розрахунки для підтвердження економічної доцільності	10.06.2022

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

Дата видачі завдання: 18.01.2022 р.

Дата подання до екзаменаційної комісії: 17.06.2022 р.

Прийнято до виконання _____ Умнякова І.С._____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 78с., 6 рис., 21 табл., 8 джерел, 8 додатків.

Об'єкт розробки: інформаційно-телекомунікаційна система комунального підприємства «CapitalS».

Предмет розробки: політика безпеки інформації інформаційно-телекомунікаційної системи комунального підприємства «CapitalS».

Мета кваліфікаційної роботи: підвищення рівня інформаційної безпеки у інформаційно- телекомунікаційній системі за рахунок розробки політики безпеки.

У першому розділі розглянуто загальний стан питання щодо ІБ, наведені передумови створення КСЗІ на підприємстві.

У другому розділі виконано обстеження об'єкту інформаційної діяльності (ОІД), де циркулює інформація з обмеженим доступом (ІзОД). Проаналізовано потенційні загрози та вразливості, розроблені моделі порушника та модель загроз. Згідно отриманих даних сформовані основні елементи політики безпеки інформації для інформаційно-телекомунікаційної системи (ІТС) на підприємстві «CapitalS» задля мінімізації втрат ресурсів компанії.

У третьому розділі надана інформація про економічну частину питання, економічну ефективність елементів створеної політики безпеки на об'єкті інформаційної діяльності.

Практичне значення роботи полягає в провадженні запропонованих політик для підвищення рівня інформаційної безпеки.

МОДЕЛЬ ПОРУШНИКА, МОДЕЛЬ ЗАГРОЗ, КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ОБ'ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, ПОЛІТИКА БЕЗПЕКИ ІНФОРМАЦІЇ

ABSTRACT

Explanatory note: 78p., 6 fig., 21 tables., 8 sources, 8 applications.

Object of development: information and telecommunication system of the utility company "CapitalS".

Subject of development: information security policy of the information and telecommunication system of the utility company "CapitalS".

The purpose of the qualification work: to increase the level of information security in the information and telecommunication system through the development of security policy.

The first section considers the general state of the issue of IS, the prerequisites for the creation of KSZI at the enterprise.

In the second section, a survey of the object of information activities (OID), which circulates information with limited access (IOS).

Potential threats and vulnerabilities are analyzed, violator models and threat models are developed. According to the obtained data, the main elements of the information security policy for the information and telecommunication system (ITS) at CapitalS have been formed in order to minimize the loss of the company's resources.

The third section provides information on the economic part of the issue, the economic efficiency of the elements of the established security policy at the object of information activities.

The practical significance of the work is to implement the proposed policies to improve information security.

INFRINGEMENT MODEL, THREATS MODEL, COMPREHENSIVE INFORMATION PROTECTION SYSTEM, INFORMATION ACTIVITY OBJECT, INFORMATION SECURITY POLICY

СПИСОК УМОВНИХ СКОРОЧЕНЬ

НСД – несанкціонований доступ;

КСЗІ – комплексна система захисту інформації;

ПЗ- програмне забезпечення;

ПК- персональний комп'ютер;

ОІД- об'єкт інформаційної діяльності;

КС- комп'ютерна система;

АС- автоматизована система;

ІТС- інформаційно-телекомунікаційна система;

ІзОД- інформація з обмеженим доступом.

БД- база даних

ЕОМ- електронно – обчислювальна машина

ІД- інформаційна діяльність

ІТС- інформаційно - телекомунікаційна система

КЗЗ- комплекс засобів захисту

КС- комп'ютерна система

НД- нормативний документ

НД ТЗІ- нормативний документ системи технічного захисту інформації

ОС- обчислювальна система

ОТЗ- основні технічні засоби

ПЗІ- підрозділ захисту інформації

ТЗІ- технічний захист інформації

ЗМІСТ

Вступ

Для багатьох підприємств побудова надійної системи інформаційної безпеки має стояти на першому місці.

Безпека підприємства – це велика проблема, яка включає як внутрішню чи приватну комерційну таємницю компанії, так і дані співробітників і клієнтів, що стосуються законів про конфіденційність.

Дуже важливо дотримуватися та підтримувати заходи правильного зберігання інформації.

Інформаційна безпека в компанії – дуже важливий елемент функціонування будь-якого бізнесу.

Метою інформаційної безпеки є забезпечення неперервної роботи організації та мінімізація розміру збитків (втрат) від подій, що є загрозою безпеці, шляхом їх нейтралізації. Система управління інформаційної безпеки дає змогу використовувати інформацію, забезпечуючи при цьому її захист, а також захист інформаційних та комунікаційних ресурсів.

Повноцінна інформаційна безпека підприємств і організацій означає безперервний контроль в реальному часі всіх важливих подій і станів, що впливають на безпеку даних.

Актуальність теми для даної кваліфікаційної роботи визначається зростанням інформаційно-технічної вразливості в компанії та необхідністю створення комплексної системи захисту для забезпечення інформаційної безпеки.

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

Предмет дослідження: політика безпеки інформації інформаційно-телекомунікаційної системи комунального підприємства «CapitalS».

Мета роботи: підвищення рівня інформаційної безпеки у інформаційно-телекомунікаційній системі за рахунок розробки політики безпеки.

Для досягнення мети у даній кваліфікаційній роботі необхідно буде виконати такі завдання:

• Обстежити ОІД;

• Розробити модель порушника;

• Розробити модель загроз;

• Визначити ризики підприємства;

• Визначити профіль захищеності;

• Розробити політику безпеки;

• Розрахувати капітальні та експлуатаційні витрати на розробку політику безпеки.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

На жаль, деякі галузі є особливими цілями кіберпреступників із-за того, наскільки ціна їхня інформація.

Підприємство «CapitalS», яке описано нижче, є фінансовим підприємством.

Згідно Статуту, метою та предметом діяльності підприємства є одержання прибутку шляхом фінансової діяльності в галузі надання фінансових послуг людям. Такі підприємства як «CapitalS» займаються аналізом ринку попиту на продукцію, котрі виробляються на інших підприємствах і визначають тенденції виробництва у певний часовий період.

Загрози безпеки постійно розвиваються, а вимоги щодо відповідності стають дедалі складнішими. Підприємства повинні створити комплексну політику інформаційної безпеки, щоб охопити обидві проблеми. Політика інформаційної безпеки дає змогу координувати та виконувати програму безпеки та повідомляти про заходи безпеки третім сторонам та зовнішнім аудиторам.

Поверхня атаки будь-якого підприємства за останні роки значно розширилася. Традиційно організації будуть відповідати за безпеку даних, що зберігаються на локальних серверах, і використовувати найсучасніші рішення безпеки для захисту від кібератак. Ці загрози зазвичай були мотивовані фінансовими чи політичними вигодами. Сьогодні компанії підключають технології, щоб охопити ширшу базу користувачів, співпрацювати з постачальниками та давати можливість працювати розподіленій робочій силі в географічно різних місцях — ваш ризик вищий, ніж будь-коли.

Зростаюча поверхня атак вимагає систем захисту, які виходять за рамки традиційних заходів кібербезпеки. Малі та великі підприємства повинні

включати безпеку на рівні підприємства, щоб визначити найкращі методи та засоби захисту кібербезпеки, щоб захистити їх від зламу даних і зупинити зловмисників від використання невідомих вразливостей.

Безпека підприємства включає стратегії, методи та процес захисту інформації та IT-активів від несанкціонованого доступу та ризиків, які можуть порушити конфіденційність, цілісність або доступність цих систем. Спираючись на традиційну передумову кібербезпеки щодо захисту цифрових активів на локальному фронті, безпека підприємства поширюється на безпеку даних, що передаються через підключену мережу, сервери та кінцевих користувачів.

Щоб бути ефективною, політика інформаційної безпеки повинна:

•охопити наскрізні процеси безпеки в організації;

•бути практичною;

•регулярно оновлюватись відповідно до потреб бізнесу та загроз;

•бути зосереджені на бізнес-цілях вашої організації;

Створення політики інформаційної безпеки може допомогти організаціям виявити прогалини безпеки, пов’язані з нормативними вимогами, та усунути їх.

Визначення заходів щодо забезпечення необхідного рівня безпеки передбачає визначення складу, структури та розташування приміщень та засобів захисту інформації, щоб забезпечити необхідний рівень захисту від реальних загроз безпеці.

1.2 Необхідні умови для створення КСЗІ

Для створення КСЗІ необхідно враховувати, що інформацію слід захищати у всіх видах її існування – документальному, електронному, що міститься і обробляється в автоматизованих системах (АС). Це відноситься до персоналу, який обробляє інформацію. Необхідно також вживати заходів щодо захисту інформації

від витоку технічними каналами. При цьому потрібно захищати інформацію не тільки від несанкціонованого доступу (НСД) до неї, але і від неправомірного втручання в процес її обробки, зберігання та передачі на всіх фазах.

Повинні бути забезпечені конфіденційність, цілісність і доступність інформації. Таким чином, захищати необхідно всі компоненти інформаційної структури підприємства - приміщення, апаратуру, інформаційні системи, документи на паперових та електронних носіях, мережі зв'язку, персонал і т. д.

Побудова комплексної системи захисту інформації на об'єкті, здійснюється згідно НД ТЗІ 3.7-003-05. НД ТЗІ 3.7-003-05 визначає порядок прийняття рішень щодо складу Компексної системи захисту інформації(КСЗІ) в залежності від умов функціонування ІТС і видів оброблюваної інформації, визначення обсягу робіт і зміст робіт, етапності робіт, основних завдань та порядку виконання робіт кожного етапу.

Планування КСЗІ рекомендується проводити у відповідності з наступною методикою:

1. Аналіз об'єкта і ресурсів котрим потрібен захист;
2. Виявлення способів несанкціонованого доступу і каналів витоку інформації;
3. Створення моделей загроз і способів їх реалізації;
4. Вибір захисних заходів;
5. Аналіз ризику;
6. Створення політики безпеки;
7. Складання КСЗІ;
8. Висновки.

Для забезпечення достатнього рівня інформаційної безпеки компанії необхідно розробити Політику інформаційної безпеки з урахуванням того, що вона є складовою системи безпеки підприємства.

1.3 Постановка задачі

Безпека інформації є дотримання необхідної безпеки будь-якого підприємства, так як на підприємстві циркулює інформація з обмеженим доступом така як: персональні дані клієнтів, персональні дані працівників, фінансові дані, тому є необхідність для створення КСЗІ.

Для створення КСЗІ потрібно виконати необхідні завдання:

• Обстежити ОІД;

• Розробити модель порушника;

• Розробити модель загроз;

• Визначити ризики підприємства;

• Визначити профіль захищеності;

• Розробити політику безпеки;

• Розрахувати капітальні та експлуатаційні витрати на розробку політику безпеки.

1.4 Висновок

В першому розділі роботи розглянуто стан питання та необхідні умови для створення КСЗІ.

Враховуючи актуальність проблеми захисту інформації на даний час, можна сказати що створення КСЗІ є дуже важливою частини для роботи любого підприємства. Під час розробки політики безпеки повинно бути проаналізовано фізичне середовище, моделі порушників і загроз та інші чинники.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Повні відомості про підприємство

Компанія «CapitalS» займається наданням фінансових послуг та аналізом рентабельності підприємств на сучасному економічному ринку.

Форма власності: «CapitalS» зареєстрована як приватне підприємство. Обслуговує фізичних та юридичних осіб.

Компанія веде підрахунки затрат та доходу при відкритті нових підприємств. Також займається просуванням на ринок приватних підприємств.

Компанія робить аналіз ринку попиту на продукцію, що виробляється на різних підприємствах і визнає основні потреби у виробництві у певний часовий період.

Характеристика підприємства:

Офіс компанії займає перший поверх будівлі.

Адреса: вул. Короленко, 11. Дніпро, Дніпропетровська область, 49000.

Графік роботи підприємства 5 днів на тиждень з 8:00 до 16:00, перерва на обід з 12:30 до 13:30.

Компанія була створена у 2003 році, та має гарну довіру серед клієнтів.

2.2 Обстеження фізичного середовища

Об’єктом інформаційної діяльності (ОІД) є приватне підприємство «CapitalS». На рисунку 2.1 наведено Ситуаційний план ОІД.

Адреса підприємства: вул. Короленко, 11. Дніпро, Дніпропетровська область, 49000. Знаходиться на першому поверсі п’яти поверхового будинку.

У таблиці 2.1 показано відстань від інших будівель до КЗ.

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

Генеральний план наведено на рисунку 2.2 (Додаток Б).

Висота стель – 2,5 м, стінні перегородки- 170 мм, стіни зовнішні з цегли – 350 мм.

Міжкімнатні двері: 4 шт., матеріал – МФД, з розміром 2000 мм * 800 мм

Підлога: паркет.

Вікна: 6 шт, металопластикові, подвійні, з розміром 1400 мм * 1500 мм

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

Площа ОІД: 130 $м^2$

Мережа 220В, світильники з LED лампами.

Каналізація да водооснащення підключені через підвальне приміщення у будинку.

Система опалення централізоване.

Відповідно до документу НД ТЗІ 2.5-005 -99 зі зміною №1, Затвердженого наказом Адміністрації Держспецзв'язку від 15.10.2008 № 172 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу», інформаційно-телекомунікаційну систему підприємства «CapitalS» можна віднести до АС класу «3».

АС класу «3», це - розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності.

В складі АС функціонують такі засоби захисту:

• сенсори розбитого скла;

• відеоспостереження;

• пожежна сигналізація;

• охоронна система;

• джерела безперебійного живлення;

• металеві решітки;

• кабельне обладнання.

Розташування охоронної системи та камер відеоспостереження наведено у ДОДАТКУ Г.

Під час аналізу фізичного середовища потрібно також знайти та локалізувати можливі канали витоку інформації, що виходять за межу контрольованої зони.

Це такі канали як:

• канали витоку інформації по ланцюгам електроживлення;

• канали витоку інформації по ланцюгам заземлення;

• канали витоку інформації по вентиляційним системам.

Територія компанії охороняється штатом охоронців у кількості 2 осіб. Крім того ведеться відео нагляд за територією, та в середині приміщення.

У компанії запроваджена система електронних пропусків, що зменшує імовірність загроз вчинити викрадення інформації зловмисником, що не є робітником фірми, не опосередковано з її території.

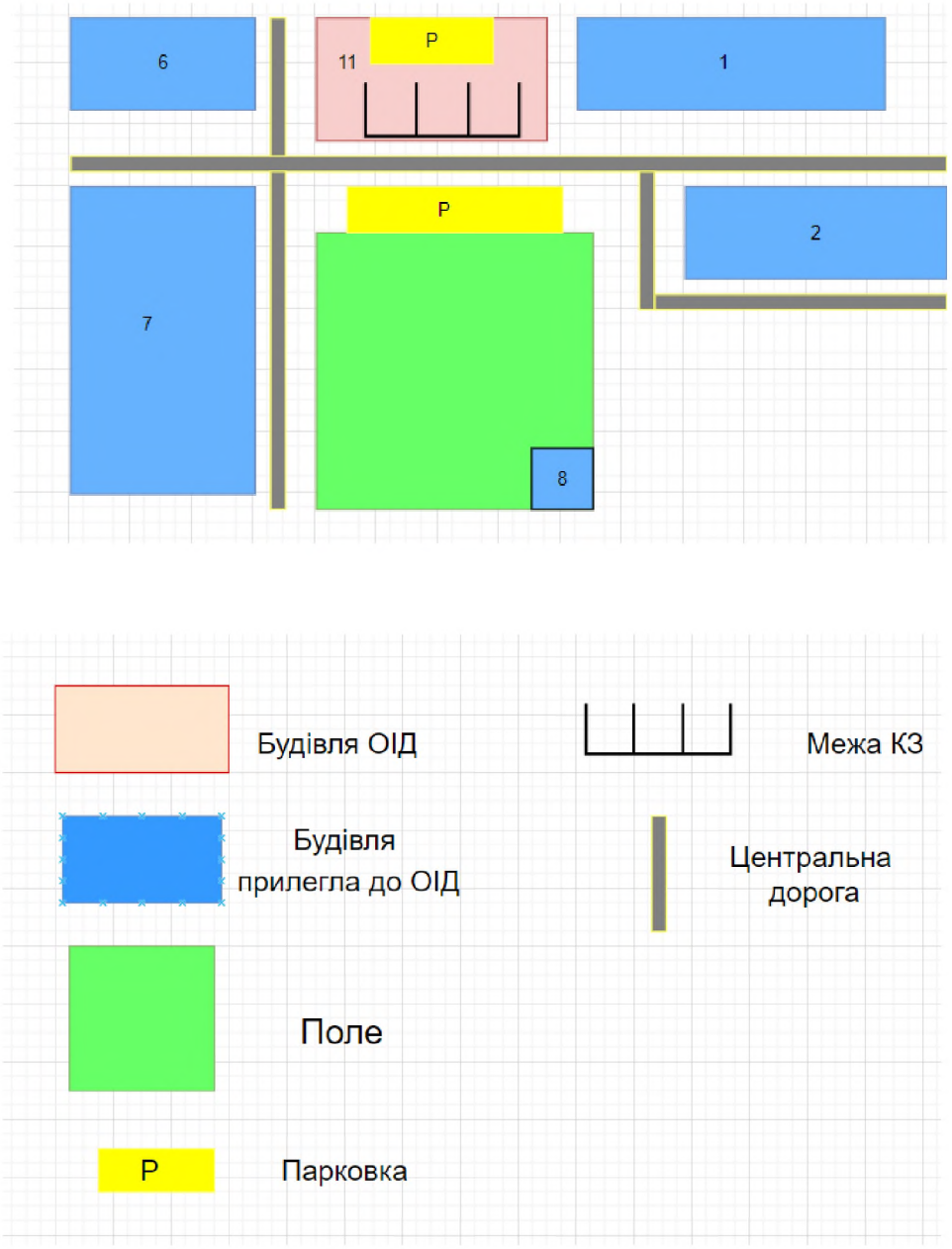


Рисунок 2.1 Ситуаційний план ОІД

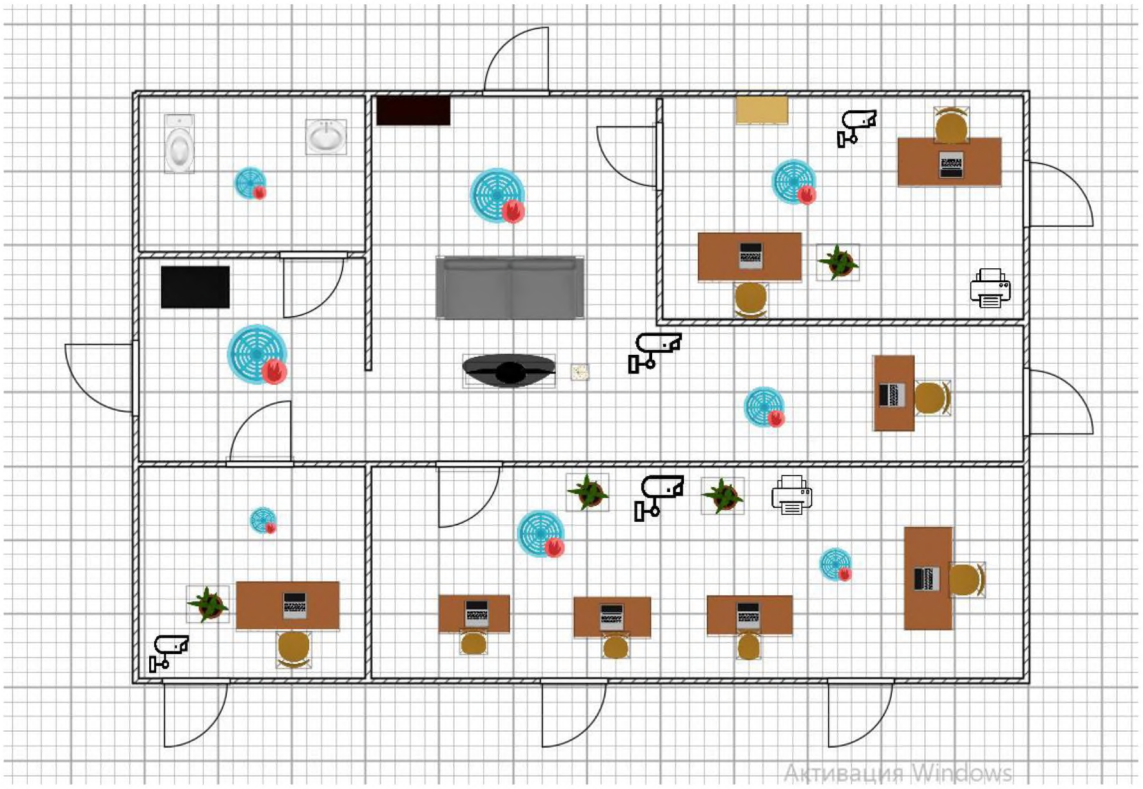


Рисунок 2.2 Генеральний план

Таблиця 2.1 Відстань від інших будівель до КЗ

№	Відстань від КЗ, м	Адреса	Призначення будівлі
1	60	Вул. Короленко 6	Житловий будинок
2	50	Вул. Яворницького 2	Будівля для оренди
3	150	Вул. Короленко 8	Поле

4	110	Вул. Короленко 7	Центральна будівля
5	30	Вул. Яворницького 1	Паркувальний майданчик

2.3Організаційна структура підприємства

До середовища персоналу установи та користувачів автоматизованої системи належать:

•Директор;

•Керівники відділів (2);

•Працівник відділу роботи з клієнтами;

•Системний адміністратор;

•Адміністратор безпеки;

•Бухгалтер;

•Маркетолог;

•Секретар;

•Технічний та обслуговуючий персонал;

•Працівники служби охорони.

Дану структуру можна побачити на рисунку 2.3

Рисунок 2.3 Організаційна структура підприємства

Обов'язки директора: укладання контрактів, приймання на роботу та вирішування організаційних питань.

Доступ до приміщень для зберігання документів, звітів про діяльність компанії, зареєстрованих носіїв інформації, даних відео нагляду та спостереження, журнали відвідувань і т. д. мають лише директор та особи, яким надається допуск до цих матеріалів.

Директору підпорядковуються керівники відділів, секретар та бухгалтер.

Обов'язки керівників відділів: керівництво відділом маркетингу, планування роботи відділу, складання звітності та навчання співробітників.

Першому керівнику підпорядковуються працівник відділу роботи з клієнтами

Другому керівнику підпорядковується працівник відділу роботи з клієнтами та адміністратор безпеки.

В обов’язки бухгалтера входить: складання звітності та нарахування заробітної плати.

Обов’язки секретаря: прийом відвідувачів, планування робочого дня керівників, прийом телефонних дзвінків, замовлення канцтоварів для офісу.

До обов’язків маркетолога входить:

•Вивчення ринку та ринкових тенденцій;

•Контроль та аналіз результатів робіт;

•Вивчення поведінки споживачів;

•Вибір цільового ринку;

•Розробка конкурентної переваги.

Працівник відділу роботи з клієнтами займається збиранням та аналізом інформації про потенційних клієнтів , налагоджує ділові зв’язки.

Також працівник відділу роботи з клієнтами займається запрошенням на особисті зустрічі, проведення профільних семінарів, презентацій, виставок, конференцій, інших заходів.

В обов’язки адміністратора безпеки входить: усунення несправностей, обмеження доступу співробітників до інформації відповідно до політики безпеки, підтримка працездатності системи, резервне копіювання даних, видалення шкідливих програм і вірусів, оновлення системи.

Також є обслуговуючий персонал:

•Прибиральниця

•Охоронники

2.4 Обстеження інформаційного середовища

Інформація зберігається як у паперових документах, так і в електронному вигляді.

В організації інформація обробляється з обмеженим доступом: технічні документи, трудові договори, персональні дані клієнтів, персональні дані працівників.

Майже всю інформацію працівники зберігають у хмарному сховищі.

Після втрати чинності, інформація знищується.

К – вимоги до конфіденційності,

Ц – вимоги до цілісності,

Д- вимоги до доступності.

Вимоги бувають:

Підвищена- 3

К3 - рівень конфіденційності інформації, при якому організація зазнає відчутних збитків у разі розкриття інформації особам, що не мають допуску до неї;

Ц3- рівень цілісності інформації, при якому організація зазнає відчутних збитків у разі втрати цілісності інформації;

Д3- рівень доступності інформації, при якому організація зазнає відчутних збитків у разі втрати доступності інформації;

Середня- 2

К2 - рівень конфіденційності інформації, при якому організація зазнає відчутних збитків у разі розкриття інформації особам, що не мають допуску до неї;

Ц2- рівень цілісності інформації, при якому компанія зазнає незначних збитків у разі втрати цілісності інформації;

Д2- рівень доступності інформації, при якому компанія зазнає незначних збитків у разі втрати доступності інформації;

Низька- 1

К1 - рівень конфіденційності інформації, при якому можна знехтувати збитками у разі розкриття інформації

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

Д1- рівень доступності інформації, при якому можна знехтувати втратою доступності інформації.

У таблиці 2.2 наведено перелік інформації, правовий режим, вид зберігання та вимогу до захисту.

Таблиця 2.2 Перелік інформації, правовий режим, вид зберігання та вимогу захисту.

Вид інформації	Режим	Правовий	Вимог	Вимоги до

	доступу	режим	и до захисту	власт. інформ.		
				К	Ц	Д
Інформація про адресу та графік роботи	Відкрита	-	Д, Ц	1	3	3
Економічні послуги	Відкрита	-	Д, Ц	3	2	2
Інформація про співробітників	ІзОД	Конфіденційна	К, Д, Ц	1	3	3
Трудові договори	ІзОД	Конфіденційна	К, Д, Ц	3	3	2
Інформація про клієнтів	ІзОД	Конфіденційна	К, Д, Ц	3	2	2
Інформація про постачальників(економіних послуг)	ІзОД	Конфіденційна	К, Д, Ц	3	3	2
База замовлень	ІзОД	Конфіденційна	К, Д, Ц	2	3	3

Продовження таблиці 2.2

Вид інформації	Режим	Правовий	Вимоги	К	Ц	Д

	доступу	режим	до захисту			
Налаштування системи безпеки	ІзОД	Конфіденційна	К, Д, Ц	3	3	3
Фінансова звітність	ІзОД	Конфіденційна	К, Д, Ц	3	3	3
Установчі документи підприємства	ІзОД	Конфіденційна	К, Д, Ц	2	3	2
Інформація про технічне обладнання	ІзОД	Конфіденційна	К, Д, Ц	2	2	2

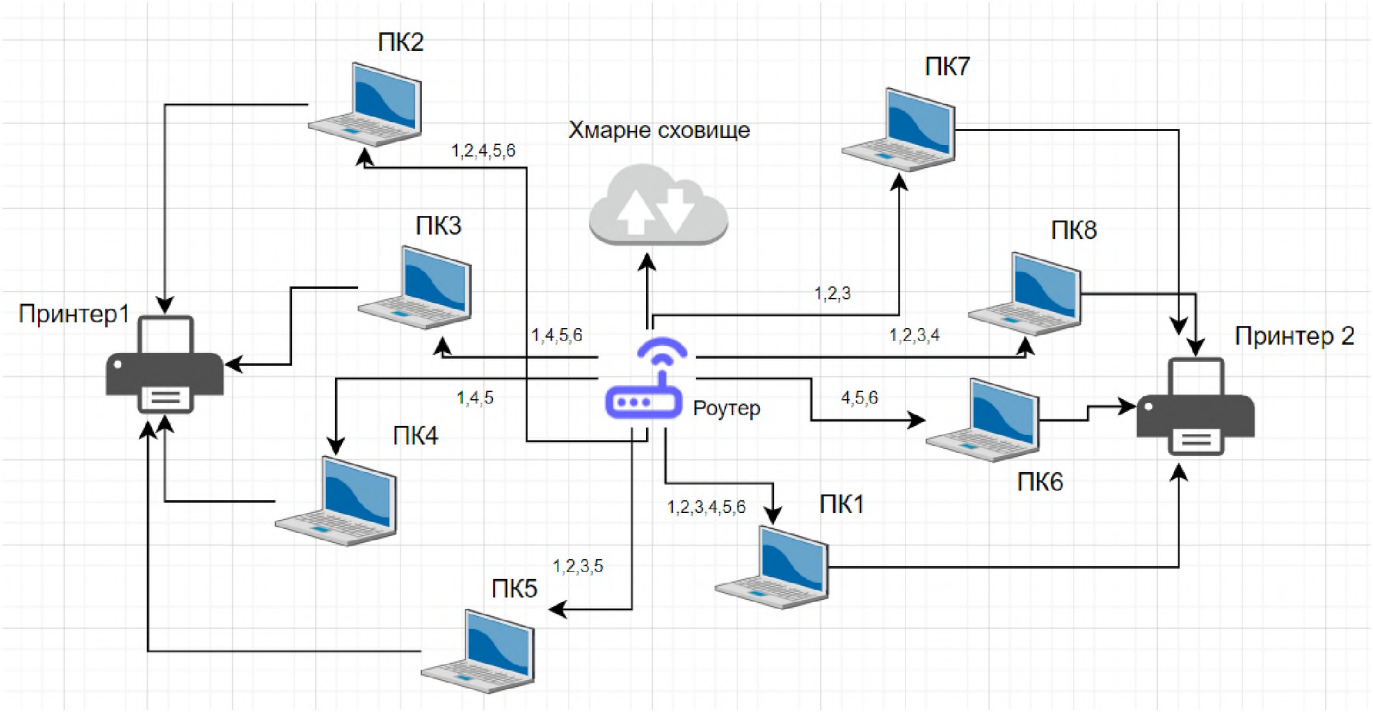


Рисунок 2.4 Схема інформаційних потоків

1-Обробка персональних даних працівників;

2-Обробка інформації про підприємство;

3-Опрацювання документів підприємства;

4-Обробка інформації про документи підприємства;

5-Обробка фінансової складової діяльності підприємства;

6-Обробка інформації про стан мережі.

2.5 Опис обчислювальної системи ОІД

Обчислювальна система даної компанії є локальною мережею, в якій числиться 8 комп'ютерів, що знаходяться в одному приміщенні.

Офіс знаходиться на одному поверсі будівлі. За генеральним планом у компанії 4 робочих кімнати:

- робочі відділи компанії (2);
- кабінет директора компанії «CapitalS»;
- приймальня з кімнатою відпочинку.

Технічне обладнання наведено у таблиці 2.3

Програмне забезпечення в ІС підприємства наведено у таблиці 2.4.

Розташування ІТС наведено на рисунку 2.5

Таблиця 2.3 Технічне обладнання

Назва у системі	Кількість	Назва обладнання	Системні характеристики	Місце розташування
ПК1, ПК2, ПК3	3	Ноутбук Acer Aspire 5 A515-45G-R9ML	Екран 15.6" IPS (1920x1080) Full HD, матовий / AMD Ryzen 5 5500U (2.1 — 4.0 ГГц) / RAM 8 ГБ / SSD 512 ГБ / AMD Radeon RX 640, 2 ГБ	Кабінет бухгалтерії. Керівників відділу
ПК4	1	Ноутбук ASUS Laptop X415FA-EB013	Дисплей 14 Intel Core i3-10110U / RAM 8 ГБ / SSD 256 ГБ	Кабінет директора
ПК5, ПК6, ПК7, ПК8,	4	Ноутбук HP ENVY x360 15-es1000ua	Дисплей – 13.3, 1920x1200 Full HD Процесор- Ryzen 5 5600U, 2,3 (4,2) ГГц Оперативна пам'ять- 8 ГБ, SSD- 256 ГБ Відеокарта- Radeon Graphics	Кабінети: Маркетолога, секретара, Системного адміністратора, Працівника відділу роботи з клієнтами, Адміністратора безпеки

Продовження таблиці 2.3

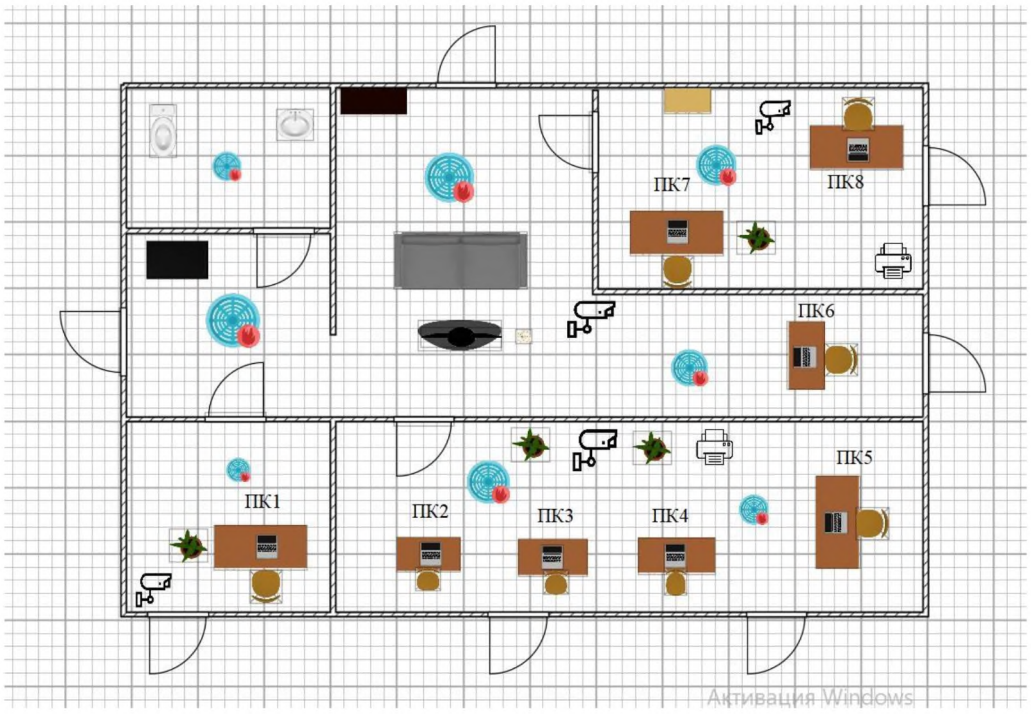
Назва у системі	Кількість	Назва обладнання	Системні характеристики	Місце розташування
Wi-Fi роутер	1	Xiaomi Mi WiFi Router 4C Global (DVB4231GL)		В залі відпочинку
Комп'ютерна миша	8	Logitech M171 Black (910-004424)	-	
Принтер	2	HP DeskJet 2710 з Wi-Fi	-	

Таблиця 2.4 Програмне забезпечення в ІС підприємства

№	Назва ПО	Тип	Ліцензія	Призначення	Термін дії	Встановлено
1	Windows 11	Системне	Commercial	Операційна система	Безстроково	ПК1, ПК2, ПК3, ПК4
2	Microsoft Office(2021)	Системне	Commercial	Операційна система	Безстроково	ПК5, ПК6, ПК7, ПК8
3	Microsoft Wod 2021	Прикладне	Commercial	Створення документів	Безстроково	ПК1…ПК8

Продовження таблиці 2.4

№	Назва ПО	Тип	Ліцензія	Призначення	Термін дії	Встановлено
4	Microsoft Exel 2021	Прикладне	Commercial	Створення таблиць	Безстроково	ПК1… ПК8
5	Антивірус Avast Premium Security	Прикладне	Commercial	Антивірусна програма	Безстроково	ПК1… ПК8
6	1С	Прикладне	Commercial	Програма для бухгалтерських обліків	Безстроково	ПК3



Умовні позначення

Рисунок 2.5

Розташування ІТС

На даному підприємстві технічне обладнання підключено до глобальної мережі. Побудова мережі виконана за технологією Wi-Fi. При такому способі побудови мережі передача даних здійснюється по сигналу; пристрої підключаються до мережі без використання кабельних з'єднань.

Схему зображено на рисунку 2.6.

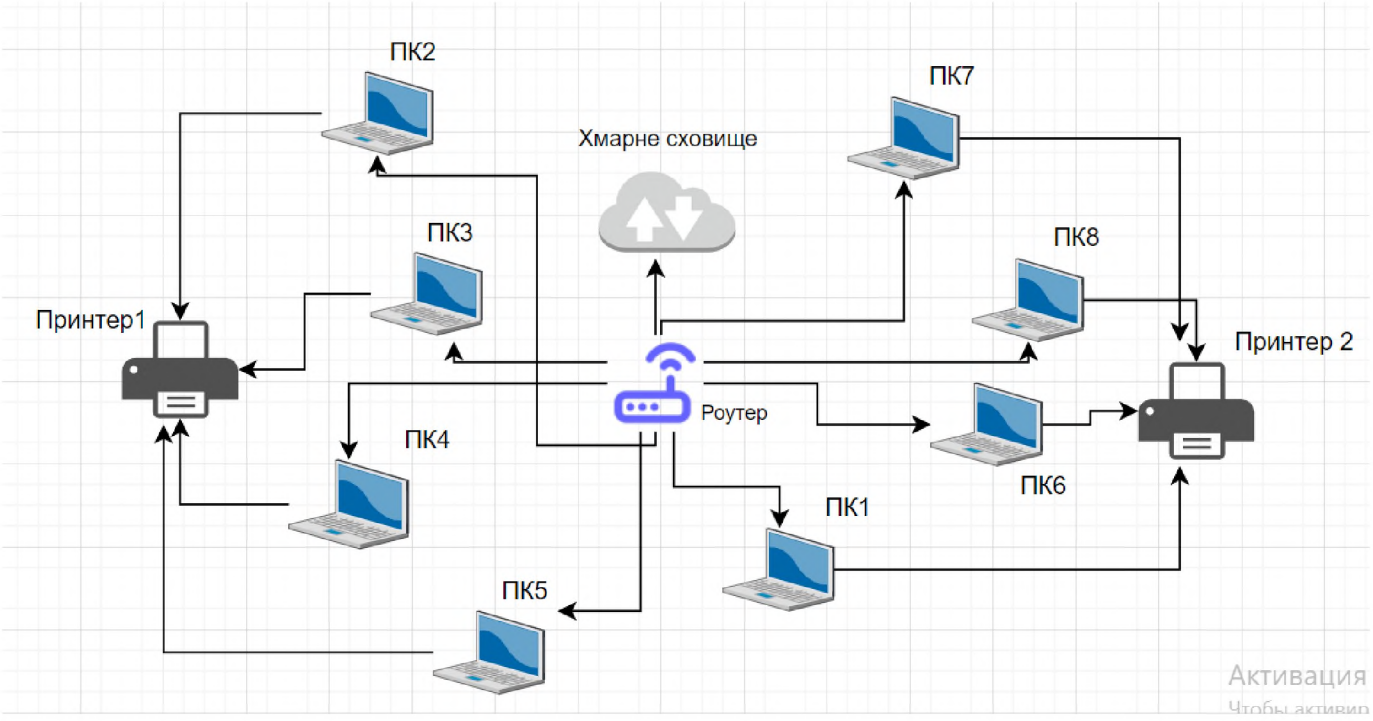


Рисунок 2.6 Схема ІТС

2.6 Модель порушника

Аналіз загроз та вразливостей включає в себе:

•Модель порушника;

•Модель загроз;

•Ідентифікація наслідків реалізації загроз;

• оцінка ризиків та ймовірності їх появи.

На цьому етапі здійснюється аналіз ризиків, а саме опрацювання моделі загроз і моделі порушника. Також визначається перелік критичних загроз, що є метою етапу формування завдання на створення КСЗІ.

Тепер розглянемо модель порушника

Для доступу до ІЗОД порушник може використовувати різні методи та інструменти. Зловмисники переглядають системи безпеки виняткової якості перед входом в ІТС. Порушник – це особа, яка за допомогою різних методів і прийомів, можливостей і засобів випадково, несвідомо чи навмисно, зі злим умислом (вигодою) чи без нього, намагається здійснити заборонені дії з метою самоствердження чи помсти.

Порушників умовно можна розділити на дві групи: зовнішні та внутрішні.

Можливі зовнішні порушники (сторонні люди):

•Технічний персонал, що обслуговує будівлю (перший рівень);

• Клієнти (перший рівень);

• Представники конкуруючих організацій (другий рівень);

• Відвідувачі запрошуються з будь-якої нагоди (другий рівень).

Можливі внутрішні порушники:

• Кінцеві користувачі (оператори системи); персонал (перший рівень);

• Особи, які обслуговують технічні засоби (третій рівень);

• Співробітники відділу розробки та підтримки програмного забезпечення (четвертий рівень);

• персонал служби безпеки АС (перший рівень);

• Менеджер (перший рівень)

Загрози для інформації, що обробляється в АС, залежать від характеристик ОС, фізичного середовища, персоналу, технологій обробки та інших чинників і можуть мати об'єктивну або суб'єктивну природу. Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні.

Таблиця 2.6 Категорії порушників. Внутрішні по відношенню к ІТС.

Позначення	Визначення категорії	Рівень загроз
ПВ1	Директор	0
ПВ2	Керівник відділу	4
ПВ3	Бухгалтер	3
ПВ4	Менеджер	2

Таблиця 2.7 Категорії порушників. Зовнішні по відношенню к ІТС.

Позначення	Визначення категорії	Рівень загроз
ПЗ1	Клієнти	2
ПЗ2	Комунальні служби	1
ПЗ3	Охоронник, прибиральниця	1
ПЗ4	Агенти конкурентів	4

Припускається, що в своєму рівні порушник - це фахівець вищої кваліфікації, який має повну інформацію про КС і КЗЗ.

Мета порушника:

•отримання необхідної інформації;

•отримання можливості вносити зміни в інформаційні потоки відповідно до своїх намірів;

•завдання збитків шляхом знищення матеріальних та інформаційних цінностей.

Таблиця 2.8 Специфікація моделі порушника за мотивами порушення

Позначення	Мотив порушення	Рівень загроз
М1	Безвідповідальність	1
М2	Самоствердження	2
М3	Професійний обов'язок	3
М4	Корисливий інтерес	4

Таблиця 2.9 Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС

Позначення	Рівень кваліфікації	Рівень загроз
К1	Володіє високим рівнем знань у галузі програмування	3
К2	Середній рівень знань, має практичний досвід з роботи з компонентами ІТС та їх обслуговування	2
К3	Володіє низьким рівнем знань, але добре працює з технічними засобами	1

К4	Знає структуру, функції і механізми дії засобів захисту	2

Таблиця 2.10 Специфікація моделі порушника за часом дії

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

Таблиця 2.11 Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту

Позначення	Характеристика можливостей порушника	Рівень загроз
З1	Підслуховування, підглядання за робочим процесом	2
З2	Взлом, підбір паролю до облікових засобів	2
З3	Несанкціоновані дії з використанням дозволених засобів	3

34	Використання технічних засобів активного впливу	4

Таблиця 2.12 Специфікація моделі порушника за місцем дії

Позначення	Характеристика місця дії порушника	Рівень загроз
Д1	З доступом у зону зберігання без даних	1
Д2	З робочих міст користувачів	4
Д3	У середині приміщень, але без доступу до технічних засобів ІТС	2
Д4	З доступами у зону керування засобами забезпечення безпеки ІТС	3

Таблиця 2.13 Модель внутрішнього порушника

Посада	Категорія	Мотив	Кваліфікація	Можливості	За часом дії	За місцем дії	Сума загроз
Директор	ПВ1	М3	К4	З3	Ч3	Д1	13
	0	3	2	3	3	2	
Керівники відділу	ПВ2	М4	К1	З4	Ч3	Д2	20
	4	4	3	4	3	2	
Бухгалт	ПВ3	М1	К2	З1	Ч3	Д1	12

ер	3	1	2	2	3	1	
Менеджер	ПВ4	М2	К3	З1	Ч4	Д4	14
	2	2	1	2	4	3	
Клієнти	ПЗ1	М2	К1	З1	Ч1	Д2	16
	2	2	3	2	3	4	
Прибиральниця	ПЗ3	М2	К1	З1	Ч3	Д1	12
	1	2	3	2	3	1	
Охоронник	ПЗ3	М2	К1	З1	Ч3	Д1	12
	1	2	3	2	3	1	
Комунальні служби	ПЗ2	М2	К1	З1	Ч3	Д1	12
	1	2	3	2	3	1	
Агенти конкурентів	ПЗ4	М4	К2	З4	Ч3	Д2	23
	4	4	2	4	3	4	

Найбільшу загрозу мають працівники підприємства: Керівники відділу оскільки вони мають доступ до системи ІТС та працюють з її компонентами.

Найбільше зовнішню загрозу несуть: агенти конкурентів та клієнти.

Тому система безпеки повинна бути більш контрольованою.

2.7 Модель загроз

Можливі способи реалізації загрози:

- технічні канали, у тому числі канали помилкового електромагнітного випромінювання та перешкод, акустичні, оптичні, радіо- та радіотехнічні, хімічні та інші канали;

-спеціальні канали впливу шляхом створення полів і сигналів для руйнування системи захисту або порушення цілісності інформації;

-Несанкціонований доступ шляхом підключення до обладнання та ліній зв'язку, видавання за зареєстрованого користувача, обхід заходів безпеки для

використання інформації або нав'язування неправдивої інформації, використання вбудованих пристроїв або програм, а також вкорінення комп'ютерних вірусів.

Перші два способи за принципом відносяться до фізичного доступу, останній – до логічного доступу.

Розрізняються наступні класи загроз інформації:

•порушення конфіденційності;

•порушення цілісності (логічної чи фізичної);

•порушення доступності чи відмовлення в обслуговуванні;

•порушення спостереженості чи керованості.

З точки зору в ІТС розрізняються наступні класи загроз інформації:

1)порушення конфіденційності;

2)порушення цілісності;

3)порушення доступності або відмова в обслуговуванні;

4)порушення спостереженості або керованості.

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

Таблиця 2.14 Загрози та можливості їх реалізації

Загроза	Реалізація	Джерело
Несанкціоноване підключення до ТЗ	•недосконала охоронна система	Зовнішнє
Відмови системи електроживлення	•стара чи неякісна електропроводка •відсутність електричних запобіжників	Внутрішнє
Стихійні явища (аварії,	•несправність обладнання	Зовнішнє

пожежа)	• легкозаймисті матеріали	
Втрата чи пошкодження носіїв інформації	•відсутність резервного копіювання	Зовнішнє
Зчитування даних на робочому екрані або залишення без нагляду робочих документів	•некомпетентність персоналу •відсутність політики безпеки	Зовнішнє
Втрата або розголошення паролів доступу до системи	•некомпетентність персоналу	Внутрішнє
Несанкціоноване підключення до каналів зв'язку	•відсутність захисту або використання застарілих •протоколів захисту Інтернет мереж •Використання слабких паролів •Некомпетентність персоналу	Зовнішнє

Продовження таблиці 2.14

Загроза	Реалізація	Джерело
Зараження системи комп'ютерними вірусами	•недосконаліть або відсутність антивірусного програмного забезпечення •несвоєчасне оновлення антивірусного програмного забезпечення •некомпетентність персоналу	Внутрішнє

Навмисне копіювання, порушення конфіденційності або цілісності інформації авторизованим користувачем	•недосконале розмежування доступу •неправильний підбір персоналу •відсутність журналу подій	Внутрішнє
Порушення цілісності інформації через ненавмисні дії користувачів	• некомпетентність персоналу • відсутність резервного копіювання	Внутрішнє
Несанкціоноване внесення змін у програмне забезпечення та технічні засоби	•відсутність або недосконалість розмежування прав користувачів у системі •некомпетентність персоналу	Внутрішнє

Продовження таблиці 2.14

Загроза	Реалізація	Джерело

Вхід у систему третіх осіб	•слабкі паролі •некомпетентність персоналу •недосконала охоронна система	Внутрішнє, зовнішнє
Соціальна інженерія	•погано підібраний персонал •низька мотивація працівників •низький рівень знань працівників	Внутрішнє

Таблиця 2.15 Шкала ймовірності реалізації загроз

Оцінка ймовірності	Характеристика
1	1%
2	25%
3	50%
4	75%
5	99%

Таблиця 2.16 Характеристика рівня загроз

Оцінка	Характеристика

Оцінка конфіденційності

0	Конфіденційність не порушується
1	Конфіденційність порушується

Оцінка цілісності

0	Цілісність не порушується
1	Цілісність порушується

Оцінка доступності

0	Доступність не порушується
1	Доступність порушується

Оцінка спостережливості

0	Спостережливість не порушується
1	Спостережливість порушується

Рівень загрози визначається= (1К+2Ц+3Д+4С) * ймовірність реалізації загрози

Таблиця 2.17 Виявлення рівнів загроз

Загроза	Ймовірність	Що порушує				Рівень загроз
		1К	2Ц	3Д	4С	
Несанкціоноване підключення до ТЗ	3	1	0	0	0	3
Відмови системи електроживлення	1	0	1	0	1	2
Стихійні явища (аварії, пожежа)	2	0	1	1	1	6

Продовження таблиці 2.17

Загроза	Ймовірність	Що порушує				Рівень загроз

Втрата чи пошкодження носіїв інформації	3	0	1	1	0	6
Зчитування даних на робочому екрані або залишення без нагляду робочих документів	4	1	0	1	0	8
Втрата або розголошення паролів доступу до системи	3	1	1	1	1	12
Несанкціоноване підключення до каналів зв'язку	2	1	0	1	0	4
Зараження системи комп'ютерними вірусами	4	1	1	1	1	16
Навмисне копіювання, порушення конфіденційності або цілісності інформації авторизованим користувачем	3	1	0	1	1	9
Порушення цілісності інформації через ненавмисні дії користувачів	3	0	1	1	0	6

Продовження таблиці 2.17

Загроза	Ймовірність	Що порушує				Рівень загроз
		1К	2Ц	3Д	4С	
Несанкціоноване внесення змін у програмне забезпечення та технічні засоби	2	1	1	1	1	8
Вхід у систему третіх осіб	2	1	1	1	1	8
Соціальна інженерія	2	1	1	1	1	8

За результатами можна побачити, що найбільшу загрозу буде завдавати «Зараження системи комп'ютерними вірусами».

Середню загрозу завдає «Втрата або розголошення паролів доступу до системи».

Найнижчу загрозу буде завдавати «Зчитування даних на робочому екрані або залишення без нагляду робочих документів» та «Навмисне копіювання, порушення конфіденційності або цілісності інформації авторизованим користувачем».

2.8 Профіль захищеності

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

Для данного підприємства обрано наступний профіль захищенності:

3.КЦ.5 = {КД-3, КА-3, КО-1, КК-1, КВ-3, ЦД-1, ЦА-3, ЦО-2, ЦВ-2, НР-4, НИ-2, НК-1, НО-3, НЦ-3, НТ-2, НВ-2, НА-1, НП-1}

Таблиця 2.18 Профіль захищеності

№	Послуга	Назва	Опис
1	КД-3	Повна довірча конфіденційність	КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта Політика довірчої конфіденційності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС

Продовження таблиці 2.18

№	Послуга	Назва	Опис

2	КА-3	Повна адміністративна конфіденційність	КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження. КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта

Продовження таблиці 2.18

№	Послуга	Назва	Опис

3	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, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною
4	КК-1	Виявлення прихованих каналів	Повинен бути виконаний аналіз прихованих каналів Всі приховані канали, які існують в апаратному і програмному забезпеченні, а також в програмах ПЗП, повинні бути документовані Має бути документована максимальна пропускна здатність кожного знайденого прихованого каналу, одержана на підставі теоретичної оцінки або вимірів Для прихованих каналів, які можуть використовуватися спільно, повинна бути документована сукупна пропускна здатність

Продовження таблиці 2.18

№	Послуга	Назва	Опис

5	КВ-3	Повна конфіденційність при обміні	Політика конфіденційності при обміні, що реалізується КЗЗ, повинна відноситись до всіх об'єктів і існуючих інтерфейсних процесів. 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. Запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу і приймальника об'єкта

Продовження таблиці 2.18

№	Послуга	Назва	Опис

6	ЦД-1	Мінімальна довірча цілісність	КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретні процеси і/або групи процесів, які мають право модифікувати об'єкт КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес. Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої цілісності мають бути
7	ЦА-3	Повна адміністративна цілісність	Політика адміністративної цілісності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС. КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу процесу і захищеного об'єкта.

Продовження таблиці 2.18

№	Послуга	Назва	Опис
8	ЦО-2	Повний 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 всі операції, виконані над захищеним об'єктом за певний проміжок часу
9	ЦВ-2	Базова цілісність при обміні	Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ран жируються на підставі повноти захисту і вибірковості керування. Політика цілісності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів КС і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовуваними механізмами, і спроможність захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу. Запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ

Продовження таблиці 2.18

№	Послуга	Назва	Опис
10	HP-4	Детальна реєстрація	Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє або непряме відношення до безпеки. 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.

Продовження таблиці 2.18

№	Послуга	Назва	Опис
11	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
12	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

Продовження таблиці 2.18

№	Послуга	Назва	Опис
13	НО-3	Розподіл обов'язків на підставі привілеїв	Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції. Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі.
14	НЦ-3	Цілісність КЗЗ	КЗЗ повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування
15	НТ-2	Самотестування при старті	Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Рівні даної послуги ран жируються на підставі можливості виконання тестів у процесі запуску або штатної роботи.

Продовження таблиці 2.18

№	Послуга	Назва	Опис
16	НВ-2	Автентифікація джерела даних	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
17	НА-1	Автентифікація відправника	Політика автентифікації відправника, що реалізується КЗЗ, повинна визначати множину властивостей і атрибутів об'єкта, що передається, користувача-відправника і інтерфейсного процесу, а також процедури, які дозволяли б однозначно встановити, що даний об'єкт був відправлений (створений) певним користувачем. Встановлення належності має виконуватися на підставі затвердженого протоколу автентифікації.

Продовження таблиці 2.18

№	Послуга	Назва	Опис
18	НП-1	Базова автентифікація одержувача	Політика автентифікації одержувача, що реалізується КЗЗ, повинна визначати множину властивостей і атрибутів об'єкта, що передається, користувача-одержувача і інтерфейсного процесу, а також процедури, які дозволяли б однозначно встановити, що даний об'єкт був одержаний певним користувачем Встановлення одержувача має виконуватися на підставі затвердженого протоколу автентифікації

2.9 Розробка політики безпеки інформації

Політика безпеки базується на наступних основних принципах:

• системності;

• комплексності;

• неперервності захисту;

•достатності механізмів і заходів захисту та їхньої адекватності загрозам;

• гнучкості керування системою захисту, простоти і зручності її використання;

•відкритості алгоритмів і механізмів захисту, якщо інше не передбачено окремо.

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

• розробка концепції безпеки інформації в ІТС;

• аналіз ризиків;

• визначення вимог до заходів, методів та засобів захисту;

• вибір основних рішень з забезпечення безпеки інформації;

• організація виконання відновлювальних робіт і забезпечення неперервного функціонування ІТС;

• документальне оформлення політики безпеки.

• Концепція безпеки інформації в ІТС викладає систему поглядів, основних принципів, розкриває основні напрями забезпечення безпеки інформації. Розроблення концепції здійснюється після вибору варіанту концепції створюваної ІТС і виконується на підставі аналізу наступних чинників:

• правових і (або) договірних засад;

• вимог до забезпечення безпеки інформації згідно з завданнями і функціями ІТС;

• загроз, яким зазнають впливу ресурси ІТС, що підлягають захисту.

• За результатами аналізу мають бути сформульовані загальні положення безпеки, які стосуються або впливають на технологію обробки інформації в ІТС:

• мета і пріоритети, яких необхідно дотримуватись в ІТС під час забезпечення безпеки інформації;

• загальні напрями діяльності, необхідні для досягнення цієї мети;

• аспекти діяльності у галузі безпеки інформації, які повинні вирішуватися на рівні організації в цілому;

• відповідальність посадових осіб та інших суб’єктів взаємовідносин в ІТС, їхні права і обов'язки щодо реалізації завдань безпеки інформації.

Політика повинна забезпечити захист конфідеційної інформації про співробітників, фінансову діяльність, клієнтів та державні акти.

Основною ціллю реалізації політики безпеки є забезпечення ефективного функціонування компанії, для чого необхідно забезпечити захист оброблюваної на підприємстві інформації від несанкціонованого доступу. Політика безпеки має на меті розробку та впровадження правил та норм внутрішнього режиму праці на підприємстві, режиму доступу та допуску до важливих об'єктів, їх охорона, середовище розміщення.

Необхідність забезпечення захисту інформації, а саме створення комплексної системи захисту інформації (КСЗІ), визначається передусім вимогами нормативно-правових документів або в окремих випадках рішенням власника інформаційних ресурсів.

На основі обстеження умов функціонування інформаційно-телекомунікаційної системи директором «Івановим О.В.» було прийнято рішення про створення КСЗІ та видано наказ «Про створення КСЗІ», що наданий у додатку Ґ.

На основі аналізу моделі загроз було обрано найбільш актуальні загрози:

• Зараження системи комп’ютерними вірусами;

• Втрата або розголошення паролів доступу до системи;

• Зчитування даних на робочому екрані або залишення без нагляду робочих документів;

• Навмисне копіювання, порушення конфіденційності або цілісності інформації авторизованим користувачем.

Тому можна сказати, що доцільно буде розробити наступні політики безпеки:

•Політика захисту паролів;

•Політика «Чистого столу»;

•Політика користування зйомними носіями інформації та збереження фізичних носіїв інформації;

•Політика антивірусного захисту.

ЗАТВЕРДЖЕНО
Директором Комунального
Підприємства «CapitalS»
Іванов О.В.
«___»_____ 20___

ПОЛІТИКА ЗАХИСТУ ПАРОЛІВ

Мета політики: створення надійних паролів і захист цих паролів.

Даною політикою повинні користуватись всі працівники підприємства «CapitalS».

Інструкція політики:

•Зміна паролю принаймні раз на 90 днів;

•Не записуйте паролі ;

•Не зберігайте паролі в Інтернеті без шифрування;

•Не використовуйте той самий пароль для облікових записів (організації), що й для доступу інших не (організації) (наприклад, особистий обліковий запис ISP, онлайн-банкінг, електронна пошта, переваги тощо);

• Не передавати паролі іншим людям;

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

Хакери шукають будь-яку можливість вкрасти конфіденційну інформацію. Вкрай важливо впровадити політики паролів, щоб захистити свій бізнес та ваших співробітників від кібератак.

Відповідальність:

Відповідні всі працівники на підприємстві.

Якщо працівник порушив дану політику, то може бути підданий дисциплінарному стягненню, чи до припинення трудових відносин.

Порядок перегляду політики:

Політика безпеки повинна переглядатись щороку директором та системним адміністратором. Можна навіть раніше, якщо це того потребує.

ЗАТВЕРДЖЕНО
Директором Комунального
Підприємства «CapitalS»
Іванов О.В.
«___»_____ 20___

ПОЛІТИКА «ЧИСТОГО СТОЛУ».

Мета політики:

Працівники повинні дати гарантію того, що вся інформаційна, котра в паперовому вигляді чи в електронному буде захищена на робочому місці в момент відсутності біля робочого місця та в кінці робочого дня.

Інструкція політики:

• Конфіденційна інформація повинна бути закрита на робочому столі, якщо у даний період вона не потрібна для користування;

• Роздруківки, котрі містять конфіденційну інформацію, повинні бути негайно видалені з принтера;

• ноутбук повинен бути заблокованим, якщо працівник відійшов;

• В кінці робочого дня ноутбук повинен бути вимкнено;

• Паролі не повинні бути записані у нотатках чи у доступному для всіх місці;

• Зберігати USB накопичувачі у закритому ящику;

•потрібно в кінці робочого дня активувати охорону систему, закрити приміщення, здати ключи на пост охорони.

Відповідальність:

Відповідальні всі працівники на підприємстві.

Якщо працівник порушив дану політику, то може бути підданий дисциплінарному стягненню, чи до припинення трудових відносин.

Порядок перегляду політики:

Дана політика також повинна переглядатись кожен рік директором чи адміністратором безпеки.

ЗАТВЕРДЖЕНО
Директором Комунального
Підприємства «CapitalS»
Іванов О.В.
«___»_____ 20___

ПОЛІТИКА КОРИСТУВАННЯ ЗЙОМНИМИ НОСІЯМИ ІНФОРМАЦІЇ ТА ЗБЕРЕЖЕННЯ ФІЗИЧНИХ НОСІЇВ ІНФОРМАЦІЇ

Мета політики:

Розробка механізмів захисту від загрози крадіжки паперових чи зйомних носіїв інформації

Інструкція політики:

• Кожен носій на підприємстві повинен підлягати обліку;

• У кожного носія повинен бути свій інвентарний номер;

• Видача та повернення зйомних носіїв повинна фіксуватись у журналі;

• Журнал повинен зберігатись у керівника відділу;

• За видачу носіїв несуть відповідальність керівники відділів;

•Забороняється зберігання носіїв без сейфів, як паперових так і зйомних;

Область дії:

Поширюється на всіх працівників підприємства.

Відповідальність:

Відповідальність покладається на керівників відділів.

Відповідальність за налаштування групових політик покладається на системного адміністратора.

Відповідальність за порушення буде оплата штрафу або звільнення, в залежності від ситуації.

Порядок перегляду політики:

Дана політика також повинна переглядатись кожен рік директором чи адміністратором безпеки.

ЗАТВЕРДЖЕНО
Директором Комунального
Підприємства «CapitalS»
Іванов О.В.
«___»_____ 20___

ПОЛІТИКА АНТИВІРУСНОГО ЗАХИСТУ

Мета політики:

Зменшення ризику зараження ІТС шкідливими програмами.

Інструкція політики:

• На кожному комп'ютері мають бути встановлені антивірусні засоби.

• Можна використовувати лише ліцензоване антивірусне програмне забезпечення, рекомендоване системним адміністратором;

• Тільки системний адміністратор налаштовує та встановлює антивірусне програмне забезпечення;

• Антивірусне програмне забезпечення має завжди своєчасно оновлюватися;

• Усі файли, завантажені з Інтернету, перед відкриттям необхідно сканувати антивірусним програмним забезпеченням;

• Якщо виникають проблеми з програмним забезпеченням, співробітники повинні негайно повідомити системного адміністратора.

Відповідальність:

Відповідні всі працівники на підприємстві.

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

Порядок перегляду політики:

Дана політика повинна переглядатись кожен рік директором чи адміністратором безпеки.

2.10 Висновок

У другій частині кваліфікаційної роботи наведено загальні відомості про комунальне підприємство «CapitalS». Інформація, яка наведена, була частково змінена на вимогу власника з метою збереження анонімності підприємства.

Результатом обстеження ОІД став аналіз загроз та вразливостей підприємства, а саме:

•класифіковано інформацію, що оброблюється підприємством;

•побудовано модель порушника та загроз;

•розроблено політику безпеки, яка включає в себе:

1.Політика захисту паролів;

2.Політика «Чистого столу»;

3. Політика користування зйомними носіями інформації та збереження фізичних носіїв інформації;

4. Політика антивірусного захисту.

За результатами аналізу моделі загроз та порушника та показників профілю безпеки розроблено ключові елементи, що відповідають найважливішим загрозам.

Функціональний профіль захищеності інформації в конкретній АС був визначений в результаті проведення аналізу загроз та оцінки ризиків та обраний на підставі класу АС відповідно до документу НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні класи захищеності оброблюваної інформації від несанкціонованого доступу".

3 ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Розрахунок витрат на впровадження політики безпеки

Економічна доцільність визначається:

-розрахунками капітальних витрат, що потребує розроблена політика безпеки;

-розрахунками експлуатаційних виплат;

-розрахунками річного економічного ефекту від розробки інформаційної політики безпеки

Для економічного обґрунтовування доцільності розробки політики безпеки інформації комунального підприємства «CapitalS» потрібно провести розрахунки, щоб визначити економічну ефективність використання основних результатів, які будуть отримані після розрахунків.

3.2 Розрахунок капітальних витрат

Інвестиції у придбання нових і тих, які були у використанні, або виготовлення власними силами для власного використання матеріальних і нематеріальних активів, витрати на капітальний ремонт та модернізацію.

Прийнято розрізняти суспільні та індивідуальні витрати виробництва. Суспільні витрати виробництва у вартісній формі знаходять свій вираз у ціні реалізації, в якій можна виділити матеріальні витрати, заробітну плату і прибуток. У рамках окремого підприємства витрати живої праці та матеріальних засобів виробництва знаходять свій вираз у формі собівартості продукції .

Поточні витрати- витрати трудових, матеріальних, нематеріальних та фінансових ресурсів, виражених у грошовій формі, для здійснення поточної господарської діяльності.

Визначення трудомісткості розробки політики безпеки інформації

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

За формулою 3.1

$$t = tmз+tв+tа+tвз+tозб+tовр+tд, \text{ годин},$$

де ttз –тривалість складання технічного завдання на розробку політики безпеки інформації, становить 7 годин;

tв-тривалість розробки концепції безпеки інформації у організації, становить 12 годин;

tа- тривалість процессу аналізу ризиків, становить 3 годин;

твз- тривалість визначення вимог до заходів, методів та засобів захисту, становить 3 годин;

тозб- тривалість вибору основних рішень з забезпечення безпеки інформації, становить 6 годин;

товр-тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації, становить 5 годин;

тд-тривалість документального оформлення політики безпеки, становить 4 години.

$$t = 7год +12год+3год+3год+6год+5год+4год =40 \text{ годин}.$$

Тепер потрібно розрахувати виплати на створення ПБ.

Формула 3.2

$$К_{рп} = З_{зп} + З_{мч}, \text{ грн}$$

Де $К_{рп}$ - витрати на створення політики безпеки;

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

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

Витрати на заробітну плату спеціаліста ІБ розраховується за формулою 3.3

$$З_{зп} = t * З_{іб}, \text{ грн},$$

Де t = 40 – загальна тривалість розробки політики безпеки, годин;

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

Средньогодинна заробітна плата спеціаліста з інформаційної безпеки становить – 99 грн/ годину.

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

$$З_{зп} = 40*99 = 3960 \text{ грн};$$

Таким чином капітальні витрати на проектування та впровадження проектного варіанту системи ІБ за формулою 3.4:

$$К = К_{пр} + К_{зпз} + К_{рп} + К_{аз} + К_{навч} + К_{н}$$

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення консультантів =3960 грн;

$К_{зпз}$ – вартість закупівель ліцензійного і основного і додаткового ПЗ, становить: 23405 грн;

$К_{рп}$ – вартість розробки політики безпеки інформації включено у вартість проекту інформаційної безпеки, тис. грн;

$К_{аз}$- вартість закупівлі апаратного забезпечення та допоміжних матеріалів, складає 5668 грн;

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

$К_{навч}$ – витрати на навчання технічних фахівців в обслуговуючого персоналу, витрати на навчання системного адміністратора 1200 грн;

Таблиця 3.1 Перелік придбаного ліцензійного ПЗ

Назва	Кількість	Вартість (грн)
Операційна система Windows 11 Для дому	4	12516
Microsoft Office для дому та бізнесу 2021	4	10889
Всього		23405

Таблиця 3.2 Перелік придбаного апаратного забезпечення і допоміжних матеріалів

Назва	Кількість	Вартість (грн)
Датчик движения Crow SRP-600	4	1740
Бездротовий датчик диму Atis-229DW	8	3928
Всього		5668

$$К = 3960 +23405+5668+1200=34233 \text{ грн}$$

За формулою (3.4)

Річні експлуатаційні витрати на систему ІБ складають:

$$С=С_в +С_к+С_{ак}, \text{ грн}$$

$С_в$- це витрати на оновлення системи;

$С_к$- вартість на керування системою в цілому, рахується за формулою 3.5:

$$С_к= С_н+ С_а +С_з +С_{єв}+С_{ел}+С_о+С_{тос}$$

Сн- це витрати на навчання адміністративного персоналу і користувачів, проведення тренінгів, становить 2000 грн;

Са - це річний фонд амортизаційних відрахувань,що відзначається від суми капітальних інвестицій. ПЗ вийшло на 23405 грн, а апаратного забеспечення на 5668 грн.

Сумарно буде 29073 грн. Ліквідаційна вартість програмногоо забезпечення для 8 комп'ютерів 2925 грн, а для апаратного забезпечення -480 грн.

$$С_а=(29073-5161)/2 =11956 \text{ грн.}$$

$$С_{а2}=5668/5=1133 \text{ грн}$$

Сз- це річний фонд заробітньої плати інженерно-технічного персоналу, котрий обслуговує систему ІБ, вираховується за формулою:

$$С_з=З_{осн}+З_{дод}, \text{ грн;}$$

Зосн - основна заробітна плата, складає 14000 грн на місяць, на рік буде 168000 грн.

Здод- додаткова заробітна плата, складає 1500 грн на місяць, на рік буде 18000 грн.

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

$$С_{єв} =168000*22\% =36960 \text{ грн}$$

$$С_з =168000+18000+36960=222960 \text{ грн}$$

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

$$С_{ел} = P * F_р * Ц_е, \text{ грн}$$

P це потужність апаратури ІБ 0,5 кВт для одного ПК, для всіх ПК, а їх в офісі всього 8,то буде 4 кВт.

Fp це річний фонд робочого часу системи ІБ складає 12 місяців * 20 роб. днів*8 робочих годин *8 ПК =15360

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

$$С_{ел} = 4*15360*1,44=88473 \text{ грн};$$

$С_{тос}$ це витрати на технічне та організаційне адміністрування та сервіс системи ІБ визначаються за даними організації. Або 1% від суми капітальних інвестицій – 342 грн.

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

$С_{ак}$- витрати викликані активністю користувачів системи ІБ. Становить 2100 грн;

Пряма допомога й додаткові настроювання	30 грн
Неформальне навчання	250 грн
Розробка додатків	270 грн
Робота з даними	400 грн
Формальне навчання	450 грн
Futz- фактор	700 грн

Таблиця 3.3 «Активність користувача» ($С_{ак}$)

$$С_к = 2000 + 11956 + 222960 + 36960 + 88473 + 342 = 362691 \text{ грн.}$$

Тепер можемо розрахувати експлуатаційні витрати:

$$С = 362691 + 2100 = 362691 \text{ грн.}$$

3.3 Оцінка величини збиту

Заробітна плата робітників на місяць

Посада	Плата за місяць, грн
Директор	25000
Керівники відділів(2)	2*15000=30000
Системний адміністратор	14500
Бухгалтер	8000
Маркетолог	10000
Секретар	9000
Адміністратор безпеки	15000
Працівник відділу роботи з клієнтами	12000
Технічний та обслуговуючий персонал (2)	6500*2=13000
Працівники служби охорони (2)	13000*2=26000
Всього	162500

Таблиця 3.4 Заробітна плата на місяць

Якщо вони погано відпрацьовують, то це впливає на її заробітну плату.

Упущена вигода від простою атакованого сегмента становить:

$$U = П_п + П_в + V$$

Пп – це виплати за простої робітників та, якщо трапляються проблеми з корпоративною мережею;

Пв- це вартість відновлення працездатності корпоративної мережі;

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

Місячний час робочого часу складає 160 годин. Час простою в наслідок атаки 7 годин:

$$Пп = (Зс/F)*t_в, \text{ грн} ;$$

Зс –це загальна кількість витрат на заробітну плату співробітників за місяць;

F- місячний фонд робочого часу;

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

$$П_п= (162500/160)*7=7109 \text{ грн};$$

Витрати на відновлення працездатності складаються з декількох частин:

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

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

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

Витрати на повторне введення інформації розраховуються за формулою:

$$П_{ви} = (Зс/F) * t_{ви};$$

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

$$П_{ви}= (162500/160)*14 =14218 \text{ грн};$$

Витрати на відновлення Ппв розраховуються за формулою:

$$Ппв=(Зо/ F)* tв;$$

$З_о$ – заробітна плата системного адміністратора;

$$Ппв= (14500/160)*7=634 грн;$$

Пзч- вартість для витрат на заміну частин складає 3000 грн.

$$Пв = Пви +Ппв+Пзч;$$

$$Пв=14218+634+3000=17852 грн.$$

Витрати від зниження працездатності під час проблеми(атаки):

$$V= (O/Fr) (tп+tв+tви);$$

Fr – це річний фонд часу роботи компанії, 1920 годин;

O- це обсяг продажів атакованого вузла або сегмента мережі, 7000000 грн.

$t_п$ – 7 годин простою після атаки;

$t_в$ – 7 годин відновлення після атаки;

$t_{ви}$ – це 14 годин повторного введення загубленої інформації під час атаки;

$$V = (7000000/ 1920) (7+7+14) =3646*28=10208 грн;$$

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

$$U= Пп + Пв+V:$$

$$7109+17852+10208=35169 грн;$$

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

$$B= \sum i \sum n U;$$

$$B= 8*8*35169=2250816 грн$$

i- число атакованих вузлів, 8 комп'ютерів.

n- середнє число атак на рік, 8.

3.4 Загальний ефект від впровадження інформаційної системи

Урахування ризиків порушення ІБ становить:

$$E = B*R-C;$$

R- це очікувана ймовірність атаки на вузол або сегмент корпоративної мережі, становить 0,25 (якщо загроза ймовірна 1 раз на 3 місяці);

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

C- це щорічні витрати на експлуатацію системи інформаційної безпеки, складає 388292,4 грн;

$$E=(2250816*0,25) - 362691 =200013 \text{ грн};$$

Аналіз показників економічної системи

$$ROSI=E/K$$

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

ROSI це коефіцієнт повернення інвестицій.

Е – це загальний ефект від впровадження системи ІБ, становить грн.

К – це капітальні затрати, становлять 34233 грн.

$$ROSI = 200013/ 34233 =5,84$$

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

$$To = K/E = 1/ ROSI, \text{ років}$$

$$To=1/\ 5{,}84\ \ =0{,}17(1\ місяць)$$

3.5 Висновок

В цьому розділі було визначено розмір капітальних інвестицій, і на засоби інформаційної безпеки.

Також було розраховано термін окупності капітальних інвестицій.

Капітальні витрати складають - 34233 грн.

Експлуатаційні витрати складають – 362691 грн.

Термін окупності капітальних інвестицій -0,17.

Загальний ефект від впровадження системи ІБ -200013 грн.

Після розрахованих даних можна зробити висновок, що дані заходи є вигідними для компанії, так як термін окупності буде менше 1 місяця.

ВИСНОВКИ

В кваліфікаційній роботі розглянуто мету та принципи створення політики безпеки та проаналізовано актуальну ситуацію в Україні щодо інформаційної безпеки.

У спеціальній частині було проаналізовано умови функціонування інформаційно-телекомунікаційної системи комунального підприємства «CapitalS» були складені моделі загроз та порушника, за результатами аналізу яких, було виявлено, що найбільші загрози виникають внаслідок зараження системи комп'ютерними вірусами, при втраті або розголошенні паролів доступу до системи, зчитувані даних на робочому екрані або залишенні без нагляду робочих документів. Тому, було розроблено наступні політики безпеки інформації інформаційно-телекомунікаційної системи комунального підприємства «CapitalS»:

- Політика захисту паролів;
- Політика «Чистого столу»;
- Політика користування зйомними носіями інформації та збереження фізичних носіїв інформації;
- Політика антивірусного захисту.

Всі ці рішення направлені на зниження ймовірності реалізації загроз зараження ПК шкідливим ПЗ, викрадення або розголошення паролів користувачів, викрадення та використання у власних цілях документації, що була залишена без нагляду та підлягала знищенню.

Запропоновані рекомендації є економічно ефективними, що було підтверджено в економічному розділі, де було визначено, що капітальні витрати на реалізацію рекомендацій окупляться менш ніж за один місяць. Тому, в даному випадку, ці рекомендації використовувати доцільно.

ПЕРЕЛІК ПОСИЛАНЬ

1.Бондаровська В. М. Людина у світі інформаційно-комунікаційних технологій / В. М. Бондаровська, Н. І. Пов'якель // Психолог. – № 25 (169). – 2005. – С. 5-9.

2. Основи охорони праці: навч. посіб. / [В.В. Березуцький, Т.С. Бондаренко, Г.Г. Валенко та ін.]; під ред. В.В.Березуцького. — [2-ге вид.]. — Х.: Факт, 2007. — 480 с.

3. Низенко Е. І., Каленяк В. П. Н61 Забезпечення інформаційної безпеки підприємництва: Навч. посіб. — К.: МАУП, 2006. — 134 с. — Бібліогр.: С. 124–130.

4. ДСТУ 3396.2 «Захист інформації. Технічний захист інформації. Терміни та визначення»

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

6. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31.05.2005 року, № 2594-IV, К., 2005.

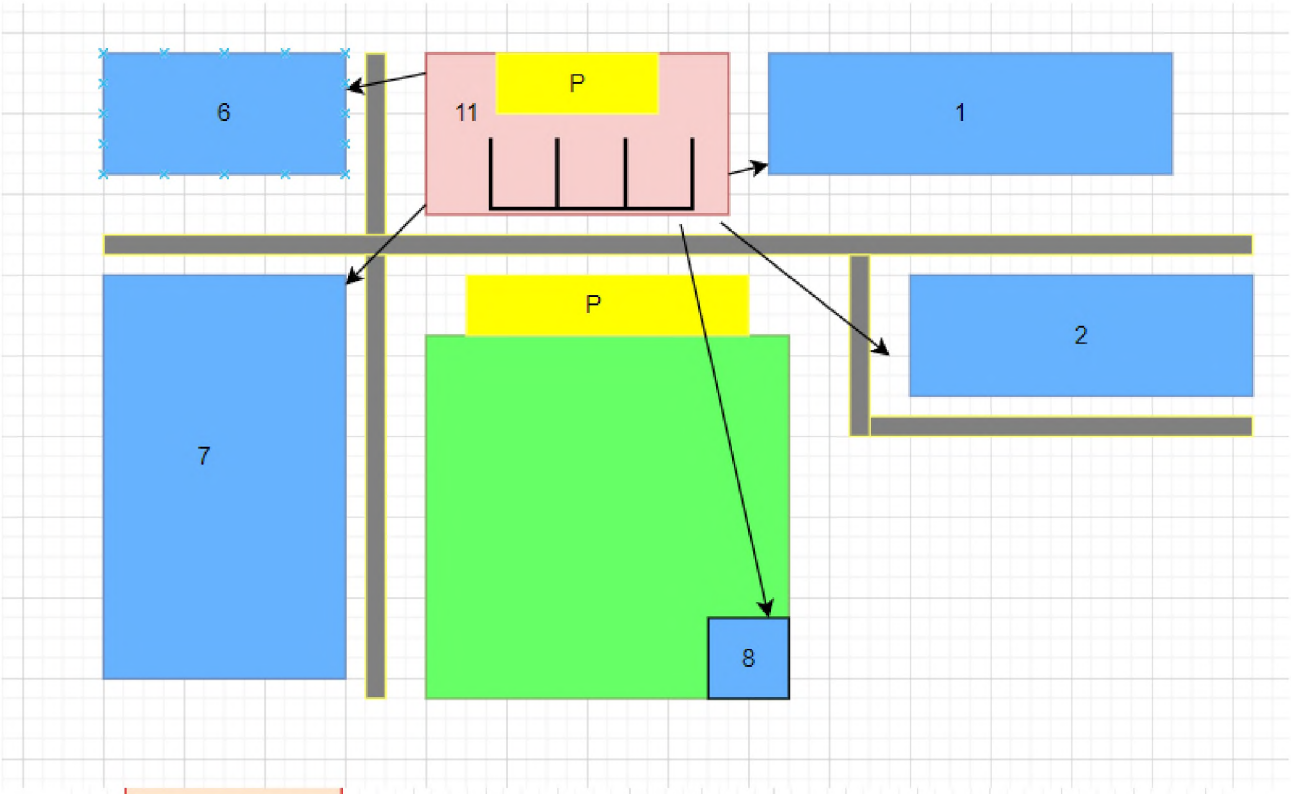
7. Principles and order of developing complex information security systems in information and telecommunication systems / U.V. Zemlyanko, A.A. Zamula, A.A. Tkach, N.I. Litvinova, Y.A. Peresechanskaya // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 460-469.

8. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу: Чинний від 1999-04-28. К.: Нормативний документ. Системи технічного захисту інформації. 1999.

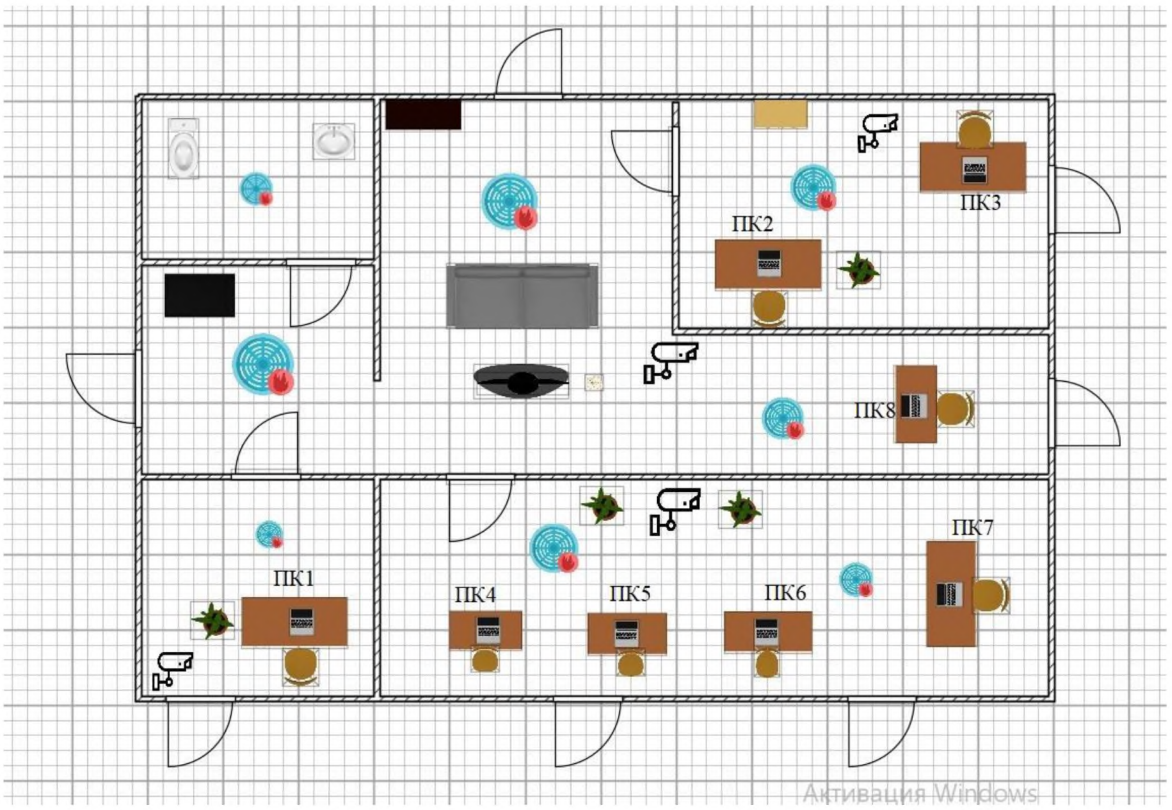
ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	1 Розділ	9	
5	А4	2 Розділ	57	
6	А4	3 Розділ	11	
7	А4	Висновки	1	
8	А4	Перелік посилань	1	
9	А4	Додаток А	1	
10	А4	Додаток Б	1	
11	А4	Додаток В	1	
12	А4	Додаток Г	1	
13	А4	Додаток Ґ	1	
14	А4	Додаток Д	1	
15	А4	Додаток Е	1	
16	А4	Додаток Є	1	

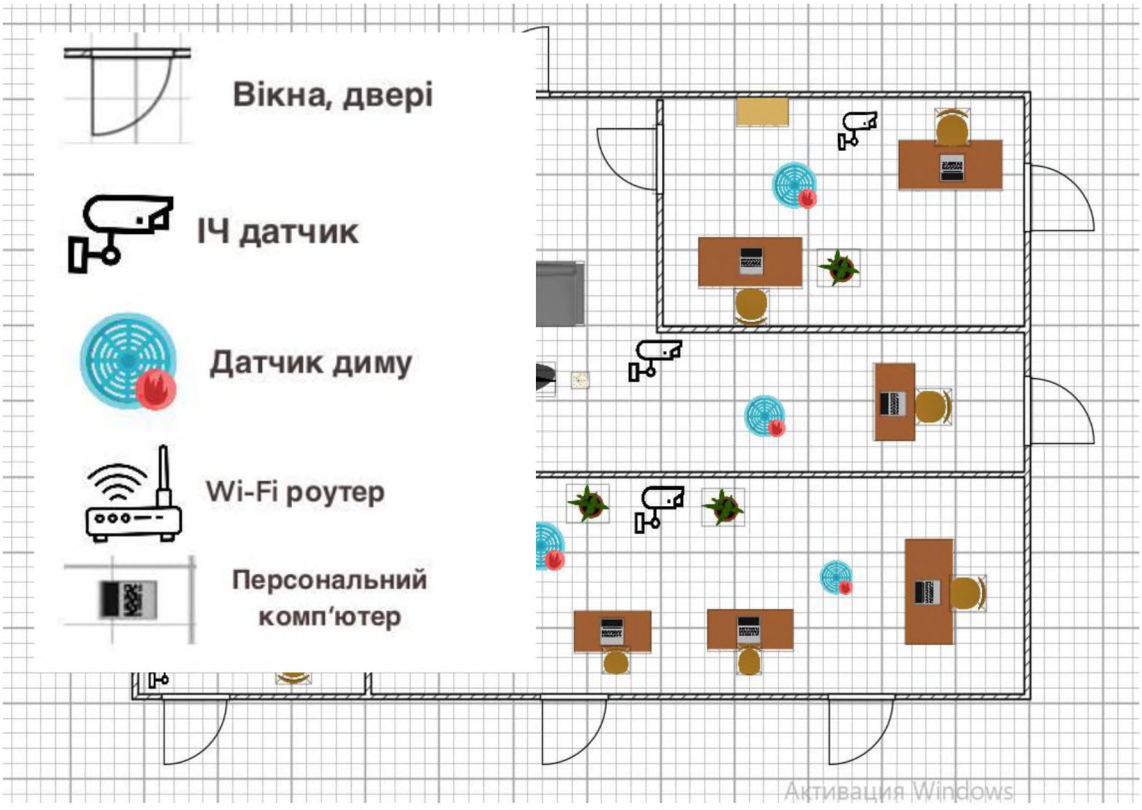
ДОДАТОК Б. Ситуаційний план ОІД



ДОДАТОК В. Генеральний план



ДОДАТОК Г. План системи охоронно-пожежної сигналізації



ДОДАТОК Ґ. Наказ на створення КСЗІ

Комунальне підприємство "CapitalS".

НАКАЗ

« ___»_____ Дніпро № _____

Про створення КСЗІ
на комунальному підприємстві
"CapitalS".

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 комунального підприємства " CapitalS ".
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 підприємства Іванов О.В.

ДОДАТОК Д. Перелік матеріалів на оптичному носії

Умнякова_І.С_125_18_3_ПЗ.docx

Умнякова_І.С_125_18_3_ДМ.pptx

Умнякова_І.С_125_18_3_ПЗ.pdf

Умнякова_І.С_125_18_3_ПЗ.pdf.p7s

ДОДАТОК Е. Відгук керівника економічного розділу

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 90 б. («Відмінно»).

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (ініціали, прізвище)

ДОДАТОК Є. Відгук керівника кваліфікаційної роботи

Відгук

на кваліфікаційну роботу студенки групи 125-18-3
Умнякової Ірини Сергіївни
на тему: «Політика безпеки інформації інформаційно-телекомунікаційної системи комунального підприємства «CapitalS».

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених 78 сторінках.

Метою кваліфікаційної роботи є підвищення рівня інформаційної безпеки у інформаційно-телекомунікаційній системі підприємства «CapitalS» за рахунок розробки політики безпеки.

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: виконання обстеження об'єкту інформаційної діяльності, розробка моделі порушника та загроз, визначення ризиків та профілю захищеності, розробка політики безпеки інформації.

У економічному розділі були розраховані витрати на впровадження політики безпеки.

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

За час виконання кваліфікаційної роботи Умнякова І.С. проявила себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації бакалавра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека».

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

Кваліфікаційна робота заслуговує оцінки « 80 / добре ».

Керівник кваліфікаційної роботи доц. Герасіна О.В.

Керівник спец. розділу ас. Мілінчук Ю.А.