ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Метод протидії витоку інформації матеріально-речовим каналом за рахунок використання сучасних технічних систем охорони»

на здобуття освітнього ступеня магістра
зі спеціальності __125 Кібербезпека та захист інформації»
(код, найменування спеціальності)
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ _____Іван_КАРПЕНКО_____
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти групи СЗДМ-61

Іван КАРПЕНКО

Керівник: КОТЕНКО Андрій
К.т.н., доцент (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім'я)

КИЇВ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ
ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра ___Технічних систем кіберзахисту_____
Ступінь вищої освіти ____магістр_____
Спеціальність ___Кібербезпека та захист інформації_____
Освітньо-професійна програма _Технічні системи інформаційного та кібернетичного захисту

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСКБ
_____Олександр Туровський

«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Карпенко Івану Сергійовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Метод протидії витоку інформації матеріально-речовим каналом за рахунок використання сучасних технічних систем охорони»

керівник кваліфікаційної роботи КОТЕНКО Андрій к.т.н., доцент
(ПРІЗВИЩЕІм'я,науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» жовтня 2025 р. № 467

2. Строк подання кваліфікаційної роботи 15.12.2025

3. Вихідні дані до кваліфікаційної роботи:
__матеріально-речовий канал витоку інформації
__Технічна система охорони
__Проект технічної системи охорони

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1.__Склад, призначення ТСО_____
2.__Аналіз загроз інформації на ОІД
3.__Проект технічної системи охорони

5. Перелік графічного матеріалу: ___Презентаційний матеріал на 13 слайдах_____

6. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
	Підбір науково-технічної літератури		
	Написання першого розділу роботи		
	Написання другого розділу роботи		
	Написання третього розділу роботи		
	Написання висновків по роботі		
	Підготовка демонстраційних матеріалів		
	Підготовка доповіді		

Здобувач вищої освіти _____ __Іван КАРПЕНКО___
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ __Андрій КОТЕНККО_
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина магістерської кваліфікаційної роботи: 91 стор., 9 рис., 1 табл., 11 джерел.

Об'єкт дослідження – процес захисту інформації на об'єктах інформаційної діяльності

Предмет дослідження – технічна система охорони

Мета роботи – Обґрунтувати доцільність використання технічних систем охорони на ОІД

Методи дослідження – системний аналіз, чисельні методи, опрацювання літератури за даною темою.

У роботі проаналізовано загрози інформації у СЕД. Розглянуто доцільність використання електронного цифрового підпису для захисту інформації

Для виконання поставленої мети, у дипломній роботі зроблено аналіз особливостей забезпечення захисту інформації у системах електронного документообігу. Зроблено дослідження системи захисту електронного документообігу на основі застосування електронного цифрового підпису

Галузь використання –захист інформації у системах едектронного документообігу.

Апробація:

А.М. Котенко, І.С. Карпенко, ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ МАТЕРИАЛЬНО-РЕЧОВИМ КАНАЛОМ ЩЛЯХОМ ВИКОРИСТАННЯ ТЕХНІЧНИХ СИСТЕМ ОХОРОНИ. *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-телекомунікаційних систем*. м. Київ, 05 листопада 2025 року, Київ: РВЦ ДУІКТ. – 2025. С.7-9. https://duikt.edu.ua/uploads/p_2779_72486260.pdf

Ключові слова: ЕЛЕКТРОННИЙ ДОКУМЕНТООБІГ,КЛЮЧ, ЗАХИСТ ІНФОРМАЦІЇ, ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС, КОНФІДЕНЦІЙНІСТЬ, ЦІЛІСНІСТЬ, ІДЕНТИФІКАЦІЯ, АУТЕНТИФІКАЦІЯ.

ABSTRACT

The text part of the bachelor's (master's) qualification work:80 pages, 9 figures, 1tables, 20sources.

*The object of the study:*is the process of information protection in electronic document management systems.

*The subject of the study:*is the protection of electronic document management systems.

*The purpose of the work:*is to substantiate the feasibility of using an electronic digital signature to protect information in the EDS.

*The methods of the study:*are system analysis, numerical methods, and literature review on this topic.

The paper analyzes the threats to information in the EDS. The feasibility of using an electronic digital signature to protect information is considered.

To achieve the goal, the thesis analyzes the features of ensuring information protection in electronic document management systems. The study of the electronic document management protection system based on the use of an electronic digital signature is carried out

The field of use is the protection of information at the object of information activity.

ELECTRONIC DOCUMENT CIRCULATION, KEY, INFORMATION PROTECTION, ELECTRONIC DIGITAL SIGNATURE, CONFIDENTIALITY, INTEGRITY, IDENTIFICATION, AUTHENTICATION.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

Вже більше 3 років в Україні йде війна, і росія використовує різноманітні засоби та методи для ураження інформаційної та критичної інфраструктури нашої країни.

Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку) опублікувала новий аналітичний звіт за перше півріччя 2025 року, який фіксує зростання масштабів та складності кібератак. Кіберпростір залишається одним із ключових напрямів гібридної агресії, а кібератаки дедалі частіше координуються із ракетно-дроновими ударами.

За перше півріччя 2025 року було зафіксовано 3018 кіберінцидентів, що на 17% більше, ніж у другій половині 2024 року. Зросла кількість атак середнього рівня критичності, натомість критичних та високих інцидентів стало менше завдяки посиленню систем кіберзахисту.

Основними цілями залишаються органи місцевого самоврядування (34%), сектор безпеки та оборони (23%) та урядові організації (19%). Серед найпоширеніших типів інцидентів — фішинг (27%), інфікування шкідливим ПЗ (21%) і компрометація облікових записів (5,4%).

Підприємство "ЖИЛСЕРВІС-5", є комунальним підприємством, частиною критичної інфраструктури міста Дніпра та області.

Метою створення і діяльності підприємства є господарська діяльність для досягнення економічних і соціальних результатів та з метою отримання прибутку. Підприємство займається різними видами діяльності, серед яких є:

- господарська діяльність спрямована на управління та утримання житлових, нежитлових будинків, споруд, гуртожитків як об'єктів комунальної власності, територіальної громади міста Дніпро та їх прибудинкових територій за рахунок і у межах коштів, отриманих від населення та інших осіб у вигляді

квартирної плати і плати за утримання будинків, споруд та прибудинкових територій.

- експлуатація житлового фонду.
- виконання робіт по ремонту та технічному обслуговуванню будинків та прибудинкових територій.
- ремонт та будівництво житла.
- організація благоустрою прибудинкових територій.
- збирання та вивіз твердих побутових та будівельних відходів, сміття, виконання будівельних і монтажних робіт.
- ізоляційні роботи.
- монтаж та обслуговування засобів обліку.
- обладнання спортивних споруд та майданів.
- монтаж системи опалення, холодного та гарячого водопостачання, водовідведення, вентиляції.
- оформлення документів, необхідних для отримання дозволу на перепланування та переобладнання житлових та нежитлових приміщень.
- будівельні роботи.

Вищеназвані види діяльності та ще багато інших – потребують стабільну та захищену інформаційно-комунікаційну систему для безперервної роботи в умовах війни.

Постійний розвиток загроз безпеки та ускладнення вимог до відповідності вимагають від підприємств постійного оновлення стандартів захисту інформації, в особливості різноманітні методи які найкраще підходять для різних вимог та сценаріїв. Таким чином різні можливі канали витоку інформації будуть максимально враховані при оновленні або створенні технічних систем охорони.

Кількість атак на комунальні підприємства за останні роки значно збільшилась. Більшість організацій зберігають дані на локальних серверах та самі несуть відповідальність за їх безпеку, але через брак фінансування та постійні атаки як кіберінциденти так і ракетні атаки по критичній інфраструктурі – більшість інформації знаходиться на папері і оцифрування зараз не на часі.Це

створює додатковий канал витоку інформації, на який треба окремо звертати увагу. Більшість загроз вмотивована військовими, політичними чи фінансовими вигодами.

Забезпечення безпеки підприємства охоплює стратегії, методи та процеси захисту інформації від несанкціонованого доступу і ризиків, які можуть порушити конфіденційність, цілісність або доступність. Враховуючи нестандартний для кібербезпеки канал витоку, запобігання можливого витоку інформації буде здійснено за рахунок дослідження сучасних методів та технічних систем охорони які найбільше підходять, аналізу їх характеристик та обрання найдієвішого варіанту.

Ефективність систем захисту інформації від витоку матеріально-речовим каналом визначається такими характеристиками:

- надійністю конструктивних та технічних рішень;
- повнотою охоплення можливих фізичних шляхів витоку інформації;
- адаптивністю систем до змін технологічних процесів та появи нових загроз;
- інтегрованістю із загальною інфраструктурою підприємства.

Розроблення та впровадження систем технічного захисту дає змогу своєчасно виявити потенційні матеріально-речові канали витоку інформації та ефективно їх нейтралізувати.

Формування комплексу заходів для забезпечення необхідного рівня захисту передбачає визначення складу, параметрів, конфігурації та розміщення технічних засобів, а також особливостей організації приміщень, у яких ці засоби експлуатуються, з метою забезпечення протидії реальним загрозам витоку інформації.

1.2 Необхідні умови для створення систем захисту інформації від витоку матеріально-речовим каналом

Під час створення сучасних систем захисту інформації від витоку матеріально-речовим каналом необхідно враховувати всі форми існування інформації — документальну, матеріальну, електронну, а також технічні засоби, що забезпечують її обробку та передачу. Особливу увагу слід приділяти персоналу, який має доступ до носіїв та обладнання, що може бути використане як фізичний канал витоку.

Необхідно забезпечувати протидію не лише несанкціонованому вилученню чи копіюванню матеріальних носіїв, але й недопущенню будь-якого неправомірного впливу на процес створення, обробки, зберігання та переміщення інформації. Система повинна підтримувати належний рівень конфіденційності, цілісності та доступності інформаційних ресурсів.

Захисту підлягають усі компоненти, у яких може виникнути ризик матеріально-речового витоку: приміщення, інженерні комунікації, технічні засоби, локальні та розподілені системи обробки інформації, матеріальні носії, транспортні маршрути документів та обладнання, а також персонал, що взаємодіє з цими компонентами.

Побудова сучасних систем захисту інформації від витоку матеріально-речовим каналом здійснюється відповідно до вимог та принципів, визначених актуальними нормативними документами у сфері ТЗІ України (НД ТЗІ), які встановлюють загальні підходи до формування структури засобів захисту, визначення умов їх функціонування та узгодження з характеристиками об’єкта.

Створення СЗІ МРК зазвичай здійснюється за такою узагальненою методологічною послідовністю:

- Аналіз об’єкта та ресурсів, що потребують захисту, включно з оцінкою їх фізичних характеристик та умов експлуатації.
- Виявлення можливих матеріально-речових каналів витоку інформації, а також чинників, що можуть сприяти їх реалізації.

- Формування моделей загроз, які враховують можливі дії порушників, технічні особливості об’єкта та сценарії ризику.
- Визначення необхідних засобів та заходів захисту, відповідно до вимог НД ТЗІ та специфіки об'єкта.
- Оцінювання ризиків та перевірка достатності запропонованих заходів.
- Встановлення загальних правил та процедур, що регламентують функціонування системи захисту інформації від витоку матеріально-речовим каналом.
- Комплексне формування системи захисту, її структурних елементів і взаємодії між ними.
- Підготовка узагальнених висновків щодо ефективності, відповідності вимогам та можливостей масштабування системи.

Для забезпечення належного рівня захисту інформації підприємству необхідно розробити внутрішні регламентовані процедури з урахуванням рекомендацій НД ТЗІ України та інтегрувати їх у загальну систему безпеки підприємства.

1.3 Аналіз нормативно-правової бази

Таблиця 1.1 – Аналіз нормативно-правової бази

Назва документу	Характеристика
Закон України «Про Інформацію»	Визначені загальні положення про інформацію, права на інформацію та на забезпечення її охорони.

Закон України «Про захист персональних даних»	Визначені суб’єкти та об’єкти персональних даних, визначені правила та обов’язки по захисту персональних даних, визначена відповідальність за їх розголошення.

Продовження таблиці 1.1

Назва документу	Характеристика
НД ТЗІ 1.1-002-99 – Загальні положення щодо захисту інформації	Методологічний документ, що визначає базові концепції вирішення завдань технічного захисту інформації в комп’ютерних системах та побудови заходів для протидії несанкціонованому доступу.
НД ТЗІ 1.1-003-99 – Термінологія у сфері ТЗІ	Узгоджує терміни та визначення, що використовуються у сфері технічного захисту інформації, забезпечуючи єдине розуміння понять у всіх документах системи.
НД ТЗІ 1.4-001-2000 – Типове положення про службу захисту інформації	Регламентує створення та діяльність служби захисту інформації на підприємстві, включно з питаннями фізичного та технічного контролю.
НД ТЗІ 1.6-005-2013 – Категоріювання об’єктів інформаційної діяльності	Визначає порядок класифікації об’єктів за критеріями ризику та загроз, що необхідно для планування систем захисту.
НД ТЗІ 2.5-004-99 – Критерії оцінки захищеності інформації	Змістовно визначає підходи та критерії оцінювання рівня захищеності

	інформації, які важливі також для оцінки ризику МРК.

Продовження таблиці 1.1

Назва документу	Характеристика
НД ТЗІ 2.5-005-99 – Класифікація автоматизованих систем	Визначає типи систем та їх функціональні профілі, що дозволяє адаптувати технічні рішення захисту під конкретні умови експлуатації.
НД ТЗІ 3.6-001-2000 – Порядок створення, впровадження та супроводження засобів ТЗІ	Описує загальні підходи до побудови та модернізації засобів технічного захисту, що може бути застосовано також до механізмів контролю МРК.
НД ТЗІ 3.7-001-99 та 3.7-003-05 – Методика та порядок робіт із створення захисту	Визначають підхід до планування та реалізації технічних заходів захисту, що корисно для систем, які повинні протидіяти витоку через МРК.
НД ТЗІ 2.7-011-2012 – Методичні вказівки з розробки методики виявлення закладних пристроїв	Містить методи та рекомендації з виявлення технічних ризиків, які можуть бути актуальними для фізичних каналів витоку.
НД ТЗІ 2.5-006-99 – Класифікатор засобів копіювально розмножувальної техніки	Регламентує класифікацію техніки та носіїв, що може бути корисною при оцінці ризику переміщення або вилучення інформації через МРК.

Правові та нормативні акти, що доповнюють ТЗІ:

1. Закон України «Про захист інформації в інформаційно-комунікаційних системах» — правова основа для захисту інформації.
2. Постанова КМУ №373 «Про забезпечення захисту інформації…» – встановлює базові вимоги до захисту інформації самих систем.
3. Постанова КМУ №736 «Типова інструкція щодо обліку та знищення матеріальних носіїв» – критично важлива для контролю витоку через фізичні носії.

1.4 Постановка задачі

Інформаційна безпека є важливою складовою захисту будь-якого підприємства, оскільки на підприємстві обробляється інформація з обмеженим доступом, така як персональні дані клієнтів, персональні дані працівників, фінансові дані. У зв'язку з цим виникає необхідність створення КСЗІ відповідно до сучасних потреб та вимог.

Завдання які треба виконати для створення КСЗІ:

- обстежити ОІД.
- розробити модель порушника.
- розробити модель загроз.
- визначити ризики підприємства.
- розробити технічну систему охорони.
- розрахувати капітальні та експлуатаційні витрати на розробку сучасної системи безпеки інформації.

1.5 Висновок

У першому розділі було проаналізовано сучасний стан питання захисту інформації від витоку матеріально-речовим каналом і те, наскільки це актуально для підприємства «ЖИЛСЕРВІС-5», яке належить до критичної інфраструктури міста Дніпро. В умовах війни та підвищених ризиків фізичного доступу до обладнання та носіїв інформації особливого значення набуває саме технічний

захист приміщень і контроль доступу. Питання безпеки вже не обмежується лише цифровими загрозами — фізичне проникнення, крадіжка носіїв або пошкодження серверного обладнання можуть мати не менший вплив на роботу підприємства.

У ході роботи було визначено, що ефективна система протидії витоку інформації матеріально-речовим каналом повинна включати контрольовані зони, сучасні системи відеоспостереження, охоронну сигналізацію, СККД, датчики проникнення, а також чіткі правила щодо доступу до приміщень та поводження з матеріальними носіями. Окрему увагу приділено нормативно-правовій базі України: законам, вимогам НД ТЗІ та чинним протоколам, які регламентують порядок захисту носіїв, приміщень та технічних засобів. Це дозволило зрозуміти, які саме вимоги потрібно враховувати під час побудови системи охорони.

У розділі була сформульована постановка задачі щодо побудови комплексу технічних і організаційних заходів, які мінімізують ризики витоку інформації. На основі цього створено модель загроз, що включає як внутрішні, так і зовнішні ризики: несанкціоноване винесення носіїв, проникнення сторонніх осіб, крадіжки, диверсії чи фізичне пошкодження обладнання. Модель допомогла визначити найбільш вразливі точки підприємства та зрозуміти, на що слід робити акцент у подальшому проєктуванні системи захисту. Отримані результати показали, що впровадження сучасних систем охорони є необхідною умовою стабільної та безпечної роботи підприємства в умовах підвищених загроз.

РОЗДІЛ 2. СПЕЦІАЛЬНИЙ РОЗДІЛ

2.1 Повні відомості про підприємство

Комунальне підприємство "ЖИЛСЕРВІС-5" займається наданням послуг та веденням різних видів діяльності з метою досягнення економічних і соціальних результатів та з метою отримання прибутку.

Форма власності: "ЖИЛСЕРВІС-5" зареєстрований як комунальне унітарне комерційне підприємство. Обслуговує фізичних та юридичних осіб.

Характеристика підприємства:

Офіс підприємства частково займає перший поверх житлової будівлі.

Адреса: Україна, 49069, Дніпропетровська обл., м. Дніпро, проспект Богдана Хмельницького, 14.

Графік роботи підприємства: з понеділка по четвер 08:00-17:00, п’ятниця 08:00-15:45 (перерва 12:00-12:45). Середа – неприймальний день.

Графік приймання громадян: понеділок 09:00-12:00, 14:00-16:00;

вівторок 14:00-16:00; четвер 09:00-12:00, 14:00-16:00; п’ятниця 09:00-11:00

Підприємство було створено відповідно до рішення Дніпровської міської ради від 26.02.2003 №35/7 на базі відокремленої частини комунальної власності територіальної громади міста Дніпра.

Підстава для надання послуг – підприємство обслуговує багатоквартирні будинки та гуртожитки відповідно до рішення виконавчого комітету Дніпровської міської ради «Про призначення управителя багатоквартирних будинків» від 25.07.2023 року №11-25/7.

Отримувачі послуг – співвласники багатоквартирних будинків.

Основнезавданняпідприємство – надання послуги з управління багатоквартирних будинків у місті Дніпрі, що самостійно не визначились з формою управління будинком.

Перелікпослугпідприємства

1. Технічне обслуговування внутрішньобудинкових систем:

- водопостачання
- водовідведення
- теплопостачання
- гарячого водопостачання (при наявності)
- зливової каналізації
- електропостачання
- газопостачання

2. Поточний ремонт внутрішньобудинковихсистем:

- водопостачання
- водовідведення
- теплопостачання
- гарячого водопостачання (при наявності)
- зливової каналізації
- електропостачання
- газопостачання

3. Інші складові послуги:

- технічне обслуговування ліфтів (при наявності крім мешканців першого поверху)
- обслуговування систем диспетчеризації
- обслуговування димових та вентиляційних каналів
- технічне обслуговування систем протипожежної автоматики та димовидалення, а також інших внутрішньобудинкових інженерних систем (у разі їх наявності)

- поточний ремонт конструктивних елементів, технічних пристроїв будинків та елементів зовнішнього упорядження, що розміщені на закріпленій в установленому порядку прибудинковій території (згідно з планами робіт)
- поточний ремонт систем протипожежної автоматики та димовидалення, а також інших внутрішньобудинкових інженерних систем (у разі їх наявності)
- дератизація
- дезінсекція
- придбання електричної енергії для освітлення місць загального користування, живлення ліфтів та забезпечення функціонування іншого спільного майна багатоквартирного будинку

2.2 Обстеження фізичного середовища

Об’єктом інформаційної діяльності (ОІД) є комунальне підприємство "ЖИЛСЕРВІС-5". На рисунку 2.1 наведено ситуаційний план ОІД.

Рисунок 2.1 – Ситуаційний план ОІД

Адреса підприємства: Україна, 49069, Дніпропетровська обл., м. Дніпро, проспект Богдана Хмельницького, 14. Знаходиться на частині першого поверху п’ятиповерхового будинку.

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

Генеральний план наведено на рисунку 2.2 (Додаток Б).

Висота стель – 2.5м, стінні перегородки – 170 мм, стіни зовнішні з цегли – 350 мм.

Міжкімнатні двері: 24 шт., матеріал –пластикові, з розміром 2000мм *800мм.

Підлога: ламінат.

Вікна: 22 шт., металопластикові, подвійні, з розміром 1400мм*1500мм.

Вхідні двері до підприємства: сталеві, розміром 1500 мм * 2000 мм.

Площа ОІД: 565,7м^2.

Мережа: 220В, світильники з LED лампами.

Каналізація та водооснащення підключені через підвальне приміщення у будинку.

Система опалення централізована.

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-комунікаційну систему комунального підприємства "ЖИЛСЕРВІС-5" можна віднести до АС класу «3».

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

В складі АС функціонують такі засоби захисту:

- сенсори розбиття скла;
- пожежна сигналізація;
- охоронна система;

- джерела безперебійного живлення;
- металеві решітки;
- кабельне обладнання.

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

Такими канали можуть бути:

- канали витоку інформації по ланцюгам електроживлення;
- канали витоку інформації по ланцюгамзаземлення;
- канали витоку інформації по вентиляційним системам;

Територія підприємства охороняється контрольно-пропускним пунктом на вході та штатом охоронців 1 особа.

У підприємстві запроваджена система особистих пропусків, що зменшує ймовірність загроз витоку інформації матеріально-речовим каналом, не працівниками підприємства.

Рисунок 2.2 – Генеральнийплан

2.3 Організаційна структура підприємства

Структурароботипідприємства:

Чисельний штат підприємства складає 180 осіб.

Керівником підприємства є директор, що має у прямому підпорядкуванні помічника, чотирьох заступників директора, головного бухгалтера, головного економіста, головного інженера, шести начальників відділів за різними видами діяльності та вісім начальників дільниць по районах міста. На рисунку 2.3 показано коротку схему організаційної структури підприємства.

Підприємство має дільниці у кожному з восьми районів міста для більш ефективного прийому звернення та швидкого реагування на них. Дільниця складається з начальника дільниці, інженерів та майстрів. Також на дільниці знаходиться бухгалтер по квартплаті, що надає консультації щодо нарахувань за послуги підприємства.

Підприємство має робітників з комплексного обслуговування, що проводять оперативні виїзди для проведення аварійних та ремонтних робіт у будинках та гуртожитках.

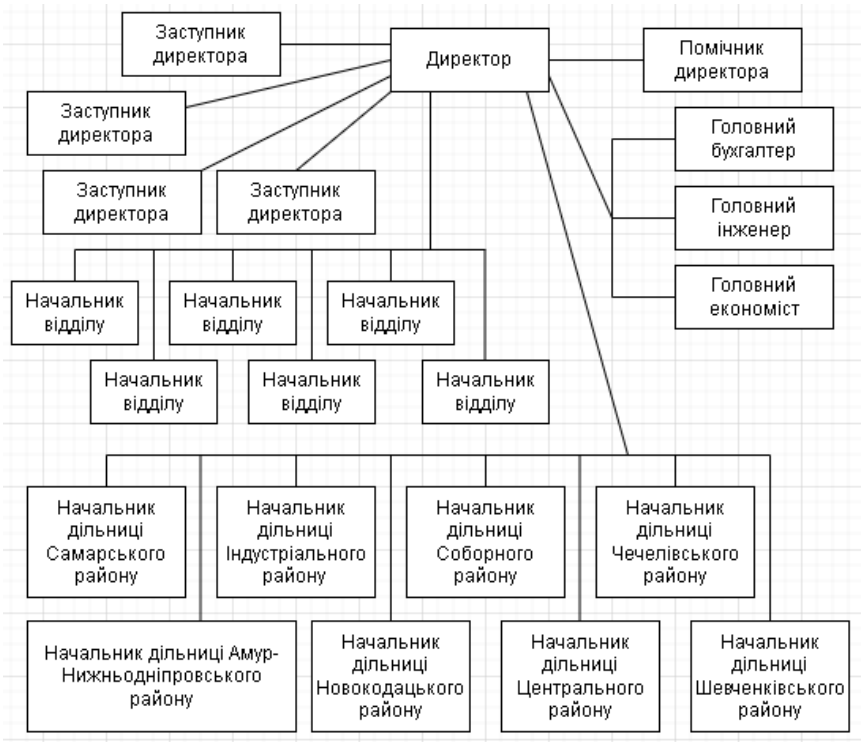


Рисунок 2.3 – Організаційна структура підприємства

2.4 Обстеження інформаційного середовища

Інформація зберігається у фізичному (паперовому) та електронному вигляді.

Інформація у підприємстві обробляється з обмеженим доступом – технічні документи, трудові договори, персональні дані клієнтів, персональні дані працівників і т. д.

Значну більшість інформації зберігають у хмарному сховищі.

К – вимоги до конфіденційності,

Ц – вимоги до цілісності,

Д – вимоги до доступності.

Рівні вимог:

1 – Низька

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.

2 – Середня

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 страти доступності інформації;

3 – Підвищення

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

ЦЗ – рівень цілісності інформації, при якому організація зазнає відчутних збитків у разі втрати цілісності інформації;

ДЗ – рівень доступності інформації, при якому організація зазнає відчутних збитків у разі втрати доступності інформації.

У таблиці 2.1 наведено перелік інформації, правового режиму, виду зберігання та вимог до захисту.

Таблиця 2.1 – Перелік інформації, правового режиму, виду зберігання та вимог захисту

Вид інформації	Режим доступу	Правовий режим	Вимоги до захисту	Вимоги до властивості інформації		
				К	Ц	Д
Інформація про адресу та графік роботи	Відкрита	–	Д, Ц	1	2	3
Перелік послуг підприємства	Відкрита	–	Д, Ц	1	2	3
Трудові договори	Відкрита	–	К, Д, Ц	1	3	3
Інформація про клієнтів	ІзОД	Конфіденційна	К, Д, Ц	3	3	3
Звернення клієнтів	ІзОД	Конфіденційна	К, Д, Ц	2	3	3
База виконаних робіт	Відкрита	–	Д, Ц	1	2	2
Інформація про постачальників (будматеріалів)	Відкрита	–	Д, Ц	2	2	2
База наявних будматеріалів	ІзОД	Конфіденційна	К, Д, Ц	1	3	3
Економічні звіти	Відкрита	–	Д, Ц	2	3	2
База оплати праці робітників	Відкрита	–	Д, Ц	3	3	3
Інформація про співробітників	Відкрита	–	Д, Ц	1	2	3
Налаштування системи безопасності	ІзОД	Конфіденційна	К, Д, Ц	3	3	3

Інформація про технічне обладнання	ІзОД	Конфіденційна	К, Д, Ц	3	3	3
Фінансові звіти	Відкрита	–	Д, Ц	1	2	3

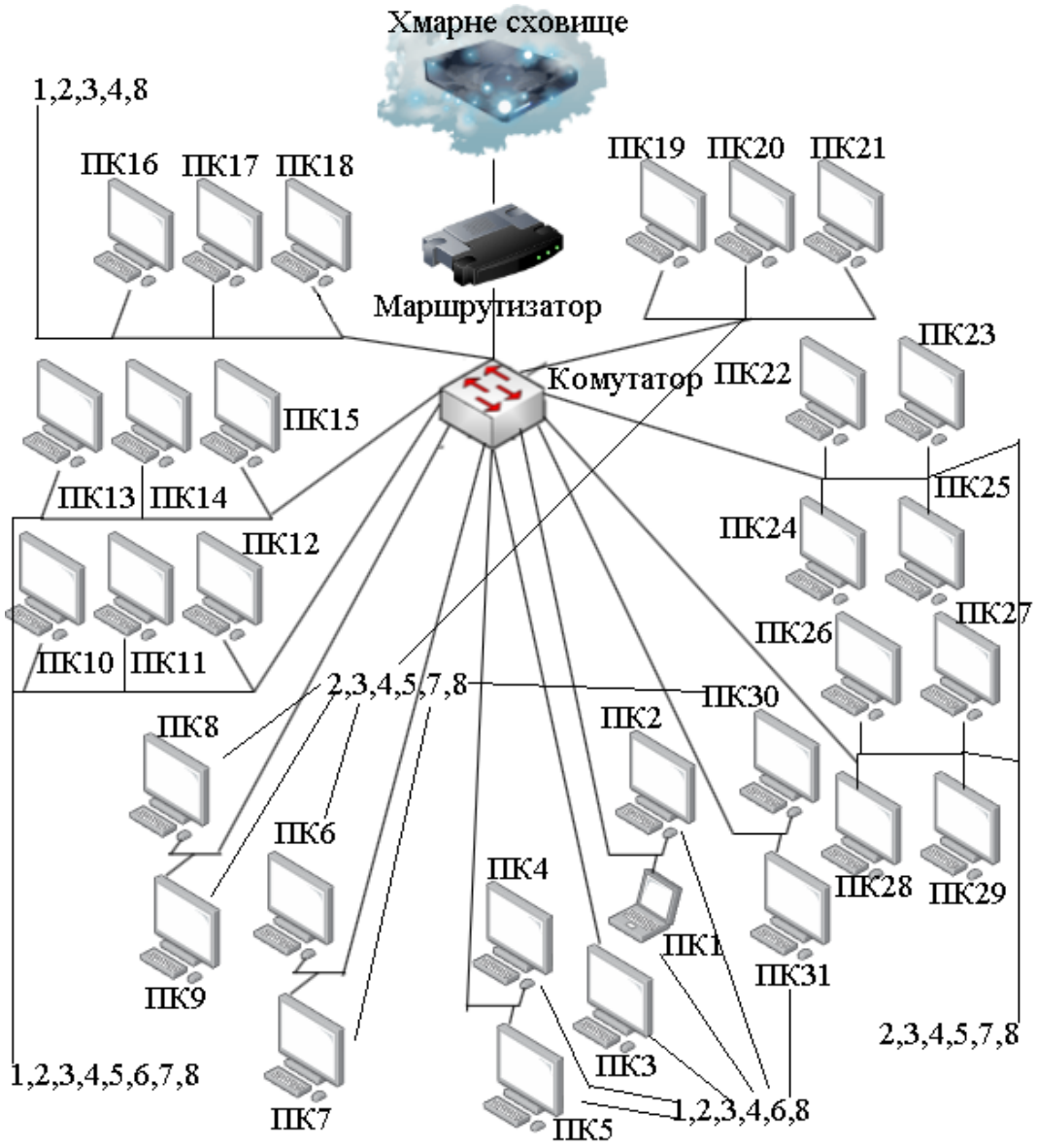


Рисунок 2.4 – Схема інформаційних потоків

1 – обробка персональних даних працівників;

2 – обробка інформації про підприємство;

3 – обробка фінансових документів підприємства;

4 – обробка звітів діяльності підприємства;

5 – обробка звернень клієнтів;

6 – обробка інформації про стан мережі;

7 – обробка інформації про стан звернень;

8 – опрацювання баз даних.

2.5 Опис обчислювальної системи ОІД

Обчислювальна система даної компанії є локальною мережею, в якій числиться 30 компьютерів і 1 ноутбук, що знаходяться в різних кімнатах приміщення підприємства.

Підприємство знаходиться на 1 поверсі будівлі. За генеральним планом до підприємства входить 18 робочих кімнат:

- кабінет директора КП «ЖИЛСЕРВІС-5»;
- робочі кабінети підприємства (11);
- приймальня (2);
- кімната для конференцій (2);
- вітальна кімната (2).

Технічне обладнання підприємства наведено у таблиці 2.2

Таблиця 2.2 – Технічне обладнання

Назва у системі	Кількість	Назва обладнання	Системні характеристики	Місце розташування
ПК2 – ПК31	30	Офіснийкомп'ютер Artline Business B27 v34	Intel Core i3-10100 (3.6 - 4.3 ГГц) / RAM 8 ГБ / SSD 240 ГБ / Intel UHD Graphics 630 / безОД / LAN / безОС	Робочі кабінети підприємства (29), кабінет диреткора (1)
ПК1	1	Ноутбук Acer Aspire 7 A715-76G-56U7	Экран 15.6" IPS (1920x1080) Full HD, матовый / Intel Core i5-12450H (2.0 - 4.4 ГГц) / RAM 16 ГБ / SSD 512 ГБ / nVidia GeForce RTX 2050, 4 ГБ / безОД / LAN / Wi-Fi / Bluetooth / веб-камера / безОС	Кабінет директора
Комутатор	1	Світч Dell PowerConnect 8024/ керований	24-Port/ 10 Gb/s	Коридор

Маршрутизатор	1	Маршрутиза-тор MikroTik B4011iGS + 5HacQ2HnD-IN	5 GHz + 2.4GHz (двухдіапазон-ний)/ 1Gbit/s	Коридор

Програмне забезпечення (ПЗ) в ІКС підприємства наведено у таблиці 2.3.

Таблиця 2.3 – ПЗ в ІКС підприємства

№	Назва ПЗ	Тип	Ліцензія	Призначення	Термін дії	Встановлено
1	Windows 10	Системне	Commercial	Операційна система	Безстроково	ПК1-ПК31
2	Microsoft Office (2021)	Системне	Commercial	Операційна система	Безстроково	ПК1-ПК31
3	Avast Premium Security	Прикладне	Commercial	Антивірус	Безстроково	ПК1-ПК31
4	Microsoft Outlook	Прикладне	Commercial	Обмін повідомленнями та інформації	Безстроково	ПК1-ПК31
5	BAS Бухгалтерія	Прикладне	Commercial	Бухгалтерія	Безстроково	ПК26-ПК29

На підприємстві технічне обладнання підключено до глобальної мережі за допомогою Wi-Fi. Пристрої підключаються до мережі без використання кабелів.

Схему зображено на рисунку 2.5

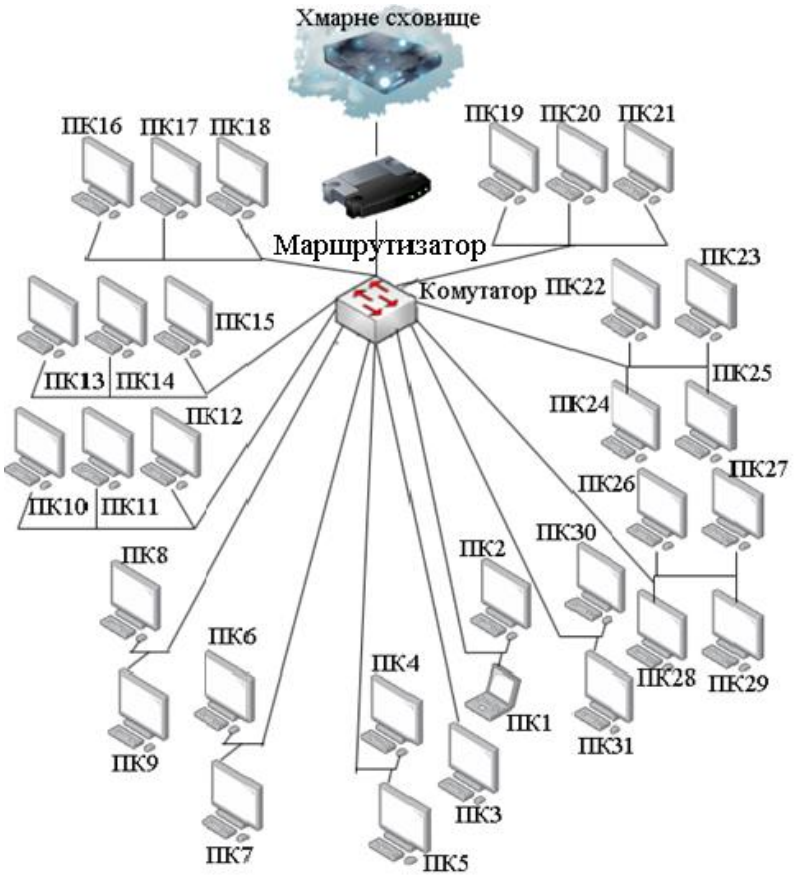


Рисунок 2.5 – Схема ІКС

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 опрацьовуються модель загроз і модель порушника, визначаються критичні загрози, що є метою формування завдання на створення сучасної системи охорони.

Розглянемо модель порушника

Порушник – це особа, яка за допомогою різних методів і засобів, свідомо або несвідомо, з поганими намірами (або без них), намагається здійснити заборонені дії для вигоди або помсти. Для доступу до ІЗОД (інформації з обмеженим доступом) порушник може використовувати різноманітні методи та

інструменти. Зловмисники ретельно вивчають системи безпеки високої якості перед проникненням у інформаційно-комунікаційні системи (ІКС).

Порушники можуть бути двох видів – внутрішні або зовнішні.

Внутрішніми порушниками можуть бути:

- Персонал, кінцеві користувачі (оператори системи);
- Помічники, заступники;
- Співробітники ІТ відділу;
- Голови відділів.

Таблиця 2.4 – Категорії внутрішніх порушників по відношенню до ІКС.

Позначення	Визначення категорії	Рівень загрози
ПВ1	Директор	0
ПВ2	Помічник / Заступник директора	1
ПВ3	Головний бухгалтер / інженер / економіст	2
ПВ4	Начальник відділу	3

Продовження таблиці 2.4

Позначення	Визначення категорії	Рівень загрози
ПВ5	Робітники	4

Зовнішніми порушниками можуть бути як працівники підприємства у чиї обов’язки не входить взаємодія з ІЗОД, так і особи які не мають нічого спільного з даним підприємством чи співпрацюючими підприємствами.

Зовнішніми порушниками можуть бути:

- Клієнти;
- Наймані робітники;
- Агенти ворогуючої країни;

Таблиця 2.5Категорії зовнішніх порушників по відношенню до ІЗОД.

Позначення	Визначення категорії	Рівень загрози

ПЗ1	Охоронник	1
ПЗ2	Прибиральниця	1
ПЗ3	Клієнт	2
ПЗ4	Агент ворога	4

Загрози для інформації, залежать від характеристик фізичного середовища, персоналу, технологій обробки та інших чинників, які мають як суб'єктивну так і об'єктивну природу. Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні.

Припускається, що порушник в своєму рівні – 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 цінностей.

Таблиця 2.6 – Специфікація моделі порушника за мотивами порушення

Позначення	Мотив	Рівень загрози
М1	Безвідповідальність	1
М2	Помста/Самоствердження	2
М3	Професійний обов'язок	3
М4	Корисливий інтерес	4

Таблиця 2.7 – Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІКС

Позначення	Рівень кваліфікації	Рівень загрози
К1	Низький рівень знань, вміє працювати з технічними засобами	1

К2	Середній рівень знань, практичний досвід обслуговування та роботи з компонентами системи охорони	2
К3	Є знання структури, функцій і механізмів дії засобів захисту	2
К4	Високий рівень знань та навичок у галузі програмування	3

Таблиця 2.8– Специфікація моделі порушника за часом дії

Позначення	Характеристика можливостей порушника	Рівень загрози
Ч1	Під час повної бездіяльності системи охорони з метою відновлення та ремонту	1

Продовження таблиці 2.8

Позначення	Характеристика можливостей порушника	Рівень загрози
Ч2	Під час призупинення компонентів системи охорони з метою технічного обслуговування та модернізації	2
Ч3	Під час функціонування системи охорони (або компонентів системи)	3
Ч4	У будь-який час, з доступом до інформації у фізичному сховищі (має відповідний допуск проходження системи охорони)	4

Таблиця 2.9– Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту

Позначення	Харкатеристика можливостей порушника	Рівень загрози
З1	Підслуховування, підглядання за робочим процесом	1
З2	Взлам, підбір паролів до системи охорони	2
З3	Несанкціоновані дії з використанням дозволених засобів	3
З4	Активний вплив усіма можливими засобами	4

Таблиця 2.10 – Специфікація моделі порушника за місцем дії

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

Таблиця 2.11 – Модель порушника

Посада	Категорія	Мотив	Кваліфікація	Можливості	За часом дії	За місцем дії	Сума загроз
Директор	ПВ1	М3	К4	З3	Ч4	Д4	17
	0	3	3	3	4	4	
Головний бухгалтер	ПВ3	М3	К3	З3	Ч3	Д4	17
	2	3	2	3	3	4	
Помічник директора	ПВ2	М3	К2	З2	Ч3	Д2	13
	1	3	2	2	3	2	
Заступник директора	ПВ2	М3	К4	З3	Ч3	Д3	16
	1	3	3	3	3	3	
Начальник відділу	ПВ4	М3	К3	З3	Ч3	Д2	16
	3	3	2	3	3	2	
Головний економіст	ПВ3	М3	К3	З3	Ч3	Д3	16
	2	3	2	3	3	3	
Головний інженер	ПВ3	М3	К4	З3	Ч3	Д4	18
	2	3	3	3	3	4	
Робітник	ПВ5	М2	К2	З2	Ч2	Д2	14
	4	2	2	2	2	2	
Клієнти	ПЗ3	М4	К1	З1	Ч1	Д2	11
	2	4	1	1	1	2	

Продовження таблиці 2.11

Посада	Категорія	Мотив	Кваліфікація	Можливості	За часом дії	За місцем дії	Сума загроз
Агенти ворога	ПЗ4	М4	К4	З4	Ч3	Д4	22
	4	4	3	4	3	4	
Прибиральниця	ПЗ2	М1	К1	З1	Ч1	Д1	6
	1	1	1	1	1	1	
Охоронник	ПЗ1	М1	К1	З1	Ч1	Д1	6
	1	1	1	1	1	1	

Найбільшу внутрішню загрозу підприємству становлять: Головний інженер, Директор, Головний бухгалтер.

Найбільшу зовнішню загрозу підприємству становлять: Агенти ворога.

Це значить що система має бути більш контрольованою.

2.7 Модель загроз

Можливі способи реалізації загроз:

- 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 реєстрованого 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 (фізичної);
- порушення доступності чи відмовлення в обслуговуванні;
- порушення спостережності чи керованості;

З точки зору ІКС розрізняються наступні класи загроз інформації:

1) порушення конфіденційності;
2) порушення цілісності;
3) порушення доступності або відмова в обслуговувані;
4) порушення спостережності або керованості;

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

Таблиця 2.12 – Загрози та можливості їх реалізацій

Загроза	Реалізація	Джерело
Несанкціонований доступ до ІзОД	- порушення правил використання системи - недостатній контроль за діями персоналу	Внутрішнє (навмисне)
Несанкціоноване копіювання інформації	- відсутність контролю та протоколювання журналу подій - порушення правил політики безпеки	Внутрішнє (навмисне)
Викрадення ІзОД шляхом використання облікового запису	- порушення правил політики безпеки	Внутрішнє (навмисне)
Ненавмисне порушення працездатності КС	- недостатній контроль за цілісністю компонентів системи - недостатній контроль з боку служби охорони	Внутрішнє (ненавмисне)

Продовження таблиці 2.12

Загроза	Реалізація	Джерело
Ненавмисне розголошення конфіденційної інформації або інформації, що становить комерційну таємницю	- недостатній контроль за діяльністю робітника	Внутрішнє (ненавмисне)
Знищення чи пошкодження складових ІКС чи всієї ІКС через війну	- направлений ракетний удар - ненаправлений удар ракетою/дроном -	Зовнішнє (навмисне)

Зсув ґрунту	- пошкодження фундаменту будівлі внаслідок землетрусу, рясних опадів чи діяльності людей	Зовнішнє (стихійне)

Найбільш актуальними загрозами до ОІД вважаються:

- несанкціонований доступ до ОІД;
- знищення чи пошкодження складових ІКС чи всієї ІКС через війну;
- несанкціоноване копіювання інформації;
- викрадення ІзОД шляхом використання облікового запису;
- ненавмисне розголошення конфіденційної інформації або інформації, що становить комерційну таємницю.

Якщо ідентифіковані загрози будуть використовувати відповідні вразливості і призведуть до інциденту інформаційної безпеки, негативними наслідками для підприємства може стати повна або часткова втрата інформації, пошкодження або заміна інформації, компрометація інформації.

Для оцінки ризиків використані такі шкали:

Таблиця 2.13– Шкала оцінювання впливу реалізації загроз на конфіденційність

Характеристика	Оцінка рівня наслідків
Практично не призводить до розкриття конфіденційної інформації	1
Призводить до розкриття окремих документів, які відносяться до ІзОД та/або персональних даних і не призводить до фінансових втрат	2
Призводить до розкриття окремих документів, які відносяться до ІзОД та/або персональних даних і призводить до незначних фінансових втрат	3

Призводить до розкриття окремих документів, які відносяться до ІзОД та/або персональних даних і призводить до значних фінансових втрат, може призвести до зупинки роботи системи підприємства	4
Призводить до зупинки роботи системи, порушення вимог нормативно-правової бази	5

Таблиця 2.14– Шкала оцінювання впливу реалізації загроз на цілісність

Характеристика	Оцінка рівня наслідків
Практично не призводить до наслідків з фінансовими втратами	1
Призводить до незначних фінансових втрат	2
Призводить до значних фінансових втрат	3
Призводить до великих фінансових втрат і може привести до зупинки роботи системи підприємства	4
Призводить до зупинки роботи системи, порушення вимог нормативно-правової бази	5

Таблиця 2.15– Шкала оцінювання пливу реалізації загроз на доступність

Характеристика	Оцінка рівня наслідків
Практично не впливає на доступність	1
Вплив на доступність незначний, не більший 10% від максимально допустимого часу простою	2
Вплив на доступність середній, не більший 25% від максимально допустимого часу простою	3
Вплив на доступність великий, до 100% від максимально допустимого часу простою	4

Призводить до зупинки роботи системи, який перевищує максимально допустимий час простою	5

Таблиця 2.16– Шкала оцінювання впливу реалізації загроз на спостережність

Характеристика	Оцінка рівня наслідків
Практично не впливає	1
Вплив незначний	2
Призводить до неможливості відстежити частину дій користувачів в системі	3
Призводить до неможливості відстежити дії користувачів і адміністраторів в системі	4
Призводить до неможливості відстежити дії всіх користувачів і адміністраторів системи, може призвести до зупинки системи на тривалий час	5

Оцінка збитків, що можуть бути нанесені ІКС внаслідок реалізації загроз складається з величин очікуваних збитків від втрати інформацією кожної з властивостей (конфіденційності, цілісності або доступності) або від встрати керованості системи внаслідок реалізації загрози. Величина можливих збитків визначається розміром фінансових втрат якісною шкалою, через визначення цього критерія кількісно.

Таблиця 2.17– Величина збитків

Оцінка	Характеристика
1	Відсутня
2	Низька
3	Середня
4	Висока
5	Неприпустимо висока

Таблиця 2.18– Шкала ймовірності реалізації загроз

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

Для оцінки ризиків використана комбінація кількісних та якісних методів, що дає змогу розрахувати доцільність створення політики безпеки як нормативної основи для запровадження сучасної технічної системи захисту інформації, адже вартість заходів безпеки, не мають біти більшими, ніж фінансові втрати інциденту інформаційної безпеки.

Рівень ризику за окремою парою загроза-вразливість визначається перемноженням оцінки ймовірності реалізації на оцінку величини можливих збитків та на максимальну величину з окремих оцінок впливу на цілісність, конфіденційність, доступність спостережність.

Для створення пари загроза-вразливість, необхідно виокремити найбільш критичну вразливість по загрозі. Рівень критичності вказує наскільки сильним є вплив загрози на ресурс з урахуванням ймовірності її реалізації.

Це виокремлення вразливостей проводяться експертним методом. До загроз, що мають більше однієї вразливості відносяться:

- несанкціонований доступ до ІзОД;
- знищення або пошкодження частин ІКС чи всієї ІКС через війну;
- несанкціоноване копіювання інформації;
- ненавмисне порушення працездатності КС.

Результати оцінки рівня ризику наведені у Таблиці2.19

Таблиця 2.19– Рівень ризику

№	Загроза / вразливість	Оцінка ймовірності реалізації загрози з використанням вказаної вразливості	Оцінка реалізації загрози на конфіденційність	Оцінка реалізації загрози на цілісність	Оцінка реалізації загрози на доступність	Оцінка реалізації загрози на спостережність	Оцінка величин можливих збитків	Рівень ризику за окремою парою загроза-вразливість
1	Несанкціонований доступ до ІзОД	2	3	1	1	2	2	18
2	Несанкціоноване копіювання інформації	3	3	2	1	1	3	30
3	Викрадення ІзОД шляхом використання облікового запису	2	3	2	1	2	3	22
4	Ненавмисне порушення працездатності КС	1	4	4	3	3	4	18
5	Ненавмисне розголошення конфіденційної інформації або інформації,	2	3	1	1	1	3	18

Продовження таблиці 2.19

№	Загроза / вразливість	Оцінка ймовірності реалізації загрози з використанням вказаної вразливості	Оцінка реалізації загрози на конфіденційність	Оцінка реалізації загрози на цілісність	Оцінка реалізації загрози на доступність	Оцінка реалізації загрози на спостережність	Оцінка величин можливих збитків	Рівень ризику за окремою парою загроза-вразливість

	що становить комерційну таємницю							
6	Знищення чи пошкодження складових ІКС чи всієї ІКС через війну	2	5	5	5	5	5	50

Отже, найбільш критичними для системи є наступні загрози: знищення чи пошкодження складових ІКС чи всієї ІКС через війну, несанкціоноване копіювання інформації (вірусною програмою, або людиною на носій) та викрадення ІзОД шляхом використання облікового запису (розголос паролів або шпигунство). Ці загрози необхідно повинні бути врахованими при створенні організаційних засобів протидії загрозам у контексті розробки технічної системи захисту інформації.

2.8 Профіль захищеності

Згідно з 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 підприємства «ЖИЛСЕРВІС-5» було 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 2.20 – Профіль захищеності підприємства

№	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.
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.

Продовження таблиці 2.20

№	Послуга	Назва	Опис
			КЗЗ повинен надавати можливість адміністратору або користувачу, що має 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.
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 пошук наявних 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.
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 визначити рівень

Продовження таблиці2.20

№	Послуга	Назва	Опис
			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.
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.
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.
8	ЦО-2	Повний відкат	Політика відкату, що реалізується КЗЗ, повинна визначити множину об’єктів КС, до яких вона відноситься.

Продовження таблиці 2.20

№	Послуга	Назва	Опис
			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 експорту/імпорту через незахищене середовище. Рівні даної послуги різняться 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, рівеньзахищеності, 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.
10	НР-4	Детальна реєстрація	Політика реєстрації, що реалізується КЗЗ, повинна визначити перелік подій, що реєструється. 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

Продовження таблиці 2.20

№	Послуга	Назва	Опис
			розпорядженні засоби перегляду і аналізу журналу реєстрації.

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 визначити 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.
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.

Продовження таблиці 2.20

№	Послуга	Назва	Опис
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 різняться на підставі можливості виконання тестів у процесі запуску або штатної роботи.
16	НВ-2	Автентифікація джерела даних	Політика ідентифікації і автентифікації 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 з 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.
18	НП-1	Базова автентифікація одержувача	Політика автентифікації одержувача, що реалізується КЗЗ, повинна визначати множину властивостей і атрибутів об’єкта, що передається,

Продовження таблиці 2.20

№	Послуга	Назва	Опис

			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 технічної системи охорони

Побудова технічних систем протидії витоку інформації матеріально-речовим каналом здійснюється з урахуванням того, що основними носіями інформації є матеріальні об’єкти, доступ до яких може бути реалізований шляхом фізичного вилучення, копіювання або навмисного пошкодження. У зв’язку з цим такі системи ґрунтуються на наступних базових положеннях:

Структурна узгодженість технічних засобів захисту передбачає інтеграцію інженерних конструкцій, систем контролю доступу та засобів зберігання інформації в єдину захисну архітектуру.

Багатокомпонентний характер технічного впливу забезпечує одночасне застосування різних типів засобів захисту, спрямованих на протидію таким загрозам, як підміна документів, копіювання матеріальних носіїв або їх приховане переміщення

Постійна підтримка захисного режиму досягається шляхом безперервного функціонування технічних систем охорони приміщень і місць зберігання носіїв інформації, що знижує ймовірність реалізації загроз, пов’язаних із тимчасовою відсутністю контролю.

Технічна співмірність захисту рівню загроз означає, що вибір засобів протидії здійснюється з урахуванням реальних способів витоку інформації матеріально-речовим каналом, зокрема несанкціонованого доступу персоналу або сторонніх осіб до носіїв інформації.

Можливість оперативного коригування параметрів захисту дозволяє адаптувати режими доступу та охорони у разі зміни умов експлуатації або появи нових загроз, пов’язаних із фізичним обігом інформації.

Регламентована прозорість технічних рішень забезпечує контрольовану відкритість принципів функціонування систем захисту, за винятком елементів, розкриття яких може призвести до спрощення реалізації загроз матеріально-речового характеру.

Розроблення технічних систем протидії витоку інформації матеріально-речовим каналом здійснюється на етапі підготовки до створення системи технічного захисту інформації відповідно до вимог НД ТЗІ 3.7-001-99, НД ТЗІ 2.5-004-99 та чинного законодавства України у сфері технічного захисту інформації.

Процес формування таких систем реалізується через послідовність взаємопов’язаних етапів:

1.Виконується обґрунтування концептуальних рішень щодо обмеження фізичного доступу до носіїв інформації, що спрямовано на зниження загроз несанкціонованого вилучення документів, знімних носіїв та інших матеріальних об’єктів.

2.Аналіз можливих шляхів витоку через матеріальні об’єкти, включаючи винесення документів, приховане копіювання, підміну або знищення носіїв інформації, що дозволяє сформувати актуальну модель загроз матеріально-речового каналу.

3.Здійснюється формування технічних вимог до засобів фізичного захисту, зокрема до систем контролю та управління доступом, охоронної сигналізації, сховищ і сейфів, з урахуванням визначених загроз.

4.Вибір та впровадженні спеціалізованих технічних рішень, спрямованих на унеможливлення несанкціонованого обігу матеріальних носіїв інформації в межах та за межами контрольованих зон.

5.Організація технічного супроводу та відновлення працездатності систем захисту, що забезпечує стійкість протидії загрозам матеріально-речового каналу у процесі тривалої експлуатації.

6.Розроблення та оформлення технічної і регламентної документації, яка визначає порядок використання, контролю та оцінювання ефективності технічних систем захисту інформації від витоку матеріально-речовим каналом.

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

- правових і/або договірних засад;
- вимог до забезпечення безпеки інформації згідно з завданнями і функціями ІКС;
- загроз, яким зазнають впливу ресурси ІКС, що підлягають захисту.

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

- мета і пріоритети, яких необхідно дотримуватись в ІКС 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 ІКС, їхні права і обов’язки щодо реалізації завдань безпеки інформації.

Сучасні технічні системи охороніповинні забезпечити захист конфіденційної інформації про співробітників, фінансову діяльність, клієнтів та державні акти.

Основною ціллю реалізації сучасних технічних систем охороніє забезпечення ефективного функціонування підприємства, для чого необхідно забезпечити захист оброблюваної на підприємстві інформації від несанкціонованого доступу. Окрім технічних систем охорони, також було обрано

створення політики безпеки інформації, які мають на меті розробку та впровадження правил та норм внутрішнього режиму праці на підприємстві, режиму доступу і допуск до важливих об’єктів, їх охорона та середовище розміщення.

Необхідність забезпечення захисту інформації, а саме створення сучанчої технічної системи захисту інформації, визначається передусім вимогами власника інформаційних ресурсів.

На основі аналізу моделі загроз було обрано найбільш актуальні загрози:

1.несанкціоноване копіювання інформації (людиною на носій);

2.викрадення ІзОД шляхом використання облікового запису (розголос паролівабо шпигунство).

Тому пропонується розробити та запровадити такі засоби протидії як сучасні технічні системи охорони та створення політик безпеки (запровадження юридичного документу з чітко прописаними пунктами його дотримання і можливих санкцій)

Було розроблено наступні політики безпеки:

Політика антивірусного захисту;

Політика користування зйомними носіямиінформації та збереження фізичних носіїв інформації;

Політика захисту паролів;

Політика «Чистого столу».

ЗАТВЕРДЖЕНО

Директором Комунального

Підприємства «ЖИЛСЕРВІС-5»

КАРПЕНКО С.С.

«__»_____ 202_

ПОЛІТИКА АНТИВІРУСНОГО ЗАХИСТУ

Мета політики: Зменшення ризику зараження інформаційно-комунікаційної системи шкідливим програмним забезпеченням.

Інструкція політики:

- На кожному комп’ютері мають бути встановлені антивірусне програмне забезпечення;
- Дозволяється використовувати лише ліцензоване антивірусне програмне забезпечення, затверджене директором підприємства;
- Налаштовувати та встановлювати антивірусне програмне забезпечення дозволено тільки директорута начальнику технічного відділу;
- Антивірусне програмне забезпечення має завжди своєчасно оновлюватися;
- Файли, завантажені з Інтернету та/або отримані від сумнівного джерела, перед відкриттям необхідно сканувати антивірусним програмним забезпеченням;
- При виникненні проблеми з роботою антивірусного програмного забезпечення, співробітник повинен негайно повідомити начальника технічного відділу.

Відповідальність:

- Відповідальність несуть всі співробітники підприємства.

- Співробітник, який порушив цю політику, може бути підданий дисциплінарному стягненню, або бути звільнений з можливим подальшим судовим провадженням.

Порядок перегляду політики:

Ця політика повинна переглядатись кожний рік директором та начальником технічного відділу.

ЗАТВЕРДЖЕНО

Директором Комунального

Підприємства «ЖИЛСЕРВІС-5»

КАРПЕНКО С.С.

«__»_____ 202_

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:

- Кожний носій на підприємстві повинен підлягати обліку;
- У кожного носія повинен бути свій інвентарний номер;
- Видача та повернення зйомних носіїв повинна фіксуватись у журналі;
- Журнал фіксацій видач та повернень зйомних носіїв повинен зберігатись у керівника технічного відділу або директора підприємства (далі відповідальні особи);
- За видачу носіїв несуть відповідальність керівник технічного відділу та/або директор підприємства.

Забороняється:

- Зберігання носіїв без сейфів, як паперових так і зйомних;
- Використання носіїв інформації отриманих не від відповідальних осіб;
- Передавати носії інформації стороннім особам;
- Передавання іншим співробітникам носії інформації отриманих не від відповідальних осіб.

Область дії політики:

- Поширюється на всіх співробітників підприємства;
- Поширюється на території підприємства.

Відповідальність:

- Відповідальність за впровадження покладається на відповідальних осіб;
- Відповідальність за виконання покладається на всіх співробітників підприємства;
- Співробітник, який порушив цю політику, може бути підданий дисциплінарному стягненню, або бути звільнений з можливим подальшим судовим провадженням.

Порядок перегляду політики:

Ця політика повинна переглядатись кожний рік директором та начальником технічного відділу.

ЗАТВЕРДЖЕНО

Директором Комунального

Підприємства «ЖИЛСЕРВІС-5»

КАРПЕНКО С.С.

«__»_____ 202_

ПОЛІТИКА ЗАХИСТУ ПАРОЛІВ

Мета політики: Створення та захист надійних паролів для співробітників підприємства.

Інструкція політики:

- Створення нових паролів здійснюється начальником технічного відділу;
- Зміна паролю принаймні кожні 60 днів;

Забороняється:

- Записувати паролі;
- Зберігати в Інтернеті без засобів захисту/шифрування;
- Використовувати пароль в особистих цілях (особисті облікові записи соціальних мереж, банкінгу, будь-яких онлайн сервісів та ресурсів тощо);
- Передавати паролі стороннім особам;
- Розголошувати паролі в повідомленнях електронної пошти, по телефону, та будь-якими іншими способами.

Відповідальність:

- Відповідальність за впровадження покладається на начальника технічного відділу;
- Відповідальність за виконання покладається на всіх співробітників підприємства;

- Співробітник, який порушив цю політику, може бути підданий дисциплінарному стягненню, або бути звільнений з можливим подальшим судовим провадженням.

Порядок перегляду політики:

Ця політика повинна переглядатись кожний рік директором та начальником технічного відділу.

ЗАТВЕРДЖЕНО

Директором Комунального

Підприємства «ЖИЛСЕРВІС-5»

КАРПЕНКО С.С.

«__»_____ 202_

ПОЛІТИКА «ЧИСТОГО СТОЛУ»

Мета політики: Створення інструкцій для захисту інформації яка може знаходитися на робочому місці співробітника підприємства та гарантувати її захист в момент відсутності співробітника або після закінчення робочого дня.

Інструкція політики:

- Конфіденційна інформація повинна бути закрита на робочому столі, якщо вона не потрібна для користування;
- Роздруківки які містять конфіденційну інформацію повинні бути закриті в столі відповідальних за неї співробітників;
- Компьютер/ноутбук повинен бути заблокований, якщо спіробітник не на місці (навіть якщо відійшов ненадовго);
- Компьютер/ноутбук повинен бути заблокований та вимкнений в кінці робочого дня;
- Зберігати носії інформації у ящиках столу та/або у шухляді поруч (при наявності);
- В кінці робочого дня закрити приміщення, здати ключі відповідній за них особі та активувати охорону систему.

Відповідальність:

- Відповідальність несуть всі співробітники підприємства.
- Співробітник, який порушив цю політику, може бути підданий дисциплінарному стягненню, або бути звільнений з можливим подальшим судовим провадженням.

Порядок перегляду політики:

Ця політика повинна переглядатись кожний рік директором та начальником технічного відділу.

При вивчені плану підприємства було розглянуто декілька варіантів сучасної технічної системи охорони, порівнюючи їх між собою та вимогами підприємства було обрану ту, яка працюватиме найефективніше. На рисунку 2.6 (а, б) показано плану підприємства (а) та технічна системи охорони (б), яка було розроблена та обрана відповідно до вимог підприємства:

Рисунок 2.6 (а, б) – Схема плану території підприємства (а), схема технічної системи охорони (б)

Таблиця 2.21 – Умовні позначення

Графічне позначення	Назва
	Точковий магнітоконтактний датчик
	Сповіщувач пожежний
	Об’ємний інфрачервоний датчик руху
	Звуковий оповіщувач
	Точковий димовий датчик
	Металеві грати

Для втілення в реальність плану технічної системи охорони необхідно знайти та порівняти різноманітні датчики, пошук проводився мережею інтернет та було порівняно характеристики надані виробниками, а також обґрунтовано вибір датчиків в категоріях відповідних таблиці 2.21, окрім металевих грат, а також, треба зазначити, що до точкових магнітоконтактнихдатчиків встановлених на вікнах були також додані акустичні датчики розбиття вікон

Таблиця 2.22 - Магнітоконтактний датчик на відкривання дверей та вікон

Вигляд датчика	Характеристики датчика
 66 грн	**Датчик відкриття Геркон СМК-1Е (білий)** Тип пристрою: датчик відкриття Тип установки накладний Тип поверхні: дерево (пластик) Режим тривоги, мм:25 Черговий режим, мм:10 Напруга живлення: не вимагає Матеріал: пластик Колір: білий Розміри 28 х 12 х 5
 72 грн	**Дротовий магнітоконтактний сповіщувач ЭСМК-1** Покриття дерево, пластик, метал Метод роботи дротовий магнітоконтактний Параметри струму 0.1 - 100 мА, 1 - 60В Відстань спрацьовування 10 - 25 мм Робоча температура -40°С - +50°С Розмір упаковки (Ш х В х Г) 12 х 28 х 7 мм Вага брутто 0.001 кг
 89 грн	**ДатчиквідкриттяАлайСОМК 1-9** Тип датчика провідний Тип установки накладний Поріг спрацьовування 1,5 см/3,4 см Можливість зовнішнього застосування є Можливість монтажу на металеві двері, ворота ні Діапазон робочих температур -40°С ~ +50°С Робоча вологість не більше 90% Розміри 29х13х6, 5 мм Вага 8,5 г

За таблицею 2.22 усі три варіанти датчиків відкриття дверей та вікон здаються на перший погляд ідентичними, однак третій варіант вирізняється додатково вказаними характеристиками які виробники інших не вказали, але підприємство на своїй території має певну кількість металевих дверей, на які немає можливості встановити третій варіант датчику, так само як і перший, через це другий варіант залишається єдиним придатним варіантом. Тому **Дротовий магнітоконтактний сповіщувач ЭСМК-1**був обраний до системи захисту підприємства як магнітоконтактний датчик на відкривання дверей та вікон.

Таблиця 2.23 - Точковий датчик на дим

Вигляд датчика	Характеристики датчика	
 194 грн	Датчик диму оптичний точковий Артон СПД-3.10	
	Тип пристрою	датчик диму
	Тип датчика	оптичний точковий
	Спосіб підключення до ППК	2-дротовий
	Спосіб формування вихідного сигналу	безконтактний
	Наявність індикації чергового режиму	є
	Внутрішній опір, Ом	500
	Напруга живлення / джерело живлення	DC 9-30 В
	Струм споживання, мА	5-30
	Робоча температура, °С	-10 ~ +55
	Розміри, мм	85 x 37
 259 грн	**Датчик диму оптичний точковий Артон СПД-3 (ИПД-3)**	
	Тип пристрою	датчик диму
	Тип датчика	оптичний точковий
	Спосіб підключення до ППК	2-дротовий
	Спосіб формування вихідного сигналу	безконтактний
	Наявність індикації чергового режиму	є
	Внутрішній опір, Ом	500
	Напруга живлення / джерело живлення	DC 9-30 В
	Струм споживання, мА	5-30
	Робоча температура, °С	-10 ~ +55
	Розміри, мм	100 x 48

Продовження таблиці 2.23

Вигляд датчика	Характеристики датчика
 414 грн	**Датчик диму оптичний точковий Артон СПД-3.2 (БН)** Тип пристрою: датчик диму Тип датчика: оптичний точковий Спосіб підключення до ППК: 4-дротовий Спосіб формування вихідного сигналу: розмикання контактів реле Наявність індикації чергового режиму: є Внутрішній опір, Ом: 500 Напруга живлення / джерело живлення: DC 12 В Струм споживання, мА: 22 Робоча температура, °С: -10 ~ +55 Розміри, мм: 100 х 48

Три варіанти датчиків детекторів диму між собою майже ідентичні, а ті відмінності що в них є не виправдовують переплату за другий та третій варіанти. Через це було обрано перший варіант**Датчик диму оптичний точковий Артон СПД-3.10**до системи захисту підприємства як точковий датчик на дим.

Таблиця 2.24 - Акустичний датчик на розбиття вікон

Вигляд датчика	Характеристики датчика
 602 грн	**Датчик розбиття скла Crow GBD-plus** Тип датчику: датчик розбиття скла Тип підключення: дротовий Дальність зв’язку: обмежено довжиною лінії та опором кабелю Тип детектування: розбиття скла Чутливий елемент: електретний мікрофон Дальність / площа детекції: 10 м Тривожний вихід датчика: нормально-замкнений, 24 В / 50 мА / 27 Ом Індикація: світлова (жовтий, зелений, червоний LED) Робоча напруга: DC 9V, DC 12V Габаритні розміри: 78 × 51 × 21 мм Вага: 70 г Діапазон температур: -20 ~ +50 °C

Продовження таблиці 2.24

Вигляд датчика	Характеристики датчика
 690 грн	Датчик розбиття скла GSN Patrol-501 дротовий Тип датчику: датчик розбиття скла Тип підключення: дротовий Дальність зв’язку: обмежено довжиною лінії та опором кабелю Тип детектування: розбиття скла Чутливий елемент: електретний мікрофон Дальність / площа детекції: 12 м, 170 ° Тривожний вихід датчика: NC, 60 В, 120 мА, 16 Ом Індикація: світлова (жовтий, зелений, червоний LED) Робоча напруга: DC 12V Габаритні розміри: 87 х 52 х 24 мм Вага: 58 г Діапазон температур: -30 ~ +50 °C
 826 грн	Датчик розбиття скла Satel MAGENTA дротовий з регулюванням чутливості та сповіщенням Тип датчику: датчик розбиття скла Тип підключення: дротовий Дальність зв’язку: обмежено довжиною лінії та опором кабелю Тип детектування: розбиття скла Чутливий елемент: електретний мікрофон Дальність / площа детекції: до 6 м Тривожний вихід датчика: 40 мА / 16 В DC Індикація: світлова Робоча напруга: DC 12V Габаритні розміри: 26 х 112 х 29 мм Вага: 40 г Діапазон температур: -10 °C ~ +55 °C

З трьох варіантів датчиків розбиття скла третій виділяється лише більшою вартістю але не відрізняється, а в деяких моментах навіть гірше, від інших двох, через це він одразу відпадає. З двох інших варіантів, які залишилися другий варіант виділяється тим що може працювати в більшому діапазоні температур та більшою дальністю детекції, це саме ті характеристики які роблять другий варіант кращим за перший, тому**Датчик розбиття скла GSN Patrol-501 дротовий**був обраний до системи захисту підприємства як акустичний датчик на розбиття вікон.

Таблиця 2.25 - Пожежна кнопка

Вигляд датчика	Характеристики датчика
 212 грн	**Сповіщувач пожежний ручний Артон SPR-1** Діапазон напругиживлення: 9 - 30 В Струм споживання в черговому режимі: 5 - 20 мА Спосіб підключення до ППК: двопровідний ШС Габаритні розміри: 102 х 102 х 38 мм Маса: 0.12 кг Наявність індикації чергового режиму: Ні Оптична індикація режиму "Пожежа": Ні Наявність додаткових клем для зручності підключення проводів, резисторів: ні
 220 грн	**Сповіщувач пожежний ручний Артон SPR-1L** Діапазон напругиживлення: 9 - 30 В Струм споживання в черговому режимі: 0.005 мА Спосіб підключення до ППК: двопровідний ШС Габаритні розміри: 102 х 102 х 38 мм Маса: 0.12 кг Наявність індикації чергового режиму: Ні Струм споживання в режимі ПОЖЕЖА: 5 - 20 мА Оптична індикація режиму "Пожежа": так Наявність додаткових клем для зручності підключення проводів, резисторів: ні

Продовження таблиці 2.25

Вигляд датчика	Характеристики датчика
 233 грн	**Сповіщувач пожежний ручний Артон SPR-3L** Діапазон напругиживлення: 9 - 30 В Струм споживання в черговому режимі: 0.05 мА Спосіб підключення до ППК: двопровідний ШС Габаритні розміри: 102 х 102 х 38 мм Маса: 0.12 кг Наявність індикації чергового режиму: Так Оптична індикація режиму "Пожежа": так Наявність додаткових клем для зручності підключення проводів, резисторів: ні

Три варіанти пожежних кнопок майже не відрізняються між собою як в ціні так і в характеристиках, але єдина цікава відмінність в третьому варіанті, яка на порядок її виділяє серед двох інших це наявність чергового режиму, саме через це було обрано **Сповіщувач пожежний ручний Артон SPR-3L**до системи захисту підприємства як пожежну кнопку.

Таблиця 2.26 - Інфрачервоний датчик руху

Вигляд датчика	Характеристики датчика
 402.55 грн	**ІЧ сповіщувач Satel Topaz** Категорія виробу: датчик (сповіщувач) руху Тип підключення: провідний Метод детектування: ІК (інфрачервоний) Кут детекції (по горизонталі): 98° Дальність детектування (м): 12 Тамперний контакт: Є Висота установки (м): 2.1 Напруга електроживлення (В): 12 Струм споживання (мА): 8.5 Умови експлуатації: -10...+55 °C Габаритні розміри: 52 х 81 х 33 Вага (г): 45

Продовження таблиці 2.26

Вигляд датчика	Характеристики датчика
 454.75 грн	**ІЧ сповіщувач руху DSCLC-100** Категорія виробу: датчик (сповіщувач) руху Тип підключення: провідний Метод детектування: ІК (інфрачервоний) Кут детекції (по горизонталі): 90° Дальність детектування (м): 15 Тамперний контакт: Є Висота установки (м): 2.4 Напруга електроживлення (В): 9-16 Струм споживання (мА): 10 Умови експлуатації: -30°С ~ +70°С Габаритні розміри: 92 х 62,5 х 40 Вага (г): 40
 558 грн	**Датчик руху Crow SRP-600** Категорія виробу: датчик (сповіщувач) руху Тип підключення: провідний Метод детектування: ІК (інфрачервоний) Кут детекції (по горизонталі): 105° Дальність детектування (м): 18 Тамперний контакт: Є Висота установки (м): 1.5-3.6 Напруга електроживлення (В): 12 Струм споживання (мА): 9 Умови експлуатації: -20°С ~ +60°С Габаритні розміри: 106 х 68,5 х 57 Вага (г): 90

При виборі датчика руху, від першого до третього окрім зростання ціни також зростає найважливіші характеристики датчику руху, а саме кут охоплення та дальність детектування, так як в приміщення було обрано не більше 2 датчиків руху то надається перевага більшому куту та більшій дальності детектування. Тому **Датчик руху Crow SRP-600** був обраний до системи захисту підприємства як інфрачервоний датчик руху.

Таблиця 2.27 - Звуковий оповіщувач

Вигляд датчика	Характеристики датчика
 109 грн	**Сирена ATIS SA-103 (black)** Тип пристрою: звуковий сповіщувач Тип встановлення: внутрішнє Тип підключення: дротове Акустична потужність, дБ: 110 Тип оповіщення: звукове Живлення: DC 12V Струм споживання, мА: 150 Матеріал: пластик Робоча температура, °С: -10 ~ +55 Розміри, мм: 59 x 47 x 40 Гарантія, міс: 12
 126 грн	**Оповіщувач SA-105 (black)** Тип пристрою: звуковий сповіщувач Тип встановлення: внутрішнє Тип підключення: дротове Акустична потужність, дБ: 105 Тип оповіщення: звукове Живлення: DC 12V Струм споживання, мА: 150 Матеріал: пластик Робоча температура, °С: -30 ~ +55 Розміри, мм: 72 x 52 x 46 Гарантія, міс: 12

У випадку звукового оповіщувача дуже виділяється робоча температура другого варіанту, з урахуванням того, що під війни і постійних довгих відключень світла, краще обрати другий варіант аби навіть при відключенні централізованого електропостачання даний оповіщувач працював справно. Не розглядалися інші варіанти, через те що вони на порядок дорожчі з мінімальними

додатковими харакетристиками, тобто їх обирати було б недоцільно з урахуванням потреб комунального підприємства. Тому **Оповіщувач SA-105 (black)** був обраний до системи захисту підприємства як звуковий оповіщувач.

Після місткого дослідження ринку елементів системи охорони, повноцінного аналізу та тривалого вибору, треба розділити територію підприємства на зони та рубежі і приписати відповідні датчики до відповідних зон та рубежів для повноцінної та ефективної роботи технічної системи охорони. На таблиці 2.28 показано до якого рубежу належать відповідні зони і до яких зон які датчики належать.

Таблиця 2.28 – Розподілення датчиків, зон та рубежів

Рубіж	Назва ділянки	Засіб виявлення
Рубіж 1(Периметр)	Зона 1(вхідні двері)	Дротовий магнітоконтактний сповіщувач ЭСМК-1
Рубіж 1(Периметр)	Зона 2(вікно1)	Дротовий магнітоконтактний сповіщувач ЭСМК-1 Датчик розбиття скла GSN Patrol-501 дротовий
Рубіж 1(Периметр)	Зона 3(вікно2)	Дротовий магнітоконтактний сповіщувач ЭСМК-1 Датчик розбиття скла GSN Patrol-501 дротовий
Рубіж 1(Периметр)	Зона 4(вікно3)	Дротовий магнітоконтактний сповіщувач ЭСМК-1 Датчик розбиття скла GSN Patrol-501 дротовий
Рубіж 2(Об’єм приміщень)	Зона 5(коридор)	Датчик руху Crow SRP-600 Датчик диму оптичний точковий Артон СПД-3.10

Продовження таблиці 2.28

Рубіж	Назва ділянки	Засіб виявлення
		Сповіщувач пожежний ручний Артон SPR-3L
Рубіж 2(Об’єм приміщень)	Зона 6 (робоча зона1)	Датчик руху Crow SRP-600 Датчик диму оптичний точковий Артон СПД-3.10
Рубіж 2(Об’єм приміщень)	Зона 7 (робоча зона2)	Датчик руху Crow SRP-600 Датчик диму оптичний точковий Артон СПД-3.10
Рубіж 2(Об’єм приміщень)	Зона 8 (робоча зона3)	Датчик руху Crow SRP-600 Датчик диму оптичний точковий Артон СПД-3.10
Рубіж 3(Внутрішні двері)	Зона 9 (двері у робочу зону1)	Дротовий магнітоконтактний сповіщувач ЭСМК-1
Рубіж 3(Внутрішні двері)	Зона 10 (двері у робочу зону2)	Дротовий магнітоконтактний сповіщувач ЭСМК-1
Рубіж 3(Внутрішні двері)	Зона 11 (двері у робочу зону3)	Дротовий магнітоконтактний сповіщувач ЭСМК-1
Рубіж 4(Пожежна кнопка)	Зона 12 (Зона пожежної кнопки)	Сповіщувач пожежний ручний Артон SPR-3L

Після того як усе було збалансовано розподілено – треба обрати ПКП до якого будуть підключені усі датчики відповідно до визначених зон та рубежів. ПКП обиратиметься на основі аналізу технічних характеристик: кількість охоронних зон, можливість розширення кількості зон, канал передачі тривожних повідомлень та канали зв’язку. В таблиці 2.29 наведені три варіанти ПКП які можуть підійти для технічної системи захисту.

Таблиця 2.29 – Приймально-контрольний прилад

Вигляд прилада	Характеристики прилада
 6 266 грн	**Прилад приймально-контрольний Лунь-25Е** Кількість зон 5 Інтерфейси зв'язку 2G Модулі розширення модулями АМ 11: +12 зон Особливості Управління: брелок, проксіміті карта, мобільний телефон Розмір упаковки (Ш х В х Г) 140 х 190 х 43 мм Вага брутто 0.6 кг
 7 838 грн	**Прилад приймально-контрольний Tipac Tiras ППК "Orion NOVA L (I)"** Шлейфи 16 Напругав зоні/шлейфі 8 - 12 В Кількість груп 128 Входи/виходи 2 релейні виходи; 2 сигнальні транзисторні виходи; 2 силові транзисторні виходи Особливості 16 базових зон сигналізації з можливістю розширення до 128 зон 128 груп; 128 користувача; Вбудований GSM (GPRS)-комунікатор; Підтримка 2-х SIM-карток; 2 системні шини RS-485 (до 15 приладів розширення); 2 універсальні слоти для дод Клас захисту IP30 Живлення 220 В Робоча температура -10 ° С - + 40 ° С Розміри 280x280x80 мм Вага 1,6 кг

Продовження таблиці 2.29

Вигляд прилада	Характеристики прилада
 8 224 грн	**Функціональний блок Дунай-16/32+Дунай-G1R ФБ (GPRS)** GPRS — Підтримує Клавіатура — Підтримує Провідні зони — 16 (до 128) Програмовані виходи — 1 (до 64) Живлення — 12В Потужність споживання — 350 мА Розміри — 230x230x100мм Розмір упаковки (Ш х В х Г) — 240 х 300 х 92 мм Вага брутто — 0.4 кг

З трьох варіантів ПКП одразу вирізняється другий, тим що в ньому одразу є достатньо велике кількість вакантних груп та зон, що дає змогу не хвилюватися про зміну ПКП при можливому майбутньому оновлені або розширені технічної системи охорони, окрім цього це єдиний ПКП виробник якого зазначив робочу температуру що в сучасних умовах дуже важливо розуміти при виборі будь-якого елементу для системи охорони. Через ці важливі відмінності і було обрано ПКП Прилад приймально-контрольний Tipac Tiras ППК "Orion NOVA L (I)" до технічної системи захисту інформації.

Наступним кроком буде розрахувати загальну вартість обраних технічних засобів системи охоронної, розрахунки наведені в таблиці 2.30.

Таблиця 2.30 – Розрахунок вартості технічної системи захисту інформації

Технічний засіб	Кількість	Ціна
Дротовий магнітоконтактний сповіщувач ЭСМК-1	47 одиинць	72 грн/одиницю 3 384 грн
Датчик диму оптичний точковий Артон СПД-3.10	24 одиниць	194 грн/одиниця 4 656 грн
Датчик розбиття скла GSN Patrol-501 дротовий	22 одиниці	690 грн/одиницю 15 180 грн
Сповіщувач пожежний ручний Артон SPR-3L	5 одиинць	233 грн/одиницю 1 165 грн
Датчик руху Crow SRP-600	26 одиниць	558 грн/одиницю 14 508 грн
Оповіщувач SA-105 (black)	6 одиниць	126 грн/одиницю 756 грн
Прилад приймально-контрольний Tipac Tiras ППК "Orion NOVA L (I)"	1 одиниця	7838 грн/одиинцю
Разом	131 одиниця	47 487 грн

2.10 Висновок

У другій частині кваліфікаційної роботи було розглянуто загальні відомості комунального підприємства «ЖИЛСЕРВІС-5», яка інформація циркулює в підприємстві, модель порушника та загроз, профіль захищеності,розроблені політики безпеки та врештірешт створено сучасну технічну систему захисту відповідно до потреб та вимог підприємства. Інформація наведена в другій частині роботи була частково змінена, зміни не впливають на технічні можливості та наявні рішення.

Результатом обстеження ОІД став аналіз загроз та вразливостей підприємства:

- зроблено обстеження стану підприємства;
- наведена схема інформаційних потоків;
- показана організаційна структура підприємства;
- побудовані моделі порушника та загроз;
- розписано обраний профіль захищеності;

Розроблено політику безпеки, яка включає в себе:

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

Створено сучасну систему захисту:

- Створено план системи захисту який ефективно покриває усю площу підприємтсва та може виявити проникнення з будь-якого напрямку;
- Обрано дієві та ефективні варіанти датчиків які в сукупності мінімізують або навіть зводять на нівець усі можливі сліпі зони;
- Розраховано вартість усього обладнання необхідного для захисту інформації як описано в двох попередніх пунктах.

Функціональний профіль захищеності в АС підприємства був обраний на підставі проведених аналізів загроз та оцінки ризиків і обраний на підставі обраного класу АС відповідно до документа НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні класи захищеності оброблюваної інформації від несанкціонованого доступу».

РОЗДІЛ 3. КОНСТРУКТИВНИЙ РОЗДІЛ

3.1 Вступ

Основною задачею конструктивного обґрунтування є визначення ефективності використання основних та супутніх результатів, що мають бути отримані при виконанні дипломного проекту.

При виконанні дипломних проектів науково-дослідницького характеру, що не приводять на даному етапі до впровадження їхніх результатів у виробництво, техніко-економічні розрахунки повинні містити: орієнтовний розрахунок одноразових (капітальних) витрат, експлуатаційних витрат, а також оцінку науково-технічної і соціальної результативності науково-дослідної роботи.

Економічна доцільність визначається:

- розрахуванням капітальних витрат, які потребує розроблені технічні системи охорони;
- розрахуванням експлуатаційних витрат;
- розрахуванням річного економічного ефекту від впровадження технічної системи безпеки інформації.

Для економічного обґрунтування доцільності розробки сучасних технічних систем охорони комунального підприємства «ЖИЛСЕРВІС-5» потрібно провести розрахунки, щоб визначити економічну ефективність використання основних результатів.

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 послуг.

У контексті кібербезпеки, до витрат також варто віднести витрати на захист даних та інформаційних систем. Зростаюча загроза кіберзлочинності вимагає значних інвестицій у розробку та впровадження ефективних засобів захисту. Ці витрати включають придбання спеціалізованого програмного забезпечення, оплату послуг експертів з кібербезпеки, створення та впровадження оновлених систем захисту інформації. Крім того, підприємства повинні враховувати потенційні втрати від можливих кібератак, які можуть вплинути на їхню репутацію та фінансову стабільність.

Поточні витрати – витрати трудових, матеріальних, нематеріальних та фінансових ресурсів, виражених у грошовій формі, для здійснення поточної господарської діяльності. Це можуть бути витрати на придбання та оновлення антивірусного програмного забезпечення, проведення регулярних аудитів безпеки, а також навчання персоналу основам кібербезпеки. Крім того, підприємства часто виділяють кошти на моніторинг мережевої активності та реагування на інциденти, що дозволяє своєчасно виявляти та усувати потенційні загрози. Ефективне управління поточними витратами на кібербезпеку сприяє захисту корпоративних даних і забезпечує стабільну роботу організації.

Нормування праці в процесі розробки сучасної системи захисту інформації істотно ускладнено для спеціалістів з інформаційної безпеки через специфіку кожного окремого об’єкта та його потреб в захисті. Проте трудомісткість розробки технічної системи захисту інформації може бути розрахована на основі трудомісткості робіт, які виконуються.

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

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

де $t_{тз}$ – тривалість складання технічного завдання на розробку технічної системи захисту інформації;

$t_в$ – тривалість розробки концепції технічної системи захисту інформації у організації;

$t_а$ – тривалість процесу аналізу ризиків;

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

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

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

$t_д$ – тривалість документального оформлення технічної системи захисту інформації.

Підставимо у цю формулу значення відповідні обраному підприємству та завданню:

t = 8год + 15год + 2год + 5год + 5год + 6год + 3год = 44 годин.

Далі потрібно провести розрахунок витрат на створення технічної системи безпеки інформації

Витрати на розробку технічної системи захисту інформації ***Крс***складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки ***Ззс***і вартості витрат машинного часу, що необхідний для розробкитехнічної системи захисту інформації***Змч***:

$$К_{рс} = З_{зс} + З_{мч}. \quad (3.2)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, атакож відрахування на соціальні потреби (пенсійне відрахування, страхування на випадок безробіття, соціальне страхування тощо) і визначається формулою:

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

де t – загальна тривалість розробки технічної системи безпеки інформації, годин;

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

$З_{зс}$= 44 * 140 = 6160грн.

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

$$З_{мч} = t * С_{мч}, \text{ грн,} \quad (3.4)$$

де t– трудомісткість розробки політики безпеки інформації на ПК, годин;

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

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = P*t_{нал}*С_е+(Ф_{зал}*Н_а)/F_р+(К_{лпз}*Н_{апз})/F_р, \text{ грн,} \quad (3.5)$$

де P – встановлена потужність ПК, кВт; (0,4)

$С_е$– тариф на електричну енергію, грн/кВт*година; (4,32)

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн.; (5000)

$Н_а$ – річна норма амортизації на ПК, частки одиниці; (0.5)

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці; (0.5)

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.; (7933)

$F_р$ – річний фонд робочого часу (за 40-годинного робочого дня$F_р$ = 1920).

Підставимо у цю формулу значення відповідні обраному підприємству та завданню:

$С_{мч}$ = 0,4*4,32+(5000*0,5)/1920+(7933*0,5)/1920=5,09 грн.

Підставляємо отримане значення у формулу 3.4:

$З_{мч}$ = 5,09 * 44 = 223,96 грн.

Підставляємо отримане значення у формулу 3.2:

$К_{рс}$ = 223,96 + 6160 = 6383,96 грн.

Визначена таким чином вартість розробки проектутехнічної системи захисту інформації $К_{рс}$є частиною одноразових капітальних витрат разом з витратами на придбання і налагодження апаратури системи інформаційної безпеки.

Таким чином, капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{рс} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} , \quad (3.6)$$

де $К_{рс}$ – вартість розробки проекту технічної системи захисту інформації та залучення для цього зовнішніх консультантів, 6383,96грн;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), 8445,14 грн;(Windows 10 + Microsoftoffice + Avastantivirus)

$К_{рп}$ – вартість розробки політики безпеки інформації включено у вартість $К_{рс}$;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, 47 487 грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговування, 2500 грн;

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, 2000грн.

Підставляємо у формулу відповідні значення:

К = 6383,96 + 8445,14 + 2500 + 2000 = 66 816,1грн.

3.3 Розрахунок експлуатаційних витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об’єкта проектування за визначений період (наприклад, рік), що виражені у грошових формах.

Отже, річні експлуатаційні витрати на функціонування технічної системи інформаційної безпеки складають:

$$С = С_{в} + С_{к} + С_{ак}, \text{ грн.} \quad (3.7)$$

де $С_{в}$ – витрати на upgrade-відновлення й модернізацію системи інформаційної безпеки;

$С_{ак}$ – витрати, викликані активністю користувачів системи інформаційної безпеки;

$С_к$ – витрати на керування системою інформаційної безпеки, і складає:

$$С_к = С_н + С_а + С_з + С_{єв} + С_{ел} + С_о + С_{тос}, \text{ грн.} \quad (3.8)$$

де $С_н$ – витрати на навчання адміністративного персоналу й кінцевих користувачів, 6500грн;

$С_а$ – річний фонд амортизаційних відрахувань, визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів (ПЗ);

$С_з$ – Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки, складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн.} \quad (3.9)$$

де $З_{осн}$, $З_{дод}$ – основна та додаткова заробітна плата відповідно, грн на рік.

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

$С_з = 20000*12 + 2000*12 = 264000$ грн.

$С_{ел}$ – вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року, визначається за формулою:

$$С_{ел} = Р * F_р * Ц_е, \text{ грн.} \quad (3.10)$$

де Р – встановлена потужність апаратури інформаційної безпеки, кВт;

$F_р$ – річний фонд робочого часу системи інформаційної безпеки (визначається виходячи з режиму роботи системи інформаційної безпеки);

$Ц_е$ – тариф на електроенергію, грн/кВт*годин.

Підставляємо у формулу відповідні значення:

$С_{ел} = (0,4*10) * (12*20*8*10) * 4,32 = 3 * 19200 * 4,32 = 248832$ грн.

$С_о$ – витрати на залучення сторонніх організацій для виконання деяких видів обслуговування, навчання та сертифікацію обслуговуючого персоналу визначаються за даними організації.

$С_{тос}$ – витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки, визначаються за даними організації або у відсотках від вартості капітальних витрат (1-3%). (356,91)

$С_{ак}$ – витрати, викликані активністю користувачів системи інформаційної безпеки. (7200)

Тепер можна підставити дані у формулу 3.8:

$С_к = 6500 + 264000 + 248832 + 356,91 = 519688,91$ грн.

Отримані значення підставимо у формулу 3.7:

$С = 519688,91 + 7200 = 526888,91$ грн.

3.4Оцінка величини збитку

Кінцевим результатом впровадження й проведення заходів щодо забезпечення інформаційної безпеки є величина відвернених втрат, що розраховується, виходячи з імовірності виникнення інциденту інформаційної безпеки й можливих економічних втрат від нього. По суті, ця величина відображає ту частину прибутку, що могла бути втрачена.

Можливі відвернені збитки можуть визначатися відповідно до створеної при розробці технічної системизахисту інформації моделі загроз та аналізу ризиків у вартісному вираженні.

Універсальних рецептів визначення можливого збитку від інформаційної атаки на вузол або сегмент корпоративної мережі не існує. У самому загальному виді передумова розрахунку потенційного збитку полягає в тому, що витрати на забезпечення інформаційної безпеки не повинні перевищувати вартість об’єкта, що захищається, або величину збитку, що може виникнути внаслідок атаки на об’єкт, що захищається.

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

Необхідні вихідні дані для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин; (5)

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин; (5)

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

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), грн на місяць; (51000)

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн на місяць; (477000)

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 3 осіб;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 28 осіб;

О – обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн у рік; (1500000)

$П_{зч}$ – вартість заміни встаткування або запасних частин, грн; 18445,14

І – число атакованих вузлів або сегментів корпоративної мережі; 10

N – середнє число атак на рік. 3

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

$$U = П_п + П_в + V, \quad (3.11)$$

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

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

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

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

$$П_п = (З_с/F)*t_п, \quad (3.12)$$

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

Підставляємо відповідні значення у формулу:

$П_п = (477000/176)*5 = 13551,14$ грн.

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

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

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

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

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн. (9222,57)

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

$$П_{ви} = (З_с/F)*t_{ви}. \quad (3.14)$$

Підставляємо відповідні значення у формулу:

$П_{ви} = (477000/176)*7 = 18971,59$ грн

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

$$П_{пв} = (З_о/F)*t_в. \quad (3.15)$$

Підставляємо відповідні значення у формулу:

$П_{пв} = (51000/176)*5 = 1448,87$ грн.

Отримані значення підставимо у формулу 3.13:

$П_в = 18971,59 + 1448,87 + 9222,57 = 29643,03$ грн.

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

$$V = (О/F_г)*(t_п + t_в + t_{ви}), \quad (3.16)$$

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

Підставляємо відповідні значення у формулу:

V = (1500000 / 2080)*(5 + 5 + 7) = 12259,62 грн.

Отримані значення підставимо у формулу 3.11:

U = 13551,14 + 2943,03 + 12259,62 = 28753,79 грн.

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

$$B = \Sigma_i \Sigma_n U. \quad (3.17)$$

Підставляємо відповідні значення у формулу:

B = 10 * 5 * 28753,79 = 1437689,5 грн.

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

$$E = B * R – C, \quad (3.18)$$

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

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

C – щорічні витрати на експлуатацію системи інформаційної безпеки, грн.

Підставляємо відповідні значення у формулу:

E = (1437689,5 * 5/12) - 526888,91 = 72148,39 грн;

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

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

$$ROSI = E/K, \text{ частки одиниці}, \quad (3.19)$$

де E – загальний ефект від впровадження системи інформаційної безпеки;

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

Підставляємо відповідні значення у формулу:

ROSI = 72148,39 / 66 816,1 = 1,079

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

$$T_o = К / Е = 1/ROSI, років, \quad (3.20)$$

Підставляємо відповідні значення у формулу:

T_o = К / Е = 1 / 1,079 = 0,927 років (338,36 днів)

3.5 Висновок

У конструктивному розділі було обґрунтовано техніко-економічну доцільність запровадження запропонованих в спеціальному розділі рішень згідно з темою розробки технічної системи захисту інформації комунального підприємства «ЖИЛСЕРВІС-5».

Капітальні витрати на впровадження інформаційної безпеки становлять – 66 816,1 грн;

Експлуатаційні витрати на впровадження технічної системи безпеки інформації становлять – 526888,91 грн;

Загальний збиток від атаки на корпоративну мережу – 1437689,5 грн;

Ефект від впровадження технічної системи безпеки інформації становить – 72148,39 грн;

Термін окупності капітальних інвестицій складатиме 0,927 років, або 339 днів.

Отже, економічна доцільність обґрунтована, а впровадження технічної системи захисту інформації буде ефективним.

ВИСНОВКИ

У першому розділі було розглянуто стан питання та необхідні умови для впровадження сучасної технічної системи захисту інформації. Його створення є складовою частиною роботи підприємства "ЖИЛСЕРВІС-5", що є частиною критичної інфраструктури міста Дніпро та області, необхідно забезпечити високий рівень інформаційної безпеки в умовах війни. Це включає захист персональних даних клієнтів і працівників, а також фінансової інформації.

Розробка включає аналіз ризиків, створення моделей загроз, політики безпеки а головне технічної системи захисту інформації. Це дозволить підприємству запобігти витоку інформації матеріально-речовим каналом, забезпечуючи стабільну роботу інформаційних систем.

У другій частині кваліфікаційної роботи було розглянуто загальні відомості комунального підприємства «ЖИЛСЕРВІС-5», яка інформація циркулює в підприємстві, модель порушника та загроз, профіль захищеності та врешті розробленатехнічна система захисту інформаціїбазована на висновках з наведених відомостей. Інформація наведена в другій частині роботи була частково змінена, зміни не впливають на технічні можливості та наявні рішення.

Результатом обстеження ОІД став аналіз загроз та вразливостей підприємства:

- зроблено обстеження стану підприємства;
- наведена схема інформаційних потоків;
- показана організаційна структура підприємства;
- побудовані моделі порушника та загроз;
- розписано обраний профіль захищеності;

Розроблено політику безпеки, яка включає в себе:

- Політику антивірусного захисту;
- Політику користування зйомними носіями інформації та збереження носіїв інформації;

- Політику захисту паролів;
- Політику «Чистого столу».

Створено сучасну систему захисту:

- Створено план системи захисту який ефективно покриває усю площу підприємтсва та може виявити проникнення з будь-якого напрямку;
- Обрано дієві та ефективні варіанти датчиків які в сукупності мінімізують або навіть зводять на нівець усі можливі сліпі зони;
- Розраховано вартість усього обладнання необхідного для захисту інформації як описано в двох попередніх пунктах.

Функціональний профіль захищеності в АС підприємства був обраний на підставі проведених аналізів загроз та оцінки ризиків і обраний на підставі обраного класу АС відповідно до документа НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні класи захищеності оброблюваної інформації від несанкціонованого доступу».

У конструктивному розділі було обґрунтовано техніко-економічну доцільність запровадження запропонованих в спеціальному розділі рішень згідно з темою розробки сучасної технічної системи захисту інформації комунального підприємства «ЖИЛСЕРВІС-5».

Капітальні витрати на впровадження інформаційної безпеки становлять – 66 816,1 грн;

Експлуатаційні витрати на впровадження технічної системи безпеки інформації становлять – 526888,91 грн;

Загальний збиток від атаки на корпоративну мережу – 1437689,5 грн;

Ефект від впровадження системи інформаційної безпеки становить – 72148,39 грн;

Термін окупності капітальних інвестицій складатиме 0,927 років, або 339 дні.

Отже, економічна доцільність обґрунтована, а впровадження технічної системи захисту інформації буде ефективним.

ПЕРЕЛІК ПОСИЛАНЬ

1. Комунальне підприємство "ЖИЛСЕРВІС-5" Дніпровської міської ради - Дніпровська міська рада. [Електронний ресурс]. – Режим доступу до ресурсу:https://dniprorada.gov.ua/uk/page/komunalne-pidpriemstvo-zhilservis-5-dniprovskoi-miskoi-radi-.

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

3. Методичні рекомендації до виконання кваліфікаційних робіт бакалаврів спеціальності 125 Кібербезпека / Упоряд.: О.В. Герасіна, Д.С. Тимофєєв, О.В. Кручинін, Ю.А. Мілінчук – Дніпро: НТУ «ДП», 2020. -47с. [Електронний ресурс]. – Режим доступу до ресурсу: https://bit.nmu.org.ua/ua/student/metod/125b/%D0%9C%D0%B5%D1%82%D0%BE%D0%B4_%D0%9A%D0%A0%D0%91_125_2020_1.pdf

4. Статут комунального підприємства "ЖИЛСЕРВІС-5" Дніпровської міської ради – Дніпровська міська рада. [Електронний ресурс]. – Режим доступу до ресурсу: https://dniprorada.gov.ua/uk/Widgets/GetWidgetContent?url=/WebSolution2/wsGetTextPublicDocument?pID=346424&name=85/4

5. НД ТЗІ 2.5-005-99 “Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу”. [Електронний ресурс]. – Режим доступу до ресурсу:https://tzi.com.ua/downloads/2.5-005%20-99.pdf

6. НД ТЗІ 3.7-001-99 “Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованих системах”. [Електронний ресурс]. – Режим доступу до ресурсу: https://tzi.com.ua/downloads/3.7-001-99.pdf

7. НД ТЗІ 3.7-003-05 “Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній

системі”. [Електронний ресурс]. – Режим доступу до ресурсу: https://tzi.com.ua/downloads/3.7-003-2005.pdf

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

9. Закон України «Про захист персональних даних» [Електронний ресурс]. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2297-17

10. Закон України «Про захист в інформаційно-комунікаційних системах» [Електронний ресурс]. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

11. Статистичний звіт за результатами роботи Системи виявлення вразливостей і реагування на кіберінциденти ті кібератаки в 2023 році. [Електронний ресурс]. – Режим доступу до ресурсу: https://scpc.gov.ua/uk/articles/334

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

МЕТОД ПРОТИДІЇ ВИТОКУ ІНФОРМАЦІЇ МАТЕРІАЛЬНО-РЕЧОВИМ КАНАЛОМ ЗА РАХУНОК ВИКОРИСТАННЯ СУЧАСНИХ ТЕХНІЧНИХ СИСТЕМ ОХОРОНИ

Студент: Карпенко І.М
Керівник: к.т.н Котенко А.М

ОБ'ЄКТ ДОСЛІДЖЕННЯ

процес захисту інформації на об’єктах інформаційної діяльності

ПРЕДМЕТ ДОСЛІДЖЕННЯ

Технічні засоби охорони об’єктів інформаційної діяльності.

3

МЕТА РОБОТИ

Розробка проекту технічної системі охорони об'є
інформаційної діяльності

ОСНОВНІ ЗАВДАННЯ

- дослідження вимог до захисту інформації;
- дослідження причин порушення конфіденційності інформації в матеріально-речовому каналу;
- дослідження існуючих складових елементів технічної системи охорони;
- на основі проведених досліджень розробити технічну систему охорони об'єкта інформаційної діяльності.

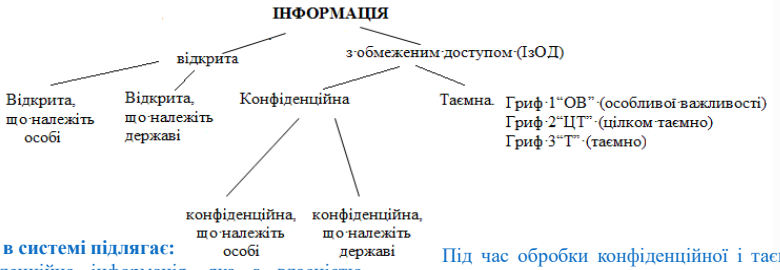
4

АКТУАЛЬНІСТЬ

Процес обробки інформації на об'єктах інформаційної діяльності потребує прийняття спеціальних заходів для забезпечення безпеки інформації. Однією з загроз інформаційній безпеці є крадіжки матеріальних носіїв інформації, які містять інформацію з обмеженим доступом, тобто виток інформації матеріально-речовим каналом. Внаслідок цього порушується така важлива властивість інформації як її конфіденційність. В останні роки якісно зріс рівень підготовки зловмисників дії яких направлені на несанкціоноване отримання інформації на об'єктах інформаційної діяльності. у тому числі і на звичайні крадіжки матеріальних носіїв інформації. Тому захист об'єктів інформаційної діяльності від витоку інформації матеріально-речовим каналом є безумовно, актуальною задачею.

Класифікація інформації, вимоги до її захисту

5



Захисту в системі підлягає:
- конфіденційна інформація, яка є власністю держави або вимога щодо захисту якої встановлена законом, у тому числі конфіденційна інформація про фізичну особу;
- інформація, що становить державну або іншу передбачену законом таємницю (таємна інформація).

Під час обробки конфіденційної і таємної інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення.

цілісність — властивість інформації бути захищеною від несанкціонованого знищення, модифікації.
конфіденційність — властивість інформації бути захищеною від несанкціонованого ознайомлення.
доступність — властивість інформації бути захищеною від несанкціонованого блокування.

Класифікація інформації, вимоги до її захисту

5

Захисту в системі підлягає:
- конфіденційна інформація, яка є власністю держави або вимога щодо захисту якої встановлена законом, у тому числі конфіденційна інформація про фізичну особу;
- інформація, що становить державну або іншу передбачену законом таємницю (таємна інформація).

Під час обробки конфіденційної і таємної інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення.

цілісність — властивість інформації бути захищеною від несанкціонованого знищення, модифікації.
конфіденційність — властивість інформації бути захищеною від несанкціонованого ознайомлення.
доступність — властивість інформації бути захищеною від несанкціонованого блокування.

6

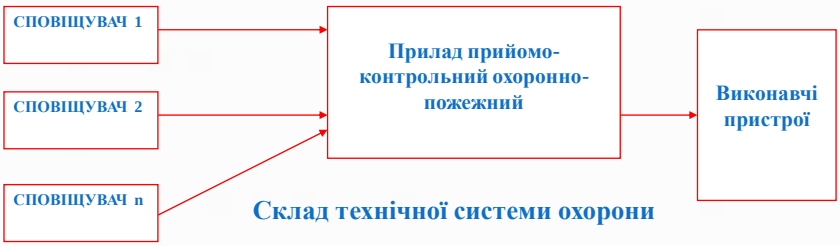
Загрози інформації

Модель технічного каналу витоку інформації

7

Матеріально-речовий канал витоку інформації

- Джерелами і носіями інформації в ньому є матеріальні об'єкти (макро і мікрочастинки), які мають чіткі просторові межі локалізації, за винятком випромінювань радіоактивних речовин. Витік інформації в цих каналах супроводжується фізичним переміщенням людей і матеріальних тіл з інформацією за межами контрольованої зони.

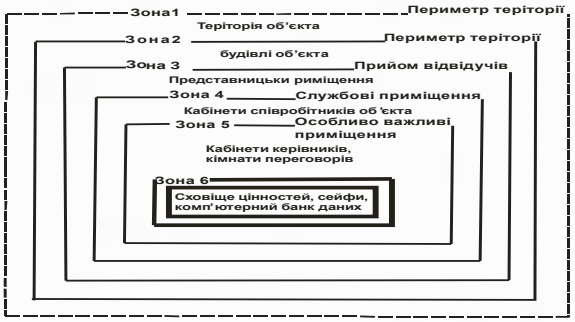


Склад технічної системи охорони

8

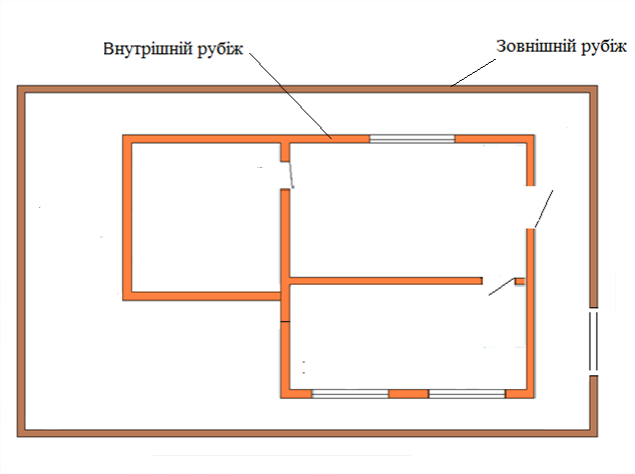
Створення рубежів охорони

У основі системи захисту об'єкту лежить принцип створення послідовних рубежів, в яких загрози мають бути своєчасно виявлені, а їх розповсюдженню повинні перешкоджати надійні перешкоди. Такі рубежі (або зони безпеки) повинні розташовуватися послідовно - від огорожі навколо території об'єкту до головного, особливо важливого приміщення і інші



9

Зовнішній та внутрішній рубіж ОІД.



8

Існуючі засоби охорони зовнішніх рубежів об'єктів

Активні інфрачервоні, радіохвильові, ємнісні засоби виявлення.

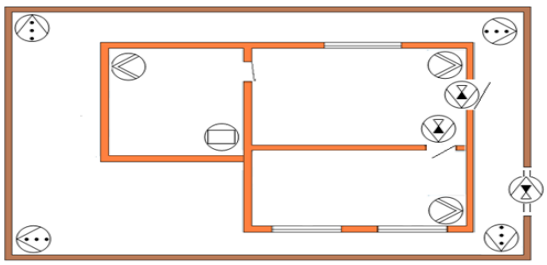
9

Існуючі заходи засоби охорони приміщень

Пасивні інфрачервоні, магнітоконтактні, радіопроменеві, сповіщувачі розбиття скла, комбінованиий інфрачервониий сповіщувач руху та розбиття скла.

10

Технічна система охорони об’єкту інформаційної діяльності



-Пасивні інфрачервоні сповіщувачі руху

- Комбінований Інфрачервоний сповіщувач руху та розбиття скла

- Активні інфрачервоні засоби виявлення

- Сповіщувач магнітоконтактний

.- прилад приймально-контрольний

11

ВИСНОВКИ

- Досліджено вимоги до захисту інформації та встановлено що основною причиною витоку інформації з обмеженим доступом з ОІД є крадіжки.
- Встановлено, що для запобігання витоку інформації матеріально-речовим каналом необхідно використовувати технічні засоби охорони.
- Встановлено, що для підвищення надійності охорони об’єкту необхідно застосовувати принцип рубіжності побудови системи охорони.
- Встановлено, що для захисту внутрішнього рубежу об’єктів інформаційної діяльності доцільно використовувати інфрачервоний сповіщувач руху, комбінований інфрачервоний сповіщувач руху та розбиття скла, магнітоконтактний сповіщувач; для захисту зовнішніх рубежів активні інфрачервоні засоби.
- Розроблена технічна система охорони об’єкту інформаційної діяльності, яка вирішує поставлену мету атестаційної роботи, а саме запобігає витоку інформації матеріально-речовим каналом.