РЕФЕРАТ

Пояснювальна записка: __ с., __ рис., _ табл., __ додатків, __ джерел.

Об’єкт розробки: інформаційно-телекомунікаційна система (ІТС) ПП «Охорона Сервіс».

Предмет дослідження: політика безпеки інформації об’єкта інформаційної діяльності (ОІД).

Мета роботи (проекту): підвищення рівня захисту інформації в ІТС ПП «Охорона Сервіс»

Методи розробки: спостереження, порівняння, аналіз, опис.

У першому розділі проведено аналіз нормативно-правової бази у сфері захисту інформації та визначена актуальність проблеми захисту інформації в ІТС комерційних підприємств, встановлені задачі на розробку комплексної системи захисту інформації КСЗІ, на ОІД, де циркулює інформація.

У спеціальній частині складено акт обстеження на об’єкті інформаційної діяльності, розглянуто загальні відомості про підприємство, його організаційну структуру, аналіз середовища функціонування об’єкта інформаційної діяльності, класифікована інформація, що обробляється у інформаційно-телекомунікаційній системі та наведено характеристику компонентів системи. Також розроблено моделі загроз та порушника безпеки інформації, проаналізовані ризики для інформації і сформовані основні положення політики безпеки інформації для комплексної системи захисту інформації.

В третьому розділі визначено економічну доцільність впровадження ПБ. Проведено розрахунки капітальних витрат, поточних витрат, оцінки величини збитку та загальний ефект від впровадження КСЗІ.

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ПОЛІТИКА БЕЗПЕКИ ІНФОРМАЦІЇ, ОБ’ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, АНАЛІЗ РИЗИКІВ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, АКТ ОБСТЕЖЕННЯ, ЕКОНОМІЧНА ДОЦІЛЬНІСТЬ, ПОКАЗНИК ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ.

РЕФЕРАТ

Пояснительная записка: __с., __рис., __табл., __прилож., __ источников.

Объект разработки: информационно-телекоммуникационная система «Охорона Сервис».

Предмет: политика безопасности информации объекта информационной деятельности (ОИД).

Цель работы (проекта): повысить уровень защити информации в ИТС ПП «Охорона Сервис».

Методы, используемые при разработке: наблюдение, сравнение, анализ.

В первом разделе проведен анализ нормативно-правовой базы в сфере защиты информации и указана актуальность вопроса, поставлены задачи на внедрение системы защиты информации на ОИД, где циркулирует информация.

В специальной части составлен акт обследования на объекте информационной деятельности, рассмотрены общие сведения о предприятии, его организационная структура, анализ среды функционирования объекта информационной деятельности, классифицирована информация, обрабатываемая в информационно-телекоммуникационной системе, и приведено описание компонентов системы. Также разработаны модели угроз и нарушителя безопасности информации, проанализированы риски для информации и сформированы основные положения политики безопасности информации для комплексной системы защиты информации.

В третьем разделе определена экономическая целесообразность внедрения информационной ПБ. Проведены расчеты капитальных расходов, текущих расходов, оценки величины ущерба и общий эффект от внедрения КСЗИ.

КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНОФРМАЦИИ, ПОЛИТИКА БЕЗОПАСНОСТИ ИНФОРМАЦИ, ОБЪЕКТ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ, АНАЛИЗ РИСКОВ, МОДЕЛЬ УГРОЗ, МОДЕЛЬ НАРУШИТЕЛЯ, АКТ ОБСЛЕДОВАНИЯ, ЭКОНОМИЧЕСКАЯ ЦЕЛЕСООБРАЗНОСТЬ, ПОКАЗАТЕЛЬ ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ.

ABSTRACT

An Explanatory Note: __ p., __ fig., __ tables., __ add., __ sources.

The object of this study is information and telecommunication system of “Ohorona service” PE.

The subject of this study: information security policy fo information activity object.

The purpose of the study: developing the security policy in information and telecommunication system.

Methods that were used: observation, comparison, analysis, description.

The first part of the study contains an analysis of regulatory documentation in information security, set tasks for the implementation of the information security system for information activity object where the information circulates.

The main part of the study considers the general statements about the enterprise; organizational structure of the computer system are contained.Information activity object`s environment for the functioning; risk assessment; threat analysis of information security; main elements of the information security policy ofinformation and telecommunication system are analyzed; the main regulations of the security policy are formulated.

In the economic part defines economic feasibility of implementing an information security policy. The calculations of capital (fixed) costs, current (operational) costs, a calculation of loss and the effect of the implementation of information security. Economic efficiency indicators of information system security are analyzed.

The analyses provide the opportunity to use the developed security policy for implementation in the information and telecommunication system of the enterprise.

INFORMATION SECURITY, INFORMATION ACTIVITY OBJECT, INFORMATION SECURITY POLICY, RISK ASSESSMENT, THREAT

ANALYSIS, ECONOMIC FEASIBILITY, CAPITAL COSTS, OPERATING COSTS, ECONOMIC EFFICIENCY INDICATORS.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС - автоматизована система;

ЕОТ - електронно-обчислювальна техніка;

ЗУ - закон України;

ІБ - інформаційна безпека;

ІТС - інформаційно-телекомунікаційна система;

КСЗІ - комплексна система захисту інформації;

НСД - несанкціонований доступ;

ОІД - об'єкт інформаційної діяльності;

ОС - операційна система;

ПП – приватне підприємство;

ПБ - політика безпеки;

ПЕОМ - персональна електронно-обчислювальна машина;

ПЗ - програмне забезпечення;

ТЗІ - технічні засоби інформації;

ВСП - виробничо-структурний підрозділ

ВСТУП

На сьогоднішній день інформатизація грає важливу роль в розвитку економіки України і є визначальною сферою суспільного життя.

Майже в кожній інформаційній системі знайдеться така інформація, розголошення якої стороннім особам може нанести збитків її власнику або ж людині, якої стосується інформація. Особливо актуальним стає питання інформаційної безпеки (ІБ) на підприємствах, організаціях, в яких обробляється інформація з обмеженим доступом.

В Україні процес інформатизації здійснюється згідно з Національною програмою інформатизації, яка визначає стратегію розв'язання проблеми забезпечення інформаційних потреб та інформаційної підтримки соціально-економічної, екологічної, науково-технічної, оборонної, національно-культурної та іншої діяльності у сферах загальнодержавного значення.
Майже в кожній інформаційній системі знайдеться така інформація, розголошення якої стороннім особам може нанести збитків її власнику або ж людині, якої стосується інформація. Особливо актуальним стає питання інформаційної безпеки (ІБ) на підприємствах, організаціях, в яких обробляється інформація з обмеженим доступом.

Одним з етапів побудови КСЗІ є розробка політики безпеки. Чим точніше буде створена політика безпеки, тим простіше буде адміністраторам безпеки розробити комплекс заходів для того, щоб запобігти успішним атакам. Важливу роль в розробці політики безпеки є визначення можливих загроз та порушень.

РОЗДІЛ 1.СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1. Стан питання

Швидкий темп розвитоку інформаційних технологій призвів до зростання важливості окремих аспектів суспільного життя, а саме інформації. На забезпечення інформаційної безпеки мільйони підприємств по всьому світові витрачають чимало грошей. Це обумовлено поступовим зростанням рівня інформаційної злочинності. Аналізуючи сучасний стан та тенденцій розвитку сучасного інформаційного простору слід зазначити, що рівень інформаційної безпеки в Україні, за окремими показниками, дуже низький.

За опублікованими данними, компанії Positive Technologies [№1] фахівці в усьому світі ведуть безперервну боротьбу з кіберзлочинністю, і це, як і раніше, змушує зловмисників вдосконалювати свої інструменти. На початку року кібератаки стали випробуванням для багатьох організацій різних сфер економіки в Україні.

Відповідно до даних судової статистики вага несанкціонованого втручання (ст. 361 КК) в структурі посягань у сфері високих технологій, становить близько 75%. Специфіка чинної редакції ст. 361 КК полягає в тому, що вона забезпечує охорону суспільних відносин двох видів: власності на комп'ютерну інформацію та надання послуг електрозв'язку. Швидкий розвиток інформаційних та комунікаційних технологій призводить до виникнення нових засобів ведення кіберзлочинності.

У І кварталі 2019 року в Україні зростання частки атак, спрямованих на отримання даних, триває. Тепер більше половини хакерських атак відбуваються з метою розкрадання інформації. Зловмисники зацікавлені в найрізноманітніших даних - від особистого листування до комерційної таємниці. Але як і раніше найбільш високо

цінюються облікові дані, персональні дані і дані платіжних карт.(Рис.1.1)

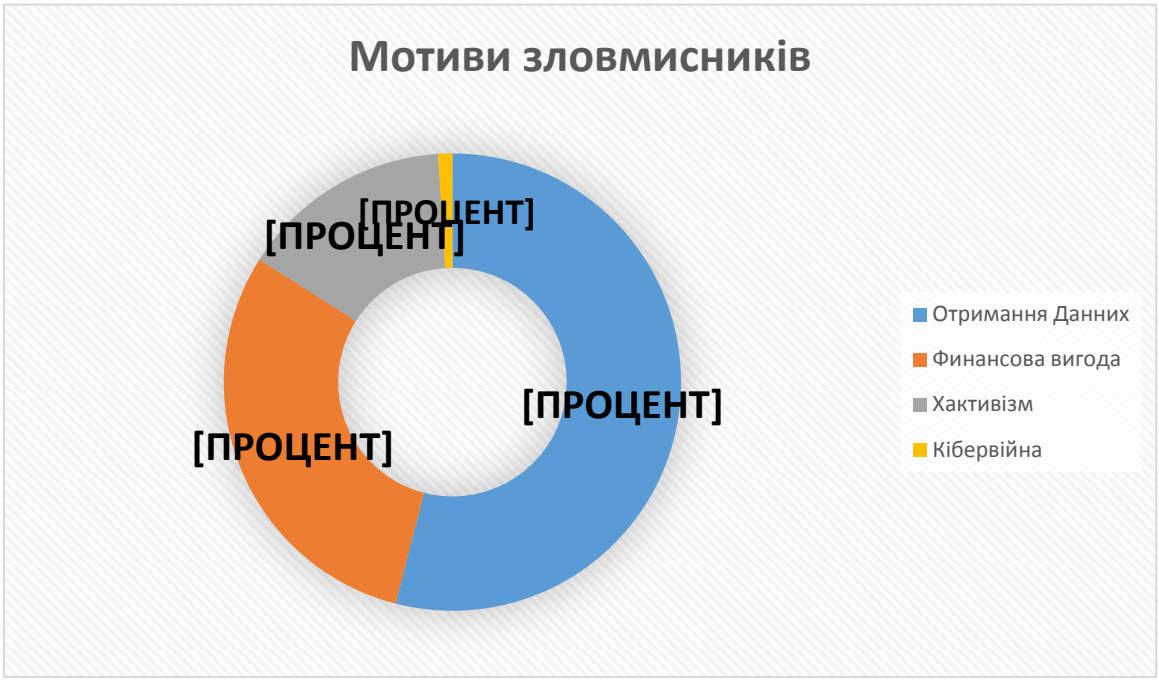

Рисунок 1.1 - Мотиви зловмісників

У I кварталі 2019 року частка цілеспрямованих атак знизилася в порівнянні з IV кварталом 2018 року і склала 47% проти 53%. Це пов'язано зі збільшенням частки атак, які не прив'язані до конкретної галузі; в основному мова йде про масові шкідливих кампаніях. Частка кіберінцідентов, в результаті яких постраждали приватні особи, практично не змінилася (21% проти 22% в IV кварталі 2018 року). На рисунку 1.2 наведено динаміка атак в 2018 і 2019 роках (по місяцях).

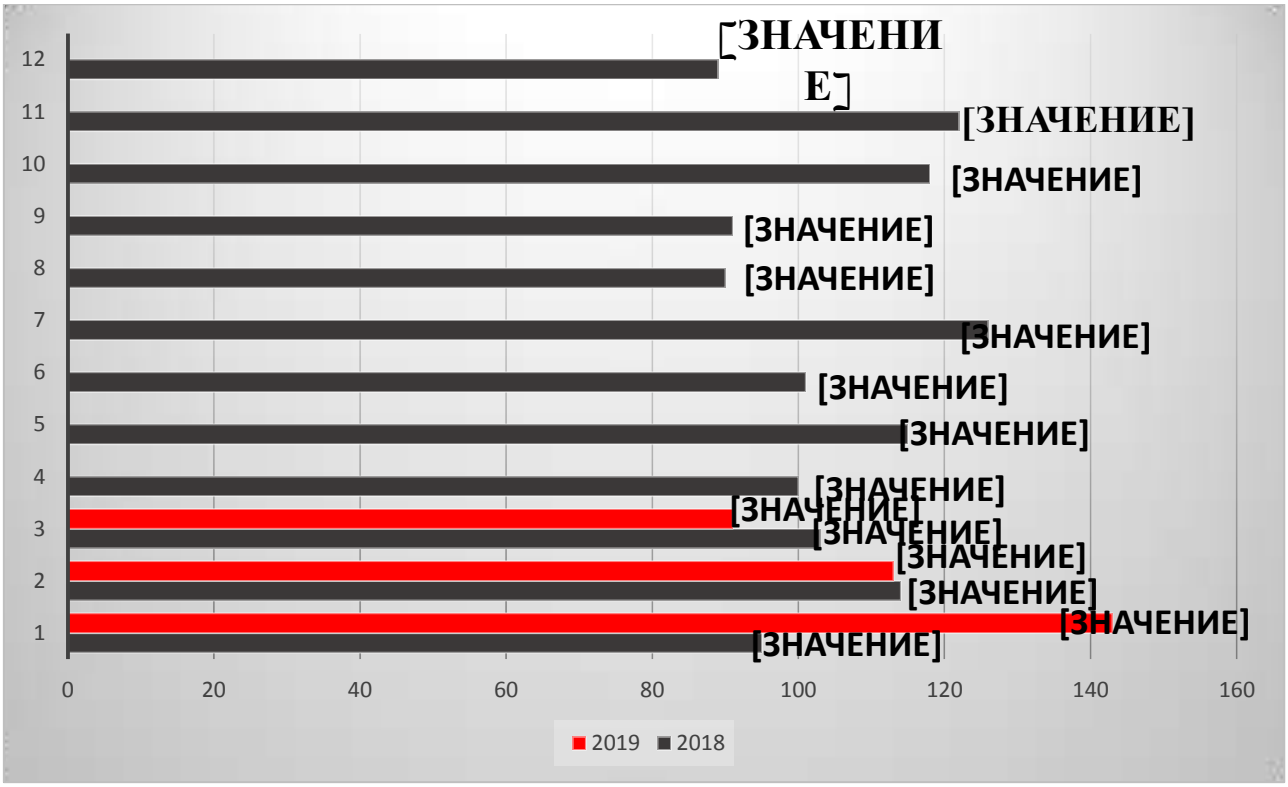

Рисунок1.2 - Кількість інцидентів в Україні на 2018 і 2019 роках (по місяцях)

Діяльність комерційних установ дедалі більше залежить від інформаційних технологій. Інформатизація відбувається в усіх сферах функціонування підприємств, що збільшує кількість загроз та ризиків. Також збільшенню кількості інцидентів інформаційної безпеки сприяють закладені в основу інтернет-технологій принципи відкритості та анонімності. При цьому на сьогодні зростає не тільки кількість атак на інформаційну інфраструктуру, але і їх складність.

Загрозу для комерційних підприємств становлять як зловмисники, що вчиняють протиправні дії з метою отримання матеріальної користі, а і несумлінні конкуренти. Також до цієї категорії відносяться навмисні та ненавмисні дії персоналу, що є загрозою для інформації, що потребує доступу.

1.2 Аналіз нормативно-правової бази у сфері захисту інформації

Згідно ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах» умови обробки інформації в системі визначаються власником системи відповідно до договору з власником інформації, якщо інше не передбачено законодавством. Порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються власником інформації. Відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

Згідно ЗУ «Про інформацію» за порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом. Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація. Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом.

Згідно НД ТЗІ 1.6-005-2013 «Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці» об’єкти, на яких здійснюватиметься обробка технічними засобами та/або озвучуватиметься інформація з обмеженим доступом, що не становить державної таємниці, підлягають обов’язковому категоріюванню.

Категоріювання може бути первинним, черговим або позачерговим.

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

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

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

Категоріювання здійснюється за ознакою:

– ступінь обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на ОІД;

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

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

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

Необхідність впровадження на реальному підприємстві комплексної системи захисту інформації продиктована вимогами стандартів України з управління інформаційною безпекою.

Відповідно до Закону України «Про інформацію», на підприємстві може циркулювати інформація відкрита та інформація з обмеженим доступом (ІзОД). Остання має бути захищена від несанкціонованого доступу. Такий поділ за режимами доступу здійснюється виключно на підставі ступеня конфіденційності інформації. Поряд з конфіденційністю істотними характеристиками інформації є її цілісність і доступність, проте на сьогоднішній день іншої класифікації інформації, крім наведеної, не запроваджено. З метою збереження загальності викладу далі в тексті замість терміну «інформація з обмеженим доступом» використовується термін «інформація», який має на увазі будь-яку інформацію, щодо якої регламентовані певні вимоги до забезпечення її конфіденційності, цілісності та доступності.

Простота і керованість інформаційної системи: принцип простоти і керованості інформаційної системи в цілому визначає можливість формального чи неформально доказу коректності реалізації механізмів захисту. Тільки в простій і керованій системі можна перевірити погодженість конфігурації різних компонентів і здійснити централізоване адміністрування.

Забезпечення загальної підтримки заходів безпеки: принцип загальної підтримки заходів безпеки − носить нетехнічний характер. Рекомендується із самого початку передбачити комплекс мір, спрямований на забезпечення лояльності персоналу, на постійне навчання, теоретичне і, головне, практичне.

Підстави для створення КСЗІ

Згідно НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» встановлений цим НД ТЗІ порядок є обов’язковим для всіх суб’єктів системи ТЗІ в Україні незалежно від їхньої організаційно-правової форми та форми власності, в ІТС яких

обробляється інформація, яка є власністю держави, належить до державної чи іншої таємниці або окремих видів інформації, необхідність захисту якої визначено законодавством. Якщо в ІТС обробляються інші види інформації, то вимоги цього нормативного документа суб'єкти системи ТЗІ можуть використовувати як рекомендації.

Роботи зі створення КСЗІ виконуються організацією-власником (розпорядником) ІТС з дотриманням вимог нормативно-правових актів щодо провадження господарської діяльності у сфері захисту інформації.

1.3 Постановка задачі

У нормативних документах зазначена необхідність впровадження системи захисту інформації, на об`єктах інформаційної діяльності, де циркулює інформація відкрита, що потребує захисту та інформація з обмеженим доступом. Власник підприємства визначає потребу в КСЗІ. Розробка КСЗІ починається з обстеження на ОІД. Під час обстеження ІТС розглядається як організаційно-технічна система, яка поєднує обчислювальну систему, фізичне середовище, середовище користувачів, оброблювану інформацію і технологію її обробки.

Повинні бути проаналізовані й описані:

- загальна характеристика ОІД;
- загальна структурна схема і склад обладнання, технічних і програмних засобів, їхні зв'язки, особливості конфігурації, архітектури й топології, програмні і програмно-апаратні засоби захисту інформації, взаємне розміщення засобів тощо;
- умови функціонування ОІД, особливостей розташування його на місцевості тощо.

Метою такого аналізу є надання загального уявлення про наявність потенційних можливостей щодо забезпечення захисту інформації, виявлення компонентів ІТС, які вимагають підвищених вимог до захисту інформації і впровадження додаткових заходів захисту.

Аналізу інформаційного середовища підлягає вся інформація, що циркулює в системі. Під час аналізу інформація повинна бути класифікована за режимом доступу, за правовим режимом, визначені й описані види її представлення в ІТС. Здійснюється аналіз фізичного середовища.

При обстеженні середовища користувачів здійснюється аналіз:

- функціонального та кількісного складу користувачів, їхніх функціональних обов'язків та рівня кваліфікації;

- повноважень користувачів щодо допуску до відомостей, які обробляються в ІТС, доступу до ІТС та її окремих компонентів;

- повноважень користувачів щодо управління КСЗІ.

Після проведення обстеження на ОІД, формуються завдання на створення КСЗІ:

- визначаються завдання захисту інформації в ІТС, мета створення КСЗІ;

- здійснюється аналіз ризиків (вивчення моделі загроз і моделі порушника, можливих наслідків від реалізації потенційних загроз, величини можливих збитків та ін.) і визначається перелік суттєвих загроз;

- визначаються загальна структура та склад КСЗІ, загальні вимоги до організаційних заходів захисту інформації, що ввійдуть до складу КСЗІ.

Згідно з виконаним обстеженням та аналізом інформаційних ризиків ставиться задача розробки політики безпеки на реальному підприємстві задля мінімізації ймовірностей реалізації ризиків через існуючі вразливості системи.

Висновки до розділу 1

Розглянуті суттєві загрози та стан злочинів в сфері інформаційної безпеки та статистика скоєних атак за І кварталі 2019 року в Україні. Виявлено значне збільшення інцидентів порушення інформаційної безпеки на території України. Зазначена актуальність розвитку кібербезпеки.

В розділі приведено перелік нормативно-правових документів в сфері захисту інформації, зазначено основні положення. Серед документів, що є правовою основою забезпечення безпеки інформації розглянуті НД ТЗІ та їх галузі використання, Закони України, положення та накази.

Обґрунтовано потребу у створенні КСЗІ на підприємстві для запобігання НСД до важливих ресурсів системи. До етапів створення КСЗІ, що використані в роботі віднесені, відповідно до нормативної документації: обґрунтування необхідності створення, обстеження на ОІД, аналіз та оцінка інформаційних ризиків та розробка політики безпеки, що враховує загрози найвищого рівня.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1Загальні відомості про ПП «Охорона Сервіс»

Об’єктом інформаційної діяльності (далі ОІД) є інформаційно-комунікаційних система підприємства "Охорона Сервіс".

«Охорона Сервіс» – приватне охоронне підприємство, що надає спеціалізовані галузеві і комплексні послуги з фізичної, технічної, інформаційної, банківської, пожежної та техногенної безпеки на основі єдиних стандартів якості.

Офіс розташований на 1 поверсі, має площу 128 $м^2$, знаходиться в першому ряді м. Дніпро вул. Зелена і має місце для паркування автомобілів.

Всього підприємство обслуговує приблизно 20000 клієнтів.

Компанії «Охорона Сервіс» надає ряд послуг, серед яких:

- Охорона об'єктів всіх форм власності;
- Охорона будівельних і промислових об'єктів;
- Фізична охорона;
- Охорона квартир;
- Охорона будинків і котеджів;
- Охорона офісних приміщень;
- Охорона магазинів, кафе, ресторанів;
- Установка автономної сигналізації;
- Установка пожежної сигналізації;
- Установка тривожної кнопки;
- Установка контролю доступа;

2.2 Обґрунтування необхідності створення КСЗІ

Підставою для необхідності створення КСЗІ є нормативно-правові акти, що розглянуті в Розділі 1, де вказані вимоги, які встановлюють обов'язковість обмеження доступу до певних видів інформації; забезпечення її цілісності та доступності. На підприємстві наявна інформації, яка підлягає автоматизованій обробці та потребує захисту і забезпечення конфіденційності, цілісності та доступності відповідно до вимог нормативно-правових актів.

На підставі проведеного аналізу власником інформації, яким виступає директор, прийняте рішення щодо створення КСЗІ та видано наказ «Про визначення відповідального за забезпечення технічного захисту інформації та створення КСЗІ на ПП «Охорона Сервіс».

Завданнями захисту інформації на підприємстві можна виділити:

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

Ці завдання можна вирішити при розробці політики безпеки шляхом таких дій:

- організація системи допуску користувачів до роботи з інформацією, яка потребує захисту;
- організація обліку, зберігання, обігу інформації, яка потребує захисту, та її носіїв;

організація і координація робіт з захисту інформації, яка обробляється та передається засобами АС.

2.3 Обстеження на об’єкті інформаційної діяльності

Акт обстеження на об’єкті інформаційної діяльності ПП «Охорона Сервіс».

Обстеження на об’єкті інформаційної діяльності проведено відповідно до Методичних вказівок щодо структури та змісту Плану захисту інформації в автоматизованій системі - НД ТЗІ 1.4-001-2000 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806 - Типове положення про службу захисту інформації в АС, здійснено обстеження середовищ функціонування. Акт оформлено відповідно до Додатку А. «Форма та зміст акта обстеження на об'єкті інформаційної діяльності стосовно створення комплексу ТЗІ, НД ТЗІ 3.1-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи». Порядок проведення обстеження відповідає ДСТУ 3396.1.

Під час обстеження розглянуто середовище функціонування ІТС: обчислювана система, фізичне середовище, середовище користувачів та оброблювана інформація. Приводиться опис кожного середовища функціонування ІТС.

Відповідно до НД ТЗІ 1.6-005-2013 «Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці», ОІД, що розглядається встановлюється категорія IV (четверта) адже на об'єкті технічними засобами обробляється інформація з обмеженим доступом, що не становить державної таємниці.

Обстеження фізичного середовища: характеристика ОІД, де розташована та функціонує інформаційно-телекомунікаційна система.

Схема розташування ОІД та об’єктів навколо нього наведена на ситуаційному плані (рисунок 2.1). На генеральному плані зазначені схеми опалення, електроживлення, відеоспостереження, пожарної та охоронної сигналізацій (рисунок 2.2, 2.3, 2.4).

Характеристика складових ОІД

Висота стель - 400 м; перекриття - 500 мм; стінні перегородки - 150 мм; стіни зовнішні з цегли - 500 мм.

3 металопластикові вікна розміром 1500мм х 2000мм, захищені металевими решітками та жалюзі.

Одні двері металеві з розміром отвору 1000мм х 2000мм.

Система електроживлення (освітлення): мережа 220В; автономний агрегат електроживлення відсутній; світильники з LED лампами. Розетки типу РШ. Кабельне підключення до Інтернет - екранована віта пара UTP 4х2х0,5 5е в коробі.

Система опалювання: автономна.

Система вентиляції за заземлення в будівлі відсутні.

Системи сигналізації:

- пожежна – димовий сповіщувач СПД 3, ручний пожежний сповіщувач, шлейфи по стелі, сигнальні пристрої.
- охоронна – магнітно-контактні датчики на відкриття дверей та вікон, оптичні датчики руху Swan – 2, клавіатура, централь. Підключення: екранований дріт 4х2.

Будівля обладнана системами електроживлення, опалення, водопостачання та каналізації, автоматичною пожежною сигналізацією. Живлення систем освітлення, електропостачання та опалення здійснюється через підключення до міських комунальних мереж. Система пожежної сигналізації підключена на центральний пульт.

Територія, навколо будівлі зі сходу обмежена забором. На півночі обмежена контрольована зона паркування для транспорту. Територія навколо будівлі має асфальтове покриття. Навколо будівлі розташовані

багатоповерхові житлові будови. На півночі – пам’ятник « Вічний вогонь»; На півдні – п’ятиповерхова житлова будівля; з сходу - двометровий паркан з металу; з заходу – п’ятиповерхова житлова будівля; з північно заходу – трансформаторна підстанція.

По ступеню надійності електрозабезпечення підприємство відноситься до споживачів ІІІ категорії, тобто допустимі перерви в електропостачанні на час, необхідний для ремонту або заміни пошкодженої ділянки мережі, але не більше однієї доби. Електрозабезпечення здійснюється від трансформаторної підстанції на напрузі ~380/220В по одній кабельній лінії. Силові електромережі виконані захищеними проводами з мідними жилами скрито, в стінах, та кабелями з мідними жилами в коробах.

Приміщення телефонізовано. Телефонізація здійснюється від існуючої телефонної мережі міста.

На вході до будівлі розташована відомча охорона, що забезпечує пропускний режим до приміщень та здійснює цілодобову охорону. На фасаді приміщення встановлена система відеоспостереження з візуальним контролем охороною приміщення на вході в будівлю.

Таблиця 2.1 - Системи комунікацій підприємства

Електропостачання	Підклю.чено до трансформаторної підстанції №3, яка має сторонніх споживачів і знаходиться за межами КЗ
Система опалення	Підключена до міської мережі опалення, знаходиться за межами КЗ (пластикові труби, однотрубна вертикальна система опалення)
Система каналізації	Підключена до міської мережі, яка знаходиться за межами КЗ
Система водопостачання	Підключена до міського водоканалу, яка знаходиться за межами КЗ (пластикові труби, однотрубна вертикальна система опалення)
Заземлення	Всі прилади, комп’ютери заземлені на спільний контур заземлення, який є замкнутий і виходить за межі КЗ
Телефонна лінія	Підключена до АТС «УКРтелеком», на офіс відведено 4 номера
Система вентиляції	Приточно-витяжна

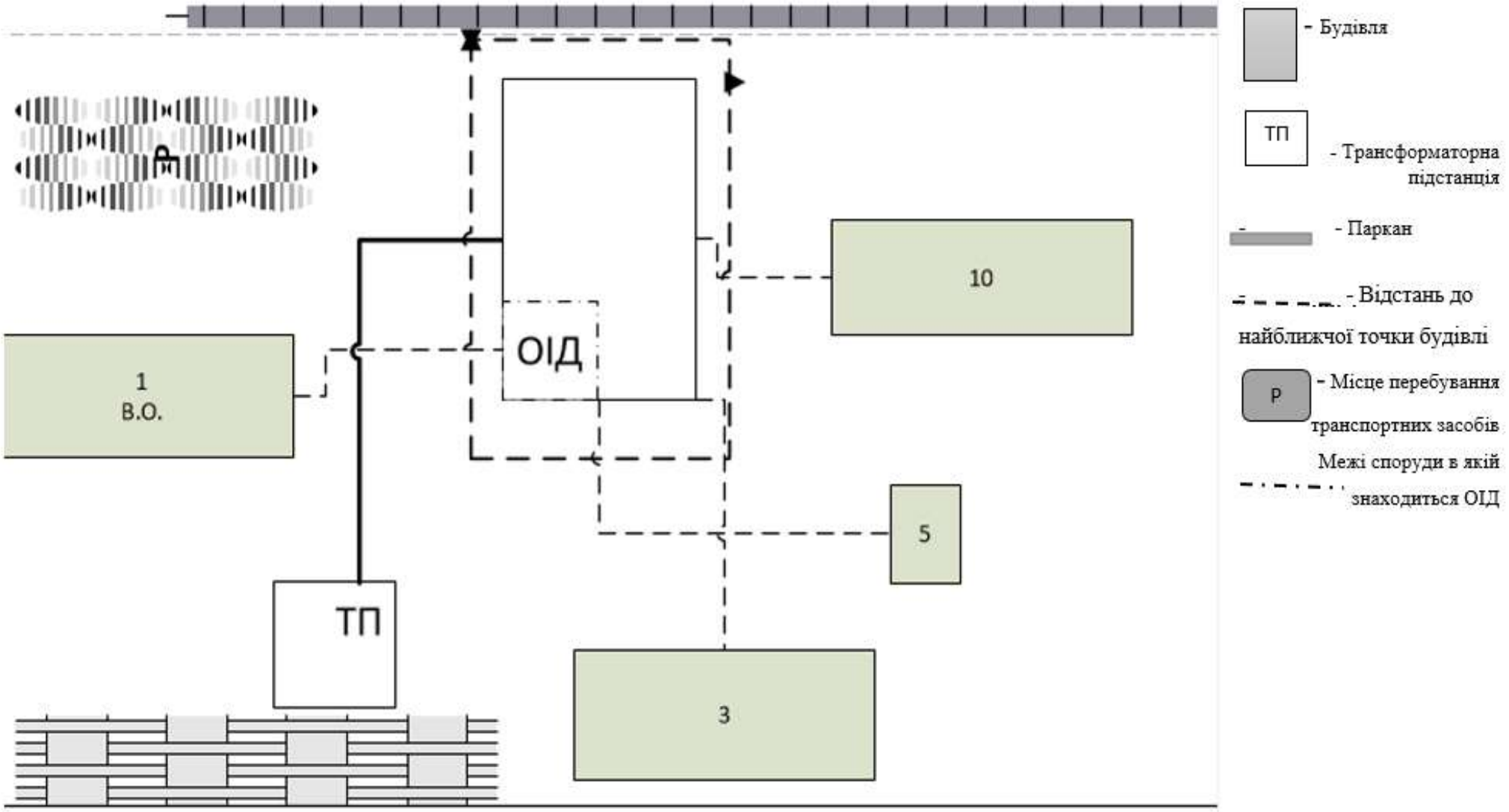

Рисунок 2.1 - Ситуаційний план

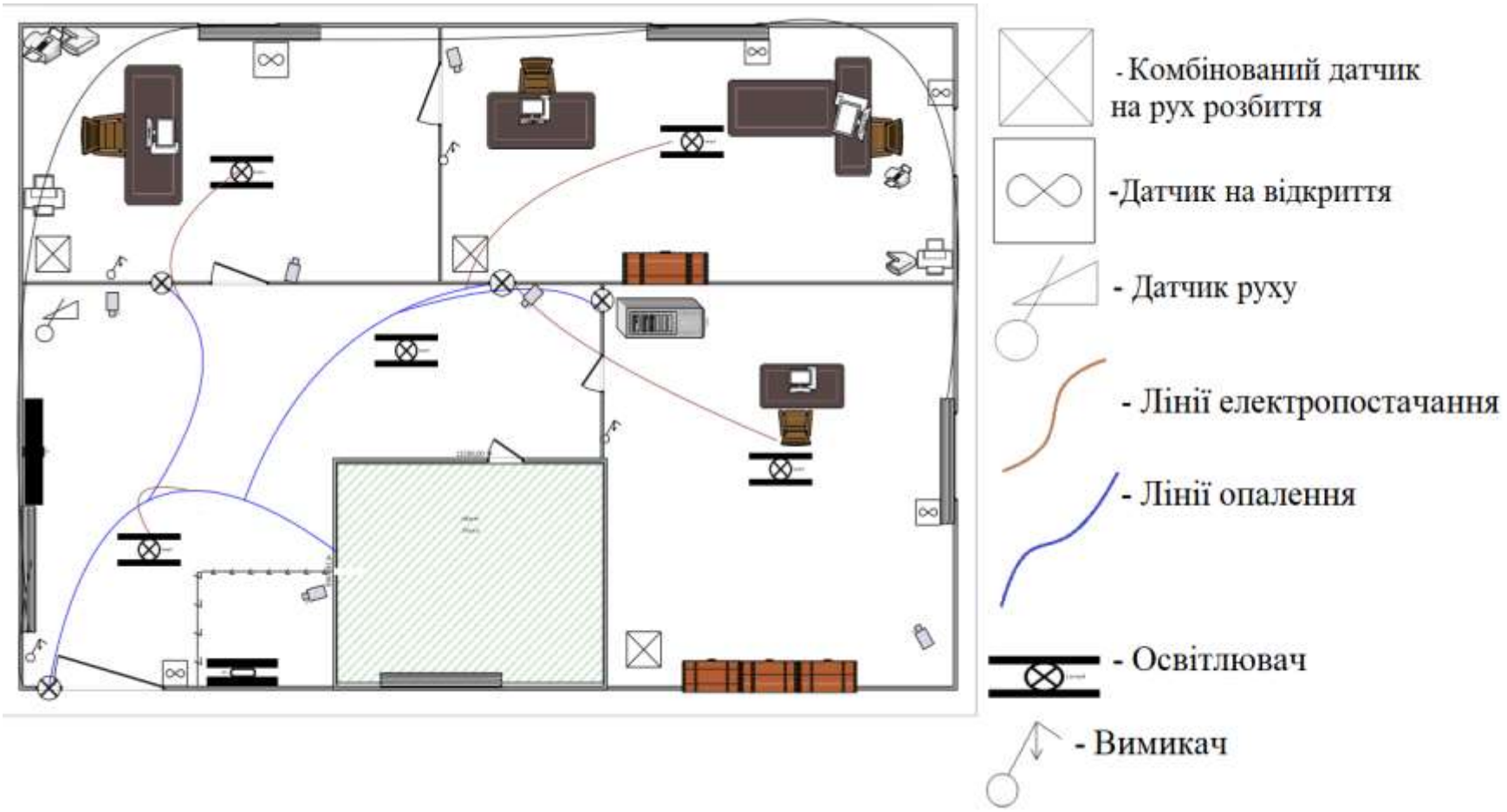

Рисунок 2.2 - Генеральний план

Штат працівників підприємства складається з 6 чоловік - директор; бухгалтер, який веде фінансовий облік підприємства; системний адміністратор – що займається налаштуванням локальних мереж; диспетчер – що веде нагляд за об’єктами у електронному режимі; охоронник – 4чол.; прибиральниця – 1 чол.

На рисунку 2.5 зображена організаційна структура підприємства.

Рисунок 2.5 - Організаційна структура підприємства

Відповідно до розподілу повноважень с приводу доступу до інформації та характеру робіт, що виконуються у процесі функціонування ІТС, доступ матимуть деякі користувачі системи.

Обов’язки персоналу відповідно посадовим інструкціям:

Обов’язки директора:

- приймати рішення в рамках своїх функціональних обов'язків, визначених у Статуті підприємства, та згідно з діючим законодавством України

- супроводження договорів із сторонніми організаціями, що надають послуги по комунікаційнім, програмному й апаратному оснащенню підприємства;
- визначати, формулювати і координувати всі види діяльності підприємства;

обов'язки бухгалтера:

- визначає, формулює, планує, здійснює та координує організацію бухгалтерського обліку господарсько-фінансової діяльності підприємства, здійснює контроль за раціональним використанням матеріальних, трудових та фінансових ресурсів;
- забезпечує раціональну організацію обліку та звітності на підприємстві;
- складає баланс підприємства;
- організовує та контролює складання розрахунків щодо використання прибутків, затрат на виробництво, платежів до бюджету, правильність та своєчасність складання звітності;
- здійснює контроль за додержанням порядку оформлення бухгалтерських звітів, документів,розрахунків та платіжних забов'язань;
- організовує складання щомісячного бухгалтерського обліку, квартальних та річних бухгалтерських звітів.

обов'язки системного адміністратора:

- забезпечення роботи комп'ютерної техніки, комп'ютерної мережі та програмного забезпечення підприємства;
- підготовка та збереження резервних копій даних, їх періодичне знищення та оновлення;
- встановлення і конфігурування оновлень операційної системи і прикладного програмного забезпечення;
- встановлення і конфігурування нового апаратного і програмного забезпечення;

- створення та підтримка в актуальному стані файлу облікових записів користувачів;
- підтримання інформаційної безпеки організації;
- усунення неполадок в комп'ютерній системі;
- настройка доступу комп'ютерної мережі до інтернету;
- установка та налаштування Windows;
- установка програмного забезпечення та його налаштування;
- зборка ПК;
- підтримка працездатності мережі;
- знищення комп'ютерних вірусів та файлів;
- відновлення інформації на жорсткому диску.

обов'язки диспетчера:

- контроль за об'єктами, що знаходяться під охороною підприємства, в онлайн режимі;
- виклик групи реагування у випадку спрацювання сигналізації.

Обстеження інформаційного середовища включає в себе інформацію, що планується до обробки за допомогою ІТС.

Власником інформації виступає директор. В автоматизованій системі відсутня таємна, службова інформація, а також інформація, що є власністю держави або відомості, які становлять державну таємницю.

За результатами обстеження в ІТС наявні наступні види інформації:

- відкрита інформація;
- конфіденційна інформація;

За режимом доступу інформація, що оброблюється за допомогою ІТС поділяється на:

- інформація з обмеженим доступом (ІзОД);
- відкрита, що потребує захисту;

ІзОД зображена в ІТС у вигляді електронних документів створених

за допомогою пакету прикладних програм Microsoft Office 2010, Adobe Reader або у друкованому паперовому вигляді. Паперові носії інформації зберігаються в сейфі.

Правила доступу до інформації встановлені власником. Доступ до ІзОД мають тільки директор та системний адміністратор. ІзОД, що циркулює в ІТС, зберігається на жорсткому магнітному диску та на комп'ютері директорі.

Документи, що містяться ІзОД, друкуються за допомогою принтерів, які входять до складу ІТС. Копіювання на гнучкі носії та флеш накопичувачі здійснюється з дозволу директора. Перелік відомостей, що включають ІзОД, а також всі відомості за режимом доступу, за правовим режимом та за типом представлення в ІТС приведені та класифіковані у таблиці. Вимоги захисту встановлено власником згідно з вимогами нормативно-правових актів.

Для всіх видів інформації, представлених в таблиці, встановлюється адміністративне керування доступом. Атрибути доступу присвоюються в момент створення документа в системі. Інформація може зберігатися в системі у текстових та графічних форматах.

Імпорт та експорт інформації в ІТС здійснюється за допомогою використання електронної пошти, сканування та друку документів.

Таблиця 2.2- Класифікація інформації

№ п/п	Опис	Детально	Правовий режим	Режим доступу	Тип представлення	Вимоги до захисту	Доступ мають
1	Облік внутрішніх документів	Накази, службові записки, інструкції	Конфіденційна	ІзОД	Зберігається в кабінеті у директора на паперовому носії	К,Ц,Д	Директор
2	Організаційно-розпорядча документація	-	Конфі-денційна	ІзОД	Зберігаються в кабінеті у директора на паперовому носії	К,Ц,Д	Директор, системний адміністратор
3	Інформація про надання послуг, тарифи, контактна інформація підприємства	-	-	Відкрита, не потребує захисту	Текстова та числова інформація в цифровому та паперовому вигляді.	Ц,Д	Директор, системний адміністратор, бухгалтер,
4	Інформація про робітників	Копії паспортів, ІПН	Конфіденційна	ІзОД	Зберігаються в кабінеті у директора на паперовому носії	К,Ц,Д	Директор, Бухгалтер
5	Статутні документи підприємства	-	-	Відкрита, не потребує захисту	Зберігається в кабінеті у директора на паперовому носії	Ц.Д	Усі
6	Облік та реєстрація вхідних та вихіднихдокументів організації	Паролі доступу до об’єктів тощо	Конфіденційна	ІзОД	Зберігається в кабінеті у директора на паперовому носії	К,Ц,Д	Директор

Продовження таблиці 2.2

№ п/п	Опис	Детально	Правовий режим	Режим доступу	Тип представлення	Вимоги до захисту	Доступ мають
	Трудові договори робітників	-	-	Відкрита, не потребує захисту	Текстова інформація в та паперовому вигляді.	Ц,Д	Усі

Обстеження обчислювальної системи

В обчислювальній системі з’єднуються пристрої, що розташовані в межах ОІД, тому вона є локальною. Підключена до глобальної мережі Internet для забезпечення взаємодії з зовнішніми організаціями. Канал зв’язку в межах корпоративної мережі та підключення до мережі Internet забезпечує провайдер «Київстар», який надає послуги з побудови, надання та підтримки відомчої телекомунікаційної мережі у відповідності до Договорів між «Охорона Сервіс» та «Київстар».

Обладнання АС, за допомогою якого обробляється інформація на ОІД: робочі станції директора, бухгалтера, системного адміністратора та диспетчира; БФП, що підключений до робочої станції директора; принтер формату А4, підключений до робочої станції головного бухгалтера та директора. Всі робочі станції підключені до мережі Internet кабельним підключенням; роутер Wi-Fi забезпечує підключення до мережі Internet.

Спосіб з'єднання мережевих пристроїв за топологією відноситься до типу «зірка», побудовану з використанням одного комутатору. Всі комп'ютери мережі приєднані до центрального вузла, тобто роутера.

Таблиця 2.3 – Характеристика складових ІТС наявних у системі

№ п/п	Назва	Умовне позначення на схемі	IP адреса пристрою	Серійний номер	Характеристика
1	Робоча станція 1 (директора) HP Z440 (T4K25EA)	ПК3	192.168.0.104	UTY13UT76R	Intel Pentium G4560 (3.5 ГГц) / RAM 8 ГБ / HDD 1 ТБ / AMD Radeon RX 470, 4 ГБ
2	Робоча станція 2 (бухгалтера) HP Z440 (T4K25EA)	ПК2	192.168.0.103	KTY13UT80D	
3	Робоча станція 3 (системного адміністратора) HP Z440 (T4K25EA)	ПК1	192.168.0.101	RRY13UT87R	
4	Робоча станція 4 (диспетчера) HP Z440 (T4K25EA)	ПК4	192.168.0.102	R TY13RR80D	

Продовження таблиці 2.3

5	БФП, підключений до ПК 3 Brother HL-L2365DWR	P1	-	JNZNR0013	Максимальна роздільна здатність друку 600x2400 dpi Технологія друку Лазерний (ч/б) Стандартний лоток: A4, Letter, A5, A6, Executive Швидкість друку: до 30 стр/хв;
6	БФП, підключений до ПК 2 Brother HL-L2365DWR	P2	-	TY JNR0013	Максимальна роздільна здатність друку 600x2400 dpi Технологія друку Лазерний (ч/б) Стандартний лоток: A4, Letter, A5, A6, Executive Швидкість друку: до 30 стр/хв;
7	БФП, підключений до ПК 1 Brother HL-L2365DWR	P3	-	UTY NR0013	Максимальна роздільна здатність друку 600x2400 dpi Технологія друку Лазерний (ч/б) Стандартний лоток: A4, Letter, A5, A6, Executive Швидкість друку: до 30 стр/хв;

Продовження таблиці 2.3

8	Комп'ютерна миша, підключена до: ПК 1; ПК 2; ПК 3; ПК 4 Logitech Wireless Mouse M185 (910-002238) Grey	-	-	910-002238 910-003501 910-002256 910-002257	Джерело живлення 1 x AA Тип датчика Оптичний Кількість кнопок 2 Інтерфейс Wireless
9	Монітор, підключений до: ПК 1; ПК 2; ПК 3; ПК 4 Philips V-line 203V5LSB26/10/62	-	-	PE19HS4P60 PE19TR5K30 PE19HS4S45 PE19NY4R69	Діагональ дисплея 19.5" Тип матриці TN+film Максимальна роздільна здатність дисплея 1600 x 900 Покриття Матове
10	Клавіатура, підключена до: ПК 1; ПК 2; ПК 3; ПК 4 Logitech K120 USB Black	-	-	C-8940 C-8745 C-8170 C-8952	Інтерфейс USB Кількість кнопок 104 Тип: мембранна

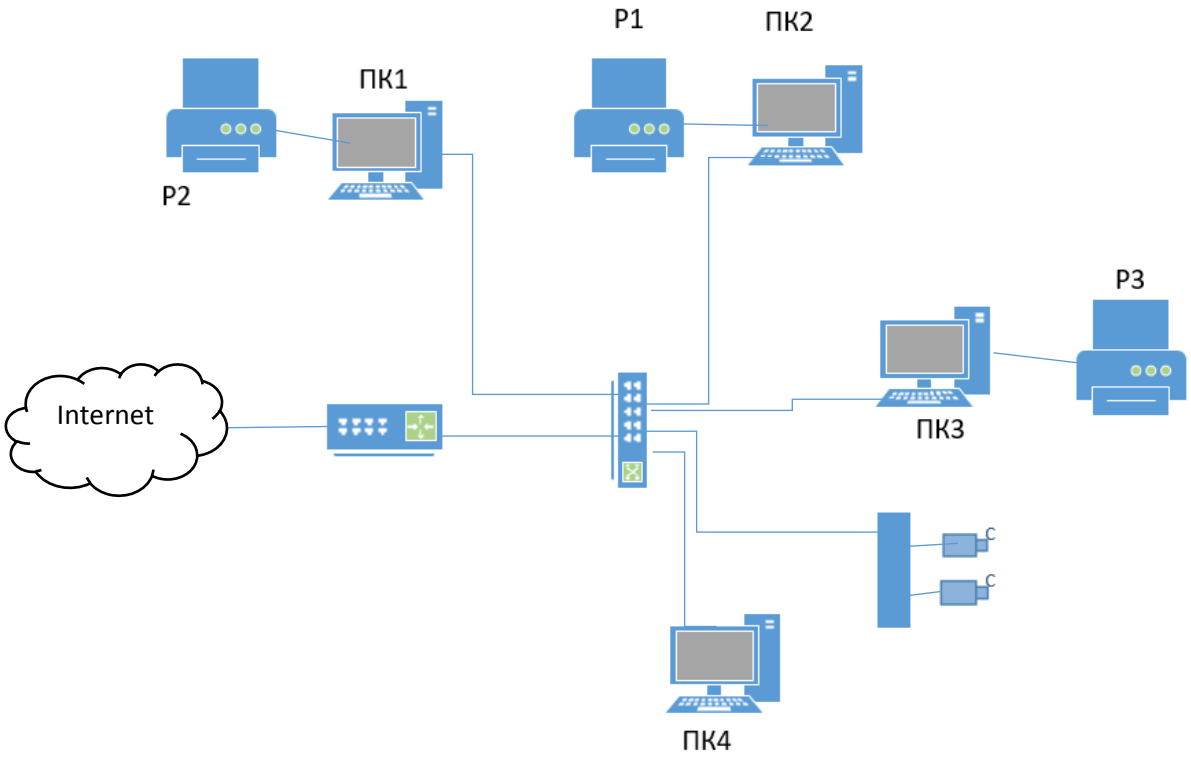

Рисунок 2.6 - Схема ІТС

На робочих станціях встановлені автоматизовані робочі місця (АРМ) з різним набором програмного забезпечення. Детально програмне забезпечення, що встановлене в системі зазначено у таблиці.

ІзОД в ІТС обробляється за допомогою наступних прикладних програм:

- АРМ «Директор» (встановлене на ПК директора - 3);
- АРМ «Бухгалтерія» (встановлене на ПК головного бухгалтера 2);
- АРМ «Адмін» (встановлене на ПК системного адміністратора - 1);
- АРМ «Диспетчир» (встановлене на ПК диспетчира – 4)

За класифікацією АС відноситься до 3 класу: розподілений багатомашинний багато користувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу. Особливість — необхідність передачі інформації через незахищене середовище або, в загальному випадку, наявність вузлів, що реалізують різну політику безпеки.

Таблиця 2.4 - Програмне забезпечення АС

№ п/п	Найменування	Версія	Тип АРМ	Місце встановлення (умовне позначення)	Ліцензійний номер
1	Операційна система Windows 7	Professional x64 (64-біт)	Керівник, Проект, Бухгалтерія	ПК1, ПК2, ПК3,	Частковий ліцензійний ключ продукту: C1 - 3GQ9T; C2 – FFYFG; C3 – 252DM; N – HPR3F.
2	Антивірус Panda Antivirus Pro	9.0			AMJ8-CS7Y-G5AT-USB3
3	Microsoft Office 2007	12.0			Частковий ліцензійний ключ продукту: UI67Y
4	Google Chrome	57.0.2987.133			-
5	VLC media player	4.4.4			-
6	Adobe Reader	10.1.8			-
7	AutoCAD 2013	19.0	Керівник, Проект	ПК3, ПК2	831H4
8	ПРИВАТ БАНК	8.2	Керівник, Бухгалтерія	ПК3, ПК2	-
9	iBank2UA РАЙФАЙЗЕН БАНК АВАЛЬ	2.0.23.6019	Бухгалтерія	ПК2	-

При аналізі технології обробки інформації виявлено особливості обігу електронних документів. Процеси виникнення, рухи й обробки інформації, що циркулює в системі створюють інформаційні потоки. (Рис.2.7)

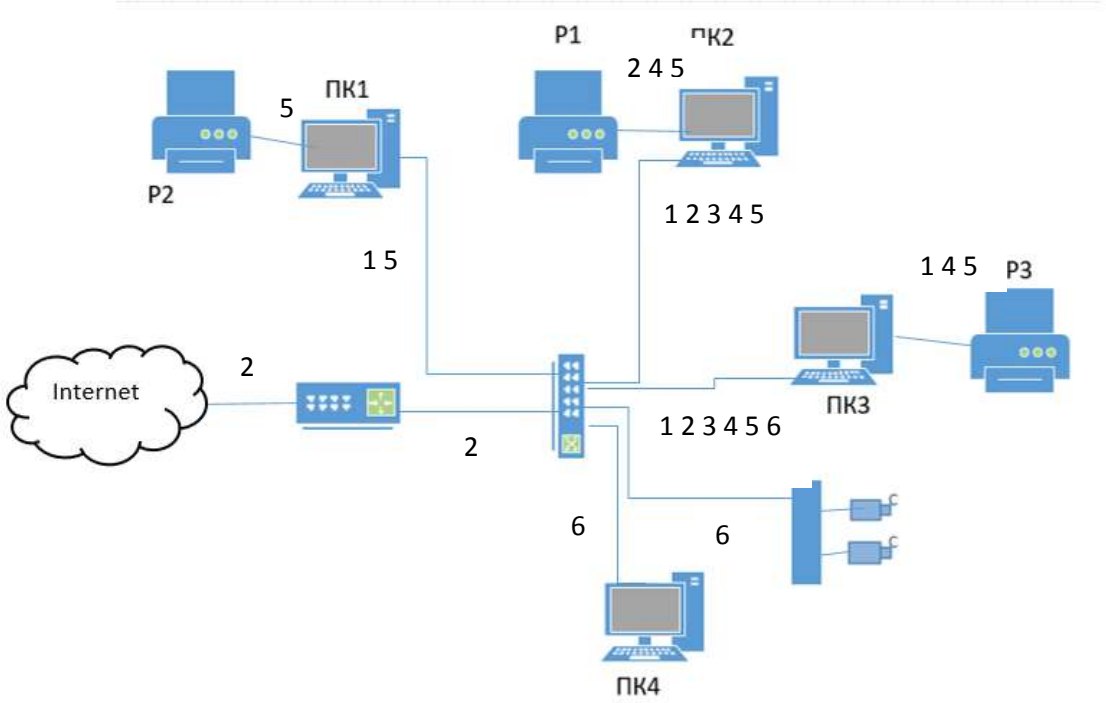

Рисунок 2.7 – Структурна схема інформаційних потоків

До основних інформаційних потоків належать:

1 Обробка проектної документації: створюється та обробляється на робочій станції системного адміністратора, за необхідністю передається на робочу станцію директора та відправляється замовникам через мережу Інтернет, може бути роздрукована.

2 Обробка документації бухгалтерського обліку: створюється та обробляється на робочій станції бухгалтера, дані можуть передаватися через мережу Інтеренет, може бути роздрукована.

3 Обробка кадрових документів: створюється та обробляється на робочій станції директора, бухгалтера та передаються між ними.

4 Обробка персональних даних: створюється та обробляється на робочій станції бухгалтера, за необхідністю передаються на робочу станцію директора, може бути роздрукована.

5 Обробка договірної документації: створюється робочих станціях директора, бухгалтера або системного адміністратора та циркулюють між ними, передаються через мережу Інтернет та друкується.

6 Обробка запису видеоспостереження: створюється та оброблюється на робочій станції диспетчира, за необхідністю передається на робочу станцію директора.

Обстеження середовища користувачів

Серед персоналу, користувачами мережі є – бухгалтер, директор. У системі прописані правила розмежування доступу. Автентифікація в системі відбувається за допомогою логіна-пароля**.**

На підприємстві існують категорії користувачів та адміністраторів, які мають повноваження доступу до ресурсів системи:

адміністратор системи (директор):

- здійснює адміністрування мережевого обладнання та мережевих засобів захисту;
- здійснює загальний контроль за станом безпеки в ІТС;
- здійснює безпосереднє управління правами доступу користувачів в системі.

користувачі (бухгалтер, системний адміністратор): зареєстровані в системі користувачі, що мають доступ до тих видів ІзОД, що необхідні для виконання посадових інструкцій. Ці користувачі виконують обробку інформації зі свого АРМ, відповідно до службових обов’язків.

Суб’єкти доступу до інформації представлені в таблиці.

Таблиця 2.5 - Підрозділи підприємства

№ п/п	Назва підрозділу	Характеристика підрозділу	Посада
1	Адміністративний	Управління підприємством. Ведення бухгалтерського та податкового обліку та аудиту. Нарахування і видача заробітної платні та грошей на відрядження.	Директор, бухгалтер
2	Виробничий	Виконання монтажних робіт, охорона об'єктів.	Директор, охорона

Таблиця 2.6 - Суб’єкти доступу до інформації

№ п/п	ФІО	Умовне позначення пристрою	Роль в інформаційній системі	Посада	Відділ	Контактні дані
1	Григоренко Анатолій Іванович	ПК3	адміністратор	директор	адміністративний	tolyag@gmail.com
2	Скорик Маргарита Петрівна	ПК2	користувач	бухгалтер	адміністративний	margosk@gmail.com
3	Девятов Юрій Володимирович	ПК1	адміністратор	Системний адміністратор	виробничий	yuradev@gmail.com
4	Кириченко Анна Юріївна	ПК4	користувач	Диспечер	адміністративній	Kirann9@gmail.com

2.4 Аналіз та оцінка інформаційних ризиків

Здійснення аналізу ризиків (опрацювання моделі загроз і моделі порушника, можливих наслідків від реалізації потенційних загроз, величини можливих збитків та ін.) та визначення переліку суттєвих загроз є метою етапу формування завдання на створення КСЗІ.

Аналіз ризиків інформаційної безпеки розроблений на основі документу ДСТУ ISO/IEC 27005:2015 - Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT) з урахуванням особливостей діяльності підприємства.

Представлений аналіз включає в себе:

- модель порушника;

-модель загроз;

- ідентифікація наслідків реалізації загроз;

- оцінку ризиків та ймовірності їх появи.

2.4.1 Модель порушника

Порушником вважається особа, яка здійснює спробу несанкціонованого доступу до об’єктів захисту (ознайомлення, модифікація, знищення, тощо).

Враховуючи умови функціонування ІТС, потенційними порушниками можуть бути персонал та користувачі АС, які безпосередньо пов'язані із забезпеченням функціонування ІТС, а також обробкою інформації, що підлягає захисту, а також наступні категорії користувачів, які не мають права обробки інформації в АС:

- особи, яким не передбачено доступ до ІзОД, але які мають доступ до приміщень, де розміщено компоненти ІТС і можуть отримати доступ до ІзОД;
- особи, які знаходяться за межами ІТС, мають можливість фізичного підключення до каналів зв’язку або інших складових мережі передачі даних та можуть здійснити дії щодо порушення діючої в ІТС політики безпеки.

Таким чином, порушники можуть бути внутрішніми (з числа

співробітників, користувачів ІТС) або зовнішніми (сторонні особи, що знаходяться за межами ОІД, або проникли в її межі несанкціонованим шляхом).

Всі зазначені особи мають можливість помилково, внаслідок необізнаності, цілеспрямовано, за злим наміром або без нього, використовуючи різні можливості, методи та засоби здійснити спробу виконати операції, які можуть призвести до порушення конфіденційності, цілісності, доступності та спостережності інформації, яка обробляється в ІТС.

Категорії порушників, що використовуються при створенні моделі, наведено в таблиці.

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

У колонці «Рівень загроз» зазначених таблиць наведено рейтингову оцінку загроз порушника (можливих збитків). Рівень загрози характеризується наступними категоріями:

1 – незначний;

2 – низький;

3 – середній;

4 – високий;

5 - неприпустимо високий.

Виходячи із результатів аналізу характеристики інформації, яка обробляється, категорій порушників, які мають потенційну можливість порушення конфіденційності та цілісності інформації вважаються найбільш: небезпечними, спостережності - менш небезпечними, а доступності - найменш небезпечними.

Таблиця 2.7 - Категорії порушників, що визначені в моделі

Позначення	Визначення категорії	Потенційний рівень загрози
П1	Авторизовані користувачі ІТС, яким надано право доступу до ІзОД (директор)	4
П2	Авторизовані користувачі, яким надано повноваження контролювати дії користувачів та персоналу та забезпечувати управління ІТС (головний бухгалтер, інженер-проектувальник)	5
П3	Особи, які забезпечують працездатність технічних і програмних засобів АРМ ІТС	2
П4	Особи, яким не передбачено доступ до ІзОД, але які мають доступ до приміщень, де розміщено ІТС і потенційно можуть отримати доступ до ІзОД (співробітники, відвідувачі тощо)	2
П5	Особи, які знаходяться за межами ІТС, мають можливість фізичного підключення до каналів зв’язку та можуть здійснити дії щодо порушення діючої в ІТС політики безпеки	5

Таблиця 2.8 - Специфікація моделі порушника за місцем дії

Позначення	Характеристика місця дії порушника	Рівень загрози
Д1	Усередині приміщення, але без доступу до технічних засобів ІТС	1
Д2	З робочих місць користувачів та персоналу ІТС, а також місць розміщення обладнання ІТС, де обробляється інформація, яка підлягає захисту	5
Д3	Без доступу до приміщень, в тому числі з зовнішніх каналів зв’язку, з можливістю застосування технічних засобів здобуття інформації оптичними, акустичними каналами.	2

Таблиця 2.9 - Специфікація моделі порушника за рівнем кваліфікації та обізнаності

Позначення	**Основні кваліфікаційні ознаки порушника**	**Рівень загрози**
К1	Не володіє знаннями та інформацією про порядок функціонування ІТС, не має навичок щодо користування штатними засобами обробки інформації системи та захисту інформації	1
К2	Має навички щодо користування ПК на рівні користувача	2
К3	Володіє базовими знаннями щодо функціонування програмного забезпечення і операційних систем, а також практичними навичками роботи з засобами обробки інформації	4
К4	Володіє знаннями щодо: функціонування засобів та механізмів обробки інформації та її захисту, що використовуються на ІТС та їх недоліків.	5

Таблиця 2.10 - Специфікація моделі порушника за показником можливостей використання засобів ІТС для реалізації загроз

Позначення	**Характеристика можливостей порушника**	**Рівень загрози**
З1	Має фізичний доступ до компонентів ІТС, але не є авторизованим користувачем ІТС	1
З2	Має можливість запуску програм, що реалізують функції обробки інформації	3
З3	Має можливість керування функціонуванням ІТС, тобто конфігурує програмне забезпечення ІТС.	5

Таблиця 2.11 - Специфікація моделі порушника за мотивами здійснення порушень

Позначення	**Мотив порушення**	**Рівень загрози**
М1	Безвідповідальність (недбалість, ненавмисне порушення)	3
М2	Корислива цілеспрямованість (зловмисне порушення)	5

Таблиця 2.12 - Специфікація моделі порушника за часом дії

Позначення	Характеристика можливостей порушника	Рівень загрози
Ч1	Під час бездіяльності компонентів системи (під час планових перерв у роботі, неробочий час)	4
Ч2	Під час функціонування ІТС	5
Ч3	Під час перерв у роботі для обслуговування та ремонту	3

Профілі порушників всіх категорій наведено в таблиці , у колонці «Рівень загроз» наведено рейтингову оцінку загроз порушника з відповідними характеристиками.

Таблиця 2.13 - Профілі можливостей порушників

Позначення	Визначення категорії	Характер дій порушника					Рівень загроз
		Мотив пору-	Кваліфікація	Можливості	Час дії	Місце дії	
П1	Авторизовані користувачі;	М1, М2	К2	З2	Ч1, Ч2	Д2	3
П2	Адміністратор системи;	М1, М2	К4	З3	Ч1, Ч2, Ч3	Д2	5
П3	Персонал, який забезпечує працездатність технічних засобів;	М2	К3	З1	Ч3	Д1, Д2	3
П4	Особи, які не повинні мати доступу до ІзОД, але мають доступ до приміщень, де розміщено обладнання ІТС і потенційно можуть отримати доступ до ІзОД;	М2	К3	З1	Ч1, Ч2	Д1, Д2	2
П5	Особи, які знаходяться за межами ІТС.	М2	К3	З1	Ч2	Д3	1

2.4.2 Модель загроз

За результатами впливу на інформацію та систему її обробки, загрози поділяються на чотири класи:

Порушення конфіденційності інформації (К) - отримання інформації користувачами або процесами всупереч встановленим правилам розмежування доступу до інформації.

Порушення цілісності інформації (Ц) - повне або часткове знищення, викривлення, модифікація інформації, нав'язування хибної інформації тощо.

Порушення доступності інформації (Д) - часткова або повна втрата працездатності системи, блокування доступу до інформації в результаті некоректних дій адміністраторів, технічного обслуговуючого персоналу.

Втрата спостережності (керованості системою) (С) - порушення процедур або процесів ідентифікації та автентифікації адміністраторів і надання їм повноважень, втрата контролю за їх діяльністю, можливість відмови від отримання або пересилання повідомлень.

Загрози потенційно можуть завдати шкоди інформації, персоналу, клієнтам, обладнанню, процесам і програмно-технічним комплексам. Загрози можуть бути навмисними (Н), випадковими (В), природними (П). Повинні бути ідентифіковані як випадкові, так і навмисні джерела загроз. Загрози можуть бути ідентифіковані в загальному вигляді або за типами.

Загрози поділяються на випадкові та навмисні. Випадкові загрози спричиняються помилками у програмному забезпеченні, відмовами апаратури та систем забезпечення, помилками персоналу тощо. Випадкові загрози, спричинені стихійними лихами (повінь, землетрус, пожежа, тощо) розглядаються окремо. Навмисні загрози зумовлені цілеспрямованими діями порушників.

Для оцінки ймовірності реалізації загроз використовуються наступна шкала:

Таблиця 2.14 - Шкала оцінки ймовірності реалізації загрози

Оцінка ймовірності	**Характеристика**
1	Виникнення інциденту практично неможливо
2	Виникнення інциденту малоймовірне (не частіше ніж 1 раз на 1 рік)
3	Виникнення інциденту ймовірне до 1 разу на 3 місяці
4	Виникнення інциденту ймовірне до 1 разу на тиждень
5	Виникнення інциденту ймовірне до 1 разу на добу

Зроблено якісну оцінку ймовірності реалізації загрози та визначено сукупний рівень загрози. Результати аналізу викладені в таблиці 2.15.

Оскільки неможливо одержати достатньо об’єктивні дані про ймовірність реалізації більшості з наведених загроз, ймовірність реалізації загроз визначено експертним методом, на основі аналізу статистичних даних.

В таблиці не розглядаються загрози, що використовують технічні канали витоку інформації (перехоплення побічних електромагнітних випромінювань і наведень, акусто-електричних перетворень інформаційних сигналів, оптичних каналів витоку інформації).

Відповідно до стовпчика «Загальна оцінка загрози» таблиці 2.15, що розраховувалась шляхом находження середнього між значенням ймовірності та рівня загрози. Загрози з загальним рівнем нижче 3 при аналізі ризиків не розглядаються та вважаються незначними. Загальний рівень загроз інформації в ІТС показано на рисунку 2.8.

Таблиця 2.15 - Результати аналізу загроз та вразливостей інформації в ІТС

№	Вид загрози	Вразливості, що призведуть до реалізації загроз	Ймовірність	Що порушує	Рівень загрози	Джерело	Загальна оцінка загрози
1. Навмисні загрози (антропогенні та техногенні)							
1.1	НСД сторонніх осіб до ІзОД в ІТС внаслідок несанкціонованого фізичного доступу до обладнання	- неефективна система охорони; - недостатній контроль за приміщеннями.	2	К,Ц,Д,С	4	зовнішнє	3,5
1.2	НСД до даних з порушенням встановлених правил розмежування доступу внаслідок використання порушником відомих вразливостей системного та прикладного ПЗ	- недосконале або нове ПЗ; - помилки при розмежуванні доступу до системи.	2	К,Ц,Д,С	3	внут-рішнє, зовнішнє	2,5
1.3	Порушення конфіденційності або цілісності інформації, що зберігається в ІТС, внаслідок навмисних дій авторизованого користувача	- відсутність резервних копій; - неправильний підбор персоналу; - неефективне	1	К,Ц,Д,С	3	внут-рішнє	2
1.4	Навмисне виведення з ладу систем життєзабезпечення мережі (електроживлення, охоронної чи пожежної сигналізації та ін.)	- неефективна система охорони; - недостатній контроль за приміщеннями.	2	Ц,Д,С	3	внут-рішнє, зовнішнє	2,5

Продовження таблиці 2.15

№	Вид загрози	Вразливості, що призведуть до реалізації загроз	Ймовірність	Що порушує	Рівень загрози	Джерело	Загальна оцінка загрози
1.5	Впровадження і використання комп'ютерних вірусів, закладних програм для порушення безпеки даних	- відсутність або неефективність антивірусного ПЗ; - наявність незахищеного з`єднання.	2	К,Ц,Д,С	3	внут-рішнє, зовнішнє	2,5
1.6	Одержання технологічної інформації (атрибутів доступу адміністраторів або інших користувачів системи) іншим користувачем ІТС атрибутами доступу для розширювання своїх повноважень або маскування під	- необізнаність персоналу; - відсутність/неефективність ідентифікації та автентифікації користувача.	3	К,Ц,Д,С	2	внут-рішнє	2,5

Продовження таблиці 2.15

№	Вид загрози	Вразливості, що призведуть до реалізації загроз	Ймовірність	Що порушує	Рівень загрози	Джерело	Загальна оцінка загроз
1.7	НСД сторонніх осіб до інформації під час її передачі каналами зв'язку внаслідок навмисного підключення до каналів зв’язку чи обладнання	- незахищене з`єднання з публічними мережами; - невикористання шифрування інформації	2	К,Ц,Д,С	4	зовнішнє	3,5
1.8	Несанкціоноване копіювання інформації	- відсутність журналу подій	3	К	4	внут-рішнє	3,5
1.9	Перевантаження каналів зв’язку або мережевого обладнання (створення умов відмови в обслуговуванні), наприклад, шляхом генерації несправжніх повідомлень для перевантаження системи	- неправильний розрахунок потужності обладнання; - відсутність належного контролю за обладнанням	2	Ц,Д,С	3	внут-рішнє, зовнішнє	2,5
2.Випадкові загрози							
2.1	Ненавмисні дії користувачів, що призводять до відмови функціонування мережі чи окремих її елементів, пошкодження обладнання (телекомунікаційного, програмних та інформаційних ресурсів)	- необізнаність персоналу в питаннях інформаційної безпеки; - доступність до елементів систем, в якій немає необхідності.	2	К,Ц,Д,С	4	внут-рішнє	3

Продовження таблиці 2.15

№	Вид загрози	Вразливості, що призведуть до реалізації загроз	Ймовірність	Що порушує	Рівень загрози	Джерело	Загальна оцінка загрози
2.2	Порушення цілісності інформації, що зберігається, внаслідок ненавмисних дій користувачів	- відсутність резервного обладнання	3	Ц,Д,С	4	внут-рішнє	3,5
2.3	Ненавмисне пошкодження носіїв інформації чи інформації, яка зберігається на цих носіях	-недосвідченість персоналу	2	Ц,Д	3	вну-трішнє	2,5
2.4	Неправомірна зміна режимів роботи обладнання, програмних засобів тощо, ініціювання процесів, які здатні призвести до незворотних змін у системі	-недосвідченість персоналу	1	К,Ц,Д,С	4	внут-рішнє	2,5
2.5	Випадкове зараження програмних засобів комп’ютерними вірусами	-необізнаність персоналу; -неякісне антивірусне ПЗ.	4	К,Ц,Д,С	4	внут-рішнє	4

Продовження таблиці 2.15

№	Вид загрози	Вразливості, що призведуть до реалізації загроз	Ймовірність	Що порушує	Рівень загрози	Джерело	Загальна оцінка загрози
2.6	Невиконання організаційних заходів, посадових і технологічних інструкцій щодо порядку та правил експлуатації чи використання мережевих ресурсів	-недбалість персоналу; -недосвідченість персоналу в питаннях інформаційної безпеки.	2	К,Ц,Д,С	2	внут-рішнє	2
2.7	Неправомірне впровадження і використання забороненого політикою безпеки ПЗ (системне та прикладне ПЗ, навчальні та ігрові програми та ін.)	-недбалість персоналу	2	К,Ц,Д,С	1	внут-рішнє	1,5
2.8	Порушенні цілісності інформації, що зберігається внаслідок апаратного або програмного збою	-відсутність резервного обладнання; -відсутність плану безперервної роботи.	3	Ц,Д,С	4	внут-рішнє	3,5
3. Стихійні (впливи природних факторів)							
3.1	Зміна умов фізичного середовища (стихійні лиха, такі як землетрус, повінь, пожежа і аварії або інші випадкові події)	-наявність легкозаймистих матеріалів; -несправність каналізаційної системи; -старе приміщення.	2	Ц,Д,С	3	зовнішнє	2,5
3.2	Впливи природних завад (грозові розряди, іскріння в електромережах, під час електрозварювання тощо)	- відсутність захисту від блискавки; -неякісна електропроводка; -відсутність резервних каналів електроживлення.	2	Ц,Д,С	3	зовнішнє	2,5

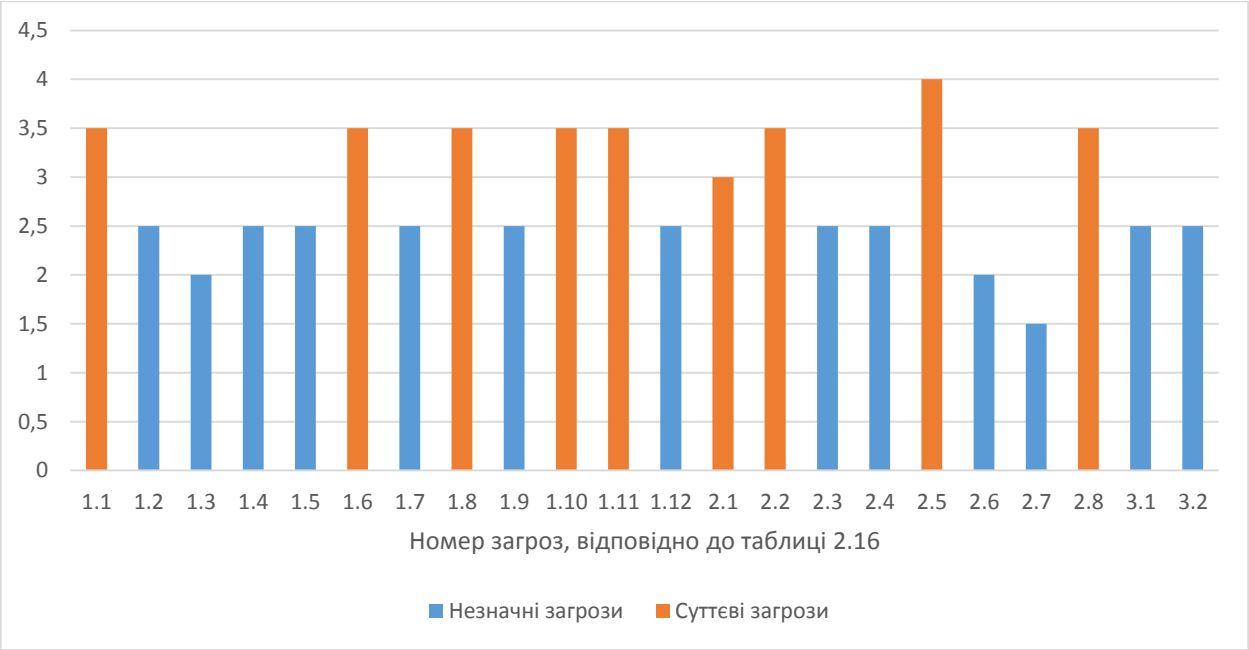

Рисунок 2.8 – Загальний рівень загроз інформації в ІТС

Актуальними загрозами для ОІД вважаються:

- НСД сторонніх осіб до ІзОД, що зберігається та обробляється в ІТС внаслідок несанкціонованого фізичного доступу до обладнання;
- соціальна інженерія (шантаж, підкуп тощо) з корисливою метою;
- одержання та використання атрибутів доступу системи сторонніми особами внаслідок необережного поводження користувачів;
- несанкціоноване копіювання носіїв інформації;
- ненавмисні дії користувачів, що призводять до відмови функціонування мережі чи окремих її елементів, пошкодження апаратурних ресурсів та обладнання, у тому числі телекомунікаційного, програмних та інформаційних ресурсів;
- порушення цілісності інформації, що зберігається, внаслідок ненавмисних (помилкових) дій авторизованого користувача;
- випадкове зараження програмних засобів комп'ютерними вірусами;
- порушення цілісності інформації, що зберігається в базах даних внаслідок апаратного або програмного збою.

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, скомпрометованість інформації. Ці інциденти вплинуть на ресурси підприємства. Таким чином, ресурсам можуть бути приписані значення їх фінансової вартості.

Для оцінки ризиків використані такі шкали:

Таблиця 2.16 - Шкала оцінювання впливу реалізації загрози на конфіденційність

Оцінка рівня наслідків	**Характеристика**
1	Практично не призводить до розкриття конфіденційної інформації
2	Призводить до розкриття окремих документів, які відносяться до ІзОД та/або персональних даних і не призводить до фінансових втрат
3	Призводить до розкриття окремих документів, які відносяться до ІзОД та/або персональних даних і призводить до незначних фінансових втрат
4	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
5	Призводить до зупинки роботи системи, порушення вимог нормативно-правової бази

Таблиця 2.17 - Шкала оцінювання впливу реалізації загрози на доступність

Оцінка рівня наслідків	**Характеристика**
1	Практично не впливає на доступність
2	Вплив на доступність незначний (не більше 1/10 від максимально допустимого часу простою)
3	Вплив на доступність середній (не більше 1/4 від максимально допустимого часу простою)
4	Вплив на доступність значний (до максимально допустимого часу простою)
5	Призводить до зупинки роботи системи на тривалий час, який перевищує максимально допустимий час простою)

Таблиця 2.18 - Шкала оцінювання впливу реалізації загрози на спостережність

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

Таблиця 2.19 - Шкала оцінювання впливу реалізації загрози на цілісність

Оцінка рівня наслідків	**Характеристика**
1	Практично не призводить до наслідків з фінансовими втратами
2	Призводить до незначних фінансовихвтрат
3	Призводить до значнихфінансових втрат
4	Призводить до великихфінансових втрат і може призвести до зупинки роботи системи підприємства
5	Призводить до зупинки роботи системи, порушення вимог нормативно-правової бази

Оцінка збитків, що можуть бути нанесені ІТС внаслідок реалізації загроз складається з величин очікуваних збитків від втрати інформацією кожної з властивостей (конфіденційності, цілісності або доступності) або від втрати керованості системи внаслідок реалізації загрози. Величина

можливих збитків визначається розміром фінансових втрат якісною шкалою, через визначення

цього критерія кількісно.

Величина збитків:

1- відсутня,

2- низька,

3- середня,

4- висока,

5- неприпустимо висока.

Для оцінки ризиків використана комбінація кількісних та якісних методів. Це дає змогу розрахувати доцільність впровадження політики безпеки, адже вартість заходів безпеки, не мають бути 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.

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

- НСД сторонніх осіб до ІзОД, що зберігається та обробляється в ІТС внаслідок несанкціонованого фізичного доступу до обладнання;

- одержання та використання атрибутів доступу системи сторонніми особами внаслідок необережного поводження користувачів;

- ненавмисні дії користувачів, що призводять до відмови функціонування мережі чи окремих її елементів, пошкодження апаратурних ресурсів та обладнання, у тому числі телекомунікаційного,

програмних та інформаційних ресурсів;

- випадкове зараження програмних засобів комп’ютерними вірусами;
- порушення цілісності інформації, що зберігається в базах даних внаслідок апаратного або програмного збою.

Таблиця 2.20 – Рівень ризику

№	Загроза/ вразливість	Оцінка ймовірності реалізації загрози з використанням вказаної вразливості	Оцінка реалізації загрози на цілісність	Оцінка реалізації загрози на конфіден-ційність	Оцінка реалізації загрози на доступ-ність	Оцінка реалізації загрози на спосте-режність	Оцінка величини можливих збитків	Рівень ризику за окремою парою загроза/ вразливість
1	Несанкціонована модифікація інформації	2	1	**1**	2	2	2	16
2	Навмисне або ненавмисне знищення ПЗ і/або технічних засобів	1	**2**	2	2	2	3	48
3	Розголошення даних аутентифікації користувачів системи	1	1	**2**	2	3	2	24

№	Загроза/ вразливість	Оцінка ймовірності реалізації загрози з використанням вказаної вразливості	Оцінка реалізації загрози на цілісність	Оцінка реалізації загрози на конфіден-ційність	Оцінка реалізації загрози на доступ-ність	Оцінка реалізації загрози на спосте-режність	Оцінка величини можливих збитків	Рівень ризику за окремою парою загроза/ вразливість
4	Навмисне або ненавмисне вимкнення антивірусного захисту	2	1	2	1	**3**	2	24
5	Навмисне або не навмисне розголошення конфіденційної інформації або інформації, що становить комерційну таємницю	2	1	**2**	3	1	3	36
6	Несанкціонований друк та копіювання інформації	2	2	1	**2**	2	3	48
7	Модифікація журналу подій	3	1	1	**1**	2	2	12

Продовження талбиці 2.20

8	Випадкове зараження програмних засобів комп’ютерними вірусами	2	2	2	**2**	1	3	48

За отриманим максимальним рівнем ризику за окремою парою, складена шкала оцінки ризику для можливості класифікувати ризики за рівнем прийнятності. Шкала оцінки ризику:

- 0-21 малий рівень ризику;
- 22-43 припустимий рівень ризику;
- 44-64 критичний рівень ризику.

Враховуючи характеристики існуючої ІТС та вимог до властивостей інформації, відповідно до НД ТЗІ 2.5-005 -99, обрано стандартний функціональний профіль захищеності для системи:

3.КЦ.1 = {КД-2, КВ-1, ЦД-1, ЦВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НВ-1}

Перелік послуг, що входять в обраний профіль захищеності приведено посилаючись на НД ТЗІ 2.5-004-99 зі змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу»:

КД-2 Базова довірча конфіденційність, відноситься до Критерії конфіденційності - Довірча конфіденційність.

Ця послуга дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Атрибути доступу об'єктів і користувачів повинні містити інформацію, що використовується КЗЗ для розмежування доступу до об'єктів з боку конкретного користувача. Додатково повинна існувати можливість встановлювати, які користувачі можуть активізувати конкретний процес, що дозволяє одержати можливість обмеженого керування потоками інформації. Керування правами доступу на даному рівні має невисоку вибірковість. Користувач, домену якого належить об'єкт (процес) може вказати, які групи користувачів і, можливо, які

конкретні користувачі мають право одержувати інформацію від об'єкта (ініціювати процес).

КВ-1 Мінімальна конфіденційність при обміні, відноситься до Критерії конфіденційності – Конфіденційність при обміні.

Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище.

Забезпечує захист від несанкціонованого ознайомлення за рахунок пасивного спостереження за лініями зв'язку або розкрадання носіїв інформації. Прикладом реалізації може служити програмне шифрування файлів перед їх передачею каналами зв'язку або прозоре шифрування файлів перед їх записуванням на диск.

ЦД-1 Мінімальна довірча цілісність,відноситься до Критерії цілісності – Довірча цілісність.

Ця послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

На даному рівні користувач, домену якого належить об'єкт, може накладати обмеження на доступ до об'єктів з боку інших користувачів. Керування правами має грубу вибірковість. Для такої системи можна побудувати часткову матрицю доступу користувачів до захищених об'єктів.

ЦВ-1 Мінімальна цілісність при обміні,відноситься до Критерії цілісності – Цілісність при обміні

Ця послуга забезпечує мінімальний захист. На включення даного рівня в свій рейтинг може претендувати система, що дозволить на підставі цифрового підпису перевіряти цілісність функціонуючого на ЕОМ ПЗ, або система електронної пошти, що забезпечує цифровий підпис повідомлень.

HP-2 Захищений журнал, відноситься до Критерії спостереженості – Реєстрація

Ця послуга дозволяє контролювати небезпечні для КС дії.Вибір фізичного носія, що використовується для зберігання даних реєстрації, повинен відповідати способу використання і обсягу даних. Будь-яке переміщення таких даних має виконуватись способом, що гарантує їх безпеку. Одним із найбезпечніших, хоч і досить дорогих рішень, є використання носіїв з одноразовим записом. В будь-якому випадку рівень захищеності даних реєстрації має бути не нижче, ніж рівень захищеності даних користувачів, яку забезпечують реалізовані послуги конфіденційності і цілісності. Повинні бути вироблені угоди щодо планування і ведення архівів даних реєстрації.

Засоби аналізу — це засоби, що виконують більш складну, ніж перегляд, оцінку журналу реєстрації з метою виявлення можливих порушень політики безпеки. Ці засоби повинні надавати адміністратору можливість виконання сортування, фільтрації за певними критеріями та інших подібних операцій. КЗЗ повинен надавати адміністратору можливість вибирати події, що реєструються. Це може бути досягнено або через "передвибірки", або "поствибірки". Передвиборка подій, що реєструються, дозволяє виділити під час ініціалізації системи з всієї множини доступних для реєстрації подій підмножину тих, що необхідно реєструвати в журналі. Використовуючи передвибірку, адміністратор може зменшити кількість реально реєстрованих подій і, отже, розмір остаточного журнального файлу. Недоліком предвибірки є те, що ті події, які не були вибрані, не можуть уже пізніше бути проаналізовані, навіть, якщо постає така необхідність. Перевага поствибірки полягає в гнучкості можливості аналізу "пост-фактум", проте така організація ведення журнального файла вимагає виділення значного обсягу пам'яті для даних реєстрації.

НИ-2 Одиночна ідентифікація і автентифікація, відноситься до Критерії спостереженості – Ідентифікація і автентифікація

Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, який намагається одержати доступ до КС. Хоч поняття ідентифікація і автентифікація відрізняються, на практиці обидва ці процеси важко буває поділити. Важливо, щоб в кінцевому підсумку були підстави стверджувати, що система має справу з конкретним відомим їй користувачем.

Пароль, персональний номер або інша подібна інформація є прикладом того, що називається "дещо, відоме користувачеві". Даний тип автентифікації є простим у реалізації і достатньо ефективним. Проте його ефективність обмежена простотою його повторення: достатньо просто обчислити або вгадати інформацію автентифікації, а для її дублювання не вимагається спеціального устаткування чи можливостей.

НК-1 Однонаправлений достовірний канал, відноситься до Критерії спостереженості – Достовірний канал

Дана послуга дозволяє гарантувати, що користувач взаємодіє безпосередньо з КЗЗ і ніякий інший користувач або процес не може втручатись у взаємодію (підслухати або модифікувати інформацію, що передається). Рівні даної послуги ранжируються в залежності від того, чи має КЗЗ можливість ініціювати захищений обмін, чи це є прерогативою користувача.

НО-1 Виділення адміністратора, відноситься до Критерії спостереженості – Розподіл обов'язків

Дана послуга дозволяє знизити ймовірність навмисних або помилкових неавторизованих дій користувача або адміністратора і величину потенційних збитків від таких дій. Рівні даної послуги ранжируються на підставі вибірковості керування можливостями користувачів і адміністраторів.

НЦ-1 КЗЗ з контролем цілісності, відноситься до Критерії спостереженості – Цілісність комплексу засобів захисту

Дана послуга визначає міру спроможності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

Жодна КС не може вважатися захищеною, якщо самі засоби захисту є об'єктом для несанкціонованого впливу. У зв'язку з цим рівень НЦ-1 даної послуги є необхідною умовою для абсолютно всіх рівнів усіх інших послуг.

Для рівня НЦ-1 даної послуги необхідно, щоб КЗЗ мав можливість перевіряти свою цілісність і в разі виявлення її порушення переводити систему в стан, з якого її може вивести тільки адміністратор.

НВ-1 Автентифікація вузла,відноситься до Критерії спостереженості – Ідентифікація і автентифікація при обміні

Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ранжируються на підставі повноти реалізації.

2.5 Розробка політики безпеки для підприємства

Під час розробки політики безпеки повинні бути враховані технологія обробки інформації, моделі порушників і загроз, особливості ОС, фізичного середовища та інші чинники. В АС може бути реалізовано декілька різних політик безпеки, які істотно відрізняються.

Як складові частини загальної політики безпеки в АС мають існувати політики забезпечення конфіденційності, цілісності, доступності оброблюваної інформації.

Політика безпеки повинна стосуватись: інформації (рівня критичності ресурсів АС), взаємодії об'єктів (правил, відповідальності за захист інформації, гарантій захисту), області застосування (яких складових компонентів АС політика безпеки стосується, а яких – ні).

Загальні правила

1 В системі необхідно ввести чіткі правила розмежування прав доступу. Кожен користувач повинен однозначно ідентифікуватися системою. Інформаційний ресурс, що підлягає захисту повинен мати свій атрибут доступу, на підставі якого здійснюється організація прав доступу користувача до інформаційного ресурсу.

2 В системі повинна виконуватися однозначна ідентифікація та автентифікація користувачів. Автентифікація користувача повинна відбуватися за допомогою захищених механізмів перш ніж дозволити користувачеві виконувати ті чи інші дії в системі (двоетапна веріфікація).

3 Для зменшення потенційних збитків від навмисних або помилкових (випадкових) дій користувача бажано обмежити авторитарність користувача. Для цього необхідно визначити рівні доступу адміністратора та користувачів системи та встановити перелік функціональних можливостей та обов'язків користувача та адміністратора.

4 Для захисту інформації в системі від комп'ютерних вірусів використовується таке програмне забезпечення як ESET NOD32 Antivirus

(ліцензійна версія 2014 року). Для коректного роботи програми необхідно регулярно проводити оновлення баз даних сигнатур та ін. з достовірного джерела.

5 Організувати процес навчання, контролю та перепідготовки персоналу за напрямом забезпечення безпеки інформації.

6 Необхідно відстежувати ризики інформаційної безпеки та вживати дії, коли зміни призводять до виникнення непередбачуваних ризиків.

7 Ситуації, що можуть призвести організацію до порушення законів та встановлених норм, не мають бути допущені.

8 Звіти про стан інформаційної безпеки мають бути доступні.

9 Інциденти інформаційної безпеки не повинні призводити до серйозних непередбачуваних втрат або до серйозних зривів діяльності підприємства.

2.5.1 Політика безпеки поштового сервісу

1 Опис

Електронна пошта використовується практично в усіх галузях і часто є основним засобом спілкування в межах організації. В той же час, неправильне використання електронної пошти може спричинити багато ризиків, що стосуються інформаційної безпеки, тому для користувача необхідно розуміти важливість належного використання електронних ресурсів.

2 Призначення

Метою даної політики є забезпечення правильного використання користувачами ПП «Охорона Сервіс» поштових сервісів, та інформувати їх про те, що саме ПП «Охорона Сервіс» вважає прийнятним і неприйнятним при використанні електронної пошти. Ця політика визначає мінімальні вимоги до використання електронної пошти в мережі.

3 Область застосування

Ця політика охоплює належне використання будь-якого електронного листа, надісланого за допомогою поштового сервісу і застосовується до всіх працівників, постачальників та агентів, які працюють від імені ПП «Охорона Сервіс».

4 Положення політики

4.1 Використання електронної пошти повинно відповідати політиці та процедурам етичного поведінки, безпеці, відповідності діючим законам та належній діловій практиці.

4.2 Необхідно проводити періодичний інструктаж для авторизованих користувачів щодо появи актуальних загроз в мережі Internet та вивести чіткі правила передачі даних.

4.3 Відкриття та відповідь на листи, отримані електронною поштою, повинна здійснюватися тільки після підтвердження особи відправника (відомість та надійність джерела).

4.4 Необхідно вимкнути опцію автоматичного завантаження додатків. У разі завантаження, перед відкриттям необхідно просканувати додаток за допомогою антивірусу.

4.5 Для читання електронної пошти використовувати обліковий запис, який має обмежені повноваження.

5 Політика відповідальності

Співробітник, що порушив цю політику, може бути предметом дисциплінарного стягнення, включаючи припинення роботи.

Зміни до документу:

07.05.2019 – Перший випуск.

2.5.2 Політика чистого столу

1. Опис

Дана політика визначає, в якому вигляді співробітники приватного підприємства повинні залишати свої робочі місця, коли вони залишають їх без нагляду або не використовують їх.

2. Метою даної політики є запобігання витоку або втрати інформації з обмеженим доступом

3. Галузь застосування

Вимоги даної політики поширюються на всіх співробітників підприємства.

4. Інструкція політики

- Співробітники зобов’язані забезпечувати збереження всієї інформації з обмеженим доступом у друкованому або електронному вигляді на своєму робочому місці, коли вони збираються покинути приміщення на короткий або тривалий проміжок часу.
- Персональні комп’ютери повинні бути заблоковані, якщо передбачається, що вони не будуть використовуватись деякий час.
- Персональні комп’ютери повинні бути повністю вимкнені в кінці робочого дня.
- Будь-яка інформація з обмеженим доступом повинна бути видалена з робочого місця і замкнена в ящику чи сейфі, коли стіл не зайнятий і в кінці робочого дня.
- Ключі, що використовуються для доступу до інформації з обмеженим доступом, не можна залишати без нагляду на столі.
- Паролі не можуть бути розміщені на комп’ютері, під ним або записані в нотатках.
- Інформація з обмеженим доступом, що була роздрукована, повинна бути негайно видалена з принтера.
- Інформація, що підлягає знищенню, повинна бути утилізована за допомогою шредера якнайшвидше.

5. Відповідальність

- Кожен співробітник повинен дотримуватись вимог даної політики.
- Відповідальність за виконання співробітниками вимог даної політики несе директор.

- Співробітники, що порушили дану політику, несуть відповідальність відповідно до внутрішніх нормативних документів підприємства.

2.5.3 Політика розмежування прав доступу

1. Опис

Політика розмежування прав доступу регламентує правила доступу користувачів і процесів до пасивних об’єктів.

2. Мета: надати доступ до інформації користувачам, яким він необхідний згідно з посадовими інструкціями.

3. Галузь застосування

Відноситься до всіх користувачів системи.

4. Інструкція політики

Відповідно до НД ТЗІ 1.4-001-2000, мають виконуватися наступні дії:

- кожне робоче місце повинно мати свого користувача, який несе відповідальність за його працездатність та за дотримання всіх вимог і процедур, пов’язаних з обробкою інформації та її захистом. Користувач повинен бути забезпечений відповідними інструкціями і навчений всім вимогам і процедурам;

- для попередження неавторизованого доступу до даних, ПЗ, інших ресурсів, керування механізмами захисту здійснюється адміністратором системи;

- за всі зміни ПЗ, створення резервних і архівних копій несе відповідальність адміністратор. Такі роботи виконуються за його дозволом;

- кожний користувач має свій унікальний ідентифікатор і пароль. Право видачі цих атрибутів надається адміністратору. Атрибути для адміністраторів надає адміністратор безпеки ІТС. Видача атрибутів дозволяється тільки після документальної реєстрації особи як

користувача;

- користувачі проходять процедуру автентифікації для отримання доступу до ресурсів ІТС;

- атрибути користувачів змінюються двічі на рік , а невикористовуванні і скомпрометовані – видаляються.

Контроль за ПРД можливий при створенні матриці керування доступом: виділяють об’єкти та суб’єкти доступу. Суб'єктами інформаційних відносин є особи, об'єктом інформаційних відносин є інформація.

1) Суб’єкти доступу:

S1 – директор;

S2 – системний адміністратор;

S3 – бухгалтер;

S4 – диспетчер;

2) Об’єкти доступа:

O1 - організаційно-розпорядча документація;

O2 - облік внутрішніх документів (накази, службові записки, інструкції);

O3 - інформація про надання послуг, тарифи, контактна інформація підприємства;

O4 - Інформація про робітників;

O5 - Статутні документи підприємства (документи, що дозволяють займатися підприємницькою діяльністю);

O6 - Облік та реєстрація вхідних та вихідних документів організації;

O7 - Трудові договори робітників;

O8 - Договори про надання послуг клієнтам;

O9 - База даних клієнтів;

O10 - Заявки на підключення обладнання;

О11 - Акти прийому виконаних спеціалістом з монтажу робіт;

О12 - Дані про лицьові рахунки замовників;

О13 - Заявки на розірвання договору про надання послуг;

О14 - Відомості про фінанси підприємства;

О15 - Плани закупівель;

О16 - Відомості постачальників;

О17 - Зміст та характер договорів, контрактів однією із сторін яких виступає підприємство;

О18 - База вхідних цін;

О19 - Коди програмного обладнання;

О20 - Інформація по ліцензійне ПО;

О21 - Повна характеристика комп'ютерної техніки (серійний номер, заводський номер і т.д.);

О22 - Звіт про виконання ремонтних послуг офісної техніки;

О23 - База даних клієнтів;

О24 - Відомості про дату заключення договору між клієнтом та підприємством;

О25 - Відомості про створення сертифіката клієнта;

О26 - Відомості про генерацію ключів ЕЦП, формування сертифікатів відкритих ключів ключей ЕЦП;

О27 - Відомості про надання послуг приватним підприємствам;

О28 - Відомості про надання послуг державним підприємствам;

О29 - Формування та ведення реєстра форм звітних документів;

О30 - Формування та відправка пакетів звітності в електронному вигляді по електронній пошті з використання криптографічного захисту.

З) Операції з файлами:

Ч – читання;

З – зберігання;

Д – друкування;

К - копіювання;

Зн – знищення;

Зм - змінення.

Табл. 2.21 Операції з файлами

	O1	O2	O3	O4	O5	O6	O7	O8	O9
S1	Ч,З,Д,ЗМ,ЗН,К	Ч,З, Д	Ч,З,Д,ЗМ,ЗН,К	Ч,З,Д,ЗН,ЗМ	Ч,З,Д,К,ЗН,ЗМ	Ч,З,Д,К,ЗМ,ЗН	Ч,З,Д,К,ЗН,ЗМ	Ч,З,Д,К,ЗН,ЗМ	Ч,З,Д,К,ЗН,ЗМ
S2	-	Ч,З,Д	Ч,З,Д,	-	Ч,К	-	Ч,З,Д,К,ЗН	Ч,З,Д,К,ЗН,ЗМ	Ч,З,К,Д,ЗМ,ЗМ
S3	-	-	Ч,З,Д,	Ч,З,Д,ЗН,ЗМ	Ч,З,Д,К	-	Ч,З,Д,К,ЗН,ЗМ	-	-
S4	-	-	-	-	Ч,З	-	Ч,З,К,Д	-	-
S5	-	-	-	-	Ч,З	-	Ч,З,К,Д	Ч,З,Д,К	Ч,З,Д,К
	O10	O11	O12	O13	O14	O15	O16	O17	O18
S1	Ч,З,К,Д,ЗМ,ЗН	Ч,З,К,Д,З,ЗМ,ЗН	Ч,З,К,Д	Ч,З,К,Д,ЗМ,ЗН	Ч,З,К,Д,ЗМ,ЗН	Ч,З,К,Д,ЗМ,ЗН	Ч,З,К,Д,ЗМ,ЗН	Ч,З,К,Д,ЗМ,ЗН	Ч,З,К,Д,ЗМ,ЗН
S2	Ч,З,К,Д,З	Ч,З,К,Д	-	-	-	-	-	Ч,З,К,Д,ЗМ,ЗН	-
S3	-	-	Ч,З,К,Д	-	Ч,З,К,Д,ЗМ,ЗН	Ч,З,К,Д,ЗМ,ЗН	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ
S4	-	Ч,З,К,Д	-	Ч,З,К,Д,ЗМ,ЗН	-	-	-	-	-
	O19	O20	O21	O22	O23	O24	O25	O26	O27
S1	Ч,З,К,Д,ЗМ,ЗН	Ч,З,Д,К,	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ,ЗН	Ч,З,К,Д,ЗМ
S2	Ч,З,К,Д	Ч,З,Д,К	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ

Продовження таблиці 2.21 Операції з файлами

S3	Ч,З,К,Д	Ч,З,К,Д	Ч,З,К,Д	-	-	-	-	-	-
S4	Ч,З,К,Д	Ч,З,К,Д	Ч,З,К,Д	-	-	-	Ч,З,К,Д,ЗМ	Ч,З,К,Д	Ч,З,К,Д
	О28	О29	О30						
S1	Ч,З,К,Д,ЗМ,ЗН	Ч,З,К,Д,ЗМ,ЗН	Ч,З,К,Д,ЗМ,ЗН						
S2	Ч,З,К,Д,ЗМ	Ч,З,К,Д	Ч,З,К,Д						
S3	-	-	-						
S4	Ч,З,К,Д	Ч,З,К,Д	Ч,З,К,Д						

Висновки до розділу 2

У другому розділі описаний об'єкт, рід діяльності, інформаційна система, інформаційні потоки, устаткування, програмне забезпечення. У технічному завданні виконаний, аналіз структури ІТС, аналіз загальної моделі загроз, визначений перелік порушників, інформаційних потоків і існуючих проблем у системі безпеки. Виконано вибір профілю захищеності підприємства.

В результаті проведеного обстеження ОІД побудовано модель загроз, що діють на дану ІТС, було класифіковано інформацію, що зберігається і циркулює на підприємстві та виявлено ресурси, які потребують найбільшого рівня інформаційної безпеки. Получені результати були використані для розробки політики безпеки на підприємстві «Охорона Сервіс».

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

3.1 Необхідність обґрунтування витрат на реалізацію політики безпеки

Метою розрахунків є економічне обґрунтування доцільності впровадження політики безпеки інформації. Для цього визначено економічну ефективність використання основних результатів, що отримані в ході виконання роботи.

Економічна доцільність визначається розрахунками:

- капітальних витрат, що потребує розроблена політика безпеки;

- експлуатаційних витрат;

- річного економічного ефекту від впровадження інформаційної політики безпеки.

Запропонована інформаційна політика безпеки передбачає необхідність витрат на її реалізацію. До заходів, що потребують витрат відносяться:

1. оновлення ліцензій антивірусного програмного забезпечення;
2. навчання персоналу в питаннях інформаційної безпеки;

3.2 Визначення трудомісткості розробки політики безпеки інформації:

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

Де $t_{mз} = 3$ год. - тривалість складання технічного завдання на розробку політики безпеки інформації;

$t_{в}$ = 2год. - тривалість розробки концепції безпеки інформації у організації;

$t_{а}$ = 3год. – тривалість процесу аналізу ризиків;

твз = 3год. – тривалість визначення вимог до заходів, методів та засобів захисту;

тозб = 2год.– тривалість вибору основних рішень з забезпечення безпеки інформації;

товр = 1год. – тривалість організації виконання відновлювальних робіт забезпечення неперервного функціонування організації;

тд = 4год.– тривалість документального оформлення політики безпеки.

t = 3 год + 2 год +3 год + 3 год + 2 год + 1 год + 4 год = 18 год

3.3 Розрахунок витрат на створення політики безпеки:

$$K_{рп} = З_{зп} + З_{мч} \qquad (3.3)$$

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

$$З_{зп} = t \cdot З_{іб} = 18*790=14220, \quad \text{грн},$$

де t – загальна тривалість розробки політики безпеки, годин;

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

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

$$З_{Мч} = t \cdot C_{Мч}, \text{ грн},$$

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

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

Вартість 1 години машинного часу ПК визначається за формулою:

$$C_{мч} = P \cdot t_{нал} \cdot C_e + \frac{Ф_{зал} \cdot Н_a}{F_p} + \frac{К_{лпз} \cdot Н_{апз}}{F_p} =$$

0,4*1*1,50+(11100*0,2/1920)=0,6+1,5=1,75 грн/год,

Де Р – встановлена потужність ПК, 0,4кВт;

$t_{нал}$ – кількість машин на яких розроблюється політика безпеки;

Се – тариф на електричну енергію, 1,50грн/кВт·година;

Фперв– первісна вартість ПК на початок року, 10000 грн.;

На – річна норма амортизації на ПК, 0.2 частки одиниці;

Напз – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

Клпз – вартість ліцензійного програмного забезпечення, 1100грн.;

Fp – річний фонд робочого часу (за 40-годинного робочого тижня Fp = 1920 год)

$$З_{мч} = t \cdot C_{мч} = 18*1,75=31,5 \text{ грн.}$$

$$К_{рп} = 14220+31,5= 14251,5 \text{ грн.}$$

3.4 Розрахунок (фіксованих) капітальних витрат:
Оновлення ліцензії антивірусного ПЗ ESET NOD32 Antivirus:

Необхідне оновлення для 4 комп'ютерів, вартість однієї ліцензії – 215 грн. Загальна вартість закупівель ліцензійного ПЗ:

Кзпз = 4*215 грн = 860 грн. (3.3)

Вартість роботи системного адміністратора розраховується з урахуванням заробітної платні робітника в час та тривалістю його роботи:

$$Кмн = 56 грн/ч*2 = 112 грн.$$

$К_{навч}$ (витрати на навчання системного адміністратора) становлять 1500 грн.

$К_{аз}$ вартість закупівлі апаратного забезпечення та допоміжних матеріалів, відсутня оскільки за розробленими політики безпеки закупівля апаратного забезпечення не є необхідною.

$К_{н}$ витрати на встановлення обладнання та налагодження системи інформаційної безпеки, відсутні оскільки не закуповується апаратне забезпечення.

Таким чином, капітальні (фіксовані) витрати на впровадження системи інформаційної безпеки складають:

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

Де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього завнішніх консультантів, тис.грн;

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

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

$К_{рп}$ – вартість розробки політики безпеки іенформації, тис. грн;

$К_{навч}$ - витрати на навчання технічних фахувців і облуговуючого первоналу, тис. грн;

$К_н$ – витрати на встановчення обладнення та налагодження системи інформаційної безпеки, тис.грн.

$$К = К_{пр} + К_{зпз} + К_{рп} + К_{аз} + К_{навч} + К_н = 10850+860+112+1500= 13322 \text{ грн.}$$

3.5 Розрахунок поточних (експлуатаційних) витрат:

1. навчання персоналу в питаннях інформаційної безпеки;

2. витрати на керування системою інформаційної безпеки.

1. Витрати на навчання персоналу в питаннях інформаційної безпеки включають в себе послуги сторонніх організацій, що створюють політику безпеки інформації та відповідно до неї розробляють інструкції для персоналу, що є користувачами системи. Вартість навчання адміністративного персоналу й кінцевих користувачів розглянутої системи:

Со = 12000 грн – витрати навчання персоналу

3. Обов'язки з керування системою інформаційної безпеки виконує директор та системний адміністратор (за відсутності директора), тому річний фонд заробітної плати складає додаткову заробітну плату директора та системного адміністратора за рік:

$$Сз = Зд+Зса = 1800+1350=3150 \text{грн. (за 1 місяць)} \quad (3.4)$$

$$Сз = 3150*12 = 37800 \text{ грн. (за 1 рік)}$$

де Зд –заробітна плата директора, грн на рік. Зса – заробітна плата системного адміністратора, грн. на рік.

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року (Се), визначається за формулою:

$$Се = Р \cdot Fр \cdot Це$$

де Р – встановлена потужність апаратури інформаційної безпеки, кВт – відсутня для даної системи;

Fр = 12 міс * 20 робочих діб/міс * 8 робочих годин * 4 комп'ютера = 7680 год – річний фонд робочого часу системи інформаційної безпеки;

Це = 1,50 грн за 1 кВт/год – тариф на електроенергію на 01.04.2017 року.

$$Се = 7680*1,50 = 11520 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки (Стос) визначаються у відсотках від вартості капітальних витрат (2%).

$$Стос = К * 0,02 = 948*0,02 = 18,96 \text{ грн.}$$

Отже, річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки складають:

$$С = Со + Спрд + Сз + Се + Стос = 2940 + 11520 + 18,96 + 12000 = 26478,96 \text{ грн}$$

Розрахунок оцінки величини збитку:

Втрати від зниження продуктивності співробітників атакованої системи мережі являють собою втрати їхньої заробітної плати за час простою внаслідок атаки ($П_п$).

Посада	Розмір заробітної платі, грн	Кількість співробітників	Витрати на заробітну плату на місяць, грн
директор	10000	1	10000
Системний адміністратор	8500	1	8500
бухгалтер	5000	1	5000
диспетчер	4200	4	16800
		Загалом	40300

Таблиця 3.1 зарплати робітників за місяць

Місячний фонд робочого часу складає 640 годин. Річний – 7680 годин. Час простою внаслідок атаки 4 години:

$$П_п = (40300/640)*4 = 251,87 \text{ грн}$$

Витрати на відновлення працездатності системи включають кілька складових:

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

$П_{пв}$ – витрати на відновлення системи, грн;

$П_{зч}$ – вартість заміни частин системи, грн.

Витрати на повторне введення інформації розраховуються виходячи з розміру заробітної плати співробітників системи $З_с$, які зайняті

повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$ = 8 год:

$$П_{ви} = (40300/640)*8 = 503,75 \text{ грн}$$

Витрати на відновлення системи визначаються часом відновлення після атаки tв = 4 год і розміром середньогодинної заробітної плати адміністратора:

$$П_{пв} = (8500/640)*4 = 53,12 \text{ грн}$$

Витрати на відновлення працездатності системи:

$$П_{в} = П_{ви} + П_{пв} + П_{зч} = 503,75 + 53,12 + 3400 = 3956,87 \text{ грн}$$

Пзч = 3400 грн

О = 2100000 грн - обсяг чистого прибутку за рік.

Втрати від зниження працездатності атакованої системи:

$$V = О/1920 * (4+8+4) = 2100000/1920 * 16 = 17500 \text{ грн}$$

Таким чином, загальний збиток від атаки на ІТС підприємства при реалізації загрози складе:

$$U=П_п + П_в + V = 251,87 + 3956,87 + 17500 = 21708,74 \text{ грн.}$$

Таким чином, загальний збиток від атак на вузол або сегмент корпоративної мережіорганізації складе

$$B= \sum_i \sum_n U= 21708,74*12*1= 260504,88$$

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням B – загального збитку від атаки;R – очікуваної ймовірності атаки на систему;C – щорічних витрат на експлуатацію системи інформаційної безпеки.

Ймовірність R (0…1). Якщо реалізація загроз наймовірніша 1 раз на 3 місяці, тобто 4 рази на рік, то R=0,25. Загальний ефект від впровадження політики безпеки:

$$E = B \cdot R – C= 260504,88 * 0,25 –26478,96 = 103773,48 \text{грн.}$$

Визначення та аналіз показників економічної ефективності системи інформаційної безпеки:

Оцінка економічної ефективності системи захисту інформації, розглянутої у спеціальній частині дипломного проекту, здійснюється на основі визначення та аналізу наступних показників:

а) коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI (Return on Investment for Security);

б) термін окупності капітальних інвестицій То.

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

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

Коефіцієнт ROSI розраховують за допомогою показників:

Е – загальний ефект від впровадження системи інформаційної безпеки тис. грн;

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

$$ROSI = 103773,78 / 26478,96 = 3,9$$

Термін окупності капітальних інвестицій показує, за скільки років інвестиції окупляться за рахунок загального ефекту від впровадження КСЗІ.

$$T_o = 1 / 3,9 = 0,3 \text{ років.} = 4 \text{ місяці.}$$

Висновки до розділу 3

Розробка і впровадження системи виявлення вторгнень для ПП «Охорона Сервіс» є економічно доцільним, так як витрати на її створення значно менші за суму збитків, завдяки не дорогій системи та мінімальній вартості комплектуючих необхідних для відновлення системи та її інформаційних ресурсів у разі успішних атак порушників.

При цьому маємо, що:

- Капітальні витрати на впровадження інформаційної політики безпеки становлять 13322 грн;
- Експлуатаційні витрати на впровадження інформаційної політики безпеки становлять 26478,96 грн.;
- Загальний збиток від атаки на вузол складає 260504,88грн.
- Ефект від впровадження системи інформаційної безпеки становить 103773,48грн;
- Термін окупності капітальних інвестицій складає 4 місяці.

Отже, економічна доцільність обґрунтована і впровадження інформаційної політики безпеки може бути ефективною та успішною.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи розглянуто суттєві загрози та стан злочинів в сфері інформаційної безпеки та статистика скоєних атак за І кварталі 2019 року в Україні. Виявлено значне збільшення інцидентів порушення інформаційної безпеки на території України. Зазначена актуальність розвитку кібербезпеки. Обґрунтовано потребу у створенні КСЗІ на підприємстві для запобігання НСД до важливих ресурсів системи. До етапів створення КСЗІ, що використані в роботі віднесені, відповідно до нормативної документації: обґрунтування необхідності створення, обстеження на ОІД, аналіз та оцінка інформаційних ризиків та розробка політики безпеки, що враховує загрози найвищого рівня. В результаті проведеного обстеження ОІД побудовано модель загроз, що діють на дану ІТС, було класифіковано інформацію, що зберігається і циркулює на підприємстві та виявлено ресурси, які потребують найбільшого рівня інформаційної безпеки. Получені результати були використані для розробки політики безпеки на підприємстві «Охорона Сервіс». Інформація, що наведена при виконанні кваліфікаційної роботи була частково змінена на вимогу керівника компанії.

ПЕРЕЛІК ПОСИЛАНЬ

1 Данні компанії Positive technologies [Електронний ресурс] – Режим доступу до ресурсу: https://www.ptsecurity.com/ru/research/analytics/cybersecurity-threatscape-q1-2019/#id3 ;

2 Закон України "Про інформацію" [Електронний ресурс]. – 101. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2657-12;

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

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

5 ДСТУ 3396.1-96 - Технічний захист інформації. Порядок проведення робіт; [Електронний ресурс] – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38911&cat_id=38836;

6 НД ТЗІ 1.1-005-07 - Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення; [Електронний ресурс] – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=102310&cat_id=46556&ctime=1344511142755;

7 НД ТЗІ 1.1-002-99 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806 - Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу [Електронний ресурс] – Режим доступу до ресурсу: www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106340;

8 НД ТЗІ 1.4-001-00 - Типове положення про службу захисту інформації в АС; [Електронний ресурс] – Режим доступу до ресурсу: www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106341;
9 НД ТЗІ 1.1-003-99 - Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу; [Електронний ресурс]– Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=46074&cat_id=38835;
10 НД ТЗІ 2.5-004- Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу; [Електронний ресурс] – Режим доступу до ресурсу: dsszzi.gov.ua/dsszzi/doccatalog/document?id=106342;
11 НД ТЗІ 1.6-005-13 - Положення про категорювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці [Електронний ресурс] – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=107993&cat_id=89734&ctime=1366373635138;
12 НД ТЗІ 3.3-001-07 - Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації; [Електронний ресурс] – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=102265&cat_id=46556&ctime=1344504841243;
13 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: lib.univd.edu.ua/?controller=service&action;
14 НД ТЗІ 3.1-001-07 - Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи; [Електронний ресурс] – Режим доступу до

ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=102310&cat_id=46556&ctime=1344511142755;

15 НД ТЗІ 3.7-003 -05 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806 - Порядок проведення робіт із створення КСЗІ в ІТС; [Електронний ресурс] – Режим доступу до ресурсу: https://pda.litres.ru/vadim-grebennikov-15/kompleksni-sistemi-zahistu-informaciyi-proektuvannya/chitat-onlayn/page-2;

16 НД ТЗІ 3.7-001-99 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806 – Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі; [Електронний ресурс] – Режим доступу до ресурсу: www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106350;

17 Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 № 373; [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF;

18 Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 р. №1229; [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/1229/99;

19 ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» [Електронний ресурс] – Режим доступу до ресурсу: www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106343;

20 Проблеми та шляхи розвитку інформатизації в Україні [Електронний ресурс] – Режим доступу до ресурсу: https://studopedia.info/1-112574.html;

21 Вимоги до системи захисту інформації [Електронний ресурс] – Режим доступу до ресурсу: https://studfiles.net/preview/6012701/page:6/;

ДОДАТОК Б. Наказ на створення КСЗІ

Приватне підприємство «Охорона Сервіс»

НАКАЗ

«___»_____ Дніпро №_____

Про створення КСЗІ
у приватному підприємстві
«Охорона Сервіс»

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

НАКАЗУЮ:

1. Провести обстеження складових інформаційно-телекомунікаційної системи приватного підприємства «Оберіг Сервіс» (далі – підприємство).
2. Створити комплексну систему захисту інформації підприємства.
3. Затвердити політики безпеки інформації інформаційно-телекомунікаційних системи підприємства.
4. Відповідальність за виконання наказу покладаю на себе.

Директор підприємства _____ Поварнін В.В.