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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Мелещука Артема Андрійовича*

академічної групи *125-19-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка політики безпеки інформаційно-комунікаційної системи підприємства ТОВ "ПКФ "Мотор""*

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

Дніпро
2023

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту *Мелещуку Артему Андрійовичу* **академічної групи** *125-19-2*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Розробка політики безпеки інформаційно-комунікаційної системи підприємства ТОВ "ПКФ "Мотор""***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 16.05.2023 № 350-с

Розділ	Зміст	Термін виконання
Розділ 1	Провести обстеження об'єкта інформаційної діяльності ТОВ "ПКФ "Мотор""	29.03.2023
Розділ 2	Розробити модель загроз та модель порушника, визначити критерії захищеності ІКС підприємства, розробити заходи щодо захисту інформації на підприємстві. Виконати розробку політики безпеки	24.05.2023
Розділ 3	Провести економічне обґрунтування доцільності розробки політики безпеки ІКС підприємства ТОВ "ПКФ "Мотор""	09.06.2023

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі: 09.01.2023р.

Дата подання до екзаменаційної комісії: 09.06.2023р.

Прийнято до виконання _____ _____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: ___ с., ___ рис., __ табл., ___ додатка, ___ джерел.

Об’єкт досліджень: інформаційно-комунікаційна система підприємства ТОВ "ПКФ "Мотор"".

Предмет розробки: політика безпеки інформаційно-комунікаційної системи підприємства ТОВ "ПКФ "Мотор"".

Мета: розробка та впровадження політики безпеки інформаційно-комунікаційної системи підприємства ТОВ "ПКФ "Мотор"".

В першому розділі розглянуто стан питання щодо важливості захисту інформаційних ресурсів підприємства у сучасному цифровому світі. Приведені загальні відомості про компанію та розписана організаційна структура підприємства. Розписані план розташування та ситуаційний план підприємства.

В спеціальній частині розписані устаткування підприємства, інформаційні потоки, інформаційно-комунікаційна структура. Складено модель загроз та модель порушників. Розглянуті критерії захищеності та розроблено основні положення політики безпеки підприємства.

В економічному розділі виконано розрахунок капітальних та експлуатаційних витрат на впровадження політики безпеки.

Зміст кваліфікаційної роботи полягає у розробці політики безпеки для інформаційно-комунікаційної системи підприємства.

Практичне значення роботи полягає у підвищенні ефективності захисту інформаційно-комунікаційної системи підприємства, за рахунок розробки та впровадження більш ефективної політики безпеки підприємства.

ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ, ІНФОРМАЦІЙНІ ПОТОКИ, ІНФОРМАЦІЯ З ОБМЕЖЕНИМ ДОСТУПОМ, ІКС, ЗАГРОЗИ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, КРИТЕРІЇ ЗАХИЩЕНОСТІ, ПОЛІТИКА БЕЗПЕКИ

ABSTRACT

Explanatory note: ___ pp., ___ pic., ___ table, ___ app, ___ sources.

Object of research: the information and communication system of the enterprise "PKF Motor" LLC.

The subject of development: the security policy of the information and communication system of the enterprise "PKF Motor" LLC.

Purpose: development and implementation of the security policy of the information and communication system of the enterprise "PKF Motor" LLC.

In the first chapter, the status of the issue regarding the importance of protecting the company's information resources in the modern digital world is considered. General information about the company and the organizational structure of the enterprise are described. The location plan and situational plan of the enterprise are painted.

In a special part, the company's equipment, information flows, information and communication structure are described. A model of threats and a model of violators have been compiled. The security criteria were considered and the main provisions of the company's security policy were developed.

In the economic section, the calculation of capital and operating costs for the implementation of the security policy is performed.

The content of the qualification work consists in the development of a security policy for the information and communication system of the enterprise.

The practical significance of the work consists in increasing the effectiveness of the protection of the information and communication system of the enterprise, due to the development and implementation of a more effective security policy of the enterprise.

PROTECTION OF INFORMATION RESOURCES, INFORMATION FLOWS, INFORMATION WITH RESTRICTED ACCESS, ICS, THREATS, THREAT MODEL, VIOLATOR MODEL, SECURITY CRITERIA, SECURITY POLICY

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ДСТУ – державний стандарт України;

ДТЗС – другорядні технічні засоби та системи;

ОТЗС – основні технічні засоби і системи;

ІзОД – інформація з обмеженим доступом;

КВІ – канали витоку інформації;

НЧ – низькочастотний;

СЗІ – система захисту інформації;

ІКС – інформаційно-комунікаційна структура;

ТЗ – технічний засіб;

ТЗІ – технічний захист інформації;

ПЕМВН – побічні електромагнітні випромінювання та наведення ;

ПК – персональний комп'ютер;

ПП – приватне підприємство;

ПБЖ – пристрій безперервного живлення;

КТЗІ – комплекс технічного захисту інформації;

ЗМІСТ

ВСТУП

Захист інформації є невід'ємною складовою сучасного суспільства, особливо в контексті зростаючої кількості кіберзагроз та кримінальної діяльності, спрямованої на незаконне отримання конфіденційних даних. Україна не є винятком і зосереджує свої зусилля на захисті інформації від таких загроз.

Останні роки свідчать про перенесення кримінальних дій з отримання конфіденційної інформації в економічну сферу. В умовах ринкової економіки, де присутня різноманітність конкуруючих структур, ризик використання технічних пристроїв для розвідки в інформаційному полі стає надзвичайно значущим. Відтак, технічний захист інформації є невід'ємною складовою боротьби з цими загрозами.

У контексті інформаційної діяльності, де зберігання, обробка та передача інформації виконуються за допомогою різних технічних засобів, виникає реальна загроза витоку конфіденційної інформації. Процеси обробки даних в об'єктах інформаційної діяльності створюють умови для можливих технічних каналів витоку обмеженої інформації. Це вимагає впровадження комплексних систем технічного захисту інформації, спрямованих на запобігання таким витокам.

Запобігання витоку конфіденційної інформації має велике значення у світлі активної кримінальної діяльності, спрямованої на незаконне отримання таких даних, особливо в економічній сфері. Враховуючи швидкий розвиток новітніх технологій у галузі обробки та передачі даних, проблема технічного захисту інформації стає ще актуальнішою. Розробка та впровадження ефективних систем технічного захисту є нагальним завданням, яке вимагає негайних рішень.

Отже, тема технічного захисту інформації в Україні має велику актуальність і вимагає глибокого та спрямованого дослідження.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1. Стан питання

У сучасному цифровому світі, де компанії широко використовують інформаційно-комунікаційні системи (ІКС) для забезпечення своєї діяльності, захист інформаційних ресурсів стає необхідністю для успішного функціонування підприємств і збереження їх конкурентної переваги. Кібербезпека стає дедалі більш актуальною, оскільки зростає кількість загроз, пов'язаних із зловмисними діями у кіберпросторі, такими як хакерські атаки, витоки даних, шкідливі програми та інші небезпечні сценарії. З цієї причини підприємствам дедалі більше потрібно активно розробляти та впроваджувати політику безпеки ІКС, щоб ефективно протистояти цим загрозам.

Метою даної кваліфікаційної роботи є розробка комплексної політики безпеки інформаційно-комунікаційної системи підприємства з фокусом на захист конфіденційності, цілісності та доступності важливої інформації, яка обробляється та зберігається в системі. Розроблена політика безпеки включатиме комплекс заходів, таких як стратегії, правила, процедури та контрольні механізми, що спрямовані на забезпечення високого рівня захисту даних та ефективного управління ризиками, пов'язаними з інформаційною безпекою.

Стратегічний аспект розробки політики безпеки включатиме вивчення специфіки підприємства, аналіз існуючих ризиків, визначення цілей і задач, що стосуються безпеки, та розробку відповідних стратегічних підходів для досягнення цих цілей. Правила і процедури будуть встановлюватися з метою запобігання загрозам і реагування на них, а також для забезпечення виконання вимог щодо безпеки в ІКС підприємства. Контрольні заходи будуть включати системи моніторингу, аудит безпеки та заходи для забезпечення відповідності політики безпеки.

Результати цієї кваліфікаційної роботи матимуть велике значення для практичного впровадження політики безпеки ІКС в підприємствах. Розроблена політика безпеки буде слугувати цінним документом, який можна буде використовувати як основу для створення безпечних інформаційних систем у різних підприємствах. Вона сприятиме забезпеченню високого рівня захисту даних, збільшенню довіри з боку клієнтів і партнерів, а також запобіганню можливим загрозам та порушенням безпеки. Дана робота також може послугувати підставою для подальших наукових досліджень у галузі інформаційної безпеки та політики ІКС підприємств.

1.2. Загальні відомості про компанію

ТОВ "ПКФ "Мотор" є провідною компанією з багаторічним досвідом у галузі закупівлі та продажу електрообладнання, являючись дистриб'ютором продукції Legrand. Однак їх діяльність не обмежується лише цим напрямком. Крім продажу електрообладнання, компанія також займається електромонтажними роботами, монтажем водопровідних мереж, систем опалення та кондиціонування, а також виконує інші будівельно-монтажні роботи.

Заснована 30 листопада 1995 року, ТОВ "ПКФ "Мотор" є товариством з обмеженою відповідальністю зареєстрованою за адресою вулиця Квітуча, 48, місто Запоріжжя, Запорізька область, 69065. Для прийому клієнтів та проведення виставок обладнання компанія орендує сучасний салон за адресою Рельєфна вулиця, 8а, у місті Запоріжжя, Запорізька область, 69000.

Одна з головних переваг ТОВ "ПКФ "Мотор" полягає в широкому асортименті продукції, яку вони пропонують своїм клієнтам. Компанія постачає різноманітні якісні електротехнічні компоненти та обладнання від виробника Legrand. Це дозволяє компанії задовольняти потреби клієнтів у різних галузях і гарантує високу якість та надійність їх продукції.

Окрім високоякісної продукції, ТОВ "ПКФ "Мотор" може пишатися своїм досвідченим персоналом. Команда компанії складається з кваліфікованих фахівців, які мають глибокі знання в галузі електротехніки і багаторічний досвід роботи з різними видами електрообладнання. Це дозволяє їм надавати своїм клієнтам професійну консультацію та експертну підтримку при виборі оптимального обладнання.

1.3. Організаційна структура підприємства

Генеральний директор:

Управління підприємством: відповідає за загальне управління підприємством. Розробляє стратегічні плани та цілі, визначає напрямок розвитку компанії та приймає рішення, необхідні для досягнення успіху компанії.

Розробка стратегії: визначає стратегічні пріоритети компанії. Аналізує ринок електрообладнання, ідентифікує потенційні можливості та виклики, та розробляє плани дій, які допоможуть підприємству досягти конкурентної переваги.

Встановлення партнерських відносин: встановлює та підтримує стратегічні партнерства з постачальниками та клієнтами. Будує довірчі відносини із ключовими зацікавленими сторонами, проводить переговори та укладає угоди, які сприятливо впливають на діяльність компанії.

Управління персоналом: керує командою керівників та координує роботу різних відділів. Наймає та керує висококваліфікованими співробітниками, заохочує їх розвиток та забезпечує ефективне функціонування всієї організації.

Подання компанії: є офіційним представником підприємства та підтримує відносини із зовнішніми стейкхолдерами, такими як клієнти, постачальники, інвестори, урядові органи та громадськість. Бере участь у конференціях, виставках та інших заходах, представляючи інтереси компанії.

Фінансовий директор:

Фінансове планування та прогнозування: розробляє фінансові стратегії та плани, а також проводить аналіз та прогнозування фінансових показників підприємства. Визначає бюджети, встановлює фінансові цілі та забезпечує їх виконання.

Управління фінансовими ресурсами: відповідає за управління грошима та іншими фінансовими ресурсами компанії. Контролює потоки коштів, управляє інвестиціями та розподілом капіталу, а також займається фінансовим плануванням.

Фінансовий аналіз та звітність: здійснює фінансовий аналіз діяльності підприємства, включаючи оцінку фінансової продуктивності, рентабельності проектів та ефективності використання ресурсів. Складає фінансові звіти та надає аналітичну інформацію для прийняття управлінських рішень.

Управління бухгалтерією та оподаткування: відповідає за організацію та контроль бухгалтерського обліку підприємства, включаючи ведення фінансових записів, складання звітності та дотримання податкових вимог. Бере участь у податковому плануванні та забезпеченні дотримання податкового законодавства.

Фінансовий контроль та аудит: здійснює контроль за фінансовими операціями підприємства та забезпечує їх відповідність встановленим правилам та процедурам. Співпрацює з внутрішніми та зовнішніми аудиторами для перевірки та оцінки фінансових систем та процесів компанії.

Фінансове планування та залучення інвестицій: розробляє фінансові плани та стратегії, необхідні для забезпечення фінансової стабільності та зростання підприємства. Займається пошуком та залученням інвестицій, обговорює фінансові умови з інвесторами та бере участь у складанні інвестиційних пропозицій.

Управління фінансовими ризиками: ідентифікує та оцінює фінансові ризики, пов'язані з діяльністю підприємства, та розробляє стратегії та заходи щодо їх зниження чи управління. Він враховує фактори, такі як валютні

коливання, відсоткові ставки, інфляція та інші чинники, які можуть спричинити фінансову стабільність компанії.

Моніторинг ринку та конкуренції: відстежує зміни на ринку електрообладнання, аналізує дії конкурентів та прогнозує тенденції. Вживає заходів для адаптації компанії до змін у галузі та розробки конкурентних стратегій.

Менеджери з продажу:

Пошук клієнтів: активно шукають нових потенційних клієнтів, які потребують електроустаткування. Використовують різні методи, такі як дослідження ринку, реклама, участь у виставках та семінарах, щоб привернути увагу потенційних клієнтів.

Консультування клієнтів: консультують клієнтів щодо пропонованого електроустаткування. Пояснюють клієнтам переваги та можливості використання, а також технічні характеристики електроустаткування.

Підготовка та подання пропозицій: складають пропозиції та комерційні пропозиції для клієнтів. Розробляють детальні специфікації продуктів, ціни, умови постачання та інші комерційні умови, щоб надати клієнтам повну інформацію про електрообладнання.

Переговори та укладання угод: проводять переговори з клієнтами щодо ціни, умов постачання та інших аспектів угоди, щоб досягти взаємовигідної угоди та укласти успішну угоду.

Управління клієнтськими відносинами: підтримують та розвивають відносини з клієнтами. Забезпечують своєчасне обслуговування клієнтів, відповідають на їхні запитання та запити, вирішують проблеми та прагнуть задовольнити потреби клієнтів.

Аналіз ринку та конкурентів: аналізують ринок електрообладнання та стежать за діями конкурентів. Вивчають попит та тенденції ринку, аналізують конкурентні переваги та розробляють стратегії для збільшення частки ринку та залучення нових клієнтів.

Складання звітів: готують звіти про продажі, прогнозують та аналізують показники продажів, обговорюють їх з керівництвом підприємства та пропонують заходи щодо покращення результатів продажів.

Офіс-менеджери:

Обробка замовлень: приймають та обробляють замовлення.

Координація доставки: працюють із відділом логістики, щоб організувати доставку електрообладнання клієнтам. Вони стежать за термінами доставки, вирішують проблеми, що виникають, і координують процес доставки.

Комунікація з клієнтами: підтримують зв'язок з клієнтами, відповідають на їх питання, надають інформацію про наявність товару, ціни, терміни поставки та інші важливі питання. Вони також вирішують проблеми, що виникають, і допомагають задовольнити потреби клієнтів.

Підготовка документації: займаються складанням та підготовкою різних документів, таких як рахунки-фактури, видаткові накладні та інші необхідні документи в рамках продажу та обслуговування клієнтів.

Керування базою даних: відстежують та оновлюють базу даних клієнтів, включаючи контактні дані, історію замовлень та іншу важливу інформацію. Це допомагає їм у ефективної організації роботи з клієнтами та забезпечення своєчасного обслуговування.

Бухгалтери:

Ведення бухгалтерії: відповідають за запис та облік фінансових операцій підприємства, таких як покупки електроустаткування, продажу, оплати постачальникам, зарплати та інші витрати. Стежать за точністю та повнотою фінансових даних.

Складання фінансової звітності: готують фінансові звіти, включаючи баланс, звіт про прибутки та збитки, звіт про рух коштів та інші звіти, що надають інформацію про фінансове становище підприємства.

Податкове планування та звітність: займаються податковим плануванням та забезпечують дотримання податкових вимог. Готують

податкові декларації, розрахунки податків та пов'язану документацію для подання до податкових органів.

Управління розрахунками та рахунками: відстежують та контролюють платежі постачальникам та взаєморозрахунки з клієнтами. Підтримують точність та своєчасність розрахунків, а також забезпечують дотримання умов договорів.

Проектанти:

Дослідження та аналіз вимог клієнтів: взаємодіють з клієнтами та отримують інформацію про їх потреби та вимоги до електроустаткування. Аналізують ці вимоги та визначають оптимальні рішення для задоволення клієнтських запитів.

Проектування електротехнічних систем: розробляють електротехнічні проекти, що включають схеми електроживлення, розподільні панелі, схеми електрообладнання та інші аспекти системи.

Створення технічної документації: готують технічну документацію, включаючи креслення, схеми, специфікації та інші необхідні матеріали для виготовлення, встановлення та підключення електроустаткування.

Вирішення технічних проблем: у разі виникнення технічних проблем чи невідповідностей у проекті, проектанти аналізують їх та пропонують відповідні рішення та модифікації проекту.

Прибиральниця офісу:

Прибирання приміщень: головний обов'язок полягає у підтримці чистоти та порядку у всіх приміщеннях підприємства. Це включає прибирання підлоги, пилососіння килимових покриттів, протирання поверхонь, очищення скла, санітарні роботи в туалетах та ванній кімнаті, а також видалення сміття та його винесення.

Догляд за санітарними приміщеннями: відповідає за підтримання чистоти та гігієни у санітарних приміщеннях. Вона забезпечує наявність необхідних засобів гігієни, таких як мило, паперові рушники та туалетний

папір. Також вона здійснює очищення унітазів, раковин та інших поверхонь, а також дезінфікує та дезодорує санітарні приміщення.

Прибирання загальних зон: прибиральниця також відповідає за збирання загальних зон, таких як холи, приймальні пункти, сходи та коридори. Вона видаляє пил, миє та дезінфікує поверхні, витирає меблі, підтримує порядок у цих областях.

Замовлення та догляд за збиральними матеріалами: стежить за наявністю необхідних збиральних матеріалів, таких як миючі засоби, ганчірки, цебра та мішки для сміття. Вона може бути відповідальною за замовлення та закупівлю цих матеріалів, а також за їх правильне використання та зберігання.

1.4. План розташування

Розробка політики безпеки інформаційно-комунікаційної системи підприємства є важливим завданням, що вимагає комплексного підходу та уваги до деталей. Одним із ключових аспектів забезпечення безпеки є відповідне розташування приміщень у салоні підприємства. З метою забезпечення ефективного функціонування та захисту інформації, яка обробляється в системі, було розроблено план розташування, який враховує не лише практичні аспекти, але й безпекові вимоги.

Кожен приміщення в салоні підприємства має свою функціональну роль і специфіку, і враховується при розташуванні. Наприклад, хол з ресепшном і виставковою залою створює перший враження про підприємство, а шоу-рум з розумним будинком, яка виконує роль і переговорної, демонструє можливості та інноваційні рішення. Офіс з кабінетами, включаючи кабінет фінансового директора, кабінет бухгалтерії, кабінет проектантів та кабінет вентиляційників, створюють комфортні умови для виконання роботи і забезпечують відповідну приватність.

Приміщення, які мають пряме відношення до інформаційно-комунікаційної системи, такі як серверна, також враховуються в плані

розташування. Важливо забезпечити їх безпеку та доступність для технічного обслуговування.

Системи водопостачання, опалення та вентиляції грають важливу роль у забезпеченні комфорту приміщень та оптимальних умов роботи. Централізовані системи дозволяють забезпечити надійну і безперебійну роботу, а також забезпечують економію ресурсів.

Загальний план розташування в салоні підприємства побудований з урахуванням не лише естетичних та функціональних аспектів, але й вимог безпеки і захисту інформації. Це створює надійне середовище для роботи, де інформація захищена, а співробітники можуть ефективно працювати з інформаційною системою підприємства.

Хол з ресепшном і виставковою залою:

- Площа холу і виставкової зали: 80 кв. м.
- Висота стелі: 3,5 м.
- Вхідні двері: металопластикові двері.
- Матеріали стін і стінних перегородок: використовується гіпсокартон або сучасні декоративні панелі.
- Вікна: два великі пластикові вікна для природного освітлення.

Шоу-рум з розумним будинком та фурнітурою/переговорна:

- Площа шоу-руму: 40 кв. м.
- Висота стелі: 3,5 м.
- Двері: дерев'яні двері.
- Вікна: відсутні для забезпечення приватності клієнтів.
- Матеріали стін і стінних перегородок: гіпсокартон з шумоізоляцією під дерев'яними панелями для створення елегантного середовища.

Офіс з кабінетами:

Офіс:

- Площа офісу: 24 кв. м.
- Висота стелі: 3,5 м.
- Площа з'єднуючого коридору: 60 кв. м.

Кабінет фінансового директора:

- Площа: 6 кв. м.
- Двері: металеві двері.

Кабінет бухгалтерії:

- Площа: 6 кв. м.
- Двері: дерев'яні двері.

Кабінет проектантів:

- Площа: 12 кв. м.
- Двері: дерев'яні двері.

Кабінет вентиляційників:

- Площа: 6 кв. м.
- Двері: дерев'яні двері.

Серверна:

- Площа: 6 кв. м.
- Двері: металеві двері.

Кухня:

- Площа кухні: 6 кв. м.
- Висота стелі: 3,5 м.
- Двері: дерев'яні двері.
-

Санвузол:

- Площа санвузла: 2 кв. м.
- Висота стелі: 3,5 м.
- Двері: дерев'яні двері.

Складські приміщення:

Чотири складські приміщення для товарів.

Кожне приміщення має площу 15 кв. м.

- Двері: металеві ролетні ворота для зручного завантаження та розвантаження товарів.

Майстерня:

- Площа майстерні: 8 кв. м.
- Висота стелі: 3,5 м.
- Двері: металеві двері для забезпечення безпеки та приватності.

Будівельні параметри:

- Зовнішні стіни: матеріал - цегла, товщина - 30 см.
- Стінні перегородки: матеріал - гіпсокартон, товщина - 10 см.

Системи:

- Водопостачання: централізована система з підведенням холодної та гарячої води до всіх необхідних зон.
- Опалення: система централізованого опалення з радіаторами у всіх приміщеннях.
- Вентиляція: централізована система вентиляції для забезпечення оптимальної циркуляції повітря.

1.5. Ситуаційний план

Розробка політики безпеки інформаційно-комунікаційної системи підприємства передбачає комплексний підхід до забезпечення безпеки як усередині, так і навколо салону підприємства. Важливо не лише забезпечити захист інформаційних ресурсів внутрішньої системи, але й створити безпечне і комфортне середовище для клієнтів та співробітників.

Перед салоном підприємства розташована парковка, яка забезпечує зручний доступ та зручне розміщення автотранспорту. Це дозволяє забезпечити зручність для клієнтів та співробітників, а також дотримуватись принципів безпеки та організації простору.

Зовнішнє освітлення відіграє важливу роль у створенні безпечної та зручної атмосфери. Відповідно розміщені лампи та освітлювальні прилади забезпечують належну видимість під час ночі та зменшують ризик нещасних випадків.

Системи безпеки, такі як камери спостереження та система сигналізації, є необхідними складовими елементами для забезпечення безпеки інформаційно-комунікаційної системи підприємства. Камери спостереження допомагають відслідковувати події та реагувати на можливі загрози, а система сигналізації попереджає про неповноважний доступ та потенційні небезпеки.

Вхід до салону підприємства організований з урахуванням безпеки та доступності. Наявність сходів з пандусом забезпечує зручний доступ для людей з обмеженими фізичними можливостями та допомагає забезпечити безпеку під час входу до приміщення.

Усі ці складові елементи перед салоном підприємства відіграють важливу роль у створенні безпечного та комфортного середовища для клієнтів та співробітників. Розробка політики безпеки інформаційно-комунікаційної системи підприємства передбачає врахування всіх цих аспектів з метою забезпечення захисту інформації, безпеки працівників та задоволення потреб клієнтів.

Парковка:

- парковка розташована перед входом до салону компанії, що забезпечує легкість припаркування та зручний доступ до входу.

Освітлення:

- зовнішнє освітлення виконане у вигляді настінних ламп, розміщених поруч з вхідними дверима.

Системи безпеки:

- камери спостереження розміщені у стратегічних місцях, щоб забезпечити відстеження подій у вхідній зоні.

- система сигналізації забезпечує захист приміщення та збереження майна.

Вхід:

- сходи з пандусом розташовані поруч з вхідними дверима та надають можливість безперешкодного проходження навіть для людей з обмеженими фізичними можливостями.

1.6. Висновок

У цьому розділі було розглянуто важливе питання захисту інформаційних ресурсів у сучасному цифровому світі і показано, що розробка комплексної політики безпеки інформаційно-комунікаційної системи є надзвичайно важливим завданням для підприємства.

Були надані загальні відомості про компанію та організаційну структуру підприємства, що дозволило отримати розуміння про його функціонування. Також був розписаний план розташування та ситуаційний план підприємства, що сприяє забезпеченню ефективного управління та виявленню потенційних загроз для безпеки інформаційних ресурсів.

Зазначена інформація підкреслює необхідність ретельного вивчення, розробки та впровадження політики безпеки інформаційно-комунікаційної системи підприємства. Це є важливим кроком для забезпечення надійності, конфіденційності та доступності інформації, а також запобігання можливим загрозам та кібератакам. Розробка комплексної політики безпеки є стратегічною задачею, що допоможе забезпечити успішну та безпечну діяльність підприємства в динамічному інформаційному середовищі.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1. Устаткування

В устаткуванні компанії використовуються різні типи персональних комп'ютерів та операційних систем для відповідних робочих завдань.

В основі робочої системи використовується програмне забезпечення БЕСТ ЗВІТ для автоматизації бізнес-процесів. Це інтегрована система управління, яка дозволяє підприємству ефективно керувати фінансами, бухгалтерією, управлінням кадрами, логістикою, продажами та іншими аспектами діяльності.

БЕСТ ЗВІТ надає можливість вести облік та аналіз фінансових операцій, контролювати запаси, планувати та відстежувати виконання замовлень, керувати процесами управління персоналом та багато іншого. Вона дозволяє зменшити ручне введення даних, покращити точність та швидкість обробки інформації, спростити процеси роботи та забезпечити надійність даних.

Серверний ПК TOWER PowerUp #30 з операційною системою Windows Server 2019 використовується для обробки та зберігання даних БЕСТ ЗВІТ. Він забезпечує безперебійну роботу програми, маючи потужний процесор Xeon E5 2680 v3, 64 ГБ оперативної пам'яті та два жорсткі диски по 1 ТБ в режимі RAID.

БЕСТ ЗВІТ інтегрується з робочими станціями та ноутбуками, які використовуються співробітниками. Ноутбуки ASUS X515EA-BQ1185 з операційною системою Xubuntu 22.10 «Kinetic Kudu» надають стабільну та безпечну робочу платформу з розширеними можливостями налаштування та підтримкою відкритого програмного забезпечення.

Дизайнери використовують робочі станції Artline WorkStation W99v21 з операційною системою Windows 11 Pro. Ці робочі станції мають потужні процесори, велику кількість оперативної пам'яті та високопродуктивні графічні картки для обробки великих обсягів графічного контенту.

Операційна система Windows 11 Pro забезпечує дизайнерам зручну та сучасну робочу середу з доступом до необхідного програмного забезпечення та інструментів.

Для забезпечення надійного та швидкого інтернет-з'єднання використовуються два провідних оптоволоконних інтернет-підключення від різних провайдерів. Основне підключення з Вега Gigabit TV Pro надає швидкісне підключення до інтернету з високою пропускною здатністю. Резервне підключення забезпечується від провайдера Воля за допомогою пакету інтернет 100. Ця конфігурація дозволяє забезпечити безперебійний доступ до інтернету у випадку, якщо одне з підключень вийде з ладу або буде недоступним. Основне підключення забезпечує швидкий та стабільний доступ до інтернету під час повсякденної роботи, тоді як резервне підключення використовується у випадку неполадок з основним постачальником або для забезпечення додаткової надійності.

Технічні характеристики робочих ПК

Сервер

TOWER PowerUp #30 Xeon E5 2680 v3 x2/64 GB/HDD 1 TB x2 Raid/Int Video

Процесор: Xeon E5 2680 v3

Кількість процесорів: 2

Система охолодження: ID Cooling 120мм

Відеокарта: int Video

Материнська плата: Asus, Supermicro Dual s2011-3

Оперативна пам'ять: DDR4 ECC 64 GB

HDD: HDD 1 TB x2 RAID

Сокет: 2011-3

Операційна система: Windows Server 2019

Монітор 27" Samsung C27R500F

Діагональ дисплея: 27"

Тип матриці: VA

Пристрій безперервного живлення

KEOP C 3000

Номінальна потужність: 3 кВА/2,4 кВт

Час роботи: 2 години 16 хвилин

Налаштування входу: однофазний

Налаштування виходу: однофазний

Номінальна вхідна напруга: 230 В (1 фаза + нейтраль)

Номінальна вихідна напруга: 230 В (1 фаза + нейтраль)

Потужність, що використовується для оцінки часу резервного живлення: 0,7 кВт (70% необхідної потужності)

ПК співробітників

ASUS X515EA-BQ1185

Процесор: Intel Core i5-1135G7 (2.4-4.2 ГГц)

Кількість ядер: 4 ядра

Оперативна пам'ять: 8 ГБ

Тип оперативної пам'яті: DDR4

Тип відеокарти: Інтегрована

Відеокарта: Intel UHD Graphics

Тип накопичувача: SSD

Накопичувач: SSD 512 ГБ

Акумуляторна батарея: 2-осередкова

Місткість акумулятора, Вт год: 37

Операційна система: Xubuntu 22.10 «Kinetic Kudu»

ПК дизайнерів

Робоча станція Artline WorkStation W99v21

Процесор: Intel 10-Core i9-10900X 3.7-4.5GHz;

Відеокарта: Quadro RTX 5000 16GB;

Оперативна пам'ять: 64GB DDR4-2666 Gaming;

Об'єм накопичувача: 500GB M.2 NVMe SSD;

Об'єм другого накопичувача: 4TB;

Материнська плата: TUF X299 MARK 2;

Блок живлення: 650W 80+ Gold;

Охолодження процесора: be quiet! Dark Rock 3;

Операційна система: Windows 11 Pro

Монітор 32" Samsung LS32BG700

Діагональ дисплея: 32"

Тип матриці: IPS

2.2. Інформаційні потоки

Види інформації у підприємстві:

ВІДКРИТА:

- Інформація про продукти та послуги: технічні специфікації, опис продуктів, характеристики, ціни та умови продажу, гарантійні терміни.

- Інформація про виробників: торгові марки, країна реєстрації торгової марки, країна виробництва продукції.

З ОБМЕЖЕНИМ ДОСТУПОМ:

- Інформація про постачальників: контактні дані, сертифікати відповідності, а також умови та строки постачання.

- Інформація про ринок та конкурентні умови: інформація про конкурентні пропозиції, ціни та вимоги клієнтів.

- Інформація про клієнтів: дані про потреби клієнтів, їх переваги, історію замовлень, контактну інформацію, умови продажу, розмір знижок, умови поставки, умови оплати.

- Фінансова інформація: дані про доходи, витрати, бюджет, інвестиції та фінансові показники.

- Юридична інформація: уставні документи компанії, договори з постачальниками продукції та інші юридичні документи.

- Логістична інформація: дані про складський облік, інвентаризацію, доставку, шляхи та терміни поставки, відвантаження, упаковку та митні процедури.

Таблиця 1. Види інформації в підприємстві

Вид інформації	Рівень доступу	Місце зберігання	Вид зберігання	Доступ до інформації (персонал)
Інформація про продукти та послуги	Відкрита	Торговий зал, сайт	Стенди зі зразками продукції, опис характеристик в буклетах, брошурах, каталогах	Весь персонал
Інформація про виробників	Відкрита	Торговий зал, сайт	Стенди зі зразками продукції, опис характеристик в буклетах, брошурах, каталогах	Весь персонал
Інформація про постачальників	З обмеженим доступом	База даних БЕСТ ЗВІТ	На сервері	Генеральний директор, фінансовий директор, бухгалтерія, логісти (менеджер по закупкам)
Інформація про ринок та конкурентні умови	З обмеженим доступом	Записи у менеджерів, котрі з цим працюють та у генерального директора	Паперовий	Генеральний директор, менеджери з продажу
Інформація про	З обмеженим	База даних	На сервері	Кожен менеджер має

клієнтів	доступом	БЕСТ ЗВІТ		повний доступ тільки до інформації о своїх клієнтів
Фінансова інформація	З обмеженим доступом	База даних БЕСТ ЗВІТ, в шафі для зберігання документацій в бухгалтерії	На сервері, рахунки та накладні у паперовому вигляді	Генеральний директор, фінансовий директор, бухгалтерія
Юридична інформація	З обмеженим доступом	Банківська комірка	Паперовий	Генеральний директор
Логістична інформація	З обмеженим доступом	База даних БЕСТ ЗВІТ, особисті записи	На сервері, паперовий	Генеральний директор, логісти (менеджер по закупкам)

2.3. Інформаційно-комунікаційна структура

Сучасні підприємства незалежно від свого розміру та галузі діяльності все більше спираються на ефективне використання інформаційних технологій для підтримки своєї роботи та забезпечення конкурентоспроможності. Одним з важливих елементів цієї інформаційної інфраструктури є інформаційно-комунікаційна структура підприємства (ІКС).

ІКС підприємства включає різноманітні компоненти та засоби, що дозволяють збирати, обробляти, зберігати та передавати інформацію всередині організації та зовні. Однією з важливих складових цієї структури є персональні комп'ютери (ПК), які використовуються різними функціональними підрозділами підприємства.

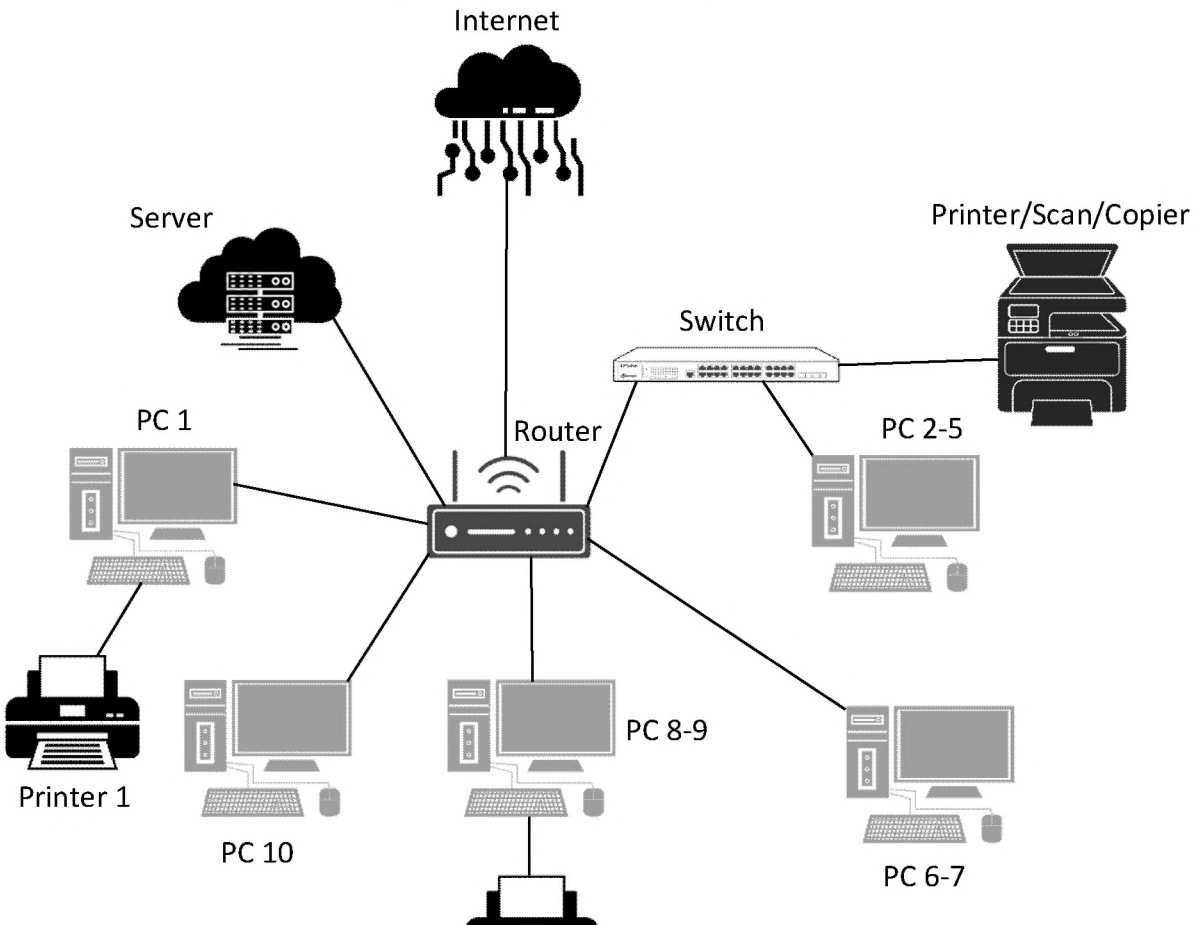
Фінансовий директор має свій власний ПК (PC 1), який дозволяє йому здійснювати фінансові операції підприємства. Цей комп'ютер підключений до мережі інтернет, що дозволяє директору здійснювати електронний

банкінг, спілкуватися з фінансовими установами та отримувати актуальну інформацію щодо фінансових показників.

Проектанти використовують ПК (PC 2-5) з встановленим спеціалізованим програмним забезпеченням для розробки різноманітних проектів для клієнтів, вентиляційники ж використовують свої ПК (PC 10) для розробки систем вентиляції. Ці комп'ютери також підключені до спільної мережі, що дозволяє спілкуватися та обмінюватися даними між колегами та іншими підрозділами підприємства.

Бухгалтерами ПК (PC 6-7) використовуються для забезпечення фінансового обліку та управління бухгалтерськими операціями. Ці комп'ютери мають встановлене спеціалізоване програмне забезпечення, що дозволяє бухгалтерам виконувати облік фінансових операцій, складати звіти, розраховувати податки та керувати фінансовими потоками підприємства.

У межах ІКС також наявні ПК менеджерів з продажу (PC 8-9), які використовуються для керування процесом продажу та ведення бази клієнтів. Ці комп'ютери дозволяють менеджерам здійснювати моніторинг замовлень, контролювати запаси та взаємодіяти з клієнтами шляхом використання електронної пошти або онлайн-комунікації. (Див. Рис. 1)



2.4. Модель загроз

Запобігання потенційним загрозам і забезпечення безпеки інформаційно-комунікаційної системи є однією з найважливіших задач підприємств, спеціалізуються в галузі закупівлі та продажу електрообладнання. Розуміння мотивів, кваліфікації та видів впливу загроз є вирішальним у формуванні ефективної політики безпеки, яка має на меті захистити інформацію підприємства від потенційних атак та негативних наслідків.

Мотиви загроз можуть походити з різних джерел. Конкуренти та інші компанії можуть бути зацікавлені в отриманні конфіденційної інформації про стратегію закупівель та продажу електрообладнання для здобуття конкурентної переваги. Зловмисники можуть намагатися отримати фінансову вигоду шляхом крадіжки фінансових даних або вимагання викупу. Також, атаки на систему можуть мати за мету порушення репутації підприємства шляхом розповсюдження негативної інформації або розкриття конфіденційних даних.

Розуміння видів впливу загроз також вкрай важливе. Несанкціонований доступ до інформації може призвести до втрати конфіденційних даних компанії, клієнтів або фінансових даних. Атаки на систему можуть вимагати значних зусиль і фінансових витрат для відновлення нормального функціонування та усунення наслідків. Крім того, порушення репутації підприємства може призвести до втрати довіри клієнтів і партнерів через розкриття конфіденційної інформації або інших репутаційних проблем.

2.5. Модель порушників

У рамках кваліфікаційної роботи модель порушників враховує специфіку галузі компанії, де електрообладнання використовується як основний продукт. При розробці політики безпеки важливо враховувати різні типи порушників, їх мотиви та методи, які можуть використовуватися для атак на інформаційно-комунікаційну систему. Серед таких порушників можуть бути конкуренти, які зацікавлені в отриманні конфіденційної інформації щодо стратегії закупівель та продажу, внутрішні зловмисники, співробітники компанії, що мають доступ до системи, а також зловмисники зовнішніх сторін, які можуть намагатися скористатися вразливостями системи.

Внутрішні порушники

Шахрайство з постачальниками

Шахрайство з постачальниками є однією з потенційних загроз безпеці інформаційно-комунікаційної системи підприємства. Воно виникає, коли співробітники підприємства укладають незаконні угоди з постачальниками або зловживають своїм статусом та повноваженнями для отримання неправомірних вигод.

Шахрайство з постачальниками може мати наступні аспекти:

Корупційні зв'язки: співробітники підприємства можуть намагатися встановити корупційні зв'язки з постачальниками, щоб отримати незаконні вигоди. Це може включати прийняття хабарів або отримання комісійних від постачальників у замін на укладання вигідних угод. Такі дії порушують принципи чесності та прозорості в бізнесі і можуть призвести до фінансових втрат для підприємства.

Невідповідність процедурам та політикам: співробітники можуть обходити внутрішні процедури та політики підприємства, що регулюють процес укладання угод з постачальниками. Вони можуть укладати угоди без необхідного контролю, проводити операції без дотримання встановлених

процедур або зловживати своїм статусом для отримання особистої вигоди. Це може призвести до порушення правил і збитків для підприємства.

Витік інформації: шахраї можуть використовувати свої зв'язки з постачальниками для отримання конфіденційної інформації про підприємство, його стратегію, цінову політику або інші конкурентні переваги. Ця інформація може використовуватися в шкідливих цілях, таких як конкурентне шпигунство, або може бути передана конкурентам, що призведе до втрати конкурентної переваги підприємства.

Підробка та маніпулювання даними: шахраї можуть впливати на процеси постачання та укладання угод, підробляючи документи, маніпулюючи даними або змінюючи умови угод. Це може призвести до некоректних угод, надмірного підвищення цін або постачання низькоякісних товарів чи послуг.

З метою запобігання шахрайству з постачальниками та забезпечення безпеки інформаційно-комунікаційної системи підприємства, необхідно вжити наступних заходів:

Розробка та впровадження політик та процедур: підприємство повинно розробити чіткі політики та процедури, що регулюють процеси постачання та укладання угод. Ці політики повинні визначати вимоги до перевірки постачальників, проведення конкурентних торгів, укладання угод та контролю за виконанням умов. Крім того, необхідно встановити процедури перевірки відповідності співробітників цим політикам та вжити заходів для запобігання обходу цих політик.

Контроль та перевірка: підприємство повинно встановити ефективну систему контролю та перевірки угод з постачальниками. Це може включати перевірку документації, проведення аудитів, виявлення несправностей та аномалій у процесах постачання. Контрольний механізм також повинен включати моніторинг фінансових операцій та аналіз звітності для виявлення підозрілих транзакцій.

Розкрадання електрообладнання

Крадіжка та розкрадання електрообладнання та його компонентів є серйозною загрозою безпеці інформаційно-комунікаційної системи підприємства. Це може призвести до втрати важливого обладнання, порушення роботи мережі і систем зв'язку, а також розголошення конфіденційної інформації, яка зберігається на обладнанні.

Для запобігання розкраданням, необхідно вжити наступні заходи:

Фізичний захист обладнання: підприємство повинно забезпечити адекватний фізичний захист обладнання, зокрема встановити системи контролю доступу, відеоспостереження та охоронні системи. Обладнання має бути захищено від несанкціонованого доступу шляхом встановлення замків, рейок, систем тривоги та інших заходів безпеки.

Ідентифікація та відстеження: кожен пристрій повинен бути чітко ідентифікований і відстежуваний. Це можна здійснити шляхом застосування унікальних маркувальних знаків, серійних номерів або інших методів ідентифікації. Детальний облік обладнання та його переміщень, а також система перевірки інвентаризації допоможуть виявити випадки зникнення обладнання та шахрайства.

Контроль доступу до приміщень: підприємство повинно встановити систему контролю доступу до приміщень, де знаходиться обладнання. Це включає електронні картки доступу, біометричні системи або інші методи ідентифікації, що обмежують доступ лише авторизованим працівникам. Крім того, слід встановити відповідні процедури контролю та моніторингу доступу працівників до обладнання.

Недотримання процедур та політик

Недотримання процедур та політик підприємства становить серйозну загрозу безпеці інформаційно-комунікаційної системи. Це може призвести до порушення конфіденційності, цілісності та доступності даних, а також

створити можливості для несанкціонованого доступу та викриття підприємства до ризиків.

Для запобігання недотриманню процедур та політик необхідно вжити наступні заходи:

Розробка чітких політик: підприємство повинно розробити документ, що містить чіткі політики та процедури безпеки інформаційно-комунікаційної системи. Цей документ повинен охоплювати всі аспекти безпеки, включаючи вимоги щодо паролів, керування доступом, обмеження привілеїв, збереження даних та процедури виявлення та реагування на інциденти.

Навчання та свідомість персоналу: всі співробітники повинні бути ознайомлені з політиками та процедурами безпеки, а також зрозуміти їх важливість. Навчання повинно проводитися регулярно, зокрема під час інтеграції нових співробітників та при оновленні політик і процедур. Розуміння персоналом ризиків та наслідків недотримання політик може допомогти запобігти порушенням.

Моніторинг та аудит: підприємство повинно встановити механізми моніторингу та аудиту для виявлення недотримання процедур. Це може включати системи журналювання, моніторинг мережі та систем, аудит контрольних дій та перевірку документації. Аналіз виявлених відхилень дозволить підприємству вжити необхідні заходи для усунення порушень та покращення безпеки системи.

Впровадження санкцій: політика безпеки повинна передбачати наслідки за недотримання процедур та політик. Це можуть бути дисциплінарні заходи, включаючи попередження, догану, призначення штрафних санкцій або навіть звільнення з роботи. Впровадження санкцій відіграє важливу роль у формуванні свідомої культури безпеки та стимулює співробітників дотримуватися політик та процедур.

Витік інформації

Витік інформації є серйозним порушенням безпеки інформаційно-комунікаційної системи підприємства, оскільки може призвести до негативних наслідків для бізнесу, зокрема до втрати конкурентної переваги, порушення довіри клієнтів та постачальників, а також правових проблем. Це може стосуватися розкриття конфіденційної інформації про клієнтські дані, внутрішні процеси, інновації, цінову політику, торговельні секрети та інші чутливі дані підприємства.

Для запобігання витоку інформації необхідно вжити наступні заходи:

Класифікація та маркування даних: Підприємство повинно провести оцінку ризиків та класифікувати дані залежно від їх конфіденційності та важливості. Потім ці дані повинні бути марковані, що дозволяє ідентифікувати конфіденційні дані та встановлювати контроль над їх рухом та доступом.

Керування доступом: Підприємство повинно встановити строгу систему керування доступом, щоб гарантувати, що співробітники отримують доступ лише до необхідної інформації для виконання своїх обов'язків. Це включає розподіл прав доступу, використання ідентифікаційних та аутентифікаційних механізмів, обмеження привілеїв та регулярне переглядання прав доступу.

Фізична безпека: Потрібно забезпечити фізичну безпеку приміщень, де зберігається чутлива інформація. Це включає обмеження доступу до серверних кімнат, використання систем відеоспостереження, захист приміщень від несанкціонованого доступу.

Саботаж та невиконання обов'язків

Саботаж та невиконання обов'язків співробітниками є серйозним порушенням безпеки інформаційно-комунікаційної системи підприємства, оскільки це може спричинити значні труднощі в роботі компанії, втрату даних, погіршення взаємодії з клієнтами та спостерігати втрату довіри до підприємства з боку партнерів та споживачів.

Детальніше розглянемо фактори, що можуть виникнути у зв'язку з саботажем та невиконанням обов'язків:

Невиконання завдань та термінів: Співробітники можуть свідомо не виконувати свої обов'язки або затримувати виконання завдань, що призводить до затримок у роботі, порушення графіків та незадоволення клієнтів. Це може мати серйозні наслідки для бізнесу, зокрема, втрату можливостей розширення та збитки у конкурентній боротьбі.

Спотворення інформації: Співробітники можуть намагатися спотворити інформацію або передавати її некоректно, що може призвести до появи помилок, неправильних рішень та загроз для безпеки даних. Наприклад, спотворення фінансової звітності або приховування проблем в роботі системи.

Ігнорування політик безпеки: Співробітники можуть свідомо ігнорувати встановлені політики безпеки, такі як вимоги до паролів, обмеження доступу до системи або використання шифрування. Це створює потенційні ризики для конфіденційності, цілісності та доступності даних.

Для запобігання саботажу та невиконанню обов'язків необхідно вжити наступні заходи:

Строгий контроль завдань та термінів: Установити систему контролю та моніторингу, яка відстежує виконання завдань та дотримання термінів. Періодичні огляди та звіти допоможуть виявити співробітників, які систематично не виконують свої обов'язки.

Освіта та навчання: Забезпечити навчання співробітників з питань етики, відповідальності та виконання обов'язків. Це може включати семінари, тренінги та інформаційні матеріали, які наголошують на важливості дотримання політик безпеки та наслідків невиконання обов'язків.

Аудит безпеки: Проводити регулярні аудити безпеки, які перевіряють дотримання політик, процедур та контрольних механізмів. Це допоможе виявити порушення та вжити відповідні заходи для їх усунення.

Зловживання повноваженнями

Зловживання повноваженнями є серйозним порушенням безпеки і може мати негативні наслідки для підприємства. Основні аспекти зловживання повноваженнями, які можуть виникнути, включають:

Дискримінація співробітників: Співробітники можуть використовувати свої повноваження для неправомірної дискримінації інших співробітників. Це може включати недоступність ресурсів, переваги або можливості, які надаються лише обраним особам на підставі особистих стосунків або неправедної обробки.

Неправомірна перевага клієнтів: Співробітники можуть надавати неправомірні переваги певним клієнтам, які порушують політику рівного обслуговування або конфіденційність інших клієнтів. Це може призводити до нерівності, недовіри і втрати довіри до підприємства.

Зловживання фінансових процесів: Співробітники, які мають доступ до фінансових процесів, можуть зловживати цими повноваженнями для особистої вигоди. Це може включати незаконні виплати, фальсифікацію фінансової звітності або використання підприємствених коштів для особистих цілей.

Для запобігання зловживанню повноваженнями необхідно вжити наступні заходи:

Розробка політики недопустимості зловживання повноваженнями: Визначити чіткі правила та процедури, що регулюють використання повноважень співробітниками. У цій політиці повинні бути визначені приклади зловживання повноважень та наслідки, які співробітникам можуть бути за це накладені.

Забезпечення прозорості та перевірок: Встановити механізми перевірок та аудиту, що дозволяють виявляти випадки зловживання повноваженнями. Це може включати використання систем моніторингу, аудиту фінансової звітності, регулярну перевірку діяльності співробітників тощо.

Навчання та свідомість: Забезпечити навчання співробітників щодо етичних стандартів, політик безпеки та наслідків зловживання повноваженнями. Проводити інформаційні кампанії та тренінги, спрямовані на формування свідомого ставлення до зловживання повноваженнями та його наслідків.

Запровадження механізмів звітності: Створити процедури, за допомогою яких співробітники можуть анонімно або конфіденційно повідомляти про випадки зловживання повноваженнями. Це може включати створення ліній довіри, електронних систем звітності або внутрішніх механізмів розгляду скарг та повідомлень.

Проведення розслідувань та застосування санкцій: Встановити процедури розслідування випадків зловживання повноваженнями та вжити необхідних заходів для усунення порушень. При виявленні зловживань повноважень, необхідно застосовувати відповідні санкції, які можуть включати дисциплінарні заходи, припинення трудового договору або правову відповідальність.

Моніторинг та вдосконалення: Проводити постійний моніторинг системи безпеки і виявлення порушень повноважень. Аналізувати випадки зловживань та вдосконалювати політику та процедури з метою запобігання подібним ситуаціям у майбутньому.

Зовнішні порушники

Постачальники з несумлінними практиками

Постачальники з несумлінними практиками є потенційними порушниками безпеки інформаційно-комунікаційної системи підприємства. їхні дії можуть створювати значні загрози для безпеки, надійності та стабільності системи. Для ефективного запобігання таким ситуаціям і зменшення ризиків, пов'язаних з постачальниками з несумлінними практиками, можна вжити наступні заходи:

Відбір та оцінка постачальників: Установити процедуру відбору та оцінки постачальників, яка включає перевірку їхньої репутації, сертифікатів відповідності, досвіду роботи та здатності виконувати вимоги безпеки. Також варто звернути увагу на наявність розгорнутої системи контролю якості у постачальників.

Укладення контрактів: Забезпечити укладення контрактів з постачальниками, в яких будуть враховані вимоги безпеки, стандарти якості та відповідні деталі щодо обліку та перевірки постачального обладнання. Контракт повинен включати механізми відшкодування збитків у разі невиконання постачальником встановлених вимог.

Аудит та моніторинг: Проводити регулярні аудити та моніторинг постачальників для перевірки дотримання вимог безпеки та якості. Це може включати перевірку їхніх виробничих процесів, дослідження відгуків клієнтів, аналіз технічних специфікацій та інші відповідні заходи.

Резервні постачальники: Розглянути можливість встановлення резервних постачальників, що забезпечать надійність постачання електроустаткування у випадку невиконання зобов'язань основним постачальником або виявлення несумлінних практик.

Співпраця зі стандартизаційними організаціями: Активно співпрацювати зі стандартизаційними організаціями, що встановлюють та контролюють вимоги безпеки та якості електрообладнання. Це дозволить підприємству бути в курсі останніх стандартів та рекомендацій, а також забезпечити співвідношення між постачальниками та вимогами цих організацій.

Перевірка отриманого обладнання: Здійснювати перевірку отриманого обладнання перед його використанням, щоб переконатися в його відповідності вимогам безпеки та якості. Це може включати тестування, перевірку сертифікатів, аналіз документації та проведення перевірок функціональності.

Система зворотного зв'язку: Забезпечити належну систему зворотного зв'язку з клієнтами та співробітниками, яка дасть можливість повідомляти про будь-які проблеми з постачальниками або спостережені несумлінні практики. Це дозволить оперативно реагувати та приймати відповідні заходи для запобігання можливим негативним наслідкам.

Клієнти з несумлінними намірами

Клієнти з несумлінними намірами є потенційними порушниками безпеки інформаційно-комунікаційної системи підприємства. Їх дії можуть призвести до фінансових втрат, порушення безпеки даних та загрози репутації підприємства. Для ефективного запобігання таким ситуаціям і зменшення ризиків, пов'язаних з клієнтами з несумлінними намірами, можна вжити наступні заходи:

Аутентифікація клієнтів: Встановити механізми аутентифікації клієнтів, що дозволять перевіряти їхню ідентичність перед наданням доступу до товарів або послуг. Це може включати вимогу доцільних даних для реєстрації, перевірку електронних підписів або використання двофакторної аутентифікації.

Моніторинг транзакцій: Здійснювати постійний моніторинг транзакцій клієнтів для виявлення незвичайних або підозрілих активностей. Використовуйте системи аналізу даних та машинного навчання для виявлення аномальних зразків інтеракцій клієнтів з системою.

Перевірка платежів: Встановити процедури перевірки платежів та підтвердження оплати перед наданням товарів або послуг. Використовуйте безпечні платіжні системи та інструменти для виявлення шахрайських та фальшивих платежів.

Захист особистих даних: Забезпечити високий рівень захисту особистих даних клієнтів, включаючи конфіденційну інформацію, платіжні дані та інші особисті дані. Використовуйте шифрування даних, застосовуйте

політику доступу до даних та забезпечуйте безпечну зберігання та обробку інформації.

Едукація клієнтів: Надавайте клієнтам інформацію про правила взаємодії з системою, процедури безпеки та обов'язки клієнтів. Це може включати надання інструкцій, вказівок та роз'яснень про потенційні загрози безпеці та шахрайські схеми.

Система зворотного зв'язку: Забезпечити механізми зворотного зв'язку, через які клієнти можуть повідомляти про підозрілі дії і поведінку інших клієнтів. Створіть процедури обробки скарг та швидкого реагування на повідомлення про можливі шахрайські дії.

Піратство та контрафактні товари

Піратство та контрафактні товари є серйозною загрозою безпеці інформаційно-комунікаційної системи підприємства. Це порушення може мати наслідки, такі як пошкодження обладнання, втрата даних, фінансові збитки та погіршення репутації підприємства. Для протидії піратству та контрафактним товарам необхідно вжити наступні заходи:

Впровадження системи контролю якості: Розробити та впровадити процеси контролю якості для впізнавання оригінального обладнання та продуктів, які використовуються в інформаційно-комунікаційній системі підприємства. Це може включати перевірку сертифікатів, маркування та ідентифікаційні коди.

Постачальники та партнери: Встановити процедури перевірки постачальників та партнерів з метою переконання в їхній легальності та дотриманні авторських прав. Заключати угоди тільки з надійними та ліцензованими постачальниками.

Співпраця з правоохоронними органами: Установити зв'язок з місцевими правоохоронними органами для обміну інформацією щодо

виявлення та припинення піратства та торгівлі контрафактними товарами. Активно співпрацювати зі службами безпеки для здійснення відповідних розслідувань.

Освітні програми та навчання: Проводити навчання для співробітників щодо розпізнавання піратства та контрафактних товарів. Ознайомлювати їх зі шкідливими наслідками використання неліцензійних продуктів та засобів, а також з правовими наслідками.

Моніторинг та реагування: Встановити механізми моніторингу ринку та інтернет-платформ для виявлення неліцензійних та контрафактних товарів, а також реагування на такі випадки. Негайно реагувати на виявлені порушення та звертатися до відповідних органів захисту авторських прав.

Правовий захист: Забезпечити, щоб у підприємства були належні правові захисти для своїх інтелектуальних прав. Заключати ліцензійні угоди, реєструвати відповідні патенти та авторські права, а також надавати повноваження правовим консультантам для захисту інтересів підприємства.

Кібератаки

Кібератаки є однією з найбільш актуальних загроз безпеці інформаційно-комунікаційної системи підприємства, особливо у сфері електрообладнання. Ці атаки можуть мати різні цілі, такі як крадіжка конфіденційної інформації, порушення безпеки систем, розповсюдження шкідливого програмного забезпечення та збурення нормального функціонування підприємства. Для захисту від кібератак необхідно вжити наступні заходи:

Встановлення міцних систем захисту: Забезпечити використання сучасних і надійних систем захисту, таких як брандмауери, антивірусне програмне забезпечення, системи виявлення вторгнень та шифрування даних. Регулярно оновлювати ці системи, щоб запобігти новим загрозам.

Проведення аудиту безпеки: Регулярно проводити аудит безпеки інформаційно-комунікаційної системи для виявлення потенційних слабких

місць та вразливостей. Заходити вчасно вносити необхідні зміни та покращення для запобігання кібератакам.

Навчання співробітників: Здійснювати регулярну освіту співробітників щодо кібербезпеки. Навчати їх розпізнавати підозрілі електронні повідомлення, використовувати складні паролі, бути уважними при роботі з веб-сайтами та не передавати конфіденційну інформацію без необхідності.

Резервне копіювання даних: Регулярно створювати резервні копії важливої інформації та зберігати їх в безпечному місці. Це дозволить відновити дані у разі успішної кібератаки або системного збою.

Моніторинг мережі: Проводити постійний моніторинг мережі для виявлення підозрілих активностей та незвичайного трафіку. Вчасно реагувати на можливі загрози і вживати заходів для їх запобігання.

Створення інцидентного реагування: Розробити план реагування на кібератаки, включаючи процедури інцидентного реагування, контактну інформацію експертів з кібербезпеки та спеціальні установки для відновлення системи.

2.6. Критерії захищеності

В сучасному цифровому світі, де інформація стала однією з найцінніших активів, безпека інформаційно-комунікаційних систем стає першочерговим завданням для будь-якого підприємства. Застосування ефективної політики безпеки є критично важливим для забезпечення конфіденційності, цілісності та доступності інформації.

Це особливо актуально для підприємств, які спеціалізуються у галузі закупівлі та продажу електрообладнання, таких як ТОВ "ПКФ "Мотор"". Враховуючи великий обсяг конфіденційної та важливої інформації, що обробляється цим підприємством, безпека інформаційної системи стає ключовим фактором успіху.

У рамках кваліфікаційної роботи "Розробка політики безпеки інформаційно-комунікаційної системи підприємства ТОВ "ПКФ "Мотор""

визначаються критерії захищеності, що сприятимуть створенню надійного і стійкого середовища для обробки інформації. Ці критерії включають в себе політику регулярного оновлення документів, механізми захисту від несанкціонованих змін, системи виявлення та реагування на інциденти, проведення навчань та тренінгів з питань кібербезпеки, а також залучення експертів з безпеки для надання консультацій та підтримки.

3.КЦД.1

КД-2. Базова довірча конфіденційність

Політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта

Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта

КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта

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

Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації. Як частина політики1,4 довірчої конфіденційності повинні бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту

НЕОБХІДНІ УМОВИ: НИ-1

КО-1. Повторне використання об'єктів

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

НЕОБХІДНІ УМОВИ: НЕМАЄ

КВ-1. Мінімальна конфіденційність при обміні

Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів і інтерфейсних процесів, до яких вона відноситься

Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуються, і спроможність користувачів і/або процесів керувати рівнем захищеності

КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається

НЕОБХІДНІ УМОВИ: НЕМАЄ

ЦД-1. Мінімальна довірча цілісність

Політика довірчої цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта

Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта

КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту

НЕОБХІДНІ УМОВИ: НИ-1

ЦО-1. Обмежений відкат

Політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься

Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу

НЕОБХІДНІ УМОВИ: НИ-1

ЦВ-1: Мінімальна цілісність при обміні

Політика цілісності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів КС і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовуваними механізмами, і спроможність користувачів і/або процесів керувати рівнем захищеності

КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається

НЕОБХІДНІ УМОВИ: НЕМАЄ

ДР-1. Квоти

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

Політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу

Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження

НЕОБХІДНІ УМОВИ: НО-1

ДВ-1. Ручне відновлення

Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов КС і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція КС

Після відмови КС або переривання обслуговування КЗЗ повинен перевести КС до стану, із якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження

Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути КС до нормального функціонування

НЕОБХІДНІ УМОВИ: НО-1

НР-2. Захищений журнал

Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються

КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки

Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події

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

НЕОБХІДНІ УМОВИ: НИ -1, НО – 1

НИ-2. Одиночна ідентифікація і автентифікація

Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ

Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен автентифікувати цього користувача з використанням захищеного механізму

КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування

НЕОБХІДНІ УМОВИ: НК-1

НК-1. Однонаправлений достовірний канал

Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ

Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем

НЕОБХІДНІ УМОВИ: НЕМАЄ

НО-2. Розподіл обов'язків адміністраторів

Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції

Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі

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

НЕОБХІДНІ УМОВИ: НИ-1

НЦ-2. КЗЗ з гарантованою цілісністю

Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів

КЗЗ повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування

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

НЕОБХІДНІ УМОВИ: НЕМАЄ

НТ-2. Самотестування при старті

Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ

КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження при ініціалізації КЗЗ

НЕОБХІДНІ УМОВИ: НО-1

НВ-1: Автентифікація вузла

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

НЕОБХІДНІ УМОВИ: НЕМАЄ

2.7. Політика безпеки

Інформація є одним з найцінніших активів у сучасному світі, особливо для компаній, що діють в галузі закупівлі та продажу електрообладнання, як наша компанія ТОВ "ПКФ "Мотор"". У світі, де технології розвиваються стрімкими темпами, ми розуміємо, що безпека наших інформаційних ресурсів є невід'ємною частиною нашої успішної діяльності і забезпечує довіру наших клієнтів та партнерів.

Ця політика безпеки ІКС розроблена з метою визначення наших стратегій та принципів забезпечення безпеки інформаційної системи. Ми прагнемо до створення надійного та безпечного середовища для обробки, передачі та зберігання інформації, що дозволить нам ефективно захищати наші цінності, включаючи конфіденційну інформацію клієнтів, партнерів та внутрішніх процесів підприємства.

Політика безпеки ІКС є чітким посібником для всіх співробітників компанії ТОВ "ПКФ "Мотор"", незалежно від їхніх посад чи ролей в організації. Кожен з нас має відповідальність за забезпечення безпеки інформаційних ресурсів та дотримання встановлених політик та процедур. Застосовуючи цю політику, ми забезпечимо неперервну захищеність наших інформаційних активів і зможемо ефективно відповідати на сучасні виклики та загрози інформаційної безпеки.

Загальні принципи безпеки:

Відповідальність за безпеку інформації на всіх рівнях організації:

Керівництво:

Керівництво підприємства має встановити чіткі лінії відповідальності за безпеку інформації. Це означає, що вони повинні визначити основні ролі та обов'язки в області інформаційної безпеки, призначити відповідальних осіб та встановити структуру управління безпекою.

Керівництво повинно забезпечити необхідні ресурси для ефективної реалізації політики безпеки, такі як фінансування, технічні засоби та персонал.

Вони мають забезпечити постійне підвищення освіти та свідомості щодо безпеки інформації серед усіх співробітників. Кожен співробітник повинен розуміти свої обов'язки щодо захисту інформації та бути свідомим важливості безпеки.

Менеджери та керівники підрозділів:

Менеджери та керівники підрозділів відповідають за впровадження та дотримання політики безпеки інформації у своїх підрозділах.

Вони повинні забезпечити, щоб співробітники розуміли свої обов'язки щодо захисту інформації та мали доступ до необхідних ресурсів для забезпечення безпеки.

Всі співробітники:

Кожен співробітник повинен розуміти важливість безпеки інформації та бути свідомим своїх обов'язків щодо захисту інформації.

Вони повинні дотримуватися політики безпеки інформації, включаючи використання безпечних паролів, обмеження доступу до конфіденційної інформації, усвідомлення ризиків використання електронної пошти та інших комунікаційних засобів.

Співробітники мають негайно повідомляти про будь-які потенційні загрози безпеці інформації або порушення безпекових правил.

Внутрішні аудитори:

Внутрішні аудитори відповідають за оцінку та перевірку ефективності політики безпеки інформації у всіх рівнях організації.

Вони мають здійснювати регулярні перевірки, аудити та оцінки ризиків забезпечення безпеки інформації та робити рекомендації щодо покращення.

Кожен працівник є важливим ланкою в забезпеченні безпеки інформації. Тільки через спільні зусилля всіх рівнів організації може бути досягнута ефективна захист інформації від потенційних загроз.

Встановлення процедур та політик для ідентифікації, класифікації та оцінки ризиків забезпечення інформаційної безпеки:

Розробка процедур і політик:

Організація повинна розробити процедури та політики, які визначають методи індентифікації, класифікації та оцінки ризиків інформаційної безпеки. Ці документи мають включати чіткі критерії та механізми для оцінки ризиків, виявлення потенційних загроз та вразливостей і визначення заходів для їх запобігання.

Оновлення процедур і політик:

Процедури і політики повинні підлягати регулярному оновленню для врахування нових загроз та вразливостей, що можуть виникнути внаслідок швидко змінюючогося інформаційного середовища. Оновлення можуть включати в себе ревізію методів оцінки ризиків, вдосконалення заходів безпеки та додавання нових політик і процедур.

Ідентифікація ризиків:

Процедури повинні передбачати методи індентифікації потенційних ризиків, які можуть загрожувати інформаційній безпеці. Це може включати аналіз зовнішніх загроз, таких як хакерські атаки або витоки інформації, а також внутрішніх загроз, наприклад, несанкціонований доступ до конфіденційної інформації.

Класифікація ризиків:

Процедури повинні включати методи класифікації ризиків забезпечення інформаційної безпеки на основі їх вагомості та ймовірності виникнення. Це допомагає організації визначити пріоритети в управлінні ризиками і прийнятті заходів безпеки.

Оцінка ризиків:

Процедури мають включати методи оцінки ризиків, що дозволяють організації оцінити наслідки потенційних загроз і визначити рівень ризику для інформаційної системи. Це допомагає виявити слабкі місця і прийняти належні заходи для запобігання або зменшення ризику.

Превентивні заходи:

Політика безпеки повинна передбачати застосування превентивних заходів для забезпечення безпеки інформаційної системи. Це може включати застосування технічних заходів, таких як захист мережі, шифрування даних, бекапи ізольованих систем, а також навчання персоналу з питань безпеки і встановлення політик безпеки щодо використання паролів та доступу до систем.

Встановлення процедур і політик для ідентифікації, класифікації та оцінки ризиків є важливим етапом в розробці політики безпеки підприємства. Це допомагає організації виявити потенційні загрози та вразливості, визначити рівень ризику та вжити необхідні заходи для забезпечення безпеки інформаційної системи.

Впровадження технічних, фізичних і організаційних заходів, що спрямовані на запобігання загрозам безпеці інформаційно-комунікаційної системи:

Встановлення заходів з захисту від несанкціонованого доступу, витоку інформації, вірусів та інших шкідливих програм:

Реалізація багаторівневої системи захисту, що включає застосування брандмауерів, систем виявлення вторгнень (IDS), систем управління доступом (ACS) та антивірусного програмного забезпечення.

Встановлення технічних засобів шифрування даних для захисту конфіденційної інформації, особливо при її передачі по мережі або зберіганні на зовнішніх носіях.

Регулярне оновлення та патчінг програмного забезпечення та операційних систем для запобігання використанню вразливостей зловмисниками.

Забезпечення належного управління доступом та ідентифікацією:

Встановлення політик і процедур для керування доступом до інформаційних ресурсів підприємства, включаючи використання сильних паролів, двофакторної аутентифікації та обмеження привілеїв користувачів.

Регулярне аудитування доступу до систем та ресурсів з метою виявлення несанкціонованого доступу або незвичайних активностей.

Використання ідентифікаційних технологій, таких як системи контролю доступу (ACS), біометричні системи або інші методи для перевірки ідентичності користувачів.

Фізична безпека:

Застосування фізичних заходів безпеки, таких як контроль доступу до приміщень, використання систем відеоспостереження, установка захисних бар'єрів (наприклад, замки, решітки, охоронні системи) для запобігання несанкціонованому доступу до приміщень, дата-центрів та інших важливих зон.

Організаційні заходи:

Проведення навчання та підвищення освітленості персоналу щодо питань безпеки, включаючи свідомості про загрози, процедури безпеки, виявлення фішингу та інші соціально інженерні атаки.

Розробка і впровадження політик безпеки, які охоплюють весь персонал, включаючи процедури повідомлення про інциденти, декларацію конфіденційності, політику використання IT-ресурсів та інші відповідні вимоги.

Встановлення системи моніторингу та аналізу безпеки для виявлення можливих загроз та подій безпеки.

Ці заходи спільно сприяють запобіганню загрозам безпеці інформаційно-комунікаційної системи, забезпечуючи технічний, фізичний та організаційний захист інформації та інфраструктури підприємства.

Встановлення процедур управління доступом, що обмежують доступ до інформаційної системи лише необхідним співробітникам і встановлюють права доступу на основі ролей і відповідальностей.

Використання механізмів ідентифікації та аутентифікації:

Встановлення політик безпеки, які вимагають від користувачів використовувати ідентифікатори та паролі для доступу до системи. Паролі повинні відповідати вимогам щодо складності і регулярно оновлюватися.

Застосування механізмів двофакторної автентифікації, які вимагають введення додаткового підтвердження, такого як одноразовий пароль, біометричні дані або фізичний токен, для забезпечення вищого рівня безпеки.

Визначення ролей і відповідальностей:

Аналіз і ідентифікація ролей, функцій і відповідальностей в організації, пов'язаних з доступом до інформаційної системи.

Встановлення системи керування ролями (Role-Based Access Control, RBAC), де права доступу призначаються на основі ролей, а не окремим користувачам. Це спрощує процес управління доступом і забезпечує консистентність в наданні прав доступу.

Політики управління доступом:

Розробка політик, що встановлюють принципи, обмеження та процедури для надання, зміни і припинення доступу до інформаційної системи.

Встановлення принципу найменшого привілею, де користувачі мають лише необхідні права доступу для виконання своїх робочих обов'язків.

Використання систем управління ідентифікацією та доступом (Identity and Access Management, IAM), що дозволяють централізовано керувати доступом до різних систем та ресурсів, автоматизувати процеси надання та скасування прав доступу.

Ці заходи спрямовані на забезпечення контролю та обмеження доступу до інформаційної системи лише авторизованим співробітникам, що мають необхідні права доступу відповідно до своїх ролей та відповідальностей. Вони забезпечують підвищений рівень безпеки та захисту інформації в організації.

Розробка та впровадження планів неперервності бізнесу, які включають процедури відновлення після інцидентів, резервне копіювання даних, а також резервування та відновлення систем.

Розробка планів неперервності бізнесу:

Ідентифікація критичних бізнес-процесів та систем, які необхідно відновити швидко після інциденту.

Аналіз ризиків та визначення потенційних загроз, що можуть вплинути на нормальне функціонування бізнесу.

Розробка планів відновлення, які включають процедури, ролі та відповідальності, необхідні для ефективного відновлення бізнес-процесів.

Резервне копіювання даних:

Визначення критичних даних, які потрібно регулярно резервувати.

Розробка процедур резервного копіювання, включаючи вибір методів, регулярність та зберігання резервних копій.

Забезпечення безпеки та конфіденційності резервних копій, наприклад, шифрування даних або зберігання в безпечних місцях.

Резервування та відновлення систем:

Розробка процедур резервування систем та налаштування автоматичного резервування для забезпечення наявності копій систем та конфігурацій.

Планування процедур відновлення систем після інциденту, включаючи встановлення пріоритетів, послідовності та контрольних точок для відновлення.

Регулярне проведення тестувань та тренувань планів відновлення, що дозволяє перевірити ефективність процедур та ідентифікувати можливі проблеми або недоліки.

Перевірки, тестування і тренування:

Проведення регулярних перевірок систем безпеки, резервного копіювання та відновлення, щоб переконатися у їхній ефективності та актуальності.

Планування та проведення тестувань системи у відновленні після інциденту для перевірки часу відновлення, виявлення потенційних проблем та вдосконалення процедур.

Організація тренувань для співробітників, що дозволяє їм ознайомитися з процедурами відновлення та набути навичок управління кризовими ситуаціями.

Ці заходи спрямовані на забезпечення неперервності бізнесу, швидкого відновлення після інцидентів та зменшення можливих збитків, а також забезпечення захисту інформації та надійності систем в організації.

Конфіденційність:

Встановлення контрольних механізмів доступу до інформації та документів, що містять конфіденційну інформацію.

Визначення типів даних, які містять конфіденційну інформацію та потребують шифрування для захисту:

Проведення аналізу даних, щоб визначити, які типи даних включають конфіденційну, особисту, комерційну або іншу чутливу інформацію.

Встановлення політик та стандартів щодо шифрування конфіденційних даних залежно від їх типу та рівня чутливості.

Використання сучасних шифрувальних алгоритмів та протоколів для шифрування даних в режимі передачі, зберігання та обробки:

Використання сильних шифрувальних алгоритмів, таких як Advanced Encryption Standard (AES) або Triple Data Encryption Standard (3DES), для захисту даних.

Застосування шифрування на різних рівнях, включаючи рівень файлової системи, рівень баз даних та рівень мережевої комунікації.

Установка політики обов'язкового шифрування для всіх важливих даних:

Визначення політики, яка передбачає обов'язкове застосування шифрування для всіх даних, що перебувають у системі, які містять конфіденційну інформацію.

Налаштування системи або додатків для автоматичного застосування шифрування до всіх важливих даних без необхідності вручну вибирати цей процес.

Застосування шифрування даних допомагає забезпечити конфіденційність інформації та запобігти несанкціонованому доступу до даних, які можуть бути скомпрометовані. Це важливий аспект безпеки інформаційної системи, який допомагає знизити ризик витоку чутливої інформації та зберегти її цілісність.

Заборона розголошення конфіденційної інформації третім особам без належних дозволів:

Встановлення чітких правил та політики щодо конфіденційності інформації, включаючи заборону розголошення даних третім особам.

Встановлення процедур контролю доступу до конфіденційної інформації та обмеження прав доступу до неї лише необхідним співробітникам або ролям.

Застосування механізмів ідентифікації та аутентифікації для перевірки прав доступу та ідентифікації користувачів, що дозволяє контролювати доступ до конфіденційної інформації.

Ці механізми контролю доступу до інформації та документів допомагають забезпечити конфіденційність та недоступність конфіденційної інформації для несанкціонованих осіб. Вони встановлюються як частина політики безпеки інформаційної системи підприємства та забезпечують захист важливих даних та інформації.

Цілісність:

Встановлення механізмів перевірки цілісності даних для виявлення та запобігання неправомірним змінам чи модифікаціям інформації.

Використання спеціалізованих систем контролю версій документів:

Встановлення системи контролю версій, яка дозволяє відстежувати зміни в документах та зберігати різні версії.

Внесення кожної зміни до документу у систему контролю версій, що дозволяє зберігати історію змін та переглядати попередні версії документу.

Установлення прав доступу до системи контролю версій:

Встановлення обмежень щодо доступу до системи контролю версій, що дозволяє змінювати документи лише авторизованим користувачам.

Надання різних рівнів доступу залежно від ролей та відповідальностей користувачів.

Встановлення процедур оцінки та затвердження змін:

Визначення процедур, які вимагають контрольоване оновлення та затвердження змін до документів.

Застосування механізмів перевірки та затвердження змін, щоб забезпечити, що кожна зміна проходить відповідну оцінку та авторизацію перед включенням до остаточної версії документу.

Застосування механізмів контролю версій документів дозволяє забезпечити систематичне та організоване керування змінами в документах. Це допомагає зберегти історію змін, відстежувати внесені модифікації та повертатися до попередніх версій, що забезпечує цілісність та надійність документів у процесі роботи.

Забезпечення актуальності документів та недоступності для несанкціонованих змін.

Установлення політики регулярного оновлення та перегляду документів:

Визначення політики, яка передбачає регулярне оновлення та перегляд документів, зокрема тих, що містять конфіденційну інформацію.

Встановлення конкретних термінів і процедур для оновлення та перегляду документів залежно від їх важливості, актуальності та критичності.

Встановлення процедур затвердження та контролю змін до документів:

Установлення процедур, які передбачають затвердження та контроль змін до документів перед їх внесенням.

Визначення відповідальних осіб або комітетів, які здійснюють перевірку, затвердження та контроль змін до документів.

Використання електронних систем управління документами для зберігання та відстеження змін до документів, включаючи історію змін та інформацію про авторство.

Застосування механізмів захисту документів від несанкціонованих змін:

Використання електронного підпису для підтвердження авторства та автентичності документів.

Застосування захисту від запису та змін у системі управління документами, що дозволяє обмежити доступ до документів лише

авторизованим користувачам та відстежувати всі зміни, внесені до документів.

Встановлення прав доступу до документів, що обмежують можливість внесення змін лише авторизованим користувачам з відповідними привілеями.

Доступність:

Забезпечення належного рівня доступності інформаційної системи для забезпечення працездатності бізнес-процесів.

Запобігання несанкціонованому блокуванню або перериванню доступу до системи:

Використання механізмів аутентифікації та авторизації, які перевіряють ідентифікацію користувачів та надають їм відповідні права доступу.

Встановлення заходів захисту від DDoS-атак та інших видів кібератак, таких як використання спеціалізованих пристроїв або послуг, що фільтрують шкідливий трафік.

Регулярне оновлення системи та застосунків з метою усунення вразливостей, що можуть бути використані для несанкціонованого доступу.

Забезпечення резервного копіювання та відновлення даних:

Розробка та впровадження планів резервного копіювання, які визначають частоту, методику та місце зберігання резервних копій даних.

Регулярна перевірка та тестування процесів відновлення даних, щоб переконатися у їх ефективності та надійності.

Застосування технологій реплікації даних або збереження даних у хмарних сервісах з метою забезпечення доступності та швидкого відновлення інформації після інцидентів.

Ці заходи дозволяють забезпечити належний рівень доступності інформаційної системи, уникнути несанкціонованого блокування або переривання доступу та забезпечити оперативне відновлення системи після інцидентів, що може мінімізувати вплив на бізнес-процеси підприємства.

Захист від кібератак:

Впровадження заходів для виявлення, запобігання та відповіді на кібератаки.

Використання спеціалізованих систем моніторингу та аналізу:

Установлення систем моніторингу, які постійно стежать за активністю в мережі, серверах, програмах та інших компонентах інформаційної системи.

Виявлення незвичайної або підозрілої активності, такої як невідомі підключення, спроби несанкціонованого доступу, аномальне використання ресурсів тощо.

Аналіз інформації, отриманої від систем моніторингу, для виявлення потенційних загроз та вразливостей.

Застосування систем інтрапревентивного виявлення загроз (Intrusion Detection System, IDS) та систем захисту від вторгнень (Intrusion Prevention System, IPS):

Встановлення систем IDS та IPS, які спрямовані на виявлення та реагування на небажані дії або атаки в реальному часі.

IDS виявляє підозрілу активність на основі підписів, аномалій або поведінкових шаблонів, відповідно до заздалегідь визначених правил.

IPS, крім виявлення, також активно блокує або обмежує небажану активність або атаки за допомогою автоматичних дій або реакцій на загрози.

Ці механізми дозволяють постійно моніторити інформаційну систему, виявляти потенційні загрози та вразливості, а також реагувати на них, забезпечуючи безпеку та недоступність для несанкціонованих дій або атак.

Налагодження системи виявлення та реагування на інциденти для швидкого виявлення, реагування та відновлення після атаки:

Розробка та впровадження плану реагування на кібератаки:

Розробка докладного плану реагування на кібератаки, який включає послідовність дій, відповідальних осіб та процедури відновлення після інциденту.

Ідентифікація типових кібератак, що можуть статися, та розробка конкретних рекомендацій щодо реагування на кожен тип атаки.

Визначення відповідальних осіб із кібербезпеки та призначення їх ролей та обов'язків у плані реагування.

Підготовка персоналу до реагування на кібератаки:

Проведення регулярних тренувань, симуляцій та навчань з питань кібербезпеки для персоналу, що відповідає за реагування на інциденти.

Організація вправ та сценаріїв, що моделюють кібератаки, для тестування та вдосконалення реагування персоналу.

Підготовка персоналу до ефективного спілкування та співпраці з іншими відділами або сторонніми експертами під час реагування на інциденти.

Використання системи централізованого журналювання подій (Security Information and Event Management, SIEM):

Встановлення системи SIEM, яка збирає, аналізує та відстежує події зі всієї інформаційної системи, включаючи зловмисну або підозрілу активність.

Визначення правил та алгоритмів для виявлення аномальної активності, яка може вказувати на кібератаку або вразливість.

Налаштування системи для автоматичного сповіщення відповідних відділів або персоналу про виявлені кібератаки або інциденти.

Свідомість та навчання:

Забезпечення свідомості працівників щодо безпеки інформації та їх ролів та обов'язків у забезпеченні безпеки.

Організація обов'язкових тренінгів та семінарів з питань кібербезпеки:

Планування регулярних тренінгів та семінарів, які охоплюють різні аспекти безпеки інформації, включаючи принципи безпеки, потенційні загрози, методи захисту та процедури реагування на інциденти.

Залучення експертів з кібербезпеки для проведення тренінгів та надання актуальної інформації щодо нових загроз та розробки захисних стратегій.

Забезпечення участі всього персоналу, якому це необхідно згідно з їхніми обов'язками та ролями в організації.

Періодичне нагадування працівникам про важливість безпеки інформації:

Розсилка інформаційних бюлетенів, які містять корисні поради, кращі практики та оновлену інформацію про потенційні загрози та засоби захисту.

Використання електронних листів, внутрішніх комунікаційних каналів або інших доступних засобів спілкування для нагадування працівникам про основні правила безпеки, наприклад, щодо паролів, використання USB-накопичувачів, відкривання невідомих поштових вкладень тощо.

Посилення усвідомлення працівників про ризики та наслідки недбалого ставлення до безпеки інформації шляхом надання реальних прикладів та історій успіху або невдач в інших організаціях.

Залучення до практичних вправ та симуляцій:

Проведення практичних вправ з тестування знань та навичок працівників щодо безпеки інформації, включаючи розпізнавання фішингових електронних листів, виконання процедур повідомлення про інциденти та реагування на них.

Організація симуляцій кібератак, що дозволяють персоналу практикувати захисні дії та виявляти слабкі місця в системі безпеки.

Проведення після аналізу симуляцій та вправ, щоб ідентифікувати проблемні аспекти, вдосконалити процедури та навчатися на помилках.

Залучення спеціалістів з безпеки для надання консультацій та підтримки у впровадженні політики безпеки:

Наявність внутрішнього або зовнішнього експерта з кібербезпеки:

Залучення спеціаліста з безпеки, який має глибокі знання і досвід у галузі кібербезпеки, для надання консультацій та рекомендацій щодо захисту інформації.

Експерт з кібербезпеки може бути внутрішнім працівником, який відповідає за безпеку інформації в організації, або зовнішнім консультантом, який надає послуги підтримки безпеки.

Залучення спеціалістів під час аудиту безпеки:

Проведення аудиту безпеки, який оцінює існуючі заходи безпеки, виявляє потенційні загрози та визначає слабкі місця, які потребують удосконалення.

Спеціалісти з безпеки можуть бути залучені для проведення цього аудиту або для надання консультаційних послуг та рекомендацій щодо покращення заходів безпеки.

2.8. Висновок

В цьому розділі спеціальної частини кваліфікаційної роботи була проведена детальна характеристика устаткування компанії, що дозволило отримати повний огляд технічних засобів, які використовуються для обробки та збереження інформації. Були описані інформаційні потоки в компанії, що вказує на шляхи руху даних усередині організації.

Також була представлена інформаційно-комунікаційна структура, яка включає опис ієрархії та зв'язків між різними компонентами системи. Були розроблені модель загроз та модель порушників, що відображають потенційні загрози та потенційних зловмисників, які можуть спричинити порушення безпеки інформації.

У розділі були встановлені критерії захищеності, які слугують основою для оцінки рівня безпеки інформаційно-комунікаційної системи. Крім того,

була розроблена політика безпеки, яка визначає стратегічні цілі та підходи до забезпечення безпеки інформаційних ресурсів компанії.

Зазначена інформація свідчить про те, що в компанії були вжиті необхідні заходи для забезпечення безпеки інформаційно-комунікаційної системи. Розроблені моделі загроз та порушників, встановлені критерії захищеності та розроблена політика безпеки допоможуть забезпечити надійний рівень захисту інформації в організації.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

3.1. Обґрунтування витрат та розробку політики безпеки

Для оцінки економічної доцільності впровадження політики безпеки інформаційно-комунікаційної системи у підприємстві ТОВ "ПКФ "Мотор", необхідно провести розрахунки, які включатимуть оцінку капітальних витрат, пов'язаних з розробкою цієї політики. Крім того, потрібно врахувати експлуатаційні виплати, які залежатимуть від розробленої політики, а також розрахувати річний економічний ефект, який може бути отриманий від використання цієї інформаційно-комунікаційної системи з політикою безпеки.

Ці розрахунки будуть корисні для обґрунтування економічної ефективності використання результатів розробки політики безпеки у підприємстві. Вони допоможуть визначити, наскільки розробка цієї політики є обґрунтованою з економічної точки зору та чи варто інвестувати кошти у впровадження такої системи.

3.2. Розрахунки витрат на розробку політики безпеки інформації

3.2.1. Розрахунок капітальних (фіксованих) витрат

Капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{пр} + К_{аз} + К_{н}$$

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

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

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

$К_{пр}$ – 12500 грн (вартість розробки проекту інформаційної безпеки та залучення зовнішніх консультантів);

$К_{аз}$ – 78000 грн (вартість закупівлі файлового серверу);

$К_{н}$ – 3400 грн (витрати на встановлення обладнання та налагодження

системи інформаційної безпеки).

Підрахуємо капітальні витрати:

$$К = 12500 + 78000 + 3400 = 93900 \text{ грн}$$

3.2.2. Розрахунок річних поточних (експлуатаційних) витрат

Річні поточні (експлуатаційні) витрати складаються з наступних витрат:

$$С = С_а + С_{ел} + С_о + С_{тос},$$

де $С_а$ - річний фонд амортизаційних відрахувань;

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

$$С_{ел} = Р \times F_р \times Ц_е,$$

де Р - встановлена потужність апаратури інформаційної безпеки, кВт.

$F_р$ - річний фонд робочого часу системи інформаційної безпеки;

$Ц_е$ - тариф на електроенергію, грн./кВт годин;

$С_о$ - витрати на залучення сторонніх організацій для навчання співробітників компанії за допомогою запрошення спеціалістів інформаційної безпеки, які організовують створення політики безпеки;

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

$С_а$ - річний фонд амортизаційних відрахувань, складає 20%;

$$С_а = К \times 0{,}2 = 93900 \times 0{,}2 = 18780 \text{ грн};$$

$С_е$ - вартість електроенергії, що споживається апаратурною системою інформаційної безпеки протягом року (Р файлового серверу = 0.665 кВт, Ер = = 8760 робочих годин (робота цілодобово), Ц. = 1,44 грн);

$$С_{ел} = Р \times F_р \times Ц_е = 0.665 \times 8760 \times 4{,}31 = 25107{,}48 \text{ грн};$$

$$С_о = 17100 \text{ грн}$$

$С_{тос}$ - витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки, визначаються ПП «Альфа Транс» і становлять 3% від вартості капітальних витрат.

$$С_{тос} = К \times 0{,}03 = 113900 \times 0{,}03 = 3417 \text{ грн};$$

Підрахуємо поточні (експлуатаційні) витрати:

$$С = С_а + С_{ел} + С_о + С_{тос} = 18780 + 25107{,}48 + 17100 + 3417$$
$$= 64404{,}48 \text{ грн};$$

3.3. Оцінка величини можливого збитку від атаки

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

$$U = П_п + П_в + V,$$

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

$П_в$ - вартість відновлення працездатності вузла корпоративної мережі, грн;

V - втрати від зниження обсягу надання послуг клієнтам за час простою файлового сервера корпоративної мережі, грн.

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

$$П_п = \frac{\sum З_с * Ч_с}{F} \times t_n ,$$

де F - місячний фонд робочого часу (при 40-а годинному робочому тижні становить 160-176 год).

$З_с$ - місячна заробітна плата співробітника атакованого вузла або сегмента корпоративної мережі з нарахуванням єдиного соціального внеску, грн на місяць;

$Ч_с$ - чисельність співробітників атакованого вузла або сегмента корпоративної мережі, осіб.;

t_n - час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин;

Посада	Кількість співробітників, осіб	Місячна заробітна плата, грн	Витрати на заробітну плату, грн	Єдиний соціальний внесок, грн	Витрати на заробітну плату з урахуванням ЄСВ, грн
Фінансовий директор	1	37000	37000	3760	40760
Проектанти	4	25000	100000	10248	110248
Вентиляційники	1	22000	22000	2180	24180
Бухгалтери	2	18000	36000	3692	39692
Менеджери з продажу	2	22000	44000	3520	47520
Всього					262400

$$П_п = \frac{262400}{168} * 3 = 4685{,}71 \text{ грн}$$

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

$$П_в = П_{ви} + П_{пв} + П_{зч},$$

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

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

$П_{зч}$ - вартість заміни устаткування або запасних частин, грн.

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

$$П_{ви} = \frac{\sum З_с * Ч_с}{F} \times t_{ви},$$

Де $t_{ви}$ - час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин;

$$П_{ви} = \frac{262400}{168} * 4 = 6247{,}62 \text{ грн}$$

Витрати на відновлення файлового сервера корпоративної мережі $П_{ви}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати системного адміністратора:

$$П_{пв} = \frac{\sum З_о * Ч_о}{F} \times t_в ,$$

де $З_о$ - місячна заробітна плата системного адміністратора та спеціаліста ІТ з нарахуванням єдиного соціального внеску, грн на місяць;

$Ч_о$ - чисельність персоналу, осіб;

$t_в$ - час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин;

Розрахунок витрат на заробітну плату системного адміністратора з нарахуванням ЄСВ:

$$З_{о1} = 22500 + 22500 * 0{,}22 = 27450 \text{ грн}$$

Розрахунок витрат на заробітну плату спеціаліста ІТ з нарахуванням ЄСВ:

$$З_{о2} = 18600 + 18600 * 0{,}22 = 22692 \text{ грн}$$

$$П_{пв} = \frac{(27450 + 22692)}{168} * 2 = 596{,}92 \text{ грн},$$

$$П_в = 6247{,}62 + 596{,}92 + 0 = 6844{,}54 \text{ грн}$$

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

$$V = \frac{O}{F_г} \times (t_п + t_в + t_{ви}),$$

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

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

$$V = \frac{700000}{2080} * (3 + 4 + 2) = 30288{,}46 \text{ грн}$$

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

$$U = П_п + П_в + V = 4685{,}71 + 6844{,}54 + 30288{,}46 = 41818{,}71 \text{ грн}$$

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

$$B = \sum\sum U * N * I,$$

де I – число атакованих вузлів корпоративної мережі;

N – середнє число можливих атак на рік.

$$B = 41818{,}71 * 4 * 1 = 167274{,}84 \text{ грн}$$

3.4. Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B \times R - C ,$$

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

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

C - щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

$$E = 167274{,}84 \times 0{,}4 - 64404{,}48 = 66909{,}93 \text{ грн} ,$$

3.5. Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

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

а) коефіцієнт повернення інвестицій у сфері інформаційної безпеки ROSI (Return on Investment for Security);

6) термін окупності капітальних інвестицій T_o.

Коефіцієнт повернення інвестицій 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.

$$\mathrm{ROSI} = \frac{\mathrm{E}}{\mathrm{K}},$$

де ROSI - коефіцієнт повернення інвестицій, частки одиниці;

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

К - капітальні інвестиції, що забезпечили цей ефект, тис. грн.

$$\mathrm{ROSI} = \frac{66909{,}93}{93900} = 0{,}71$$

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

$$\mathrm{T_o} = \frac{\mathrm{K}}{\mathrm{E}} = \frac{1}{\mathrm{RC}},$$

де T_o - термін окупності капітальних інвестицій, років.

$$T_o = \frac{93900}{66909{,}93} = 1{,}4\,,$$

що становить 1 рік 3 місяця.

3.6. Висновок

В цьому розділі проаналізовано доцільність впровадження політики інформаційної безпеки на підприємстві. Визначено її економічну ефективність.

Розраховано капітальні та експлуатаційній витрати на впровадження інформаційної політики безпеки, які склали 93900 грн. та 64404,48 грн. відповідно.

Загальний збиток від атаки на підприємство через упущену вигоду складає 167274,84 грн.

Термін окупності капітальних інвестицій складає 1 рік 3 місяця.

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

ВИСНОВКИ

В даній кваліфікаційній роботі було детально розглянуто питання захисту інформаційних ресурсів підприємства ТОВ "ПКФ "Мотор"" у сучасному цифровому світі. Були представлені загальні відомості про компанію, її організаційну структуру, а також план розташування та ситуаційний план, що дозволило отримати повний огляд функціонування підприємства.

Також були розглянуті деталі устаткування підприємства, інформаційні потоки та інформаційно-комунікаційна структура. Розроблені модель загроз та модель порушників, що допомогли ідентифікувати потенційні загрози та визначити потенційних зловмисників, які можуть вплинути на безпеку інформації.

У роботі були розглянуті критерії захищеності та розроблені основні положення політики безпеки підприємства. Були також проведені розрахунки капітальних та експлуатаційних витрат, пов'язаних із впровадженням політики безпеки.

Практичне значення цієї роботи полягає у покращенні ефективності захисту інформаційно-комунікаційної системи підприємства. Розробка та впровадження більш ефективної політики безпеки сприятимуть забезпеченню надійного рівня захисту інформації та запобіганню можливим загрозам. Отже, результати цієї роботи мають практичне значення для підприємства ТОВ "ПКФ "Мотор"", сприяючи підвищенню рівня безпеки його інформаційно-комунікаційної системи.

ПЕРЕЛІК ПОСИЛАНЬ

1. НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу».

2. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу».

3. НД ТЗІ 2.5-005 -99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу».

4. НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі».

5. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу».

6. 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».

7. Закон України № 1280-IV«Про телекомунікації»(Електрон. ресурс) / Спосіб доступу: URL: *zakon.rada.gov.ua/go/1280-15*- Загол. з екрана.

8. Закон України №2938-17 від 13.01.2011р."Про інформацію"//Відомості Верховної Ради України. – 2011. -№ 32, с.313.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	1 Розділ	13	
6	А4	2 Розділ	46	
7	А4	3 Розділ	8	
8	А4	Висновки	1	
9	А4	Перелік посилань	1	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	
14	А4	Додаток Д	2	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

16 Додаток Д.doc

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК

на кваліфікаційну роботу бакалавра на тему:
Розробка політики безпеки інформаційно-комунікаційної системи підприємства ТОВ "ПКФ "Мотор""
студента групи 125-19-2
Мелещука Артема Андрійовича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на __ сторінках та містить __ рисунків, __ таблиць, __ джерел та __ додатка.

Об'єкт розробки: політика безпеки інформаційно-комунікаційної системи підприємства ТОВ "ПКФ "Мотор"".

Мета роботи: розробити та впровадити політику безпеки інформаційно-комунікаційної системи підприємства ТОВ "ПКФ "Мотор"".

У розділі «СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ» розглянуто стан питання щодо важливості захисту інформаційних ресурсів підприємства у сучасному цифровому світі. Приведені загальні відомості про компанію та розписана організаційна структура підприємства. Розписані план розташування та ситуаційний план підприємства.

У розділі «СПЕЦІАЛЬНА ЧАСТИНА» розписані устаткування підприємства, інформаційні потоки, інформаційно-комунікаційна структура. Складено модель загроз та модель порушників. Розглянуті критерії захищеності та розроблено основні положення політики безпеки підприємства.

В економічному розділі виконано розрахунок капітальних та експлуатаційних витрат на впровадження політики безпеки у підприємство ТОВ "ПКФ "Мотор"".

Практична цінність роботи полягає у підвищенні ефективності захисту інформаційно-комунікаційної системи підприємства, за рахунок розробки та впровадження більш ефективної політики безпеки підприємства.

Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому робота задовольняє усім вимогам і може бути допущена до захисту, а його автор заслуговує на оцінку «_____».

Керівник

Таблиця моделі загроз

Вид загрози	Причина виникнення	Методи боротьби
Шахрайство з постачальниками	постачальники зловживають довірою підприємства шляхом недоставки товарів, надання неконкурентоспроможних продуктів або завищення цін.	встановити механізми перевірки постачальників, підписувати угоди з надійними контрагентами та контролювати виконання договірних зобов'язань.
Розкрадання електрообладнання	незаконне заволодіння електрообладнанням підприємства	встановити систему контролю за вхідно-вихідними процедурами, використовувати захисні пристрої, такі як камери спостереження, та проводити періодичну інвентаризацію активів.
Недотримання процедур та політик	співробітники не дотримуються встановлених процедур та політик щодо безпеки інформації	проводити регулярну навчання та підвищення кваліфікації співробітників,
Витік інформації	конфіденційна інформація підприємства потрапляє в руки несанкціонованих осіб	встановити механізми контролю доступу до інформації, шифрування даних, забезпечити фізичну та логічну безпеку серверів і комп'ютерів, а також навчати співробітників основам кібербезпеки.
Саботаж та невиконання обов'язків	співробітники навмисно завдають шкоди інформаційній системі підприємства або не виконують свої обов'язки з безпеки	ретельно відбирати персонал, проводити періодичні аудити безпеки, встановлювати систему моніторингу та реагування на інциденти безпеки.
Зловживання повноваженнями	співробітники зловживають своїм статусом або	встановити принцип найменших привілеїв, обмежити доступ до

	повноваженнями для незаконного доступу до конфіденційної інформації або вчинення інших злочинних дій	критичних ресурсів та інформації, і регулярно перевіряти привілеї співробітників.
Постачальники з несумлінними практиками	постачальники надають низькоякісні продукти, використовують неетичні практики або не дотримуються стандартів безпеки.	проводити оцінку постачальників, встановлювати вимоги до якості і безпеки продукції, підписувати угоди з надійними постачальниками та проводити регулярний контроль якості.
Клієнти з несумлінними намірами	клієнти вчиняють шахрайські дії, намагаються отримати доступ до конфіденційної інформації або завдати шкоди системі.	встановити систему перевірки клієнтів, використовувати безпечні методи аутентифікації та шифрування даних.
Піратство та контрафактні товари	підприємство стикається з незаконним використанням свого бренду, крадіжками ідеї або поширенням контрафактних товарів.	реєструвати і захищати права інтелектуальної власності, співпрацювати з відповідними органами з боротьби з контрафактом та забезпечити якість та надійність продукції.
Кібератаки	включає різноманітні види хакерських атак, такі як вторгнення, віруси, фішинг, DDoS-атаки тощо, з метою заволодіння інформацією, порушення роботи системи або вимагання викупу.	встановити захисні фаєрволи, антивірусне програмне забезпечення, шифрування даних, а також регулярно оновлювати програмне забезпечення та проводити аудит безпеки.