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 *Дробот Тетяни Сергіївни*

академічної групи *125-20-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка політики безпеки інформації інформаційно-комунікаційної системи ТОВ «Компсофт»*

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

Дніпро
2024

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Дробот Тетяні Сергіївні*** **академічної групи** ***125-20-1***
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Розробка політики безпеки інформації інформаційно-комунікаційної системи ТОВ «Компсофт»***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 23.05.2024 № 469-с

Розділ	Зміст	Термін виконання
Розділ 1	Визначити актуальність розробки засобів захисту інформаційних ресурсів підприємства, організаційну структура, види інформації які циркулюють в ІКС підприємства, виконати аналіз ІКС	15.03.2024
Розділ 2	Виконати аналіз загроз та ризиків, побудувати модель порушника, визначити вимоги до системи інформаційної безпеки, розробити політику інформаційної безпеки підприємства	10.05.2024
Розділ 3	Виконати розрахунки економічних показників та довести економічну доцільність розробки	11.06.2024

Завдання видано _____ Вадим МЄШКОВ
(підпис керівника) (ім'я, прізвище)

Дата видачі: 15.01.2024р.

Дата подання до екзаменаційної комісії: 28.06.2024р.

Прийнято до виконання _____ Тетяна ДРОБОТ
(підпис студента) (ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 106 с., 2 рис., 4 табл., 4 додатка, 15 джерел.

Метою розробки політики інформаційної безпеки ТОВ "Компсофт" є створення комплексної системи заходів і процедур для забезпечення цілісності, конфіденційності та доступності інформаційних ресурсів компанії.

Об'єктом розробки є інформаційно-комунікаційна система ТОВ "Компсофт", яка включає апаратне та програмне забезпечення, дані, мережеву інфраструктуру, а також всі процеси та процедури, пов'язані з обробкою, зберіганням і передачею інформації.

Предметом розробки є заходи, процедури та політики, спрямовані на забезпечення інформаційної безпеки.

У першому розділі визначено актуальність розробки засобів захисту інформаційних ресурсів підприємства, визначена організаційна структура, види інформації які циркулюють в ІКС підприємства, виконано аналіз ІКС.

У другому розділі виконано аналіз загроз та ризиків, побудована модель порушника, визначені вимоги до системи інформаційної безпеки, розроблена політика інформаційної безпеки підприємства.

У третьому розділі виконано розрахунок економічних показників та наведено економічне обґрунтування доцільності розробки політики інформаційної безпеки.

Практична цінність розробки політики інформаційної безпеки ТОВ "Компсофт" полягає у створенні систематизованого та ефективного підходу до захисту інформаційних активів компанії. Це дозволяє компанії не лише відповідати сучасним вимогам інформаційної безпеки, але й забезпечувати стабільність та надійність бізнес-процесів.

ПОЛІТИКА ІНФОРМАЦІНОЇ БЕЗПЕКИ, МОДЕЛЬ ЗАГРОЗ, АНАЛІЗ РИЗИКІВ, МОДЕЛЬ ПОРУШНИКА, КІБЕРБЕЗПЕКА.

ABSTRACT

Explanatory note: 106 pp., 2 pic., 4 table, 4 app, 15 sources.

The purpose of developing the Information Security Policy of CompSoft LLC is to create a comprehensive system of measures and procedures to ensure the integrity, confidentiality and availability of the company's information resources.

The object of development is the information and communication system of CompSoft LLC, which includes hardware, software, data, network infrastructure, as well as all processes and procedures related to the processing, storage and transmission of information.

The subject of the development is measures, procedures and policies aimed at ensuring information security.

The first section defines the relevance of developing means of protecting information resources of an enterprise, determines the organizational structure, types of information circulating in the enterprise's ICS, and analyzes the ICS.

The second section analyzes the threats and risks, builds a model of an intruder, defines the requirements for the information security system, and develops an enterprise information security policy.

The third section calculates economic indicators and provides an economic justification for the feasibility of developing an information security policy.

The practical value of the development of the Information Security Policy of CompSoft LLC is to create a systematized and effective approach to protecting the company's information assets. This allows the company not only to meet modern information security requirements, but also to ensure the stability and reliability of business processes.

INFORMATION SECURITY POLICY, THREAT MODEL, RISK ANALYSIS, INTRUDER MODEL, CYBERSECURITY.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ІКС – інформаційно-комунікаційна система;

ІТ – інформаційні технології;

ОС – операційна система;

НСД – несанкціонований доступ;

ПБ – політика безпеки;

ПЗ – програмне забезпечення;

ТОВ – товариство з обмеженою відповідальністю;

IAM – Identity and Access Management;

IDS – Intrusion Detection System;

IoT – Internet of Things;

IPS – Intrusion Prevention System;

VPN – Virtual Private Network.

ЗМІСТ

с.

ВСТУП

У сучасному світі, де інформація є одним з найважливіших активів будь-якої організації, забезпечення безпеки інформації стає ключовою пріоритетною задачею. Актуальність розробки політики безпеки інформації для інформаційно-комунікаційної системи обумовлена зростаючою кількістю кіберзагроз, а також необхідністю захисту конфіденційності, цілісності та доступності інформації.

Об'єкт розробки – інформаційно-комунікаційна система ТОВ "Компсофт", яка спеціалізується на розробці програмного забезпечення.

Предмет розробки – політика безпеки інформації в рамках зазначеної системи, що включає в себе ідентифікацію, аналіз ризиків, розробку заходів щодо зниження цих ризиків та впровадження ефективних механізмів захисту.

Мета роботи – розробка політики безпеки інформації для інформаційно-комунікаційної системи ТОВ "Компсофт", спрямованої на підвищення рівня захищеності інформаційних ресурсів компанії від внутрішніх та зовнішніх загроз.

Завдання роботи включають:

1. Аналіз існуючого стану безпеки інформації в компанії.
2. Виявлення потенційних загроз та вразливостей.
3. Розробка рекомендацій щодо удосконалення заходів безпеки.
4. Розробка політики безпеки інформації.
5. Впровадження політики безпеки інформації.

Практичне значення роботи полягає у створенні ефективної системи захисту інформації, здатної адаптуватися до змін у сфері ІТ.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Актуальність розробки засобів захисту інформаційних ресурсів

Актуальність розробки засобів захисту інформаційних ресурсів з обмеженим доступом в сучасному цифровому світі не може бути переоцінена. В умовах стрімкого розвитку інформаційних технологій та збільшення обсягів цифрових даних, захист конфіденційної інформації стає важливим пріоритетом для організацій усіх масштабів. Сучасні загрози інформаційної безпеки включають різноманітні форми кібератак, такі як фішинг, віруси, троянські програми, атаки на веб-додатки, а також внутрішні загрози, пов'язані з помилками співробітників або навіть умисними діями інсайдерів.

Розвиток технологій штучного інтелекту та машинного навчання надає зловмисникам додаткові інструменти для автоматизації та підвищення ефективності кібератак. Водночас, зростання кількості пристроїв, підключених до Інтернету речей (IoT), створює нові вектори атак та збільшує кількість потенційних вразливостей. У зв'язку з цим, розробка ефективних засобів захисту, що враховують як технічні, так і організаційні аспекти безпеки, є ключовим завданням.

Засоби захисту повинні включати комплексні підходи, починаючи від фізичного захисту та антивірусного захисту, закінчуючи складними системами шифрування, аутентифікації та контролю доступу. Особливу увагу слід приділити розробці процедур реагування на інциденти та впровадженню політики безпеки, яка включає регулярне навчання персоналу та створення культури усвідомлення важливості інформаційної безпеки. Враховуючи динамічність кіберзагроз, системи захисту інформаційних ресурсів повинні бути гнучкими та здатними адаптуватися до нових викликів, забезпечуючи ефективний захист від поточних та майбутніх загроз.

При розробці засобів захисту інформаційних ресурсів з обмеженим доступом для інформаційно-комунікаційної системи необхідно виконати наступні кроки:

1. Визначення ризиків. Необхідно визначити потенційні загрози та вразливості, що можуть вплинути на інформаційні ресурси, здійснюючи аналіз як внутрішніх, так і зовнішніх ризиків.

2. Створення політики безпеки інформації. Слід створити документ, що чітко визначає правила, процедури та стандарти для забезпечення безпеки інформації, при цьому орієнтуючись на міжнародні стандарти, як-от ISO/IEC серії 27000.

3. Імплементація захисних технологій. Необхідно забезпечити впровадження технологічних рішень, таких як шифрування даних, системи управління доступом, антивірусне програмне забезпечення, фаєрволи та захист від DDoS-атак.

4. Управління доступом. Важливо встановити процедури та політики для контролю доступу до інформаційних ресурсів, що включає ідентифікацію користувачів, аутентифікацію, авторизацію та ведення обліку дій.

5. Навчання та підвищення обізнаності персоналу. Потрібно забезпечити регулярне навчання співробітників з питань безпеки інформації, щоб підвищити рівень їхньої обізнаності та відповідальності у захисті інформаційних активів.

6. Моніторинг та оновлення. Необхідно забезпечити постійний моніторинг стану безпеки інформаційних систем та вжити заходів для реагування на інциденти, а також періодично оновлювати політики та процедури з урахуванням нових загроз і викликів.

7. Проведення аудиту та перевірок. Необхідно регулярно проводити аудит безпеки інформації та перевіряти ефективність впроваджених заходів, залучаючи при цьому як внутрішні, так і зовнішні ресурси.

Виконання цих кроків дозволить створити комплексну та ефективну систему захисту інформаційних ресурсів, адаптовану до сучасних умов та вимог.

Основний напрямок у створенні засобів захисту обмежених інформаційних ресурсів інформаційно-комунікаційних систем включає інтеграцію технічних та організаційних заходів для забезпечення інформаційної безпеки. Серед цих

заходів є важливими дії, спрямовані на фізичний захист устаткування та пристроїв ІКС від несанкціонованого доступу.

Ключовим елементом є також впровадження криптографічних засобів безпеки для захисту даних від несанкціонованого проникнення, з використанням різноманітних методів шифрування.

Забезпечення безпеки мережі, включаючи налаштування мережевих з'єднань, ідентифікацію користувачів, а також використання брандмауерів та систем виявлення вторгнень, є вирішальним для захисту від зовнішніх атак.

Встановлення організаційних процедур, таких як управління доступом, політика використання даних та правила поведінки користувачів при роботі з даними, є невід'ємною частиною загального захисту.

Регулярні аудити безпеки є необхідними для ідентифікації потенційних загроз та вразливих місць у системі, дозволяючи своєчасно вживати необхідні заходи.

У процесі створення засобів захисту інформаційних ресурсів ІКС слід враховувати різноманітність загроз, використовувати відповідні технічні та організаційні заходи, проводити тестування та моніторинг системи, а також систематично здійснювати аудит безпеки.

Не менш важливо приділяти увагу законодавчим вимогам і рекомендаціям щодо захисту даних, зокрема, слід враховувати вимоги національного законодавства та міжнародні стандарти, як-от ISO/IEC 27001.

Врахування специфіки конкретної системи та її вимог є ключовим для ефективності заходів захисту, при цьому важливо розглядати можливості відновлення даних та встановлювати механізми резервного копіювання.

У підсумку, розробка засобів захисту інформаційних ресурсів ІКС є складним, але важливим завданням, що вимагає ґрунтовного підходу та професійної компетентності, а ефективно впроваджені заходи є ключем до забезпечення безпеки цінних даних та захисту від несанкціонованого доступу.

1.1.1 Аналіз ризиків

Аналіз ризиків становить фундаментальний перший крок у розробці засобів захисту інформаційних ресурсів з обмеженим доступом в інформаційно-комунікаційних системах, особливо в контексті діяльності ТОВ "Компсофт", що спеціалізується на розробці програмного забезпечення. Цей процес включає ідентифікацію потенційних загроз безпеці даних та оцінку ризиків їх реалізації. Відтак, аналіз загроз та ризиків дозволяє виявити ключові напрями захисту та розробити відповідні заходи для забезпечення безпеки даних.

Для проведення цього аналізу в ТОВ "Компсофт" рекомендується:

1. Ідентифікація інформаційних ресурсів та їх значущості. Спочатку важливо визначити, які дані є конфіденційними та критично важливими для діяльності компанії. Потім слід встановити, які ресурси та обладнання відповідають за зберігання та обробку цих даних.

2. Виявлення загроз. Потрібно ідентифікувати потенційні загрози, які можуть призвести до витоку або порушення цілісності конфіденційної інформації, включаючи зовнішні (наприклад, хакерські атаки, віруси) та внутрішні (наприклад, людські помилки або недостатній контроль доступу) фактори.

3. Оцінка ризиків. Необхідно оцінити рівень ризику для кожної загрози та можливі наслідки їх реалізації, враховуючи як імовірність виникнення загрози, так і потенційні наслідки.

4. Розробка заходів захисту. На основі оцінки ризиків важливо визначити необхідні технічні та організаційні заходи захисту, а також плани дій на випадок надзвичайних ситуацій для їх ефективного впровадження.

5. Планування та реалізація. Після визначення заходів захисту необхідно розробити план їх реалізації, включаючи встановлення термінів, бюджетування та інші ключові аспекти.

Аналіз загроз та ризиків є критичним для розробки ефективних засобів захисту інформаційних ресурсів ІКС в ТОВ "Компсофт", дозволяючи виявити

необхідні зміни в системі безпеки для надійного захисту важливих даних від різноманітних загроз.

Після завершення аналізу потенційних загроз та ризиків, критично важливим є постійне відстеження стану безпеки інформаційних ресурсів та реалізація заходів, спрямованих на запобігання виявленим ризикам. Зокрема, це може означати впровадження систем детекції вторгнення та інших загроз, які будуть попереджати про потенційні атаки на систему. Інструменти для моніторингу безпеки, такі як системи реєстрації подій, відіграють ключову роль у відстеженні дій користувачів та виявленні нестандартних активностей в системі.

Регулярне оновлення та впровадження патчів для програмного забезпечення та операційних систем є важливим для мінімізації ризику використання програмних вразливостей зловмисниками.

Крім того, можуть бути застосовані заходи технічного контролю доступу, такі як системи карток доступу чи біометрична ідентифікація, для ефективного контролю над доступом до конфіденційних даних.

Розроблення плану дій на випадок надзвичайних ситуацій, який включає процедури реагування на інциденти інформаційної безпеки, є невід'ємним елементом комплексної стратегії безпеки.

Також фундаментальною є потреба в навчанні співробітників, що взаємодіють з інформаційними ресурсами, забезпечуючи їх свідоме ставлення до правил та процедур безпеки.

Загалом, аналіз загроз та ризиків є важливим кроком у створенні засобів захисту обмежених інформаційних ресурсів ІКС. Це передбачає не лише одноразові дії, але й неперервний процес моніторингу, оновлення та адаптації заходів захисту до нових загроз. Розвиток плану надзвичайних ситуацій та просвітницька робота з персоналом є ключовими для забезпечення довгострокової безпеки даних і успішного захисту від несанкціонованого доступу.

1.1.2 Визначення обмеженого доступу

Розробка механізмів контролю обмеженого доступу до інформаційних ресурсів в компанії ТОВ "Компсофт", що займається розробкою програмного забезпечення, включає другий важливий етап – встановлення правил доступу користувачів до цих ресурсів та обладнання системи. Метою цього етапу є створення ефективної системи контролю доступу до важливої інформації та запобігання потенційним загрозам безпеки даних.

План дій для визначення обмеженого доступу включає:

1. Визначення ролей користувачів. Необхідно встановити різні ролі користувачів системи, наприклад, від інженерів-програмістів до адміністраторів системи, та визначити для них відповідні права доступу до інформаційних ресурсів.

2. Розробка політик доступу. Необхідно створити правила та процедури, які регулюють доступ до інформаційних ресурсів, відповідно до визначених ролей користувачів. Це може включати політики щодо паролів, обмеження доступу до конфіденційних даних та контроль доступу до мережі.

3. Імплементація системи авторизації та аутентифікації. Слід розробити систему, яка дозволяє ідентифікувати користувачів та надавати їм права доступу до інформаційних ресурсів, використовуючи паролі, картки доступу, біометричні системи та інші методи ідентифікації.

4. Впровадження системи контролю доступу. Важливо встановити систему, що контролює доступ користувачів до інформаційних ресурсів на рівні мережі, операційних систем та додатків.

5. Розробка правил доступу. Необхідно чітко визначити права доступу користувачів відповідно до їхніх робочих обов'язків, від звичайних користувачів до адміністраторів.

6. Створення системи моніторингу доступу. Слід впровадити систему, яка відстежує дії користувачів в системі та виявляє можливі аномалії, щоб своєчасно виявляти загрози безпеці даних.

7. Розробка системи аудиту доступу. Важливо встановити систему, яка реєструє всі дії користувачів та зберігає ці дані для аналізу та виявлення потенційних проблем в системі безпеки.

Встановлення обмеженого доступу до інформаційних ресурсів є ключовим для забезпечення контролю доступу до конфіденційної інформації та запобігання можливим загрозам безпеки даних у ТОВ "Компсофт". Після визначення прав доступу необхідно регулярно перевіряти їхню ефективність і адаптувати за потребою, щоб забезпечити максимальний захист даних.

1.1.3 Захист від несанкціонованого доступу

Захист інформаційних ресурсів від несанкціонованого доступу в компанії ТОВ "Компсофт" включає третій ключовий етап в розробці механізмів безпеки ІКС. Цей етап передбачає впровадження специфічних заходів захисту, спрямованих на недопущення несанкціонованого доступу до важливих інформаційних ресурсів.

Процедури, що слід виконати для забезпечення захисту, включають:

1. Створення політики паролів. Розробка надійної політики паролів, включаючи сучасні методи хешування та шифрування, щоб забезпечити безпеку доступу до системи.

2. Фізичний захист обладнання. Встановлення заходів фізичного захисту для серверних приміщень та іншого критичного обладнання, включаючи системи контролю доступу та відеоспостереження.

3. Захист мережі. Імплементація систем захисту мережі для контролю доступу до мережевих ресурсів та запобігання несанкціонованому доступу.

4. Впровадження шифрування. Розробка систем шифрування для захисту конфіденційної інформації у мережах, базах даних та інших важливих ресурсах.

5. Система виявлення інтрузій. Встановлення систем, що виявляють незвичайну активність та потенційні атаки на систему.

6. Антивірусний захист. Використання програмного забезпечення для захисту від вірусів та інших шкідливих програм для запобігання інфікуванню системи.

7. Резервне копіювання даних. Створення надійної системи резервного копіювання для зберігання копій даних на випадок їх втрати чи пошкодження.

8. Система аудиту доступу. Встановлення системи, що реєструє всі дії користувачів, для аналізу та виявлення потенційних проблем у системі безпеки.

9. Захист даних. Визначення та впровадження системи захисту даних для забезпечення безпеки конфіденційної інформації.

10. Розробка процедур безпеки. Створення правил та процедур безпеки для користувачів системи, включаючи правила зміни паролів, використання сильних паролів та заборону певних дій.

Встановлення цих заходів захисту в ТОВ "Компсофт" є вирішальним для захисту інформаційних ресурсів від несанкціонованого доступу, забезпечення цілісності та конфіденційності даних. Регулярний аудит та періодичне оновлення заходів безпеки є необхідними для забезпечення їх актуальності та ефективності в динамічному середовищі кіберзагроз.

1.1.4 Моніторинг системи

Моніторинг системи в ТОВ "Компсофт", що займається розробкою програмного забезпечення, є важливим четвертим етапом у розробці засобів захисту інформаційних ресурсів з обмеженим доступом. Цей етап включає розгортання системи моніторингу, яка дозволяє стежити за станом системи та виявляти потенційні проблеми та загрози безпеці даних.

Для ефективного моніторингу системи в "Компсофт" рекомендується:

1. Визначення важливих параметрів системи.

Необхідно ідентифікувати ключові параметри, такі як використання пам'яті, завантаження процесора, використання дискового простору, які вимагають моніторингу для виявлення потенційних проблем та загроз.

2. Впровадження системи моніторингу.

Встановлення програмного забезпечення, що дозволяє стежити за станом системи та важливими показниками, передаючи дані на центральний сервер моніторингу.

3. Реалізація системи сповіщення.

Встановлення механізмів сповіщення, які надсилають повідомлення про незвичайні стани системи чи потенційні загрози, використовуючи електронну пошту, SMS та інші канали спілкування.

4. Установка порогових значень.

Визначення порогів для кожного ключового параметра, за перевищення яких система вважатиметься у небезпечному стані.

5. Розробка процедур реагування.

Створення чітких дій на випадок виявлення проблем чи загроз, включаючи автоматичне відновлення системи та блокування користувачів, які порушують правила безпеки.

6. Засоби збереження даних моніторингу.

Встановлення засобів для архівування даних моніторингу, що дозволяє зберігати історію стану системи для аналізу трендів та потенційних загроз.

7. Аналітичні інструменти.

Використання спеціальних аналітичних засобів для обробки та аналізу зібраних даних, що дозволяє виявити закономірності та причини проблем.

8. Система захисту від вторгнень.

Встановлення механізмів, які дозволяють виявляти та запобігати спробам несанкціонованого доступу.

9. Система моніторингу та аудиту.

Впровадження системи, яка дозволяє відстежувати користувацькі дії та виявляти потенційні загрози безпеці.

Моніторинг системи є фундаментальним для забезпечення високого рівня безпеки даних у "Компсофт", мінімізації ризику виникнення проблем та своєчасного реагування на загрози. Дані, зібрані через систему моніторингу, є цінними для виявлення та попередження потенційних загроз безпеці даних, а також для виявлення проблем у функціонуванні системи, що допомагає в запобіганні відмов та забезпеченні безперебійної роботи. Результати моніторингу також можуть бути використані для оптимізації процедур безпеки та посилення захисних заходів, підвищуючи таким чином загальний рівень безпеки системи.

1.1.5 Тестування та аналіз результатів

Тестування та аналіз результатів є п'ятим етапом розробки засобів захисту інформаційних ресурсів з обмеженим доступом (ІКС). Цей етап передбачає проведення випробувань для перевірки ефективності та правильності роботи засобів захисту та аналіз отриманих результатів.

Для ефективного проведення тестування та аналізу результатів необхідно виконати такі дії:

1. Визначення тестових випадків.

Важливо визначити сценарії тестування, які дозволять оцінити ефективність та коректність функціонування засобів захисту. Ці сценарії можуть включати ситуації з несанкціонованим доступом до системи, атаки з мережі, передачу шкідливого програмного коду та інші можливі загрози.

2. Виконання тестів.

Після визначення сценаріїв тестування виконуються перевірки, щоб оцінити ефективність та коректність роботи засобів захисту. Ці перевірки можуть бути проведені за допомогою спеціалізованих програм, які емулюють можливі загрози безпеки даних.

3. Аналіз результатів.

Після завершення тестування важливо аналізувати результати і визначити рівень захисту від можливих загроз, виявити проблеми та вразливі місця в системі захисту, а також оцінити, наскільки ефективно виявляються та блокуються можливі загрози.

4. Внесення змін.

На підставі аналізу отриманих результатів може виникнути потреба внести зміни до засобів захисту та процедур безпеки. Це може включати в себе впровадження нових заходів захисту, зміну параметрів системи, що відповідає за захист, а також коригування процедур безпеки з метою підвищення загального рівня безпеки та зниження ризику загроз.

5. Повторне тестування.

Після впровадження змін важливо знову провести тестування з метою перевірки ефективності та правильності роботи засобів захисту та оцінки впливу внесених змін. Це допомагає переконатися, що внесені зміни працюють ефективно та відповідають вимогам безпеки.

6. Документування результатів.

Після завершення тестування та аналізу результатів важливо створити документацію з отриманих результатів. Ця документація служить як запис щодо ефективності та правильності роботи засобів захисту та може бути використана для подальших вдосконалень системи захисту.

Тестування та аналіз результатів є важливим етапом у розробці засобів захисту інформаційних ресурсів з обмеженим доступом ІКС підприємства. Цей процес дозволяє перевірити ефективність роботи засобів захисту інформації, виявити потенційні проблеми в системі захисту, а також внести зміни для покращення рівня безпеки та зменшення ризиків. Тестування та аналіз результатів є невід'ємною частиною процесу забезпечення кібербезпеки ІКС.

1.2 Опис виду діяльності підприємства

Компанія "Компсофт" – це інноваційне технологічне підприємство, яке фокусується на розробці, тестуванні, та впровадженні широкого спектру програмних продуктів та рішень. Основна діяльність компанії включає наступні аспекти:

– розробка ПЗ – створення високоякісного програмного забезпечення, від проєктування до реалізації, з урахуванням потреб і вимог замовників. Це включає індивідуальні рішення та стандартні програмні пакети.

– тестування та забезпечення якості – проведення ретельного тестування програмних продуктів з метою виявлення та усунення помилок, гарантування надійності та відповідності стандартам якості.

– технічна підтримка та сервіс – надання послуг технічної підтримки та консультацій для користувачів, що включає усунення проблем, оновлення ПЗ, та інструктажі з експлуатації.

– маркетинг та продажі – розробка маркетингових стратегій та реалізація програмного забезпечення на ринку, а також налагодження відносин з потенційними та існуючими клієнтами.

– управління проєктами – ефективне планування, координація та керування проєктами з розробки ПЗ, включаючи розподіл ресурсів, контроль виконання задач та звітність.

– управління ресурсами та операціями – включає в себе фінансове планування, бухгалтерський облік, управління персоналом, а також забезпечення необхідної інфраструктури та ресурсів для роботи підприємства.

– дослідження та розвиток (R&D) – новаторська діяльність, спрямована на пошук нових технологій та рішень, що можуть бути інтегровані у продукти компанії, підвищуючи їх конкурентоспроможність.

– забезпечення безпеки – імплементація та підтримка заходів кібербезпеки для захисту програмних продуктів та корпоративних даних.

1.3 Посадові обов'язки персоналу підприємства

До переліку персоналу ТОВ "Компсофт" входять (рис.1.1) :

- Виконавчий директор: 1 шт.
- Заступник директора: 1 шт.
- Секретар: 1 шт.
- Маркетологи: 2 шт.
- Менеджери з продажів: 4 шт.
- Фахівці служби підтримки клієнтів: 4 шт.
- Головний бухгалтер: 1 шт.
- Бухгалтери: 3 шт.
- HR-менеджер: 1 шт.
- Інженери-програмісти: 12 шт.
- QA інженери (тестувальники): 4 шт.
- Адміністратор баз даних: 1 шт.
- Керівники проєктів: 2 шт.

- Системний адміністратор: 1 шт.
- Спеціаліст з кібербезпеки: 1 шт.
- Охоронці: 2 шт.
- Прибиральниці: 2 шт.

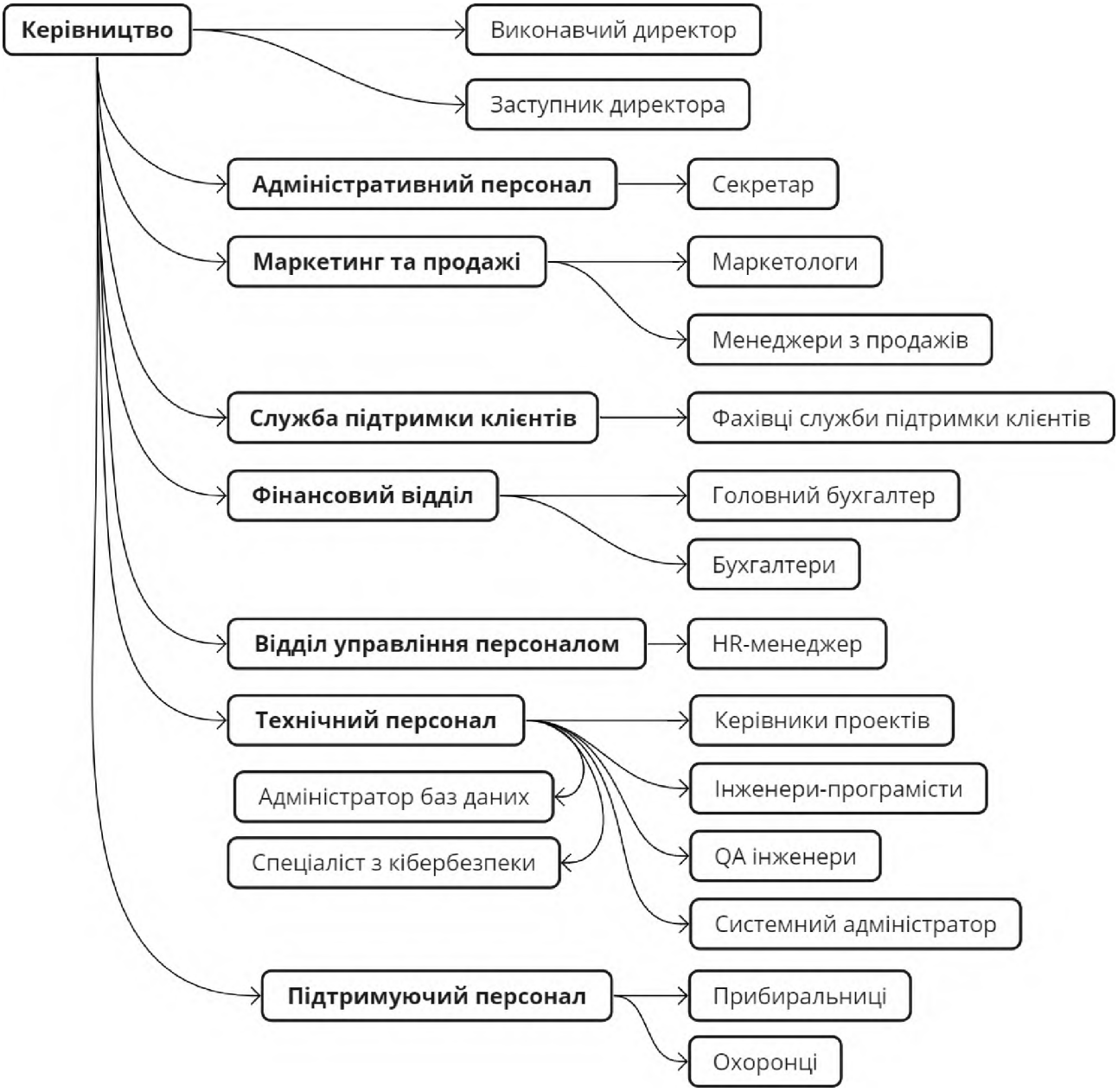

Рисунок 1.1 – Організаційна структура підприємства ТОВ "Компсофт"

Посадові обов'язки персоналу підприємства ТОВ "Компсофт":

1. Керівництво (Виконавчий директор та Заступник директора): відповідають за загальне керівництво компанією, розробку стратегій, планування та управління ресурсами. Вони також займаються ухваленням ключових рішень і представляють компанію в зовнішніх відносинах.

2. Адміністративний персонал (Секретар): відповідає за організаційну підтримку, управління офісом, координацію зустрічей та підготовку документації.

3. Маркетинг та продажі (Маркетологи, Менеджери з продажів): розробка маркетингових стратегій та кампаній, проведення ринкових аналізів, а також прямі продажі програмного забезпечення, налагодження відносин з клієнтами.

4. Служба підтримки клієнтів: надання технічної підтримки і консультацій клієнтам, розв'язання проблем, пов'язаних з програмним забезпеченням.

5. Фінансовий відділ (Головний бухгалтер, Бухгалтери): управління фінансами компанії, бухгалтерський облік, планування бюджетів та звітність.

6. Відділ управління персоналом (HR-менеджер): рекрутинг, оцінка та розвиток персоналу, управління кадровою політикою та корпоративною культурою.

7. Технічний персонал:

- Інженери-програмісти: розробка нового програмного забезпечення, вдосконалення існуючих продуктів.

- QA інженери (тестувальники): забезпечення якості продукції, виявлення та усунення помилок у програмному забезпеченні.

- Адміністратор баз даних: управління базами даних, забезпечення їх безпеки та ефективності.

- Керівники проєктів: планування, координація та контроль проєктів з розробки програмного забезпечення.

- Системний адміністратор: забезпечення стабільної та безпечної роботи інформаційних систем.

- Спеціаліст з кібербезпеки: захист інформаційних систем від зовнішніх та внутрішніх загроз.

8. Підтримуючий персонал (Охоронці, Прибиральниці): забезпечення безпеки та чистоти на робочому місці.

Кожен з цих відділів відіграє важливу роль у загальному процесі розробки, впровадження та підтримки програмного забезпечення, а також у забезпеченні ефективної роботи компанії.

1.4 Інформація яка циркулює в ІКС підприємства

В інформаційній системі (ІКС) підприємства "Компсофт", яке спеціалізується на розробці та впровадженні програмного забезпечення, різні види інформації можуть циркулювати між користувачами. Основні види цієї інформації включають:

– Інформація про технічну документацію: включає специфікації продуктів, технічні описи, інструкції з використання, а також інструкції для внутрішнього використання, такі як процедури кодування чи налаштування систем.

– Інформація про проєктну документацію: включає документацію, пов'язану з управлінням проєктами, включаючи плани проєктів, звіти про хід робіт, бюджети проєктів, та оцінки ризиків.

– Інформація про комерційну діяльність: включає інформацію про продажі, маркетингові стратегії, аналізи ринку, договори з клієнтами, а також цінові політики.

– Інформація про фінансову діяльність: включає фінансові звіти, бухгалтерський облік, бюджети, інформацію про витрати та доходи, інвестиційні плани.

– Інформація про персонал: включає дані про персонал, включаючи особисті дані, документацію з найму, результати оцінювання працівників, записи про навчання та розвиток кар'єри.

– Інформація про клієнтів: включає дані про клієнтів, історію взаємодій, запити на обслуговування, відгуки та скарги.

– Інформація про внутрішні комунікації: включає електронні листи, меморандуми, звіти з нарад, внутрішні повідомлення та спілкування, пов'язане з управлінням компанією та її діяльністю.

– Інформація про нормативно-правову базу: включає законодавчі акти, нормативні документи, ліцензійні угоди, патенти та інші документи, що регулюють правові аспекти діяльності компанії.

– Інформація про безпеку та конфіденційність: включає інформацію, пов'язану з кібербезпекою, протоколи безпеки, документацію з аудиту безпеки, звіти про інциденти.

– Інформація про дослідження та розвиток: включає інформацію, отриману в ході досліджень, аналізу конкурентів, ринкових тенденцій, технологічних інновацій тощо.

Ці категорії інформації можуть циркулювати між різними учасниками інформаційної системи компанії, як у онлайн, так і в офлайн режимах. Ключовим аспектом такого обміну є забезпечення безпеки інформації та контролювання доступу до неї для попередження неавторизованого втручання в конфіденційні дані. Система управління інформацією компанії повинна гарантувати ефективний обмін даними між користувачами з різними рівнями доступу, забезпечувати інтеграцію даних з різноманітних джерел, автоматизувати процеси аналізу та обробки даних, а також виконувати зберігання та архівацію інформації.

Таблиця 1.1 – Види інформації які циркулюють на підприємстві

Співробітник	Види інформації
Виконавчий директор	комерційна інформація, фінансова інформація, внутрішні комунікації, дані безпеки та конфіденційності
Заступник директора	комерційна інформація, проєктна документація, фінансова інформація
Секретар	внутрішні комунікації, персональні дані співробітників
Маркетологи	комерційна інформація, дослідницькі та розвідувальні дані

Співробітник	Види інформації
Менеджери з продажів	комерційна інформація, інформація про клієнтів
Фахівці служби підтримки клієнтів	технічна документація, інформація про клієнтів
Головний бухгалтер	фінансова інформація
Бухгалтери	фінансова інформація
HR-менеджер	персональні дані співробітників
Інженери-програмісти	технічна документація, проєктна документація
QA інженери	технічна документація, проєктна документація
Адміністратор баз даних	технічна документація
Керівники проєктів	проєктна документація, внутрішні комунікації
Системний адміністратор	дані безпеки та конфіденційності, технічна документація
Спеціаліст з кібербезпеки	дані безпеки та конфіденційності
Охоронці	дані безпеки та конфіденційності
Прибиральниці	-

1.5 Інформаційна система підприємства

На підприємстві, спеціалізованому на розробці та впровадженні програмного забезпечення, співробітники можуть використовувати різноманітне програмне забезпечення залежно від їхніх ролей та завдань.

1. Для технічного персоналу (інженери-програмісти, QA інженери, адміністратори баз даних):

- інтегровані середовища розробки (IDE) – IntelliJ IDEA.
- системи контролю версій – Git.
- системи управління базами даних (DBMS) Microsoft SQL Server.
- інструменти для тестування та QA – Selenium.
- фреймворки та бібліотеки, специфічні для розробки.

2. Для керівництва та адміністративного персоналу (виконавчий директор, заступник директора, секретар):

- офісні пакети Microsoft Office 365 та Google Workspace для обробки текстів, електронних таблиць, презентацій.

- системи управління проєктами, Microsoft Project.

- CRM-системи для управління взаємовідносинами з клієнтами.

3. Для маркетингу та продажів (маркетологи, менеджери з продажів):

- інструменти для цифрового маркетингу – Google Analytics

- CRM-системи для управління взаємовідносинами з клієнтами.

- платформи електронної пошти та соціальних мереж для кампаній та комунікацій.

4. Для фінансового відділу (головний бухгалтер, бухгалтери)

- бухгалтерські програми.

- інструменти для фінансового аналізу та звітності.

5. Для HR-відділу (HR-менеджер):

- системи управління персоналом (HRM) – HURMA.

- інструменти для рекрутингу, як-от LinkedIn Recruiter, Indeed або засоби відстеження кандидатів (ATS).

6. Для відділу безпеки (спеціаліст з кібербезпеки, системний адміністратор):

- інструменти для моніторингу мережі та безпеки, Wireshark, Norton Security.

- системи керування патчами та оновленнями.

- антивірусне та антималварне програмне забезпечення.

- системи резервного копіювання.

7. Підтримуючий персонал (охоронці, прибиральниці):

- можуть використовувати базові додатки для комунікації та координації, наприклад мобільні додатки або системи внутрішнього обміну повідомленнями.

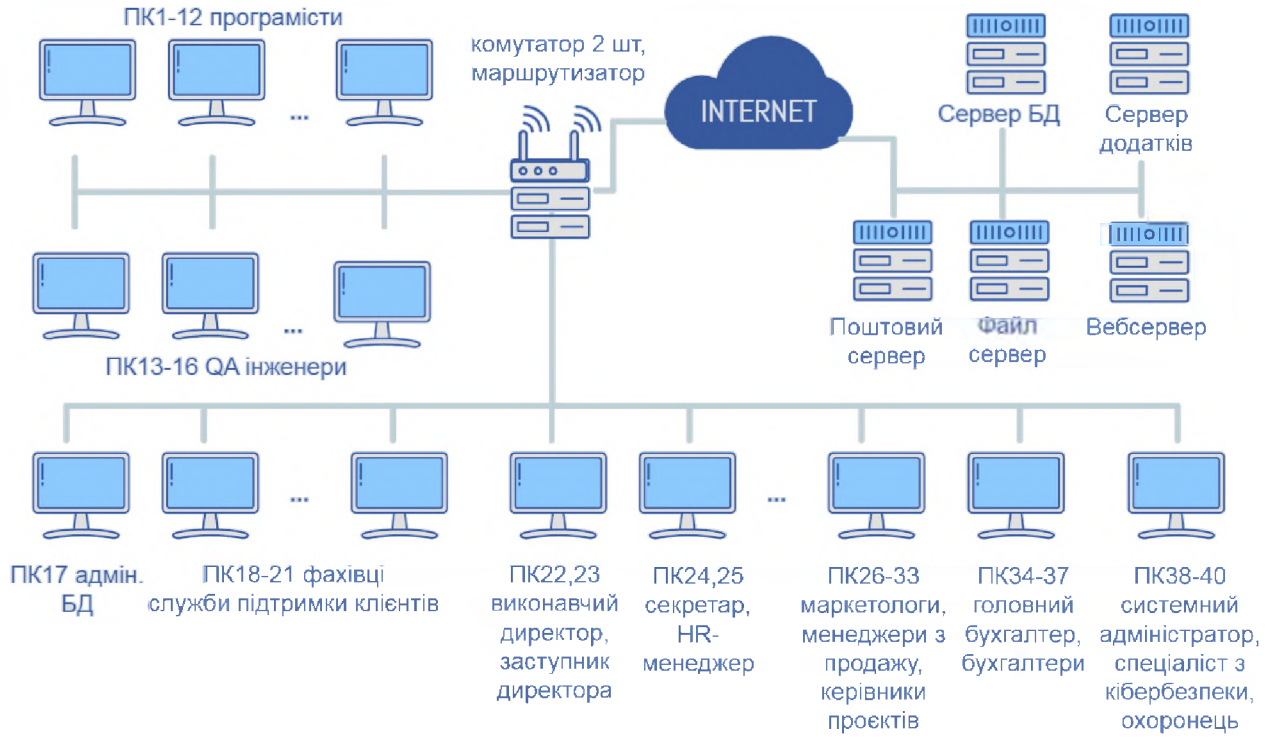

Рисунок 1.2 – Інформаційна система підприємства

1.6 ПЗ інформаційної системи

Програмне забезпечення для розробки програмного забезпечення є ключовим для успішного ведення проєктів у сфері IT.

Інтегровані середовища розробки (IDE) – IntelliJ IDEA

IntelliJ IDEA – це передове інтегроване середовище розробки для Java, Kotlin, Scala та інших мов програмування. Воно надає розширену підтримку фреймворків, інструментів збирання проектів (наприклад, Maven, Gradle) та систем контролю версій.

Переваги:

- покращене автодоповнення коду і аналіз коду на льоту для виявлення потенційних проблем до їх виконання;

- вбудована підтримка різноманітних фреймворків і технологій;

- легкість рефакторингу коду і висока інтеграція з різними інструментами та сервісами;

- підтримка розробки мобільних додатків та вебдодатків.

Системи контролю версій – Git

Git – це вільно розповсюджувана система контролю версій, яка підтримує розподілену роботу, дає можливість ефективно управляти великими проектами.

Переваги:

- забезпечує високий рівень гнучкості у керуванні версіями проєкту;

- підтримує паралельну розробку, дозволяючи кільком розробникам працювати над одним проєктом без конфліктів;

- мінімалізує ризики втрати даних завдяки розподіленій архітектурі;

- велика кількість інструментів та сервісів інтеграції.

Системи управління базами даних (DBMS) – Microsoft SQL Server

Microsoft SQL Server – це комплексна система управління базами даних, що підтримує широкий спектр даних, включаючи структуровані, напівструктуровані та неструктуровані дані.

Переваги:

- висока надійність і масштабованість;

- підтримка транзакцій, що гарантує цілісність даних;

- розширені можливості аналізу та звітності;

- інтеграція з іншими продуктами Microsoft для підвищення продуктивності.

Інструменти для тестування та QA – Selenium

Selenium – це набір інструментів для автоматизації веббраузерів, що дозволяє автоматизувати тестування вебдодатків для різних браузерів і платформ.

Переваги:

- підтримка мультиплатформеності дозволяє виконувати тести на різних операційних системах і веббраузерах;

- можливість писати тести на багатьох мовах програмування, включаючи Java, C#, Python і Ruby;

- велика спільнота та велика кількість навчальних ресурсів і плагінів;

- інтеграція з фреймворками для тестування та системами неперервної інтеграції.

Фреймворки та бібліотеки, специфічні для розробки

Фреймворки та бібліотеки є компонентами, які надають готові до використання рішення для загальних задач програмування, таких як взаємодія з базами даних, розробка вебінтерфейсів, робота з мережею тощо.

Переваги:

- значно прискорюють процес розробки, надаючи стандартні рішення для рутинних задач;

- забезпечують високий рівень абстракції, що дозволяє розробникам зосереджуватися на бізнес-логіці, а не на низькорівневих деталях реалізації;

- сприяють написанню більш безпечного та надійного коду завдяки ретельній оптимізації і тестуванню спільнотою;

- покращують сумісність та інтеграцію різних компонентів програмного забезпечення.

Офісні пакети Microsoft Office 365 та Google Workspace

Microsoft Office 365 є комплексним набором офісних застосунків, що включає Word, Excel, PowerPoint, Outlook та інші інструменти, що базуються на хмарних технологіях.

Google Workspace пропонує схожий набір інструментів, включаючи Документи Google, Таблиці Google, Презентації Google та Gmail, з орієнтацією на співпрацю в реальному часі та інтеграцію з хмарними сервісами.

Переваги:

- обидва пакети сприяють підвищенню продуктивності за рахунок забезпечення широкого спектру інструментів для створення та редагування документів, електронних таблиць та презентацій.

- спрощують співпрацю та спільну роботу над документами в реальному часі, незалежно від місцезнаходження команди.

- інтеграція з хмарними сервісами гарантує доступ до документів з будь-якого пристрою та в будь-який час.

Системи управління проєктами – Microsoft Project

Microsoft Project є однією з провідних систем управління проектами, що надає потужні інструменти для планування, контролю та адміністрування проектів різної складності.

Переваги:

- дозволяє ефективно планувати ресурси, відстежувати прогрес та управляти бюджетами проекту.

- забезпечує високий рівень деталізації і гнучкість у створенні розкладів задач та залежностей між ними.

- інтеграція з іншими продуктами Microsoft Office для звітності та аналізу.

CRM-системи для управління взаємовідносинами з клієнтами

CRM-системи (Customer Relationship Management) допомагають компаніям вести облік взаємовідносин з клієнтами, управління контактами, продажами, взаємодіями з клієнтами та маркетинговими кампаніями.

Переваги:

- забезпечують централізований доступ до інформації про клієнтів, історію їхніх замовлень, взаємодій та уподобань, що дозволяє підвищити ефективність обслуговування та персоналізацію спілкування.

- покращують управління продажами завдяки відстеженню воронки продажів, аналізу продуктивності команди та прогнозуванню продажів.

- автоматизують маркетингові кампанії, спрощуючи сегментацію клієнтів, розсилку електронних листів та вимірювання ефективності маркетингових дій.

- інтеграція з іншими системами та додатками, такими як електронна пошта, календарі та більш спеціалізоване програмне забезпечення, забезпечує широкі можливості для оптимізації робочих процесів.

Інструменти для цифрового маркетингу – Google Analytics

Google Analytics – це вебсервіс від Google, який дозволяє збирати та аналізувати детальну статистику відвідуваності вебсайтів та мобільних додатків. Цей інструмент є незамінним для вимірювання ефективності маркетингових кампаній, розуміння поведінки користувачів та оптимізації веб-ресурсів для покращення їхньої взаємодії з аудиторією.

Переваги:

- Google Analytics надає інформацію про вікові категорії, інтереси, географічне розташування відвідувачів та багато іншого, дозволяючи налаштувати контент та маркетингові стратегії під конкретну цільову аудиторію.

- визначає, звідки приходять відвідувачі, які канали найефективніші для приваблення трафіку та як користувачі взаємодіють з сайтом, що допомагає оптимізувати воронку продажів.

- аналізує, які сторінки сайту найпопулярніші, як довго користувачі перебувають на них, що сприяє покращенню контент-стратегії.

- легко інтегрується з інструментами, такими як Google Ads, Google Search Console, що дозволяє узгоджувати дані та оптимізувати рекламні кампанії.

- можливість створювати налаштовані звіти та інтерактивні панелі управління для відображення найважливішої інформації для прийняття рішень.

Інструменти для моніторингу мережі та безпеки – Wireshark, Norton Security

- Wireshark є потужним аналізатором мережі, який використовується для діагностики проблем у мережах, розробки та аналізу мережевих протоколів.

- Norton Security є комплексним рішенням для захисту від вірусів, шпигунського ПЗ, мережевих атак та інших загроз.

Переваги:

- Wireshark дозволяє детально вивчати мережевий трафік та виявляти проблеми в реальному часі, що є незамінним для мережевих адміністраторів і спеціалістів з безпеки.

- Norton Security забезпечує всебічний захист пристроїв від найрізноманітніших загроз з використанням передових технологій, зокрема, хмарного сканування та поведінкового аналізу.

Системи керування патчами та оновленнями

Це програмне забезпечення автоматизує процес виявлення, завантаження та інсталяції оновлень та патчів для операційних систем і застосунків, забезпечуючи актуальність та безпеку IT-інфраструктури.

Переваги:

- зниження ризику вразливостей шляхом забезпечення своєчасного оновлення програмного забезпечення.

- зменшення ручної роботи для IT-персоналу, звільняючи час для виконання інших завдань.

- забезпечення послідовності та комплексності застосування оновлень в масштабах всієї організації.

Антивірусне та антималварне програмне забезпечення

Антивірусне та антималварне програмне забезпечення захищає комп'ютери та мережі від шкідливих програм, вірусів, троянів, шпигунського ПЗ та інших загроз.

Переваги:

- активний моніторинг та захист в реальному часі від відомих та нових загроз.

- сканування та видалення шкідливих програм, запобігання їх поширенню.

- захист персональних даних та конфіденційної інформації від несанкціонованого доступу.

Системи резервного копіювання

Системи резервного копіювання забезпечують збереження копій важливих даних та систем на випадок їх втрати або пошкодженення через збої обладнання, програмні помилки, вірусні атаки чи інші непередбачені обставини.

Переваги:

- гарантує можливість відновлення даних після будь-яких втрат, забезпечуючи безперервність бізнес-процесів.

- підтримка різноманітних методів копіювання (повне, інкрементне, диференційне) дозволяє оптимізувати процес з огляду на потреби компанії та доступні ресурси.

- заплановане резервне копіювання знижує ризик людської помилки та звільняє час IT-персоналу для виконання інших завдань.

- системи можуть адаптуватися до зростання обсягу даних і зміни структури IT-інфраструктури, забезпечуючи ефективне управління резервними копіями.

1.7 Висновок

Інформаційна система підприємства, яке спеціалізується на розробці програмного забезпечення, представляє собою складну та високо інтегровану структуру, що включає різноманітне програмне забезпечення, інформаційні потоки та кваліфікований персонал.

Інформаційні потоки, які об'єднують технічну документацію, проектну документацію, комерційну та фінансову інформацію, дані про персонал та клієнтів, а також внутрішні комунікації та дані про безпеку. Ці потоки забезпечують плавний обмін інформацією між відділами та сприяють ефективному управлінню проектами та ресурсами компанії.

Програмне забезпечення, яке використовується на підприємстві, включає інтегровані середовища розробки, системи контролю версій, DBMS, інструменти для тестування та QA, фреймворки, а також інструменти для цифрового маркетингу, моніторингу мережі, безпеки, управління патчами та резервного копіювання. Використання цих інструментів дозволяє підприємству підвищити ефективність розробки, забезпечити високий рівень безпеки та оперативно реагувати на зміни у вимогах до продуктів.

Персонал підприємства складається з різних категорій співробітників, включаючи технічних спеціалістів (інженерів-програмістів, QA інженерів), адміністративний персонал, спеціалістів з маркетингу та продажів, фінансового відділу, HR-менеджерів та підтримуючий персонал. Висока кваліфікація та взаємодія між цими відділами є ключовим фактором успіху в розробці та впровадженні програмного забезпечення.

Ефективна інформаційна система підприємства з розробки програмного забезпечення базується на синергії між інформаційними потоками, використовуваним програмним забезпеченням та кваліфікованим персоналом. Це забезпечує не тільки високу продуктивність та конкурентоспроможність

продуктів на ринку, але й гарантує безпеку, надійність та адаптивність до змінних умов ведення бізнесу. Інтеграція та оптимізація інформаційних потоків та програмного забезпечення дозволяють підприємству швидко реагувати на запити клієнтів, ефективно управляти ресурсами та підтримувати високий рівень інноваційності в розробці продуктів.

Забезпечення безперервного професійного розвитку персоналу та інвестиції в оновлення технічної бази та програмного забезпечення є критично важливими для підтримки конкурентоспроможності підприємства. Управління знаннями, ефективна комунікація між відділами та фокус на безпеку даних і систем забезпечують стабільне та безпечне середовище для розробки високоякісного програмного забезпечення, яке відповідає потребам ринку та вимогам користувачів.

РОЗДІЛ 2. СПЕЦІАЛЬНИЙ РОЗДІЛ

2.1 Модель загроз інформації

Модель загроз інформації є ключовим інструментом у процесі ідентифікації потенційних ризиків для інформаційних систем та даних організації. Вона допомагає зрозуміти, які загрози існують, які активи є вразливими, і як можливі атаки можуть бути здійснені проти цих активів.

2.1.1 Ідентифікація активів

Першим кроком є визначення активів, які потребують захисту. Це можуть бути фізичні сервери, мережеве обладнання, бази даних, критичне програмне забезпечення, а також інформація, така як персональні дані клієнтів, фінансові дані, комерційні таємниці тощо.

Таблиця 2.1 – Ідентифіковані активи

Категорія активів	Назва активу	Опис активу
Фізичні активи	Персональні комп'ютери (40 штук)	40 робочих станцій для повсякденної роботи співробітників
Віддалені сервери	Сервер баз даних	Зберігає всі корпоративні бази даних
Віддалені сервери	Поштовий сервер	Обробка, зберігання та доставка електронної пошти
Віддалені сервери	Файловий сервер	Зберігання спільних файлів та документів
Віддалені сервери	Вебсервер	Хостинг корпоративного вебсайту та вебпорталів
Віддалені сервери	Сервер додатків	Запуск та управління бізнес-додатками
Програмні активи	Операційні системи	Операційні системи, встановлені на всіх комп'ютерах та серверах
Програмні активи	Бізнес-додатки та утиліти	Програмне забезпечення для виконання бізнес-функцій
Програмні активи	Системи безпеки	Захист комп'ютерів і мереж від шкідливих програм і атак
Інформаційні активи	Дані користувачів	Інформація про клієнтів, співробітників і партнерів

Інформаційні активи	Корпоративні документи	Договори, фінансові документи, маркетингові матеріали
Інформаційні активи	Документація та програмний код	Технічна документація, програмний код проєктів
Службові активи	Мережева інфраструктура	Маршрутизатори, комутатори, Wi-Fi точки доступу

2.1.2 Визначення загроз

При визначенні загроз для інформаційної системи підприємства, особливо того, яке спеціалізується на розробці та впровадженні програмного забезпечення, важливо провести всебічний аналіз можливих ризиків. Загрози можуть мати різну природу і походження, і їх адекватне розуміння допоможе в розробці ефективних заходів безпеки.

Цей етап передбачає аналіз потенційних загроз для ідентифікованих активів. Загрози можуть бути:

- антропогенні зовнішні (хакери, конкуренти, зловмисники).
- антропогенні внутрішні (співробітники).
- природні (пожежі, повені, землетруси).
- технічні (помилки програмного забезпечення, відмова обладнання).

Аналіз вразливостей

На цьому етапі оцінюються існуючі слабкі місця у захисті активів. Вразливості можуть бути пов'язані з недоліками у фізичному захисті, програмному забезпеченні, політиках безпеки або процедурах обробки даних.

Таблиця 2.2 – Аналіз вразливостей та загроз

Вразливість	**Загроза**	**Порушення властивості інформації**	**Рівень загрози**
Слабкі паролі	Неавторизований доступ	Конфіденційність	Високий
Відсутність шифрування даних	Перехоплення даних	Конфіденційність	Високий
Фізичний доступ до серверної	Крадіжка або пошкодження обладнання	Цілісність, Доступність	Високий

Відсутність регулярного бекапу	Втрата даних при збоях	Доступність	Середній
Недостатні заходи захисту від DDoS	Відмова в обслуговуванні (DDoS)	Доступність	Високий
Ненадійна система верифікації даних	Підробка даних	Цілісність	Середній
Недостатня освіта співробітників щодо фішингу	Фішинг	Конфіденційність	Високий
Слабкі контролі за доступом	Невірний доступ	Конфіденційність	Високий
Недостатній антивірусний захист	Віруси та інші віддалені загрози	Конфіденційність, Цілісність	Високий
Недостатні мережеві заходи безпеки	Атаки на служби	Цілісність	Середній
Неоновлене програмне забезпечення	Використання застарілих версій програмного забезпечення	Цілісність	Середній

2.1.3 Оцінка ризиків

Визначається потенційний вплив кожної загрози на вразливі активи та ймовірність її реалізації. Цей процес дозволяє більш точно зрозуміти потенційні ризики для підприємства, що допомагає приоритизувати заходи безпеки.

2.1.3.1 Оцінка ризиків для загрози "Неавторизований доступ"

Контекст загрози:

"Неавторизований доступ" стосується ситуацій, коли особи, що не мають на це права, здобувають доступ до систем, даних або ресурсів підприємства. Це може включати вхід до систем через слабкі паролі, експлуатацію вразливостей, соціальну інженерію та інші методи обходу захисту.

Вразливість:

- слабкі паролі;

- неналежне управління привілеями;

- відсутність багаторівневої аутентифікації;

- вразливості програмного забезпечення.

Вплив:

- фінансові втрати: високі, особливо якщо викрадені дані мають важливе комерційне значення.

- шкода репутації: висока, оскільки втрата даних може суттєво підірвати довіру клієнтів і партнерів.

- переривання діяльності: середнє до високого, залежно від специфіки атаки та її масштабу.

Ймовірність:

- висока, оскільки неавторизований доступ є однією з найбільш поширених цілей для кіберзлочинців, особливо в компаніях, які не застосовують сучасні методи захисту.

Калькуляція ризику:

- рівень ризику: високий, враховуючи значний потенційний вплив на бізнес та високу ймовірність таких інцидентів.

Стратегії мінімізації ризиків:

1. Поліпшення політик парольної безпеки. Впровадження складних вимог до паролів та регулярна зміна паролів.

2. Багаторівнева аутентифікація. Застосування додаткових рівнів перевірки для критично важливих систем.

3. Управління привілеями. Обмеження доступу до найнеобхіднішого, згідно з принципом найменших привілеїв.

4. Регулярні огляди безпеки та аудити. Виявлення та усунення вразливостей перед тим, як вони будуть експлуатовані.

5. Шифрування даних. Забезпечення захисту даних на всіх етапах їхнього зберігання та передачі.

6. Навчання персоналу. Підвищення обізнаності співробітників щодо загроз і методів їх запобігання, особливо у сфері соціальної інженерії та фішингу.

2.1.3.2 Оцінка ризиків для загрози "Перехоплення даних"

Контекст загрози:

"Перехоплення даних" відноситься до несанкціонованого доступу до інформації, що передається, як в мережі, так і під час зберігання. Це може включати перехоплення мережевого трафіку, доступ до незашифрованих файлів або комунікацій, а також інші методи доступу до конфіденційних даних.

Вразливість:

- відсутність шифрування даних;

- незахищені мережеві канали;

- ненадійні методи зберігання даних.

Вплив:

- фінансові втрати: можуть бути значними, особливо якщо перехоплені дані мають фінансову цінність або використовуються для шахрайства.

- шкода репутації: висока, оскільки компрометація конфіденційності може серйозно підірвати довіру клієнтів та партнерів.

Ймовірність:

- середня до високої, особливо в середовищах, де мережева безпека є недостатньою, або де не використовуються сучасні методи шифрування.

Калькуляція ризику:

- рівень ризику: високий, враховуючи потенційно серйозний вплив на бізнес і відносно високу ймовірність виникнення.

Стратегії мінімізації ризиків:

1. Застосування шифрування. Використання сучасних стандартів шифрування для всіх даних, що передаються та зберігаються.

2. Захист мережі. Встановлення брандмауерів, VPN, і використання захищених протоколів для передачі даних.

3. Регулярний аудит безпеки. Проведення регулярних перевірок безпеки для виявлення і усунення потенційних вразливостей.

4. Освіта співробітників. Навчання персоналу безпечним методам роботи з даними та усвідомленню загроз, пов'язаних з їх перехопленням.

5. Моніторинг та виявлення. Використання інструментів моніторингу та виявлення інцидентів для вчасного реагування на можливі спроби перехоплення.

2.1.3.3 Оцінка ризиків для загрози "Крадіжка або пошкодження обладнання"

Контекст загрози:

"Крадіжка або пошкодження обладнання" означає втрату або ушкодження фізичних активів підприємства, таких як комп'ютери, сервери, мобільні пристрої, та інше обладнання. Ця загроза може бути результатом злочинної діяльності, недбалості, природних катастроф або інших подій.

Вразливість:

- недостатній фізичний захист (наприклад, незахищені приміщення);

- відсутність адекватних заходів контролю доступу;

- відсутність належних процедур моніторингу та реагування.

Вплив:

- фінансові втрати: високі, через вартість заміни обладнання та потенційну втрату бізнес-даних.

- шкода репутації: середня до високої, особливо якщо втрата обладнання призводить до розголошення конфіденційної інформації.

- переривання діяльності: високе, залежно від того, наскільки критичне обладнання було втрачено або пошкоджено.

Ймовірність:

- середня до високої, залежно від розташування, заходів безпеки, та виду обладнання.

Калькуляція ризику:

- рівень ризику: високий, враховуючи потенційний значний вплив та можливу ймовірність події.

Стратегії мінімізації ризиків:

1. Покращення фізичного захисту. Встановлення надійних замків, охоронних систем, та систем відеоспостереження.

2. Контроль доступу. Застосування систем контролю доступу для обмеження входу в критичні зони лише для авторизованого персоналу.

3. Страхування обладнання. Покриття потенційних фінансових втрат через страхування важливого обладнання.

4. Регулярні аудити безпеки. Періодичні перевірки заходів безпеки та виявлення можливих вразливостей.

5. Моніторинг та реагування. Використання систем моніторингу для виявлення незаконних спроб доступу або неавторизованих рухів обладнання.

2.1.3.4 Оцінка ризиків для загрози "Втрата даних при збоях"

Контекст загрози:

"Втрата даних при збоях" відноситься до неочікуваних подій, які можуть призвести до втрати цінної інформації, таких як технічні збої, збій обладнання, помилки програмного забезпечення, або збій електроживлення. Ці події можуть серйозно вплинути на операційну здатність бізнесу і призвести до довготривалих наслідків.

Вразливість:

- відсутність регулярного бекапу;
- недостатнє відновлення після катастроф;
- застаріле або ненадійне обладнання;
- відсутність редундантності систем.

Вплив:

- фінансові втрати: високі, включаючи витрати на відновлення даних та можливу втрату доходу через перерву у роботі.
- шкода репутації: середня до високої, особливо якщо збій впливає на обслуговування клієнтів або призводить до втрати клієнтських даних.
- переривання діяльності: високе, особливо якщо критичні бізнес-процеси залежать від постраждалих систем.

Ймовірність:

- середня до високої, залежно від стану технічного обслуговування та інфраструктури.

Калькуляція ризику:

- рівень ризику: високий, з огляду на потенційний серйозний вплив на оперативну діяльність і можливу високу ймовірність події.

Стратегії мінімізації ризиків:

1. Регулярні бекапи. Налаштування автоматизованих регулярних резервних копій усіх критичних даних.

2. План відновлення після катастроф. Розробка і тестування планів відновлення для гарантії швидкого відновлення після збоїв.

3. Оновлення обладнання. Заміна застарілого або схильного до збоїв обладнання на більш сучасне і надійне.

4. Редундантність систем. Впровадження редундантних систем для забезпечення неперервності роботи при відмові одного з компонентів.

5. Моніторинг стану систем. Використання інструментів моніторингу для раннього виявлення ознак збоїв або проблем з обладнанням.

6. Навчання персоналу. Забезпечення, що співробітники знають, як коректно використовувати обладнання та виконувати процедури бекапу.

2.1.3.5 Оцінка ризиків для загрози "Відмова в обслуговуванні (DDoS)"

Контекст загрози:

Атака типу "Відмова в обслуговуванні" (DDoS) відбувається, коли зловмисники навмисно навантажують мережеві або серверні ресурси таким чином, що система не може обробити законні запити користувачів. Це може включати переповнення мережі, серверів, або інфраструктури програмного забезпечення, що призводить до зупинки сервісів або веб-сайтів.

Вразливість:

- відсутність захисту від DDoS-атак;

- недостатньо розширювана інфраструктура;

- відсутність географічного розподілу серверів.

Вплив:

- фінансові втрати: можуть бути значними, особливо для бізнесів, що залежать від онлайн-послуг, як електронна комерція або надання цифрових послуг.

- шкода репутації: висока, оскільки тривалі перерви в роботі можуть підірвати довіру клієнтів.

- переривання діяльності: високе, зупинка послуг може мати далекосяжні наслідки для операційної діяльності.

Ймовірність:

- середня до високої, залежно від видимості та вразливості організації в Інтернеті.

Калькуляція ризику:

- рівень ризику: високий, враховуючи потенціал впливу на бізнес і середню до високої ймовірність атаки.

Стратегії мінімізації ризиків:

1. Захист від DDoS-атак. Впровадження спеціалізованих рішень для захисту від DDoS, які можуть включати скейлінг ресурсів при великому навантаженні, фільтрацію трафіку, та ізоляцію атакуючих запитів.

2. Планування пропускної спроможності. Забезпечення достатньої пропускної спроможності мережі для обробки неочікуваних піків трафіку.

3. Резервне копіювання та редундантність. Впровадження резервних та географічно розподілених серверів для забезпечення неперервності роботи.

4. План відновлення після катастроф. Розробка плану дій для швидкого відновлення послуг після DDoS-атак.

5. Постійний моніторинг та аналіз. Моніторинг мережевого трафіку та швидке реагування на аномалії, що можуть вказувати на початок DDoS-атаки.

2.1.3.6 Оцінка ризиків для загрози "Підробка даних"

Контекст загрози:

"Підробка даних" означає несанкціоноване або зловмисне змінення даних з метою обману або шахрайства. Це може включати зміну фінансових

документів, маніпуляцію базами даних, фальсифікацію електронних записів або будь-які інші дії, що спотворюють істинність інформації.

Вразливість:

- недостатній контроль цілісності даних;

- відсутність або слабкість цифрових підписів та механізмів верифікації;

- слабка політика доступу до критичних даних.

Вплив:

- фінансові втрати: можуть бути значними, зокрема через шахрайство або юридичні наслідки внаслідок недостовірної інформації.

- шкода репутації: висока, особливо якщо підроблені дані призводять до громадського скандалу або юридичних проблем.

- юридичні наслідки: можливі судові позови, штрафи та інші санкції з боку регулюючих органів.

Ймовірність:

- середня, залежно від заходів безпеки, що вже існують у компанії, та рівня доступу до чутливої інформації.

Калькуляція ризику:

- рівень ризику: високий, з огляду на потенційні наслідки для бізнесу та ймовірність подій.

Стратегії мінімізації ризиків:

1. Верифікація та цифрові підписи. Впровадження строгих механізмів перевірки та автентифікації даних, зокрема цифрових підписів для важливих документів.

2. Контроль цілісності. Регулярний моніторинг і аудит даних для виявлення та реагування на несанкціоновані зміни.

3. Обмеження доступу. Застосування принципу найменших привілеїв для забезпечення доступу до даних тільки для авторизованих осіб.

4. Навчання персоналу. Проведення регулярних тренінгів з кібербезпеки для підвищення обізнаності співробітників щодо потенційних загроз і методів запобігання підробці даних.

2.1.3.7 Оцінка ризиків для загрози "Фішинг"

Контекст загрози:

"Фішинг" – це вид соціальної інженерії, де зловмисники намагаються обманом змусити жертву надати конфіденційну інформацію, таку як логіни, паролі, банківські дані, або інші персональні дані, часто через підроблені електронні листи, вебсайти або повідомлення.

Вразливість:

- недостатнє навчання співробітників щодо методів фішингу;
- відсутність ефективних систем фільтрації пошти та моніторингу;
- слабке або відсутнє багаторівневе аутентифікація.

Вплив:

- фінансові втрати: від помірних до високих, в залежності від вкраденої інформації.
- шкода репутації: висока, особливо якщо через фішинг стаються масштабні витоки даних.
- юридичні наслідки: можливі, особливо якщо компрометація веде до порушення законів про захист даних.

Ймовірність:

- висока, оскільки фішинг є одним з найпоширеніших методів кібератаки, доступний для широкого спектру зловмисників.

Калькуляція ризику:

- рівень ризику: високий, з огляду на широку поширеність фішингу та значний потенційний вплив.

Стратегії мінімізації ризиків:

1. Навчання та освіта співробітників. Регулярні тренінги щодо розпізнавання фішингових атак, особливо ознак підроблених електронних листів та вебсайтів.

2. Захист електронної пошти. Використання рішень для фільтрації спаму та фішингу, які можуть виявляти підроблені або шкідливі повідомлення.

3. Багаторівнева аутентифікація. Запровадження багаторівневої аутентифікації для усіх систем, особливо тих, що містять чутливі або важливі дані.

4. Моніторинг і відповіді на інциденти. Встановлення процесів для швидкого реагування на підозрілі дії, що можуть свідчити про спробу фішингу.

5. Комунікаційна стратегія. Розробка чіткої процедури зв'язку у випадках підозрілих запитів або повідомлень для зменшення ризику шахрайства.

2.1.3.8 Оцінка ризиків для загрози "Невірний доступ"

Контекст загрози:

"Невірний доступ" відноситься до ситуацій, коли особи, що мають деякі обмежені права доступу, отримують доступ до ресурсів або даних, що перевищують ці обмеження через помилки в налаштуваннях системи безпеки, програмні помилки, або через соціальну інженерію.

Вразливість:

- недоліки в налаштуваннях системи управління доступом;

- відсутність достатнього контролю за привілеями;

- слабка політика аутентифікації та авторизації.

Вплив:

- фінансові втрати: можуть бути помірними до високих, залежно від чутливості доступної інформації.

- шкода репутації: середня до високої, залежно від публічності інциденту.

- переривання діяльності: можливе, якщо невірний доступ впливає на критичні системи або процеси.

Ймовірність:

- середня, враховуючи, що помилки в налаштуваннях та системах контролю можуть легко виникнути в складних IT-середовищах.

Калькуляція ризику:

- Рівень ризику: середній, з огляду на потенційний вплив та ймовірність.

Стратегії мінімізації ризиків:

1. Посилення контролю за привілеями. Впровадження суворих політик управління доступом, що базуються на принципі найменших привілеїв.

2. Багаторівнева аутентифікація. Використання багаторівневої аутентифікації для важливих систем і даних для додаткового захисту.

3. Регулярні аудити та перевірки. Проведення регулярних аудитів систем безпеки та доступу для виявлення та виправлення недоліків.

4. Обмеження адміністративного доступу. Забезпечення, щоб адміністративний доступ надавався лише тим, хто дійсно потребує його для виконання своїх обов'язків.

5. Навчання персоналу. Проведення регулярних тренінгів для співробітників з питань безпеки, зокрема на тему важливості налаштувань безпеки та контролю доступу.

2.1.3.9 Оцінка ризиків для загрози "Віруси та інші віддалені загрози"

Контекст загрози:

Загрози, такі як віруси, трояни, шпигунське програмне забезпечення, і ransomware, є формами зловмисного програмного забезпечення, що призначені для завдання шкоди або викрадення даних. Ці загрози можуть бути передані через інфіковані файли, мережеві атаки, електронні листи та інші цифрові канали.

Вразливість:

- недостатній антивірусний захист;

- відсутність регулярних оновлень програмного забезпечення та операційних систем;

- слабка інформаційна безпека і політики використання інтернету.

Вплив:

- фінансові втрати: високі, можуть включати витрати на відновлення систем, втрату доходу.

- шкода репутації: висока, особливо якщо атака призводить до значного витоку конфіденційної інформації.

- переривання діяльності: може бути від помірного до високого, залежно від масштабу інфекції та здатності швидко реагувати на неї.

Ймовірність:

- висока, враховуючи широкий спектр джерел інфекцій та постійно зростаючу кількість нових типів зловмисного програмного забезпечення.

Калькуляція ризику:

- рівень ризику: високий, через високу ймовірність виникнення та серйозні потенційні наслідки.

Стратегії мінімізації ризиків:

1. Антивірусний захист. Встановлення та оновлення надійного антивірусного програмного забезпечення на всіх кінцевих точках і серверах.

2. Регулярні оновлення. Автоматичне оновлення операційних систем, додатків та іншого програмного забезпечення для закриття відомих вразливостей.

3. Освіта співробітників. Проведення регулярних навчань для співробітників з питань розпізнавання підозрілих електронних листів, вебсайтів та повідомлень.

4. Моніторинг та виявлення. Впровадження систем моніторингу та виявлення інцидентів для вчасного реагування на зловмисні дії.

5. Резервне копіювання даних. Регулярне створення резервних копій важливих даних та їх зберігання в безпечному місці.

6. Розробка плану реагування на інциденти. Забезпечення наявності чіткого плану дій для реагування на випадки зараження зловмисним програмним забезпеченням.

2.1.3.10 Оцінка ризиків для загрози "Атаки на служби"

Контекст загрози:

"Атаки на служби" (Service Attacks) включають спроби експлуатації вразливостей у вебслужбах, серверах, базах даних або інших мережевих сервісах. Це може включати атаки типу SQL injection, Cross-Site Scripting (XSS), Denial-of-Service (DoS), і інші, які цілять на порушення нормального

функціонування служби чи отримання несанкціонованого доступу до системних ресурсів.

Вразливість:

- недоліки у програмному забезпеченні, такі як застарілі версії або некоректне налаштування;

- відсутність достатнього моніторингу та відповіді на інциденти;

- слабкі механізми аутентифікації та контролю доступу.

Вплив:

- фінансові втрати: можуть бути високими, особливо якщо атака призводить до зупинки важливих бізнес-процесів або витоку конфіденційної інформації.

- шкода репутації: висока, ушкодження репутації через недостатню безпеку або перерви в обслуговуванні.

- переривання діяльності: високе, залежно від тривалості та обсягу атаки.

Ймовірність:

- Середня до високої, залежно від рівня захисту і актуальності програмного забезпечення.

Калькуляція ризику:

- рівень ризику: високий, через потенційні серйозні наслідки для операційної діяльності і бізнесу в цілому.

Стратегії мінімізації ризиків:

1. Оновлення та патчування. Регулярне оновлення програмного забезпечення та оперативне застосування патчів безпеки для закриття відомих вразливостей.

2. Вдосконалення моніторингу. Використання інструментів моніторингу для виявлення аномальної активності та швидкого реагування на потенційні атаки.

3. Фільтрація трафіку. Застосування межових фаєрволів та систем виявлення вторгнень для фільтрації потенційно шкідливого трафіку.

4. Розробка плану реагування на інциденти. Забезпечення наявності чіткого плану дій для відповіді на інциденти безпеки.

5. Навчання персоналу. Освіта співробітників щодо основних практик безпеки та важливості виконання політик безпеки.

6. Резервне копіювання та редундантність. Забезпечення резервного копіювання важливих даних та редундантності систем для зниження ризиків пов'язаних із зупинкою служб.

2.1.3.11 Оцінка ризиків для загрози "Використання застарілих версій програмного забезпечення"

Контекст загрози:

Використання застарілих версій програмного забезпечення може відкрити двері для численних вразливостей, оскільки старі версії часто не отримують оновлень безпеки і можуть містити відомі баги, які зловмисники можуть використовувати для проведення атак.

Вразливість:

- відсутність оновлень безпеки для старих версій програмного забезпечення;

- слабке управління патчами та оновленнями;

- недостатня увага до ризиків, пов'язаних із старим програмним забезпеченням.

Вплив:

- фінансові втрати: можуть бути значними у разі успішної кібератаки, яка веде до витоку даних, шахрайства, або вимагання викупу.

- шкода репутації: висока, особливо якщо витік даних або інші інциденти безпеки стають відомими публічно.

- переривання діяльності: може бути від помірного до високого, залежно від серйозності атаки та часу, необхідного для відновлення.

Ймовірність:

- висока, оскільки вразливості в застарілих системах часто добре відомі у кіберзлочинному світі та широко використовуються.

Калькуляція ризику:

- рівень ризику: високий, через високу ймовірність та серйозний потенційний вплив атак.

Стратегії мінімізації ризиків:

1. Регулярне оновлення програмного забезпечення. Забезпечення, що всі системи та програмне забезпечення регулярно оновлюються до останніх версій, які підтримуються виробником.

2. Політика управління патчами. Впровадження строгих процедур для виявлення, тестування та встановлення оновлень безпеки у відповідні терміни.

3. Аудит і моніторинг програмного забезпечення. Регулярний перегляд та аудит використовуваного програмного забезпечення для ідентифікації застарілих або непідтримуваних продуктів.

4. Освіта та навчання персоналу. Підвищення обізнаності серед співробітників щодо ризиків, пов'язаних із використанням застарілого програмного забезпечення.

5. Розробка плану відновлення після аварій. Забезпечення наявності ефективного плану відновлення для мінімізації наслідків можливих інцидентів, пов'язаних із застарілим ПЗ.

2.1.4 Узагальнена стратегія мінімізації ризиків

Узагальнити «Стратегії мінімізації ризиків» можна наступним:

– Регулярні оновлення програмного забезпечення та патчування:

Впровадження строгих процедур оновлення програмного забезпечення для забезпечення того, що всі системи залишаються захищеними від відомих вразливостей.

– Розробка та впровадження політик безпеки:

Створення та дотримання чітких політик і процедур безпеки, що включають управління доступом, моніторинг та реагування на інциденти.

– Багаторівнева аутентифікація:

Використання багаторівневих методів аутентифікації для забезпечення додаткового рівня захисту, особливо для систем, що зберігають чутливу або критичну інформацію.

– Освіта та тренінги співробітників:

Проведення регулярних навчань для співробітників, щоб підвищити обізнаність щодо потенційних кіберзагроз і правильних практик кібербезпеки.

– Моніторинг та виявлення інцидентів:

Використання сучасних інструментів для моніторингу мережі та систем, що дозволяє швидко виявляти та реагувати на аномальні дії або потенційні загрози.

– Резервне копіювання та відновлення даних:

Забезпечення регулярного резервного копіювання важливих даних та розробка ефективного плану відновлення після аварій для мінімізації переривань у роботі.

– Фізичний захист інфраструктури:

Забезпечення адекватного фізичного захисту критичних інфраструктурних компонентів, включаючи серверні кімнати та центри даних.

– Розробка плану реагування на інциденти:

Мати чітко визначений план реагування на інциденти, щоб швидко та ефективно вирішувати безпекові проблеми, які можуть виникнути.

Застосування такої моделі загроз та оцінки ризиків інформації дозволяє підприємству забезпечити комплексний захист своїх активів, знизити потенційні ризики та підтримувати надійне та безпечне інформаційне середовище.

2.2 Модель порушника

Модель порушника у контексті кібербезпеки визначає потенційні мотивації, здатності та можливості зловмисників, які можуть атакувати організацію.

Типи порушників:

Зловмисні програмісти. Індивідуали, які мають технічні навички для створення та розповсюдження зловмисного програмного забезпечення.

Хакерські групи. Організовані групи, що проводять цілеспрямовані атаки для крадіжки даних, вимагання, або політично мотивованого втручання.

Корпоративні шпигуни. Індивіди або компанії, що намагаються отримати конкурентну перевагу через крадіжку таємної інформації.

Державні агенти. Агенти або організації, які працюють від імені урядів, здійснюючи кібератаки для досягнення національної безпеки або геополітичних цілей.

Недобросовісні співробітники. Співробітники або колишні працівники, які використовують свій доступ для шкідливих дій проти компанії.

Рівень навичок:

- низький: використання готових наборів інструментів для атак;
- середній: модифікація існуючих інструментів, базове програмування;
- високий: розробка власних складних атак.

Спосіб доступу:

- віддалений доступ: через Інтернет;
- локальний доступ: через корпоративну мережу або фізичний доступ до приміщень;
- змішаний доступ: використання комбінації віддаленого та локального доступу.

Місце здійснення атаки:

- внутрішній: зсередини організації.
- зовнішній: ззовні організації, можливо з іншої країни або регіону.

Рівень злому:

- поверхневий: обмежений доступ до системи;
- глибокий: повний контроль над системою або мережею.

Таблиця 2.3 – Модель порушника

Зловмисник	**Спеціалізація**	**Мотивація**	**Методи та засоби атак**	**Рівень навичок**	**Спосіб доступу**	**Місце здійснення атаки**	**Рівень злому**	**Вплив на систему**
Хакерська група	DDoS, фішинг, вебатаки	Фінансова вигода, політичний вплив	Фішингові емейли, експлуатація вразливостей	Високий	Віддалений	Зовнішній	Поверхневий / Глибокий	Високий
Корпоративний шпигун	Крадіжка торгових секретів	Конкурентна перевага	Шпигунське ПЗ, соціальна інженерія	Середній	Змішаний	Зовнішній / Внутрішній	Поверхневий	Середній до високого
Недобросовісний співробітник	Внутрішні атаки, саботаж	Особисті мотиви, помста	Крадіжка даних, логічні бомби	Середній	Локальний	Внутрішній	Поверхневий / Глибокий	Середній до високого
Державний агент	Кібервійна, розвідувальні атаки	Національна безпека, геополітика	Розробка складних вірусів, використання 0-day вразливостей	Високий	Віддалений	Зовнішній	Глибокий	Дуже високий
Зловмисні програмісти	Розповсюдження вірусів, троянів	Фінансова вигода	Масове розповсюдження шкідливого ПЗ	Високий	Віддалений	Зовнішній / Внутрішній	Поверхневий / Глибокий	Високий

2.3 Визначення критеріїв захищеності та надання рекомендацій щодо реалізації системи захисту ІКС підприємства

Профіль захищеності 3.КЦД.1 відповідно до документа НД ТЗІ 2.5-005-99 визначає вимоги до забезпечення безпеки в автоматизованих системах, що містять конфіденційну інформацію.

3.КЦД.1 = { КД-2, КО-1, КВ-1, ЦД-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }

КД-2. Базова довірча конфіденційність;

КО-1. Повторне використання об'єктів;

КВ-1. Мінімальна конфіденційність при обміні;

ЦД-1. Мінімальна довірча цілісність;

ЦО-1. Обмежений відкат;

ЦВ-1: Мінімальна цілісність при обміні;

ДР-1. Квоти;

ДВ-1. Ручне відновлення;

НР-2. Захищений журнал;

НИ-2. Одиночна ідентифікація і автентифікація;

НК-1. Однонаправлений достовірний канал;

НО-2. Розподіл обов'язків адміністраторів;

НЦ-2. КЗЗ з гарантованою цілісністю;

НТ-2. Самотестування при старті;

НВ-1: Автентифікація вузла.

Ці функціональні критерії захищеності визначають вимоги до автоматизованих систем класу 3, що містять конфіденційну інформацію, та дозволяють забезпечити високий рівень захищеності інформації в цих системах.

Система захисту має відповідати наступним вимогам:

– Захист від несанкціонованого доступу;

Налаштування системи для захисту від несанкціонованого доступу є критично важливим для забезпечення безпеки інформації та обладнання. Ця

секція документації описує процедури і технології, які повинні бути впроваджені для ідентифікації, аутентифікації та контролю доступу до системних ресурсів.

Ідентифікація та аутентифікація користувачів

Кожен користувач системи повинен мати унікальний ідентифікатор (ID користувача), який використовується для відстеження та контролю його дій в системі. Процес аутентифікації повинен включати використання сильних паролів, які містять мінімум 12 символів, з обов'язковим включенням цифр, великих та малих літер, та спеціальних символів. Рекомендується використання багаторівневої аутентифікації (MFA), що може включати одноразові паролі, біометричні дані, або електронні ключі доступу.

Контроль доступу

Системи контролю доступу мають бути налаштовані на основі принципу найменших привілеїв, де користувачі отримують мінімально необхідний доступ до ресурсів для виконання своїх робочих обов'язків. Налаштування доступу повинні бути підтверджені та переглянуті системним адміністратором на регулярній основі, щоб забезпечити актуальність прав доступу. Всі спроби доступу до ресурсів повинні логуватися для подальшого аналізу та аудиту.

Моніторинг та реагування на інциденти

Система моніторингу повинна бути впроваджена для нагляду за всіма вхідними та вихідними підключеннями до мережі. Логи безпеки мають бути аналізовані в реальному часі для виявлення незвичайних або підозрілих дій. У випадку виявлення несанкціонованого доступу, система повинна автоматично блокувати доступ користувача та повідомляти системного адміністратора для негайного реагування.

Процедури відновлення

У випадку виявлення несанкціонованого доступу необхідно мати чітко визначену процедуру відновлення, яка включає кроки по відновленню системи та даних до стабільного стану. Процедура повинна також включати аналіз інциденту для виявлення його причин та впровадження заходів для запобігання подібних інцидентів у майбутньому.

– Захист мережі від вторгнень;

Захист мережі від вторгнень є ключовим аспектом загальної стратегії безпеки будь-якої організації. Ефективне налаштування захисту мережі дозволяє ідентифікувати, запобігати та реагувати на потенційні загрози, що забезпечує неперервність бізнесу та захист даних.

Встановлення систем виявлення та запобігання вторгненням (IDS/IPS)

Системи IDS (виявлення вторгнень) та IPS (запобігання вторгненням) повинні бути розміщені в стратегічно важливих точках мережі для моніторингу вхідного і вихідного трафіку на наявність шкідливих активностей або аномалій. Системи повинні налаштовуватися на автоматичне блокування підозрілого трафіку та відразу ж сповіщати системних адміністраторів про будь-які інциденти.

Впровадження фаєрволів

Фаєрволи мають бути встановлені на всіх периметрах мережі, включно з крайніми точками з'єднання з Інтернетом. Фаєрволи повинні бути налаштовані для обмеження доступу відповідно до політики безпеки організації, з чітким визначенням дозволених та заборонених сервісів, протоколів та IP-адрес. Налаштування фаєрволів має регулярно переглядатися і оновлюватися з метою забезпечення актуальності захисту.

Використання VPN та шифрування

Для захисту даних, що передаються через публічні мережі, використання віртуальних приватних мереж (VPN) і шифрування повинно бути обов'язковим. VPN забезпечує захищений канал для комунікації даних між віддаленими користувачами та корпоративними ресурсами, тоді як шифрування гарантує, що дані залишаться конфіденційними та недоступними для сторонніх осіб.

Регулярний аудит та тестування безпеки

Регулярний аудит налаштувань безпеки та виконання тестувань на проникнення є важливими для ідентифікації потенційних слабких місць у захисті мережі. Тестування на проникнення дозволяє моделювати атаки з метою

перевірки ефективності існуючих заходів безпеки та виявлення необхідності їх удосконалення.

– Захист від витоку інформації;

Захист від витоку інформації вимагає комплексного підходу, що включає впровадження технічних, організаційних та правових заходів. Ця частина документації визначає ключові технології та процедури, які мають бути імплементовані для запобігання несанкціонованому доступу та розповсюдженню конфіденційної інформації.

Шифрування даних

Для забезпечення конфіденційності даних, всі чутливі дані, які зберігаються або передаються через мережу, повинні бути зашифровані за допомогою сучасних алгоритмів шифрування. Шифрування даних повинно охоплювати файли даних, бази даних, електронні листи та інші форми передачі даних. Використання сертифікованих криптографічних модулів та бібліотек є обов'язковим.

Контроль витоку даних (DLP)

Системи DLP повинні бути впроваджені для моніторингу, контролю та запобігання передачі конфіденційної інформації за межі корпоративної мережі. DLP системи повинні бути налаштовані на ідентифікацію та блокування передачі чутливих даних через електронну пошту, веб-трафік, і файлообмінні сервіси.

Управління цифровими правами (DRM)

Використання технологій DRM дозволяє контролювати та обмежувати використання інформації, що включає перегляд, друк, зміну та розповсюдження документів. DRM надає можливість впровадження політик безпеки, які забезпечують виконання правил обробки та доступу до інформації.

Маркування даних

Маркування даних повинно бути впроваджено для класифікації інформації за рівнями конфіденційності. Автоматизовані інструменти повинні використовуватись для маркування нових та існуючих документів згідно з внутрішньою політикою безпеки.

Перевірка та аудит

Регулярні аудити та перевірки повинні проводитися для виявлення можливих витоків інформації. Логи доступу та діяльності користувачів повинні аналізуватись для виявлення аномалій або незвичайних патернів, які можуть вказувати на спроби витоку інформації.

Правова та організаційна підтримка

Політики безпеки та процедури повинні бути підтримані правовими заходами, включаючи підписання угод про нерозголошення (NDA) співробітниками та контрагентами. Персонал повинен проходити регулярне навчання з питань захисту інформації та знати основні принципи роботи з конфіденційними даними.

– Захист від вірусів та шкідливих програм;

Захист від вірусів та шкідливих програм є ключовим аспектом загальної стратегії безпеки організації. Ефективне використання антивірусного програмного забезпечення, постійні оновлення та проактивний моніторинг системи допомагають мінімізувати ризики, пов'язані зі шкідливими програмами.

Встановлення антивірусного програмного забезпечення

Встановіть надійне антивірусне програмне забезпечення на всі кінцеві точки та сервери. Антивірусні програми повинні бути налаштовані на автоматичне виконання регулярних сканувань системи, а також на моніторинг в реальному часі для негайного виявлення та видалення шкідливих програм. Вибирайте рішення, що включає широкий спектр захисту від різноманітних типів загроз.

Регулярні оновлення програмного забезпечення

Необхідно забезпечити автоматичне оновлення антивірусного програмного забезпечення та всіх інших програм і операційних систем для захисту від відомих вразливостей. Налаштувати систему на автоматичне отримання та встановлення оновлень безпеки, які можуть запобігти використанню вразливостей зловмисниками.

Застосування антивірусних політик

Розробити та імплементувати політики безпеки, які визначають обов'язкове використання антивірусних програм на всіх пристроях, які підключаються до корпоративної мережі. Ці політики мають включати вимоги до антивірусного захисту, процедури поведінки користувачів у випадку виявлення вірусів та шкідливих програм.

Проведення регулярних аудитів безпеки

Регулярно проводити аудит безпеки для перевірки ефективності встановлених антивірусних заходів. Аудити допоможуть виявити потенційні слабкі місця в захисті та необхідність удосконалення існуючих методів захисту.

Навчання персоналу

Персонал повинен регулярно проходити тренінги для співробітників щодо основ кібербезпеки, зокрема, розпізнавання шкідливих електронних листів, безпечного використання Інтернету та належного поводження з непідозрілими файлами. Освіченість персоналу зменшує ризики вірусних атак та інших кіберзагроз.

– Захист фізичної інфраструктури;

Фізичний захист інфраструктури є невід'ємною частиною загальної стратегії безпеки організації. Він включає в себе заходи для захисту апаратних засобів, серверних кімнат, даних та персоналу від несанкціонованого доступу, пошкоджень або інших загроз.

Контроль доступу

Забезпечення надійного контролю доступу до всіх фізичних об'єктів, де зберігаються важливі апаратні та інформаційні ресурси. Використання електронних систем контролю доступу, таких як картки доступу, біометричні системи (відбитки пальців, розпізнавання обличчя), може допомогти обмежити вхід в чутливі зони лише для уповноважених осіб. Всі події входу та виходу повинні бути записані для подальшого аналізу і аудиту.

Відеоспостереження

Встановити систему відеоспостереження для моніторингу важливих об'єктів та периметра організації. Відеокамери повинні розміщуватися у

стратегічних локаціях для огляду всіх доступних входів/виходів та чутливих зон. Записи з камер повинні зберігатися для можливості перегляду у випадку безпекових інцидентів.

Фізичне забезпечення серверних кімнат

Серверні кімнати, де зберігаються основні мережеві та серверні ресурси, повинні мати посилений фізичний захист. Це включає в себе не лише контроль доступу, але й заходи проти фізичного втручання, такі як водонепроникні та вогнетривкі стіни, спеціалізовані замки та засоби безпеки для захисту від стихійних лих.

Захист від природних стихій

Забезпечити заходи захисту від природних стихій, таких як пожежі, повені, землетруси. Це може включати встановлення датчиків диму та тепла, системи гасіння пожеж, а також виконання спеціального проектування споруд для стійкості до природних катастроф.

Плани евакуації та надзвичайних ситуацій

Розробити та впровадити плани евакуації для усіх співробітників у випадку надзвичайних ситуацій. Спланувати регулярні тренінги та навчання для забезпечення готовності персоналу діяти ефективно та безпечно під час таких подій.

– Забезпечення цілісності та конфіденційності даних;

Забезпечення цілісності та конфіденційності даних є фундаментальними компонентами інформаційної безпеки. Ця документація описує важливі налаштування та практики, які повинні бути впроваджені для захисту даних від несанкціонованих змін, доступу та інших форм зловмисного використання.

Шифрування даних

Використання шифрування є критично важливим для захисту конфіденційності даних під час зберігання та передачі. Всі чутливі дані, включаючи персональну інформацію, фінансові записи та інші конфіденційні документи, повинні бути зашифровані за допомогою сучасних криптографічних

алгоритмів. Шифрування повинно охоплювати дані, які перебувають у стані спокою, та дані, які передаються по мережі.

Цілісність даних

Заходи для забезпечення цілісності даних включають використання контрольних сум, хеш-функцій та цифрових підписів. Ці технології дозволяють виявляти будь-які несанкціоновані або випадкові зміни в даних. Системи повинні бути налаштовані на автоматичне виявлення та сповіщення про будь-які інциденти, що впливають на цілісність даних.

Управління доступом

Контроль доступу до даних повинен базуватися на принципах найменших привілеїв, де користувачам надається лише той доступ, який необхідний для виконання їхніх робочих завдань. Використання ролей і політик доступу допомагає запобігти несанкціонованому доступу та забезпечує відстеження дій користувачів у системі.

– Забезпечення доступності.

Аудит та моніторинг

Регулярний аудит та моніторинг доступу до даних та їх використання є необхідними для виявлення та реагування на інциденти безпеки. Логи доступу повинні зберігатися в безпечному місці та аналізуватися для виявлення незвичайних або підозрілих дій.

Резервне копіювання даних

Систематичне резервне копіювання даних є одним з основних методів забезпечення доступності. Важливо регулярно створювати резервні копії всіх критичних даних, які зберігаються на окремих фізичних носіях або в хмарних сховищах. Резервні копії мають бути доступні для швидкого відновлення в разі втрати даних через апаратні збої, програмні помилки, або зловмисні атаки.

Відновлення після аварії

Розробка і тестування плану відновлення після аварії (disaster recovery plan) є важливими для забезпечення можливості відновлення системи та її компонентів після серйозних інцидентів. План повинен описувати детальні

кроки для відновлення операційних систем, баз даних, програмного забезпечення та апаратних засобів.

Кластеризація та висока доступність

Використання кластерів серверів та інших технологій високої доступності може забезпечити неперервність служб за рахунок автоматичного переключення на резервні системи у випадку збою первинних систем. Такі технології включають балансування навантаження, реплікацію даних, та автоматизоване відновлення послуг.

Моніторинг системи

Постійний моніторинг стану системних ресурсів, таких як використання ЦПУ, пам'яті, дискового простору та мережевої активності, дозволяє вчасно виявляти потенційні проблеми, що можуть призвести до збоїв системи. Системи моніторингу повинні бути налаштовані таким чином, щоб сповіщати адміністраторів про аномальні стани, що вимагають втручання.

Підтримка обладнання та програмного забезпечення

Регулярне обслуговування та оновлення апаратного та програмного забезпечення є важливими для запобігання технічним проблемам, які можуть вплинути на доступність системи. Застосування новітніх патчів безпеки та оновлень може допомогти уникнути вразливостей, які зловмисники могли б використати для атаки.

2.4 Політика інформаційної безпеки

1. Вступ

У сучасному світі, де інформація є одним із ключових активів для будь-якої організації, належне управління інформаційною безпекою стає надзвичайно важливим. ТОВ "Компсофт", визнаючи значення забезпечення безпеки своїх інформаційних ресурсів, розробило цю Політику Інформаційної Безпеки для захисту своїх активів від всіх форм загроз, чи то випадкових, чи умисних.

Ця політика є засобом для захисту не тільки конфіденційності та цілісності корпоративної інформації, але й її доступності, забезпечуючи тим самим

неперервність бізнес-процесів компанії та зменшуючи ризики, які можуть негативно позначитися на репутації та фінансовому становищі.

Метою цієї політики є встановлення розуміння важливості інформаційної безпеки серед усіх співробітників ТОВ "Компсофт" та залучених сторін, визначення основних вимог до захисту інформаційних ресурсів і впровадження ефективного механізму управління ризиками інформаційної безпеки.

Політика визначає основні принципи та вимоги, які мають бути реалізовані через конкретні процедури та інструкції, що регулюють повсякденні операції інформаційної безпеки. Кожен співробітник, від керівного складу до нових працівників, має бути повністю обізнаний з положеннями цієї політики і розуміти свою особисту відповідальність за захист інформаційних активів компанії.

Політика Інформаційної Безпеки ТОВ "Компсофт" підлягає регулярному перегляду та оновленню, щоб забезпечити її актуальність, відповідність сучасним загрозам інформаційній безпеці та вимогам законодавства. Це забезпечить, що компанія може швидко реагувати на зміни в технологічному ландшафті та зовнішньому середовищі.

2. *Визначення та скорочення*

Конфіденційність – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем та/або процесом.

Цілісність – властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем та/або процесом.

Доступність – властивість досяжності й можливості використання інформації на вимогу авторизованого об’єкта.

Спостережність – властивість системи, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об’єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки та/або забезпечення відповідальності за певні дії.

Політика – Політика інформаційної безпеки.

Ризик – ймовірність шкідливого впливу на бізнес в результаті порушення конфіденційності, цілісності та доступності інформації.

СУІБ – система управління інформаційною безпекою.

Інформаційна безпека – багаторівневий комплекс організаційних заходів підприємства, програмних і технічних засобів, які забезпечують захист інформації від випадкових і навмисних загроз, у результаті реалізації яких можливе порушення доступності, цілісності, конфіденційності інформації, а також які забезпечують безперервність бізнес-процесів, зниження операційних ризиків і оптимізацію витрат підприємства.

Інцидент інформаційної безпеки (інцидент ІБ) – це поява одного або декількох небажаних або несподіваних подій інформаційної безпеки, які пов'язані з настанням або значною вірогідністю настання негативних наслідків для інформаційної безпеки, інформації, інформаційних активів, бізнес-процесів або завдати шкоди підприємству та системі захисту.

Інформаційний ресурс – сукупність людських, апаратних та програмних ресурсів в інформаційних системах та процесах підприємства.

Інші терміни, що вживаються в Політиці, використовуються в значеннях, визначених законами України та ДСТУ ISO/IEC 27000:2015.

3. Область застосування

Ця політика застосовується до всіх відділів, співробітників, підрядників, консультантів, тимчасових працівників та інших робітників у компанії ТОВ "Компсофт", а також до всіх інформаційних систем, що використовуються в організації. Вона стосується всіх форм інформації, включаючи електронні дані, друковані документи та особисті комунікації.

4. Організаційна структура процесу управління інформаційною безпекою

4.1. Організаційна структура управління інформаційною безпекою в ІКС підприємства включає наступні посади та відповідальності:

4.1.1. Виконавчий директор відповідає за затвердження політики інформаційної безпеки та забезпечення необхідних ресурсів для її реалізації.

4.1.2. Заступник директора відповідає за оперативне впровадження цієї політики та координацію діяльності всіх відділів у сфері безпеки.

4.1.3. Адміністратор системи забезпечує належну роботу комп'ютерної системи та мережі, встановлює та контролює правила доступу, а також забезпечує контроль рівня доступу користувачів.

4.1.4. Користувачі ІКС повинні знати про політику інформаційної безпеки, дотримуватися правил та процедур, встановлених адміністратором системи, та повідомляти про будь-які виявлені загрози безпеки.

4.1.5. Робоча група з інформаційної безпеки відповідає за розгляд і вирішення питань, що стосуються безпеки даних в ІКС підприємства, включаючи розгляд і аналіз виявлених загроз, розробку стратегії безпеки та прийняття рішень.

5. Відповідальність за безпеку

5.1 Відповідальність за забезпечення інформаційної безпеки лежить на всіх рівнях організації ТОВ "Компсофт".

Виконавчий директор несе загальну відповідальність за інформаційну безпеку в компанії, включаючи:

– затвердження політики інформаційної безпеки.

– забезпечення ресурсів для впровадження та підтримки заходів безпеки.

– моніторинг загальної ефективності системи управління інформаційною безпекою.

Заступник директора відповідає за:

– координацію діяльності з впровадження та підтримки політики інформаційної безпеки.

– нагляд за дотриманням процедур інформаційної безпеки у всіх відділах.

– підготовку та подання звітів виконавчому директору про стан інформаційної безпеки.

Керівники відділів несуть відповідальність за забезпечення інформаційної безпеки у своїх підрозділах:

– технічний персонал (Інженери-програмісти, QA інженери, Адміністратори баз даних, Системні адміністратори): впровадження технічних заходів безпеки, регулярне оновлення програмного забезпечення, моніторинг систем на наявність вразливостей.

– фінансовий відділ (Головний бухгалтер, Бухгалтери): захист фінансових даних, контроль за виконанням фінансових операцій згідно з політикою безпеки.

– HR відділ (HR-менеджер): проведення перевірок кандидатів при наймі, навчання співробітників з питань інформаційної безпеки з залученням профільних фахівців, контроль доступу до конфіденційної інформації.

– відділ маркетингу і продажів (Маркетологи, Менеджери з продажу): захист даних клієнтів, забезпечення конфіденційності маркетингової інформації, впровадження заходів безпеки при взаємодії з клієнтами.

Робоча група з інформаційної безпеки відповідає за:

– розробку та впровадження політики інформаційної безпеки.

– проведення регулярних аудитів та оцінок ризиків.

– розробку та впровадження заходів реагування на інциденти безпеки.

– підготовку звітів та рекомендацій для вищого керівництва.

Кожен співробітник ТОВ "Компсофт" зобов'язаний:

– дотримуватися політики та процедур інформаційної безпеки.

– негайно повідомляти керівництво про будь-які інциденти або підозрілі активності.

– брати участь у навчальних програмах та тренінгах з інформаційної безпеки.

6. Процедури захисту від несанкціонованого доступу

6.1. Визначення загроз та ризиків безпеки інформації

Для забезпечення ефективного захисту інформаційних ресурсів ТОВ "Компсофт" необхідно регулярно проводити оцінки ризиків і визначати потенційні загрози інформаційній безпеці.

6.1.1 Проведення регулярних оцінок ризиків для виявлення потенційних загроз інформаційній безпеці

6.1.1.1 Регулярне проведення формальних оцінок ризиків не рідше одного разу на рік, а також після значних змін у IT-інфраструктурі або організаційній структурі.

6.1.1.2 Використання стандартних методик оцінки ризиків, таких як ISO/IEC 27005 або NIST SP 800-30, для структурованого підходу до виявлення, аналізу та оцінки ризиків.

6.1.1.3 Залучення всіх відповідних відділів до процесу оцінки ризиків для забезпечення всебічного розуміння загроз.

6.1.2 Ідентифікація та класифікація активів, які потребують захисту

6.1.2.1 Створення і підтримка реєстру всіх інформаційних активів компанії, включаючи апаратне забезпечення, програмне забезпечення, дані та інші ресурси.

6.1.2.2 Класифікація активів на основі їх критичності для бізнес-процесів, визначення рівнів чутливості даних (конфіденційні, внутрішні, публічні).

6.1.2.3 Призначення відповідальних за кожен актив, які будуть відповідати за його захист та актуальність інформації про актив.

6.1.3 Оцінка впливу потенційних загроз на інформаційні активи компанії

6.1.3.1 Визначення можливих загроз для кожного класифікованого активу, включаючи внутрішні та зовнішні загрози (хакери, віруси, збої обладнання, природні катастрофи).

6.1.3.2 Оцінка ймовірності реалізації кожної загрози та її можливого впливу на активи компанії.

6.1.3.3 Визначення та документування потенційних наслідків реалізації кожної загрози, включаючи фінансові втрати, порушення репутації, юридичні наслідки.

6.1.4 Розробка та впровадження заходів для мінімізації виявлених ризиків

6.1.4.1 Розробка плану дій для мінімізації виявлених ризиків, що включає технічні, адміністративні та організаційні заходи.

6.1.4.2 Впровадження заходів безпеки, таких як шифрування даних, встановлення антивірусного програмного забезпечення, регулярне оновлення програмного забезпечення, та навчання персоналу.

6.1.4.3 Постійний моніторинг та оцінка ефективності впроваджених заходів, регулярний перегляд плану дій та адаптація до нових загроз і змін у бізнес-середовищі.

6.1.4.4 Забезпечення документування всіх заходів та їх реалізації для подальшого аудиту та перевірки.

6.2. Встановлення правил користування ІКС підприємства та інструкцій з доступу до ресурсів

6.2.1. Розробка та документування правил користування інформаційно-комунікаційними системами (ІКС) підприємства

6.2.1.1. Визначення ключових принципів і правил користування ІКС підприємства, що включають безпечну роботу з інформаційними системами, захист від шкідливого програмного забезпечення, та заходи по захисту конфіденційної інформації.

6.2.1.2. Розробка документації, яка детально описує всі правила користування ІКС, включаючи процедури для входу в систему, використання корпоративних ресурсів, обробки конфіденційної інформації та поводження з зовнішніми носіями інформації.

6.2.1.3. Впровадження механізмів забезпечення дотримання правил користування, включаючи санкції за їх порушення.

6.2.2. Встановлення інструкцій для всіх співробітників щодо доступу до корпоративних ресурсів

6.2.2.1. Розробка детальних інструкцій для кожного рівня доступу, що включають процедури автентифікації, використання паролів, та заходи безпеки при роботі з конфіденційними даними.

6.2.2.2. Проведення навчальних сесій для співробітників, що пояснюють нові правила та інструкції, а також регулярне оновлення знань через періодичні тренінги.

6.2.2.3. Встановлення зручного доступу до інструкцій для всіх співробітників, включаючи онлайн-доступ через корпоративний портал.

6.2.3. Забезпечення доступу до ресурсів виключно на основі ролей та обов'язків співробітників

6.2.3.1. Визначення ролей і обов'язків кожного співробітника з точки зору необхідного рівня доступу до інформаційних ресурсів.

6.2.3.2. Впровадження системи управління доступом на основі ролей (RBAC), яка автоматично призначає відповідні права доступу на основі посадових обов'язків.

6.2.3.3. Регулярний перегляд та актуалізація списків прав доступу для забезпечення відповідності поточним обов'язкам співробітників.

6.2.4. Регулярне оновлення правил та інструкцій з урахуванням змін в ІКС та організаційній структурі

6.2.4.1. Проведення регулярних оглядів і оцінок правил користування ІКС для виявлення необхідності в змінах та оновленнях.

6.2.4.2. Впровадження механізмів збору зворотного зв'язку від співробітників щодо ефективності та зручності чинних правил та інструкцій.

6.2.4.3. Оновлення документації та інструкцій у випадку змін в ІКС, організаційній структурі або в результаті виявлення нових загроз.

6.2.4.4. Інформування всіх співробітників про внесені зміни та організація додаткових навчальних сесій при необхідності.

6.3. Політики щодо паролів, управління доступом та аудиту доступу

6.3.1. Встановлення вимог до складності паролів

6.3.1.1. Визначення мінімальних вимог до складності паролів: паролі повинні містити не менше 10 символів, включаючи великі та малі літери, цифри та спеціальні символи.

6.3.1.2. Заборона використання простих та загальновідомих паролів, таких як "password123" або "admin".

6.3.1.3. Забезпечення інструментів для автоматичної перевірки складності паролів при їх створенні та зміні.

6.3.2. Забезпечення регулярної зміни паролів

6.3.2.1. Встановлення політики, яка вимагає обов'язкову зміну паролів кожні 90 днів.

6.3.2.2. Налаштування системи для автоматичного нагадування користувачам про необхідність зміни паролів перед закінченням 90-денного терміну.

6.3.2.3. Забезпечення механізмів для безпечної зміни паролів та верифікації нових паролів.

6.3.3. Впровадження багаторівневої аутентифікації (MFA) для критичних систем

6.3.3.1. Визначення критичних систем та ресурсів, для яких необхідно впровадити багаторівневу аутентифікацію.

6.3.3.2. Встановлення додаткових рівнів захисту, таких як SMS-коди, апаратні токени, біометричні дані або мобільні додатки для генерації одноразових паролів.

6.3.3.3. Забезпечення підтримки та управління MFA, включаючи процеси відновлення доступу для користувачів, які втратили доступ до своїх засобів аутентифікації.

6.3.4. Використання систем управління доступом (IAM) для централізованого контролю прав доступу

6.3.4.1. Впровадження системи управління ідентифікацією та доступом (IAM) для централізованого контролю доступу до інформаційних ресурсів.

6.3.4.2. Використання IAM для автоматичного надання та відкликання прав доступу на основі ролей і посадових обов'язків співробітників.

6.3.4.3. Інтеграція IAM з іншими системами безпеки для забезпечення єдиного контрольного центру для управління доступом та моніторингу.

6.3.5. Проведення регулярних аудитів доступу для виявлення та виправлення неправомірних привілеїв

6.3.5.1. Встановлення регулярного графіку проведення аудитів доступу, не рідше одного разу на квартал.

6.3.5.2. Використання автоматизованих інструментів для перевірки відповідності прав доступу поточним обов'язкам співробітників.

6.3.5.3. Виявлення та негайне виправлення випадків неправомірного доступу або перевищення привілеїв.

6.3.5.4. Документування результатів аудитів та надання звітів керівництву для аналізу та подальших дій.

6.4. Управління аккаунтами користувачів

6.4.1. Ведення реєстру користувачів з вказанням їхніх ролей та прав доступу

6.4.1.1. Створення та підтримка централізованого реєстру користувачів, який містить інформацію про всі активні облікові записи, ролі та рівні доступу.

6.4.1.2. Ведення детальної документації про права доступу кожного користувача, включаючи історію змін та дати останнього оновлення.

6.4.1.3. Використання системи управління ідентифікацією та доступом (IAM) для автоматичного оновлення реєстру на основі змін у ролях та обов'язках співробітників.

6.4.2. Забезпечення створення, модифікації та видалення аккаунтів лише уповноваженими особами

6.4.2.1. Визначення уповноважених осіб, відповідальних за створення, модифікацію та видалення облікових записів користувачів.

6.4.2.2. Впровадження процесу затвердження для створення нових облікових записів, включаючи перевірку необхідності доступу та його відповідність ролям і обов'язкам.

6.4.2.3. Використання IAM-системи для забезпечення прозорості та контролю всіх дій, пов'язаних з управлінням обліковими записами.

6.4.3. Регулярний перегляд і оновлення прав доступу відповідно до змін в обов'язках співробітників

6.4.3.1. Встановлення регулярного графіку перегляду прав доступу користувачів, не рідше одного разу на квартал.

6.4.3.2. Проведення перевірок прав доступу при зміні посадових обов'язків або переведенні співробітників на інші посади.

6.4.3.3. Використання IAM-системи для автоматичного оновлення прав доступу на основі змін в обов'язках користувачів.

6.4.4. Забезпечення видалення або блокування аккаунтів користувачів, які більше не потребують доступу до систем

6.4.4.1. Встановлення процедури негайного видалення або блокування облікових записів співробітників, які звільняються або більше не потребують доступу до систем.

6.4.4.2. Проведення регулярних перевірок для виявлення та деактивації облікових записів, які не використовувалися протягом визначеного періоду часу (наприклад, 90 днів).

6.4.4.3. Використання автоматизованих інструментів для моніторингу активності облікових записів та своєчасного виявлення невикористовуваних або підозрілих облікових записів.

6.5. Захист системи від шкідливих програм та вірусів

6.5.1. Встановлення та підтримка антивірусного програмного забезпечення на всіх кінцевих точках та серверах

6.5.1.1. Встановлення антивірусного програмного забезпечення на всі кінцеві точки (персональні комп'ютери, ноутбуки) та сервери, що використовуються в ТОВ "Компсофт".

6.5.1.2. Регулярне оновлення антивірусного програмного забезпечення для забезпечення захисту від новітніх загроз.

6.5.1.3. Впровадження моніторингу стану антивірусного програмного забезпечення для забезпечення його безперервної роботи та своєчасного виявлення можливих проблем.

6.5.2. Налаштування автоматичного оновлення антивірусних баз даних

6.5.2.1. Налаштування антивірусного програмного забезпечення на автоматичне оновлення баз даних вірусних сигнатур не менше одного разу на день.

6.5.2.2. Забезпечення безперебійного інтернет-з'єднання для своєчасного отримання оновлень.

6.5.2.3. Контроль за процесом оновлення баз даних та вирішення будь-яких проблем, пов'язаних з оновленням.

6.5.3. Регулярне проведення повного сканування систем на наявність шкідливих програм

6.5.3.1. Встановлення розкладу для регулярного проведення повного сканування всіх систем на наявність шкідливих програм (наприклад, щотижня).

6.5.3.2. Забезпечення проведення додаткового сканування після кожного оновлення антивірусних баз даних або в разі підозри на інфекцію.

6.5.3.3. Аналіз результатів сканування та вжиття відповідних заходів для видалення виявлених шкідливих програм.

6.5.4. Впровадження політики щодо завантаження та встановлення програмного забезпечення лише з перевірених джерел

6.5.4.1. Розробка та впровадження політики, яка дозволяє завантаження та встановлення програмного забезпечення лише з офіційних та перевірених джерел.

6.5.4.2. Заборона завантаження та встановлення програмного забезпечення з неофіційних або підозрілих вебсайтів.

6.5.4.3. Впровадження процедури затвердження для встановлення нового програмного забезпечення, яка включає перевірку безпеки та відповідності вимогам компанії.

6.5.4.4. Проведення навчальних сесій для співробітників щодо важливості дотримання цієї політики та можливих наслідків її порушення.

6.6. Процедури випадкових аудитів доступу

6.6.1. Проведення нерегулярних аудитів доступу для перевірки дотримання політик безпеки

6.6.1.1. Встановлення графіку нерегулярних аудитів доступу, щоб уникнути передбачуваності та забезпечити ефективність перевірок.

6.6.1.2. Використання автоматизованих інструментів для перевірки прав доступу, журналів доступу та активності користувачів.

6.6.1.3. Проведення аудитів незалежними внутрішніми або зовнішніми аудиторами для забезпечення об'єктивності та неупередженості перевірок.

6.6.2. Виявлення та документування порушень політики доступу

6.6.2.1. Ідентифікація випадків порушення політики доступу, включаючи несанкціоновані спроби доступу, перевищення привілеїв та інші відхилення від встановлених правил.

6.6.2.2. Документування всіх виявлених порушень, включаючи дату, час, користувача, тип порушення та заходи, вжиті для усунення порушення.

6.6.2.3. Аналіз причин порушень для виявлення слабких місць у політиці доступу та процесах управління доступом.

6.6.3. Оцінка ефективності впроваджених заходів безпеки та коригування процедур відповідно до результатів аудитів

6.6.3.1. Аналіз результатів аудитів для оцінки ефективності існуючих заходів безпеки та процедур.

6.6.3.2. Розробка та впровадження коригувальних заходів для усунення виявлених слабких місць та підвищення рівня безпеки.

6.6.3.3. Оновлення політик та процедур доступу на основі отриманих результатів аудитів, включаючи внесення змін до технічних та організаційних заходів.

6.6.4. Забезпечення звітності про результати аудитів вищому керівництву

6.6.4.1. Підготовка детальних звітів про результати проведених аудитів, включаючи виявлені порушення, вжиті заходи та рекомендації щодо покращення безпеки.

6.6.4.2. Представлення результатів аудитів вищому керівництву для забезпечення належного контролю та прийняття стратегічних рішень.

6.6.4.3. Забезпечення прозорості та відкритості процесу аудиту для підвищення довіри співробітників та залучення їх до підтримки політик безпеки.

6.7. Процедури відключення доступу для звільнених або змінивших підрозділ

6.7.1. Негайне відключення доступу до систем для звільнених співробітників

6.7.1.1. Встановлення процедури негайного відключення доступу до всіх систем для звільнених співробітників у день їхнього звільнення.

6.7.1.2. Залучення менеджерів з персоналу та керівників відділів для своєчасного інформування IT-відділу про звільнення співробітників.

6.7.1.3. Використання автоматизованих інструментів для швидкого відкликання доступу до систем і видалення облікових записів звільнених співробітників.

6.7.2. Актуалізація прав доступу для співробітників, які змінили підрозділ або посаду

6.7.2.1. Проведення регулярного перегляду прав доступу співробітників, які змінили підрозділ або посаду.

6.7.2.2. Залучення керівників підрозділів для підтвердження необхідності доступу до відповідних ресурсів для нових посад.

6.7.2.3. Забезпечення своєчасного оновлення прав доступу відповідно до нових обов'язків співробітників.

6.7.3. Видалення або блокування облікових записів та доступу до систем для співробітників, які більше не потребують доступу

6.7.3.1. Встановлення процедури перевірки та видалення облікових записів співробітників, які більше не потребують доступу до систем (наприклад, завершення проєкту).

6.7.3.2. Використання автоматизованих інструментів для блокування облікових записів, які більше не використовуються, з можливістю подальшого видалення.

6.7.3.3. Документування всіх змін доступу та збереження історії видалення або блокування облікових записів.

6.7.4. Перевірка та видалення тимчасових акаунтів, які більше не використовуються

6.7.4.1. Встановлення регулярного графіку перевірки тимчасових акаунтів для виявлення невикористовуваних облікових записів.

6.7.4.2. Забезпечення створення тимчасових акаунтів з автоматичним обмеженням терміну дії, після якого обліковий запис блокується або видаляється.

6.7.4.3. Документування всіх тимчасових облікових записів та контроль за їхнім видаленням після завершення терміну дії або використання.

6.8. Заходи у разі порушення безпеки

6.8.1. Виявлення та ідентифікація порушення

6.8.1.1. Використання систем моніторингу та виявлення вторгнень (IDS/IPS) для постійного контролю мережі та інформаційних систем на предмет можливих порушень безпеки.

6.8.1.2. Встановлення процесів для оперативного виявлення та ідентифікації підозрілої активності або інцидентів безпеки.

6.8.1.3. Навчання персоналу щодо розпізнавання ознак порушень безпеки та правильного реагування на них.

6.8.2. Повідомлення про інцидент

6.8.2.1. Встановлення чіткої процедури для повідомлення про виявлені порушення безпеки всіх зацікавлених сторін, включаючи IT-відділ, керівництво та робочу групу з інформаційної безпеки.

6.8.2.2. Визначення контактних осіб для повідомлень про інциденти безпеки, а також каналів комунікації для оперативного обміну інформацією.

6.8.2.3. Забезпечення конфіденційності інформації про інциденти до їх повного розслідування.

6.8.3. Реагування на інцидент

6.8.3.1. Розробка та впровадження плану реагування на інциденти, що включає дії для швидкого ізолювання та нейтралізації загрози.

6.8.3.2. Визначення відповідальних осіб за виконання плану реагування на інциденти та координацію дій усіх залучених відділів.

6.8.3.3. Використання засобів резервного копіювання для відновлення систем та даних до стану до інциденту.

6.8.4. Розслідування інциденту

6.8.4.1. Проведення ретельного розслідування інциденту для визначення його причин, масштабу та наслідків.

6.8.4.2. Збір доказів та ведення журналу всіх дій, пов'язаних з інцидентом, для подальшого аналізу та можливих юридичних дій.

6.8.4.3. Залучення зовнішніх експертів за потреби для отримання незалежної оцінки та допомоги у розслідуванні.

6.8.5. Усунення наслідків інциденту

6.8.5.1. Відновлення систем та даних, що постраждали внаслідок інциденту, з використанням резервних копій та інших заходів відновлення.

6.8.5.2. Оцінка та мінімізація збитків, заподіяних інцидентом, включаючи фінансові, репутаційні та операційні втрати.

6.8.5.3. Впровадження додаткових заходів безпеки для запобігання повторенню аналогічних інцидентів у майбутньому.

6.8.6. Інформування та звітність

6.8.6.1. Підготовка детальних звітів про інцидент, включаючи його причини, наслідки та вжиті заходи для його усунення.

6.8.6.2. Інформування вищого керівництва про результати розслідування та дії, вжиті для відновлення нормальної роботи.

6.8.6.3. Повідомлення відповідних зовнішніх органів та зацікавлених сторін про інцидент, якщо це необхідно відповідно до законодавства або договірних зобов'язань.

7. Мережева безпека

Забезпечення мережевої безпеки є критичним елементом загальної стратегії інформаційної безпеки ТОВ "Компсофт". У розділі описані заходи, які необхідно вжити для захисту мережевої інфраструктури від несанкціонованого доступу, атак та інших загроз.

7.1. Захист периметра мережі

7.1.1. Встановлення та конфігурація фаєрволів для контролю вхідного та вихідного трафіку, забезпечення правил доступу до внутрішніх ресурсів компанії.

7.1.2. Використання засобів запобігання вторгненням (IPS) для виявлення та блокування підозрілої активності в реальному часі.

7.1.3. Налаштування фільтрації трафіку на основі IP-адрес, портів та протоколів для обмеження доступу до мережі з невідомих або небезпечних джерел.

7.2. Віртуальні приватні мережі (VPN)

7.2.1. Впровадження VPN для забезпечення захищеного віддаленого доступу до корпоративної мережі для співробітників та підрядників.

7.2.2. Використання надійних методів аутентифікації, таких як багаторівнева аутентифікація (MFA), для доступу до VPN.

7.2.3. Шифрування всього трафіку, що передається через VPN, для забезпечення конфіденційності та цілісності даних.

7.3. Сегментація мережі

7.3.1. Розподіл корпоративної мережі на ізольовані сегменти на основі функціональних груп, таких як фінансовий відділ, відділ розробки, відділ підтримки клієнтів, тощо.

7.3.2. Використання віртуальних локальних мереж (VLAN) для сегментації мережі та обмеження трафіку між сегментами.

7.3.3. Впровадження політик безпеки для контролю доступу між сегментами мережі на основі ролей та необхідності доступу.

7.4. Моніторинг та виявлення аномалій

7.4.1. Встановлення систем моніторингу мережевого трафіку для виявлення аномальних або підозрілих дій.

7.4.2. Використання систем виявлення вторгнень (IDS) для аналізу трафіку та виявлення потенційних загроз.

7.4.3. Впровадження засобів для централізованого збору та аналізу журналів подій з мережевих пристроїв та систем безпеки.

7.5. Оновлення та патчі безпеки

7.5.1. Регулярне оновлення програмного забезпечення та прошивки мережевих пристроїв, таких як маршрутизатори, комутатори, фаєрволи та інші мережеві компоненти.

7.5.2. Впровадження процесів тестування та встановлення патчів безпеки для запобігання експлуатації відомих вразливостей.

7.5.3. Ведення журналу встановлених оновлень та патчів для забезпечення відповідності політикам безпеки.

7.6. Захист від DDoS атак

7.6.1. Встановлення засобів захисту від розподілених атак на відмову в обслуговуванні (DDoS), таких як спеціалізовані сервіси та апаратні засоби.

7.6.2. Налаштування політик обмеження трафіку та використання засобів виявлення та блокування DDoS атак у реальному часі.

7.6.3. Співпраця з провайдерами інтернет-послуг для реалізації заходів захисту на рівні інфраструктури провайдера.

7.7. Навчання та підвищення обізнаності персоналу

7.7.1. Проведення регулярних навчальних сесій для співробітників з питань мережевої безпеки, включаючи розпізнавання фішингових атак та безпечного користування мережею.

7.7.2. Розробка та поширення матеріалів для підвищення обізнаності про загрози мережевої безпеки та методи їх уникнення.

7.7.3. Залучення співробітників до участі у тренінгах та симуляціях для практичного відпрацювання навичок реагування на інциденти.

8. Фізична безпека

Фізична безпека є ключовим елементом захисту інформаційних ресурсів ТОВ "Компсофт". У розділі описані заходи, спрямовані на забезпечення фізичної безпеки обладнання, серверних кімнат та інших важливих об'єктів компанії.

8.1. Контроль доступу до приміщень

8.1.1. Встановлення систем контролю доступу для обмеження входу до приміщень, де зберігається або обробляється конфіденційна інформація, лише уповноваженим особам.

8.1.2. Використання електронних карт доступу, біометричних систем (наприклад, відбитків пальців) або інших надійних методів автентифікації для контролю доступу.

8.1.3. Ведення журналів входу та виходу з приміщень, що зберігаються в захищеному місці та доступні для аудиту.

8.2. Відеоспостереження

8.2.1. Встановлення систем відеоспостереження у критичних зонах, таких як серверні кімнати, входи до будівель та інші важливі приміщення.

8.2.2. Забезпечення цілодобового моніторингу відеокамер та зберігання записів протягом визначеного періоду для можливого подальшого аналізу.

8.2.3. Встановлення знаків, що попереджають про ведення відеоспостереження, для підвищення обізнаності персоналу та відвідувачів.

8.3. Захист серверних кімнат

8.3.1. Розміщення серверних кімнат у добре захищених приміщеннях з обмеженим доступом.

8.3.2. Встановлення систем кондиціювання повітря та контролю температури для забезпечення належних умов експлуатації обладнання.

8.3.3. Впровадження систем пожежної безпеки, включаючи детектори диму, системи пожежогасіння та регулярні перевірки їхнього стану.

8.4. Захист від природних катастроф

8.4.1. Визначення потенційних природних ризиків (пожежі, повені, землетруси) та розробка планів захисту.

8.4.2. Використання водонепроникних та вогнестійких матеріалів для захисту критичних приміщень та обладнання.

8.4.3. Розміщення резервних копій даних та критичного обладнання у віддалених місцях для забезпечення відновлення після катастроф.

8.5. Планування та проведення навчань

8.5.1. Розробка планів евакуації та дій у надзвичайних ситуаціях, таких як пожежа або землетрус.

8.5.2. Проведення регулярних навчань та тренувань для персоналу з питань безпеки, включаючи евакуаційні тренування.

8.5.3. Забезпечення наявності необхідного обладнання для аварійних ситуацій, такого як вогнегасники, аптечки першої допомоги, аварійне освітлення.

8.6. Фізична безпека обладнання

8.6.1. Встановлення захисних кожухів та кріплень для запобігання крадіжці обладнання.

8.6.2. Використання захисних шаф та сейфів для зберігання портативних пристроїв, таких як ноутбуки та зовнішні жорсткі диски.

8.6.3. Маркування обладнання та ведення реєстру для спрощення інвентаризації та відстеження стану.

8.7. Охоронна служба

8.7.1. Наявність охоронної служби для забезпечення безпеки приміщень та обладнання, зокрема під час неробочих годин.

8.7.2. Встановлення регулярних перевірок території та приміщень.

8.7.3. Співпраця з місцевими правоохоронними органами для швидкого реагування на інциденти безпеки.

9. Оцінка ефективності політики безпеки

Оцінка ефективності політики безпеки є критично важливим процесом для забезпечення постійного вдосконалення заходів безпеки та відповідності поточним загрозам і ризикам.

9.1. Встановлення ключових показників ефективності (KPI)

9.1.1. Визначення ключових показників ефективності (KPI) для оцінки різних аспектів політики безпеки, таких як кількість інцидентів безпеки, час реагування на інциденти, кількість успішних та неуспішних спроб доступу тощо.

9.1.2. Встановлення цільових значень для кожного KPI та регулярний моніторинг їх досягнення.

9.1.3. Використання KPI для оцінки ефективності впроваджених заходів безпеки та виявлення областей, які потребують покращення.

9.2. Регулярні аудити безпеки

9.2.1. Проведення регулярних внутрішніх та зовнішніх аудитів безпеки для оцінки відповідності політики безпеки та процедур стандартам та найкращим практикам.

9.2.2. Залучення незалежних аудиторів для забезпечення об'єктивності та неупередженості оцінки.

9.2.3. Документування результатів аудитів, виявлених вразливостей та рекомендацій щодо їх усунення.

9.3. Аналіз інцидентів безпеки

9.3.1. Збір та аналіз даних про всі інциденти безпеки, що сталися у компанії, включаючи їх причини, наслідки та заходи реагування.

9.3.2. Використання результатів аналізу для вдосконалення політики безпеки та процедур, спрямованих на запобігання подібним інцидентам у майбутньому.

9.3.3. Розробка звітів про інциденти безпеки та представлення їх керівництву для прийняття стратегічних рішень.

9.4. Оцінка ризиків

9.4.1. Проведення регулярних оцінок ризиків для виявлення нових загроз та вразливостей, а також для перегляду існуючих ризиків.

9.4.2. Використання результатів оцінки ризиків для коригування заходів безпеки та оновлення політики безпеки.

9.4.3. Включення оцінки ризиків до загального процесу управління ризиками в компанії.

9.5. Оцінка відповідності політики безпеки законодавчим та регуляторним вимогам

9.5.1. Постійний моніторинг змін у законодавстві та регуляторних вимогах, що стосуються інформаційної безпеки.

9.5.2. Перегляд політики безпеки для забезпечення її відповідності актуальним вимогам.

9.5.3. Проведення аудитів на відповідність законодавчим та регуляторним вимогам з залученням юридичних експертів.

9.6. Зворотній зв'язок від співробітників

9.6.1. Створення механізмів для збору зворотного зв'язку від співробітників щодо ефективності та зручності політики безпеки.

9.6.2. Проведення опитувань та інтерв'ю для виявлення проблем та пропозицій щодо покращення політики безпеки.

9.6.3. Використання отриманих даних для вдосконалення політики безпеки та процедур.

9.7. Безперервне вдосконалення

9.7.1. Впровадження циклу безперервного вдосконалення (Plan-Do-Check-Act) для постійного оновлення та покращення політики безпеки.

9.7.2. Регулярний перегляд та оновлення політики безпеки на основі результатів оцінок ефективності, аналізу інцидентів, аудитів та зворотного зв'язку.

9.7.3. Забезпечення залучення всіх зацікавлених сторін до процесу вдосконалення політики безпеки.

10. Заключні положення

10.1. Затвердження та введення в дію

10.1.1. Ця Політика Інформаційної Безпеки затверджується виконавчим директором ТОВ "Компсофт" та вступає в дію з моменту її підписання.

10.1.2. Всі співробітники компанії зобов'язані ознайомитися з цією політикою, підписати документ про ознайомлення та дотримуватися всіх її положень.

10.2. Перегляд та оновлення політики

10.2.1. Політика Інформаційної Безпеки підлягає регулярному перегляду не рідше одного разу на рік, а також при наявності значних змін в IT-інфраструктурі, організаційній структурі або законодавчих вимогах.

10.2.2. Відповідальність за ініціювання перегляду політики покладається на робочу групу з інформаційної безпеки під керівництвом заступника директора.

10.2.3. Будь-які зміни до політики повинні бути затверджені виконавчим директором перед їх введенням в дію.

10.3. Відповідальність за виконання

10.3.1. Виконання політики Інформаційної Безпеки є обов'язком кожного співробітника ТОВ "Компсофт". Невиконання положень політики може призвести до дисциплінарних заходів, включаючи звільнення.

10.3.2. Керівники відділів несуть відповідальність за контроль виконання політики своїми підлеглими та забезпечення відповідності всіх операцій вимогам цієї політики.

10.3.3. Робоча група з інформаційної безпеки відповідає за моніторинг дотримання політики, проведення аудитів та звітування перед керівництвом про виявлені порушення.

10.4. Інформування та навчання співробітників

10.4.1. Всі нові співробітники повинні пройти обов'язкове навчання з інформаційної безпеки в рамках програми введення в посаду.

10.4.2. Регулярні тренінги та навчальні сесії повинні проводитися для всіх співробітників з метою підвищення обізнаності про загрози інформаційній безпеці та методи їх запобігання.

10.4.3. HR відділ відповідає за організацію та проведення навчальних заходів, а також за ведення обліку відвідуваності тренінгів.

10.5. Документування та звітність

10.5.1. Всі заходи, пов'язані з інформаційною безпекою, повинні бути належним чином задокументовані, включаючи аудити, інциденти, заходи реагування та результати оцінки ризиків.

10.5.2. Робоча група з інформаційної безпеки повинна підготовлювати регулярні звіти для вищого керівництва про стан інформаційної безпеки, виконання політики та рекомендації щодо її вдосконалення.

10.5.3. Документація та звіти повинні зберігатися в захищеному місці з обмеженим доступом, відповідно до вимог законодавства та внутрішніх політик компанії.

10.6. Співпраця з зовнішніми організаціями

10.6.1. ТОВ "Компсофт" повинно підтримувати зв'язки з зовнішніми організаціями, такими як правоохоронні органи, регуляторні органи, постачальники послуг та партнери для обміну інформацією про загрози та інциденти безпеки.

10.6.2. У випадку інцидентів, які можуть вплинути на зовнішні сторони або вимагати взаємодії з зовнішніми організаціями, компанія повинна своєчасно інформувати відповідні організації та співпрацювати з ними для вирішення інциденту.

2.5 Висновок

Для ІКС ТОВ "Компсофт" розроблено комплексну та багаторівневу Політику Інформаційної Безпеки, спрямовану на захист інформаційних активів компанії від широкого спектру загроз. Політика охоплює всі ключові аспекти безпеки, включаючи фізичну безпеку, мережеву безпеку, захист від шкідливих програм та вірусів, управління доступом, а також заходи реагування на інциденти.

Визначення загроз та ризиків безпеки інформації здійснюється через регулярні оцінки ризиків та ідентифікацію активів для забезпечення цілісності, конфіденційності та доступності інформації. Чітко визначені правила користування ІКС та інструкції з доступу до ресурсів для всіх співробітників оновлюються відповідно до змін в ІТ-інфраструктурі та організаційній структурі. Політики щодо паролів та управління доступом передбачають встановлення вимог до складності паролів, регулярну зміну паролів, впровадження багаторівневої аутентифікації та проведення регулярних аудитів доступу.

Управління аккаунтами користувачів здійснюється через ведення реєстру користувачів, забезпечення створення, модифікації та видалення облікових записів лише уповноваженими особами та регулярний перегляд прав доступу.

Захист від шкідливих програм забезпечується встановленням антивірусного програмного забезпечення, регулярними оновленнями баз даних, проведенням повного сканування систем та впровадженням політики завантаження програмного забезпечення лише з перевірених джерел.

Процедури випадкових аудитів доступу передбачають проведення нерегулярних перевірок для виявлення порушень та коригування заходів безпеки. У разі порушення безпеки проводяться заходи з виявлення, повідомлення, реагування, розслідування та усунення наслідків інцидентів.

Мережева безпека забезпечується захистом периметра мережі, використанням VPN, сегментацією мережі, моніторингом та виявленням аномалій, регулярним оновленням та встановленням патчів безпеки, а також захистом від DDoS атак. Фізична безпека охоплює контроль доступу до приміщень, відеоспостереження, захист серверних кімнат, заходи захисту від природних катастроф та організацію охоронної служби.

Ефективність політики безпеки оцінюється через встановлення ключових показників ефективності (KPI), регулярні аудити, аналіз інцидентів, оцінку ризиків, відповідність законодавчим вимогам, збір зворотного зв'язку від співробітників та впровадження циклу безперервного вдосконалення. Заключні положення визначають основні принципи введення в дію, перегляду, відповідальності, інформування та навчання співробітників, документування та звітності, а також співпраці з зовнішніми організаціями.

ТОВ "Компсофт" впровадило систематичний підхід до управління інформаційною безпекою, який забезпечує всебічний захист інформаційних ресурсів компанії. Політика Інформаційної Безпеки сприяє підтримці високого рівня безпеки, адаптації до нових загроз та відповідності законодавчим вимогам. Постійний моніторинг, оцінка ефективності та вдосконалення заходів безпеки дозволяють компанії ефективно захищати свої активи та забезпечувати стабільність бізнес-процесів.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Постановка задачі

Метою економічного розділу є обґрунтування доцільності розробки політики безпеки інформаційно-комунікаційної системи підприємства ТОВ «Компсофт» що спеціалізується на розробці програмного забезпечення.

Завданням був розрахунок капітальних та експлуатаційних витрат на розробку політики безпеки. А також визначення та аналіз показників економічної ефективності створеної політики.

3.2 Визначення капітальних витрат на створення політики безпеки

3.2.1 Визначення трудомісткості розробки та опрацювання ПБ

При проведенні нормування праці робітників, що займаються створенням політики безпеки, виникає проблема, пов'язана з тим, що ця праця є творчою.

Трудомісткість створення політики безпеки визначається тривалістю кожної робочої операції. При умові, що весь об'єм робіт буде виконано одним робітником, розраховується за формулою 3.1:

$$t = t_{mз} + t_{в} + t_{а} + t_{пр} + t_{опр}, \text{ годин}, \quad (3.1)$$

де $t_{mз}$ – тривалість складання політики безпеки;

$t_{в}$ – тривалість вивчення технічного завдання (ТЗ), літературних джерел за темою тощо;

$t_{а}$ – тривалість розробки алгоритму створення політики безпеки;

$t_{пр}$ – тривалість розробки політики безпеки інформаційно-комунікаційної системи підприємства;

$t_{опр}$ – тривалість опрацювання.

Отже трудомісткість створеної ПБ складає:

$$t = 12 + 28 + 15 + 85 + 30 = 170, \text{ годин.}$$

3.2.2 Розрахунок витрат на створення політики безпеки

При підрахунку витрати на створення політики безпеки $К_м$ за формулою 3.2 треба знайти загальні витрати на оплату заробітної плати розробнику політики безпеки $З_{зп}$ та вартість машинного часу, що необхідний для розробки та опрацювання політики безпеки на ПК $З_{мч}$:

$$К_м = З_{зп} + З_{мч} . \quad (3.2)$$

Заробітна плата розробника політики безпеки враховує основну і додаткову заробітну плату, відрахування на соціальні потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою 3.3:

$$Ззп = t \cdot Зпр , \text{ грн,} \quad (3.3)$$

де t – загальна тривалість створення ПБ, годин;

Зпр – средньогодинна заробітна плата розробника з нарахуваннями, грн/годину.

Таким чином, заробітна плата розробника за весь період праці складатиме:

$$З_{зп} = 170 \cdot 194 = 32980, \text{ грн.}$$

До загальної суми потрібно включити вартість машинного часу для розробки політики безпеки на ПК, що визначається за формулою 3.4:

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

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

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

Вартість 1 години машинного часу ПК визначається за формулою 3.5:

$$Смч = P \cdot Ce + \frac{Фзал \cdot Ha}{F p} + \frac{Клпз \cdot Hапз}{F p}, \text{ грн./година,} \qquad (3.5)$$

де P – встановлена потужність ПК (0,6 кВт);

$С_е$ – тариф на електричну енергію (2,64 грн/кВт·година);

$Ф_{зал}$ – залишкова вартість ПК на поточний рік (17000 грн.);

$Н_а$ – річна норма амортизації на ПК, частки одиниці (0,3);

$К_{лпз}$ – вартість ліцензійного програмного забезпечення (ОС Microsoft Windows 11 – 5800 грн., Microsoft Office 365 – 5700 грн.);

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці (0,3);

$F_р$ – річний фонд робочого часу (2096 годин (2024 рік)).

Отже, 1 година машинного часу ПК вартує:

$$С_{мч} = 0{,}6 \cdot 2{,}64 + \frac{17000 \cdot 0{,}3}{2096} + \frac{(5800+5700) \cdot 0{,}3}{2096} = 5.66 \text{ , грн./година.}$$

$$З_{мч} = 170 \cdot 5.66 = 962{,}20, \text{ грн.}$$

$$К_м = 32980 + 962{,}20 = 33942{,}20, \text{ грн.}$$

Таким чином, після всіх проведених розрахунків, загальні витрати на розробку політики безпеки, складають 33942,20 грн.

3.3 Розрахунок експлуатаційних витрат

До експлуатаційних витрат віднесено:

− річну заробітну плату співробітника, що проводить оцінку загроз інформаційній безпеці;

– відрахування на соціальні заходи від річної заробітної плати співробітника;

– витрати машинного часу.

3.3.1 Річна заробітна плата співробітника, що проводить оцінку загроз інформаційній безпеці

Годинна заробітна плата становить:

$$З_{прс} = 165 \text{ грн./год.}$$

Для підрахунку заробітної плати працівника, що проводить оцінку загроз інформаційній безпеці, використовується формула 3.6:

$$З_{зпс} = t * З_{прс}, \text{ грн.}, \quad (3.6)$$

де t – загальна тривалість роботи працівника за рік, годин.

Середня тривалість одного сеансу роботи щодо перевірки дотримання вимог політики безпеки становить 4 години, з періодичністю 2 раз на місяць. Тобто за рік t = 12 * 4 * 2 = 96 години.

Витрати на оплату заробітної плати за рік:

$$З_{зпс} = 96 * 165 = 15840, \text{ грн.}$$

3.3.2 Відрахування на соціальні заходи від річної заробітної плати співробітника, що проводить оцінку загроз інформаційній безпеці

Відрахування на соціальні заходи від річної заробітної плати співробітника, що проводить оцінку загроз інформаційній безпеці, розраховують за формулою 3.7:

$$З_{ссв} = 22\% * З_{зпс}, \text{ грн.} \quad (3.7)$$

Що, з урахуванням 96 годин робочого часу в рік, складуть:

$$З_{ссв} = 0,22 * 15840 = 3484,80 \text{ грн.}$$

3.3.3 Витрати машинного часу

Година машинного часу була розрахована раніше та становить:

$$С_{мч} = 0,6 \cdot 2,64 + \frac{17000 \cdot 0,3}{2096} + \frac{(5800+5700) \cdot 0,3}{2096} = 5.66, \text{ грн./година.}$$

Тобто, за рік роботи потрібно витратити, розрахувавши за формулою 3.8:

$$В_{мч} = t * С_{мч}, \text{ грн.} \quad (3.8)$$

Що становитиме:

$$В_{мч} = 96 * 5.66 = 543,36, \text{ грн.}$$

3.3.4 Загальні витрати на експлуатацію

Загальні витрати на експлуатацію розраховуються за формулою 3.9:

$$В_{екп} = З_{зпс} + З_{єсв} + В_{мч}, \text{ грн.} \quad (3.9)$$

$$В_{екп} = 15840 + 3484,80 + 543,36 = 19868,16 \text{ грн.}$$

3.4 Визначення збитку від поломок обладнання

Запобігти поломкам обладнання практично не можливо. Природно, первинна передумова наступна: витрати на ремонт або заміну деяких деталей обладнання не повинні перевищувати вартість самого обладнання.

Вихідні дані для підрахунку збитку:

– час простою внаслідок поломки, $t_п$ (в годинах), $t_п$ = 6 год;

– час відновлення після поломки, $t_в$ (в годинах), $t_в$ = 4 год;

– час повторного введення втраченої інформації, $t_{ви}$ (в годинах), $t_{ви}$ = 4 год;

– заробітна плата обслуговуючого персоналу, Z_0 (грн. в місяць з податками), Z_0 = 34100 грн.;

– заробітна плата співробітників, Z_c (грн. в місяць з податками), Z_c = 25000 грн.;

– кількість обслуговуючого персоналу, N_0, N_0 = 1;

– число співробітників, N_c, N_c = 43;

– прибуток , О (грн. на рік), О = 24963800 грн.;

– вартість заміни обладнання та запасних частин, виправлення помилок в роботі системи, $П_{зч}$ (грн.), $П_{зч}$ = 0 грн;

– число зламаного обладнання, I, I = 1;

– число поломок на рік, n, n = 20.

Вартість втрат від зниження продуктивності співробітників несправного обладнання розраховується за формулою 3.10:

$$П_п = \frac{\sum N_c Z_c}{176} \cdot t_п, \text{ грн.}, \quad (3.10)$$

де місячний фонд робочого часу при 40-а годинний робочий тиждень 176 годин.

Підставивши вихідні дані отримаємо:

$$П_п = (43*25000/176)*6 = 36647{,}73 \text{ , грн.}$$

Вартість відновлення зламаного обладнання розраховується за формулою 3.11:

$$П_в = П_{ви} + П_{пв} + П_{зч}, \text{ грн.} \quad (3.11)$$

де $П_{ви}$ – вартість повторного введення інформації(формула 3.12),

$П_{пв}$ – вартість відновлення обладнання(формула 3.13).

$$П_{ви} = \frac{\sum N_c Z_c}{176} \cdot t_{ви}, \text{ грн.} \quad (3.12)$$

$$П_{пв} = \frac{\sum_{N_o} Z_o}{176} \cdot t_в, \text{ грн.} \quad (3.13)$$

Отримаємо:

$$П_{ви} = (43*25000/176)*4 = 24431,82 \text{ грн.}$$
$$П_{пв} = (1*34100/176)*4 = 775 \text{ грн.}$$

Вартість заміни обладнання та запасних частин, виправлення помилок в системі, $П_{зч}$ (грн.) $П_{зч} = 0$ грн.

Підставивши отримані результати в загальну формулу отримаємо:

$$П_в = 24431,82 + 775 + 0 = 25206,82 \text{ грн.}$$

Втрачена вигода від простою зламаного обладнання становить та розраховується за формулою 3.14 й 3.15 відповідно:

$$U = П_п + П_в + V, \text{ грн.} \quad (3.14)$$

$$V = \frac{O}{Fг} \cdot (t_п + t_в + t_{ви}), \text{ грн,} \quad (3.15)$$

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

$$V = (24963800/2096)*(6+4+4) = 186781,11 \text{ грн.}$$
$$U = 36647,73 + 25206,82 + 186781,11 = 248635,66 \text{ грн.}$$

Таким чином, загальний збиток від поломки обладнання, повторного введення інформації в системі, виявлення та усунення помилок в системі складе (формула 3.16):

$$ОУ = \sum_{n}\sum_{I} U \text{, грн.} \quad (3.16)$$

$$ОУ = 20 * 1 * 248635,66 = 4972713,20, грн.$$

3.5 Загальний ефект від впровадження ПБ

Загальний ефект від впровадження політики безпеки, визначається за формулою 3.17 з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = ОУ \cdot R - C, грн, \quad (3.17)$$

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

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

С – щорічні витрати на експлуатацію, грн.

Таким чином, загальний ефект від впровадження становить:

$$E = 4972713,20 * 0,15 - 19868,16 = 726038,82 грн.$$

3.6 Визначення та аналіз показників економічної ефективності

Оцінка економічної ефективності, розглянутої у спеціальній частині роботи, здійснюється на основі визначення та аналізу коефіцієнта повернення інвестицій ROSI (Return on Investment for Security) за формулою 3.18 та терміну окупності капітальних інвестицій T_o за формулою 3.20.

$$ROSI = \frac{E}{K} \text{, частки одиниці,} \quad (3.18)$$

де Е – загальний ефект від впровадження системи захисту, грн.;

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

Підставивши відповідні значення, маємо:

$$ROSI = 726038,82 / 33942,20 = 21,39$$

Організація здійснює фінансування капітальних інвестицій за рахунок реінвестування власних коштів (частини прибутку та амортизаційних відрахувань).

Проєкт визнається економічно доцільним, якщо розрахунковий коефіцієнт ефективності перевищує річний рівень прибутковості альтернативного варіанта формула 3.19:

$$ROSI > (N_{деп} - N_{інф})/100) \quad (3.19)$$

де $N_{деп}$ – річна депозитна ставка, (16,5% – Полтава банк, Український капітал);

$N_{інф}$ – річний рівень інфляції, (5,1% - період січень-грудень 2023).

Підставивши відповідні значення, маємо:

$$ROSI > (16,5 - 5,1)/100),$$

$$21,39 > 0,114.$$

Отже, проєкт є економічно доцільним.

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

$$T_O = \frac{K}{E} = \frac{1}{ROSI}, \text{ років.} \quad (3.19)$$

Підставимо значення:

$$To = 1 / 21,39 = 0,046 року. (17 днів)$$

3.7 Висновок

Розрахувавши збитки від реалізації можливих атак та несправностей ІКС підприємства, які склали 4972713,20 грн., і порівнявши їх з витратами на забезпечення підтримки працездатності системи 19868,16 грн., та витратами на розробку 33942,20 грн., можна зробити висновок, що витрати на забезпечення інформаційної безпеки є не значними у співвідношенні до збитків, впровадження системи є економічно доцільним заходом (ROSI = 21,39), термін окупності системи безпеки становить 0,046 року (17 днів). Для подальшого розвитку діяльності підприємства впровадження даних заходів є необхідною умовою для виконання.

ВИСНОВКИ

Для ІКС ТОВ "Компсофт" розроблено всебічну Політику Інформаційної Безпеки, яка враховує організаційну структуру підприємства, аналіз загроз, модель порушника та конкретні заходи захисту інформаційних активів компанії. Ця політика спрямована на забезпечення цілісності, конфіденційності та доступності інформаційних ресурсів, що є критичними для стабільного функціонування компанії.

Організаційна структура ТОВ "Компсофт" включає керівництво, адміністративний персонал, відділ маркетингу та продажів, службу підтримки клієнтів, фінансовий відділ, HR-відділ, технічний персонал, підтримуючий персонал та охорону. Виконавчий директор і заступник директора координують реалізацію політики інформаційної безпеки. Кожен відділ має свої конкретні обов'язки та відповідальність за дотримання політики безпеки.

Аналіз загроз визначив основні ризики для інформаційної безпеки, включаючи антропогенні загрози (внутрішні та зовнішні), природні катастрофи та технічні збої. Було проведено детальну оцінку впливу потенційних загроз на інформаційні активи компанії, що дозволило розробити та впровадити відповідні заходи для мінімізації цих ризиків. Модель порушника враховує різні типи потенційних зловмисників, їх мотивацію, методи атак, засоби, рівень навичок, способи доступу, місця здійснення атаки, рівень злому та вплив на систему. Ця модель дозволила компанії розробити специфічні заходи для захисту від кожного типу загроз, включаючи технічні та організаційні заходи.

Розробка Політики Інформаційної Безпеки охоплює всі ключові аспекти безпеки: правила користування ІКС та інструкції з доступу до ресурсів для всіх співробітників; вимоги до складності паролів та регулярної зміни паролів; впровадження багаторівневої аутентифікації; управління аккаунтами користувачів; захист від шкідливих програм та вірусів; процедури випадкових аудитів доступу; негайне відключення доступу для звільнених співробітників та актуалізацію прав доступу для тих, хто змінив підрозділ; мережеву безпеку,

включаючи захист периметра мережі, використання VPN, сегментацію мережі, моніторинг та виявлення аномалій, регулярне оновлення та встановлення патчів безпеки, а також захист від DDoS атак; фізичну безпеку, включаючи контроль доступу до приміщень, відеоспостереження, захист серверних кімнат та заходи захисту від природних катастроф.

Ефективність політики безпеки оцінюється через встановлення ключових показників ефективності (KPI), регулярні аудити, аналіз інцидентів, оцінку ризиків, відповідність законодавчим вимогам, збір зворотного зв'язку від співробітників та впровадження циклу безперервного вдосконалення. Заключні положення визначають основні принципи введення в дію, перегляду, відповідальності, інформування та навчання співробітників, документування та звітності, а також співпраці з зовнішніми організаціями.

ТОВ "Компсофт" впровадило системний підхід до управління інформаційною безпекою, який забезпечує всебічний захист інформаційних ресурсів компанії. Політика Інформаційної Безпеки сприяє підтримці високого рівня безпеки, адаптації до нових загроз та відповідності законодавчим вимогам. Постійний моніторинг, оцінка ефективності та вдосконалення заходів безпеки дозволяють компанії ефективно захищати свої активи та забезпечувати стабільність бізнес-процесів.

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. НД ТЗІ 3.7-003-05. «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі».

8. Закон України "Про захист інформації в інформаційно-комунікаційних системах";

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

10. НД ТЗІ 2.5-010-2003 Вимоги до захисту інформації WEB – сторінки від несанкціонованого доступу.

11. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.

12. НД ТЗІ 3.6-005-21 Порядок категоріювання безпеки інформаційної системи та інформації.

13. НД ТЗІ 3.6 -004-21. Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці.

14. НД ТЗІ 3.6-006-21. Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем.

15. НД ТЗІ 3.6-007-21. Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	3	
4	А4	Вступ	1	
5	А4	1 Розділ	26	
6	А4	2 Розділ	53	
7	А4	3 Розділ	10	
8	А4	Висновки	2	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

Пояснювальна записка.docx

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 інформації інформаційно-комунікаційної системи ТОВ «Компсофт»
студентки групи 125-20-1
Дробот Тетяни Сергіївни

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 106 сторінках та містить 2 рисунка, 4 таблиці, 15 джерел та 4 додатка.

Метою розробки політики інформаційної безпеки ТОВ "Компсофт" є створення комплексної системи заходів і процедур для забезпечення цілісності, конфіденційності та доступності інформаційних ресурсів компанії.

Предметом розробки є заходи, процедури та політики, спрямовані на забезпечення інформаційної безпеки.

У першому розділі визначено актуальність розробки засобів захисту ІКС підприємства, визначена організаційна структура ТОВ "Компсофт", види інформації які циркулюють в ІКС підприємства.

У другому розділі виконано аналіз загроз та ризиків, побудована модель порушника, визначені вимоги до системи інформаційної безпеки, розроблена політика інформаційної безпеки підприємства.

У третьому розділі виконано розрахунок економічних показників та наведено економічне обґрунтування доцільності розробки політики інформаційної безпеки.

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

Робота оформлена та написана грамотною мовою, відповідає вимогам положення про систему запобігання та виявлення плагіату у Національному технічному університеті «Дніпровська політехніка». 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 спец. розділу
ст. викладач каф. БІТ Вадим МЄШКОВ