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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Данюка Ільї Ігоровича*

академічної групи *гр. 125-19-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

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

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доц. Ковальова Ю.В.			
розділів:				
спеціальний	к.т.н., доц. Ковальова Ю.В.			
економічний	к. е. н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2023

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту *Данюку І.І.* **академічної групи** *125-19-1*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації _____

за освітньо-професійною програмою *Кібербезпека*

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

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

Розділ	Зміст	Термін виконання
1	Проаналізувати нормативно-правову базу та підстави для створення КСЗІ та розробки політики безпеки.	30.04.2023
2	Виконати обстеження середовищ функціонування об'єкта інформаційної діяльності. Розробити моделі загроз та порушника безпеки інформації, проаналізувати ризики та сформувати основні положення політики безпеки інформації.	24.05.2023
3	Розрахувати економічну доцільність впровадження політики безпеки.	02.06.2023

Завдання видано _____ Ковальова Ю.В.
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: 17.04.2023 р.

Дата подання до екзаменаційної комісії: 12.06.2023 р.

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

РЕФЕРАТ

Пояснювальна записка: 81 с., 3 рис., 12 табл., 7 додатків, 15 джерел.

Об'єкт розробки: політика безпеки інформації інформаційно-комунікаційної системи ТОВ «Пауер системз».

Мета проекту: підвищення рівня безпеки інформації в інформаційно-комунікаційній системі ТОВ «Пауер системз», розробка рішень для захисту від загроз інформаційної безпеки.

У першому розділі описаний об'єкт: рід діяльності, фізичне середовище, в якому знаходиться об’єкт, устаткування, інформаційна система, програмне забезпечення, інформаційні потоки. Виконано класифікацію інформації, що циркулює в інформаційно-комунікаційній системі, визначений перелік джерел загроз, перелік вразливостей та перелік актуальних для інформаційно-комунікаційній системі загроз.

У другому розділі описано наявні в інформаційно-комунікаційній системі критерії захищеності та виконано вибір нових додаткових рекомендованих критеріїв захищеності, були розроблені рекомендації щодо розділів політики безпеки, що забезпечують реалізацію рекомендованих критеріїв захищеності та захист від актуальних для підприємства загроз.

В третьому розділі були розраховані витрати на впровадження та щорічну підтримку засобів та заходів, описаних у запропонованих розділах політики безпеки, оцінено можливі збитки від реалізації актуальних загроз. Була визначена економічна доцільність введення в експлуатацію рекомендацій щодо політики безпеки, розроблених в другому розділі.

Практичне значення проекту полягає в підвищенні інформаційної безпеки ТОВ «Пауер системз».

ПОЛІТИКА БЕЗПЕКИ, МОДЕЛЬ ЗАГРОЗ, ІНФОРМАЦІЙНА БЕЗПЕКА, ВРАЗЛИВОСТІ.

THE ABSTRACT

Explanatory note: 81 p., 3 fig., 12 tab., 7 appendices, 15 sources.

Object of elaboration: Development of the information security policy of the information and communication system of Power Systems LLC.

The purpose of the project: increasing the level of information security in information and communication system of Power Systems LLC, creation of solutions for protection against threats to information security.

In the first section the object has been described: type of activity, the physical environment in which the object is located, equipment, information system, software, information flows. The classification of information that circulates in the information and communication system has been made, the list of threats sources, the list of vulnerabilities and the list of threats relevant to ICS have been defined.

In the second section has been described the security criteria available in the information and communication system and selected new additional recommended security criteria, have been created recommendations for security policy sections that ensure the implementation of the recommended security criteria and protection from current threats.

In the third section, the costs of implementation and annual support of the means and measures, described in the proposed sections of the security policy, have been calculated, and possible losses from the realization of relevant threats have been defined. The economic benefit of safety policy recommendations, developed in the second section, implementation has been determined.

The practical significance of the project is to increase information security of Power Systems LLC.

SECURITY POLICY, MODEL OF THREATS, INFORMATION SECURITY, VULNERABILITIES.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ІКС – інформаційно-комунікаційна система;

КСЗІ – комплексна система захисту інформації;

НД ТЗІ – нормативний документ в галузі технічний захист інформації;

ОІД – об'єкт інформаційної діяльності;

ПЗ – програмне забезпечення;

ТОВ – товариство з обмеженою відповідальністю.

ЗМІСТ

ВСТУП

Підприємницька (комерційна) діяльність тісно пов'язана з отриманням, накопиченням, зберіганням, обробкою і використанням різноманітних інформаційних потоків. Однак захисту підлягає не вся інформація, а тільки та, яка представляє цінність для підприємства. При визначенні цінності підприємницької інформації необхідно керуватися такими критеріями (властивостями), як цілісність, доступність та конфіденційність.

Розробку заходів щодо збереження комерційної таємниці підприємства слід здійснювати, дотримуючись принципу комплексного перекриття можливих каналів витоку інформації та забезпечення рівнозначної надійності захисту всіх її носіїв. Загрози збереження комерційної таємниці можуть бути зовнішніми і внутрішніми.

Зовнішні дії можуть бути спрямовані на викрадення документів або зняття копій, знищення інформації або пошкодження носіїв, донесення інформації до конкурентів.

Зовнішні дії також можуть бути спрямовані на персонал компанії і виражатися підкупом, погрозами, шантажем, вивідуванням інформації, що становить таємницю.

Внутрішні загрози – це найбільші загрози для нових колективів, або колективів де не встигли скластися традиції підтримки високої репутації підприємства.

Глобальна комп’ютеризація у багатьох сферах управління та виробництва супроводжується появою принципово нових загроз інтересам особистості, підприємства, суспільства, держави.

РОЗДІЛ 1
СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧ

1.1 Стан питання

Бурхливий розвиток інформаційних технологій наприкінці XX ст. призвів до зростання відносної важливості окремих аспектів суспільного життя. Внаслідок інформаційної революції основною цінністю для суспільства взагалі й окремої людини зокрема поступово стають інформаційні ресурси. Організація соціуму почала трансформуватися у напрямку перерозподілу реальної влади від традиційних структур до центрів управління інформаційними потоками, зросла впливовість засобів масової інформації (ЗМІ). Інформатизація та комп'ютеризація докорінно змінюють обличчя суспільства. За таких обставин забезпечення інформаційної безпеки поступово виходить на перший план у проблематиці комерційної безпеки.

Успіх виробничої і підприємницької діяльності в чималому ступені залежить від уміння розпоряджатися таким найціннішим товаром, як інформація, але вигідно використовувати можна лише ту інформацію, яка потрібна ринку, але невідома йому. Тому в умовах посилення конкуренції успіх підприємництва, гарантія отримання прибутку все більшою мірою залежать від збереження в таємниці секретів виробництва, що спираються на певний інтелектуальний потенціал і конкретну технологію.

Підприємницька (комерційна) діяльність тісно пов'язана з отриманням, накопиченням, зберіганням, обробкою і використанням різноманітних інформаційних потоків. Однак захисту підлягає не вся інформація, а тільки та, яка представляє цінність для підприємства. При визначенні цінності підприємницької інформації необхідно керуватися такими критеріями (властивостями), як цілісність, доступність та конфіденційність.

Розробку заходів щодо збереження комерційної таємниці підприємства слід здійснювати, дотримуючись принципу комплексного перекриття можливих каналів витоку інформації та забезпечення рівнозначної надійності захисту всіх її носіїв. Загрози збереження комерційної таємниці можуть бути зовнішніми і внутрішніми.

Зовнішні дії можуть бути спрямовані на викрадення документів або зняття копій, знищення інформації або пошкодження носіїв, донесення інформації до конкурентів.

Зовнішні дії також можуть бути спрямовані на персонал компанії і виражатися підкупом, погрозами, шантажем, вивідуванням інформації, що становить таємницю.

Внутрішні загрози – це найбільші загрози для нових колективів, або колективів де не встигли скластися традиції підтримки високої репутації підприємства.

Глобальна комп'ютеризація у багатьох сферах управління та виробництва супроводжується появою принципово нових загроз інтересам особистості, підприємства, суспільства, держави.

Паралельно з розвитком і ускладненням засобів, методів, форм автоматизації процесів обробки інформації підвищується залежність суб'єктів підприємництва від ступеню безпеки використовуваних ними інформаційних технологій.

1.2 Аналіз нормативно-правової бази у сфері захисту інформації

Таблиця 1.1 – Аналіз нормативно-правової бази

Назва документу	Короткий зміст
Закон України «Про Інформацію»	У цьому документі визначені загальні положення про інформацію, а також права на інформацію та на забезпечення її охорони
Закон України «Про захист персональних даних»	У цьому документі визначені суб'єкти та об'єкти персональних даних. А також визначені правила та обов'язки по захисту персональних даних. Також визначена відповідальність за їх розголошення.

Продовження таблиці 1.1

Назва документу	Короткий зміст
Закон України «Про захист інформації в інформаційно-комунікаційних системах»	У цьому документі визначений порядок доступу до інформації. Також у цьому документі були визначені умови обробки інформації в системі і порядок її захисту.
НД ТЗІ 1.1-002 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу	Цей нормативний документ технічного захисту інформації (НД ТЗІ) визначає методологічні основи (концепцію) вирішення завдань захисту інформації в комп'ютерних системах і створення нормативних і методологічних документів, регламентуючих питання: - визначення вимог щодо захисту комп'ютерних систем від несанкціонованого доступу; - створення захищених комп'ютерних систем і засобів їх захисту від несанкціонованого доступу; - оцінки захищеності комп'ютерних систем і їх придатності для вирішення завдань споживача.
НД ТЗІ 3.7-001 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі	Цей нормативний документ встановлює вимоги до порядку розробки, складу і змісту технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі, призначеній для оброблення, зберігання і передачі інформації з обмеженим доступом або інформації, захист якої гарантується державою.

Продовження таблиці 1.1

Назва документу	Короткий зміст
НД ТЗІ 1.4-001 Типове положення про службу захисту інформації в автоматизованій системі	Цей нормативний документ системи технічного захисту інформації (НД ТЗІ) встановлює вимоги до структури та змісту нормативного документу, що регламентує діяльність служби захисту інформації в автоматизованій системі - “Положення про службу захисту інформації в автоматизованій системі”. НД ТЗІ призначений для суб’єктів відносин (власників або розпорядників АС, користувачів), діяльність яких пов’язана з обробкою в автоматизованих системах інформації, що підлягає захисту згідно з нормативно-правовими актами, а також для розробників комплексних систем захисту інформації в автоматизованих системах.
НД ТЗІ 2.5-004 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу	Цей нормативний документ (далі — Критерії) — установлює критерії оцінки захищеності інформації, оброблюваної в комп'ютерних системах, від несанкціонованого доступу. Критерії є методологічною базою для визначення вимог з захисту інформації в комп'ютерних системах від несанкціонованого доступу; створення захищених комп'ютерних систем і засобів захисту від несанкціонованого доступу.

Продовження таблиці 1.1

Назва документу	Короткий зміст
НД ТЗІ 2.5-005 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу	Цей документ установлює принципи класифікації автоматизованих систем і утворення стандартних функціональних профілів захищеності оброблюваної інформації від несанкціонованого доступу. Цей документ призначений для постачальників (розробників), споживачів (замовників, користувачів) автоматизованих систем, які використовуються для обробки (в тому числі збирання, зберігання, передачі і т. ін.) критичної інформації (інформації, яка потребує захисту), а також для державних органів, які здійснюють функції контролю за обробкою такої інформації. Мета цього документа — надання нормативно-методологічної бази для вибору і реалізації вимог з захисту інформації в автоматизованій системі.
НД ТЗІ 3.7-003 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі	Цей документ визначає основи організації та порядок виконання робіт із захисту інформації в інформаційно-комунікаційних системах (далі - ІКС) - порядок прийняття рішень в залежності від умов функціонування ІКС і видів оброблюваної інформації, визначення обсягу і змісту робіт, етапності робіт, основних завдань та порядку виконання робіт кожного етапу.

Продовження таблиці 1.1

Назва документу	Короткий зміст
ISO 27001	Цей міжнародний стандарт був підготовлений для того, щоб представити модель для створення, експлуатації, моніторингу, аналізу, супроводження Системою Управління Інформаційною Безпекою. Прийняття СУІБ повинно бути стратегічним рішенням для організації. На проектування та впровадження СУІБ здійснюють вплив бізнес цілі та потреби організації, витікаючи з них потреби безпеки.

1.3 Постановка задачі

Сучасні методи обробки, передачі та накопичення інформації сприяли появі погроз, пов'язаних з можливістю втрати, перекручування та розкриття даних, адресованих або належать кінцевим користувачам. Тому забезпечення інформаційної безпеки комп'ютерних систем і мереж є одним з провідних напрямків розвитку IT. Кількість загроз неможливо полічити, а статистика дає зрозуміти, що випадків з нанесенням шкоди стає дедалі більше.

В Україні є дуже добра нормативно-правова база, яка дозволяє на кожному рівні захищати інформацію. При вірному підході до захисту інформації, кількість загроз та ризиків для безпеки підприємств буде постійно зменшуватись.

Висновки до першого розділу

В наш час неможливо уявити підприємство на якому б не циркулювала інформація з обмеженим доступом. І багато підприємств у наш час не дотримується простих правил по їх захисту. Хоча у нашій державі існує достатня правова база для забезпечення безпеки інформації.

Було розглянуто статистику, загрози та ризики в інформаційній сфері, Ці дані дали зрозуміти, що захист інформації в сучасному світі є необхідною складовою. Для цього існує нормативно-правова база, яка допоможе на всіх рівнях забезпечити захист інформації.

РОЗДІЛ 2
СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальні відомості про підприємство

Об'єктом інформаційної діяльності є приватне підприємство «Пауер системз». ТОВ «Пауер системз» є постачальником сонячної електроенергії.

Режим роботи

Фірма працює з 8.00 до 19.00. Графік роботи постійний з понеділка по п'ятницю. Перерва з 12.00 до 14.00.

Прибирання приміщення проводиться кожного буднього дня після закінчення роботи офісів і контролюється охоронцем.

Охорона цілодобова, графік позмінний.

Підприємство займає увесь п'ятий поверх восьмиповерхового будинку.

Штат працівників

Директор - 1 людина. Координує роботу всіх ділянок.

Заступник директора – 1 людина. Виконує ті ж самі функції що і директор.

Бухгалтер - 1 людина. Веде бухгалтерську та іншу фінансову документацію, економічні розрахунки.

Відділ продажу - 4 людини. Приймають замовлення, укладають договори, забезпечують просування продукції.

Відділ кадрів – 2 людини. Виписують відрядження та проводять співбесіди щодо прийому на роботу.

Системний адміністратор – 2 людини. Займаються адмініструванням комп'ютерної мережі підприємства.

Служба інформаційної безпеки – 2 людини.

Охоронець - 2 людини.

Прибиральник – 2 людини.

Всього 19 осіб.

Контрольована зона (КЗ) визначена наказом керівника підприємства №1 від 30.01.2005 р. і обмежена п'ятим поверхом будівлі. ОІД обладнано системою

пожежної сигналізації та контролю доступу. Режим доступу здійснюється через контрольно-пропускний пункт (тобто вхід в будівлю здійснюється за пропусками та через охорону). Офіс підключено до пульту приватного охоронного підприємства «Ягуар» і також контролюється електронними перепустками-картками.

2.2 Обстеження об'єкта інформаційної діяльності.

Об'єкт знаходиться в БЦ «Pantex», розташований на вулиці із середнім транспортним рухом, і знаходиться в районі автовокзалу, де знаходиться кілька офісних будівель, а так само, торгових центрів. Спереду і ззаду будівлі знаходяться склади продовольчих товарів, а по краях будівлі два бізнес-центри.

На ситуаційному плані на малюнку 2.1 відображено положення об'єкта інформаційної діяльності щодо об'єктів місцевості.

Організація розташована на п'ятому поверсі восьмиповерхового будинку по вул. Середня, 35.

На даному підприємстві є 12 кімнат, а саме: бухгалтерія, відділ кадрів, адміністраторська, кабінет директора, конференц-зал, їдальня, приймальня, туалет (4 шт.), коридор.

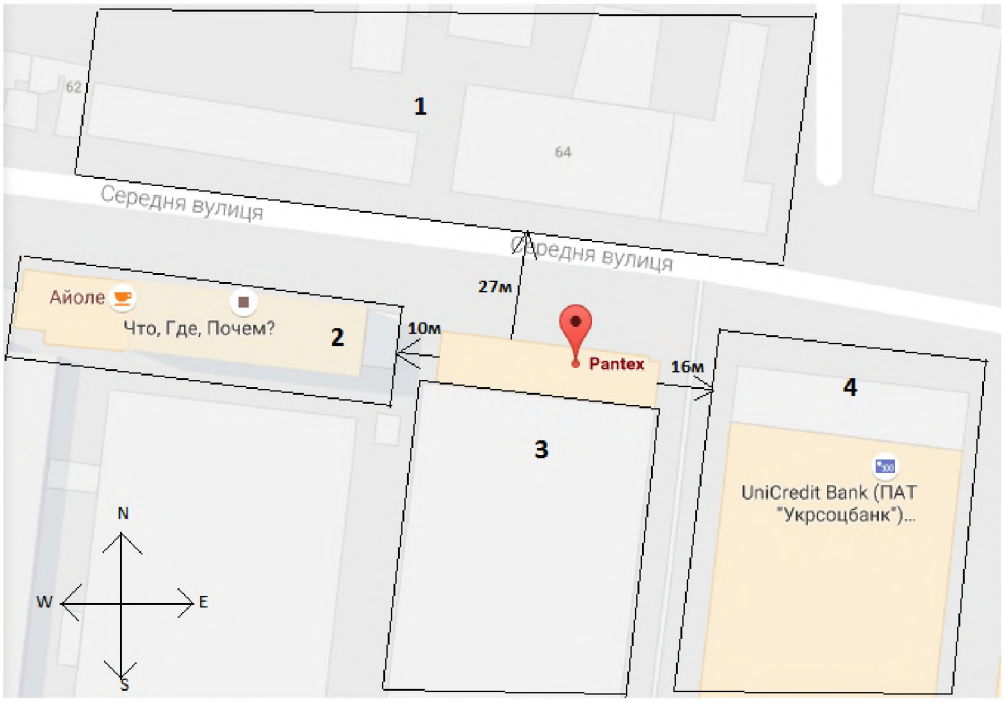

Рисунок 2.1 – Ситуаційний план

Площа офісу – 737 кв.м.

У тому числі:

- Коридор – 95 кв.м.
- Їдальня – 72 кв.м.
- Кабінет директора – 68 кв.м.
- Приймальня – 46 кв.м.
- Конференц-зал – 213 кв.м.
- Туалет (х4) – 4 кв.м.
- Відділ кадрів – 113 кв.м.
- Бухгалтерія – 60 кв.м.
- Адміністраторська – 54 кв.м.

На малюнку 2.2. вказана схема підприємства (генеральний план), розташування меблів і допоміжних приладів.

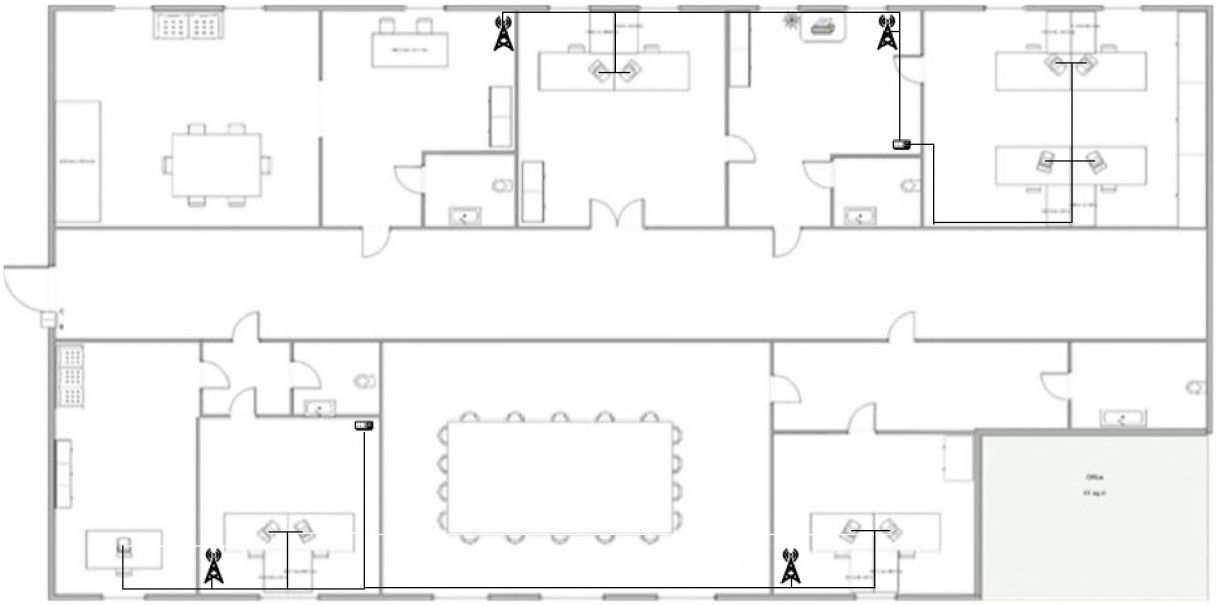

Рисунок 2.2 – Генеральний план

На досліджуваному ОІД циркулює інформація з обмеженим доступом: конфіденційна.

В мережі кожному комп'ютеру присвоєні імена, а саму мережу розділено на мережеві (робочі) групи (директор, адміністратор, останні користувачі). Кожна з цих груп має доступ лише до певних файлів, програм та інформації в цілому, у кожного

користувача свої права доступу. Вихід комп'ютерів до мережі Інтернет забезпечується через кабель.

У разі обміну, конфіденційну інформацію передають через захищений канал до хмарового сховища до якого приєднана уся мережа. Також обмін інформацією може відбуватись за допомогою електронної пошти яка контролюється системним адміністратором.

В приміщенні також є принтер, МФУ, телефони. Сервер виконує функцію проксі-сервера із подальшим збереженням інформації до хмарового сховища.
На рисунку 2.3 зображена схема мережі інформаційно-комунікаційної системи ТОВ «Пауер системз».

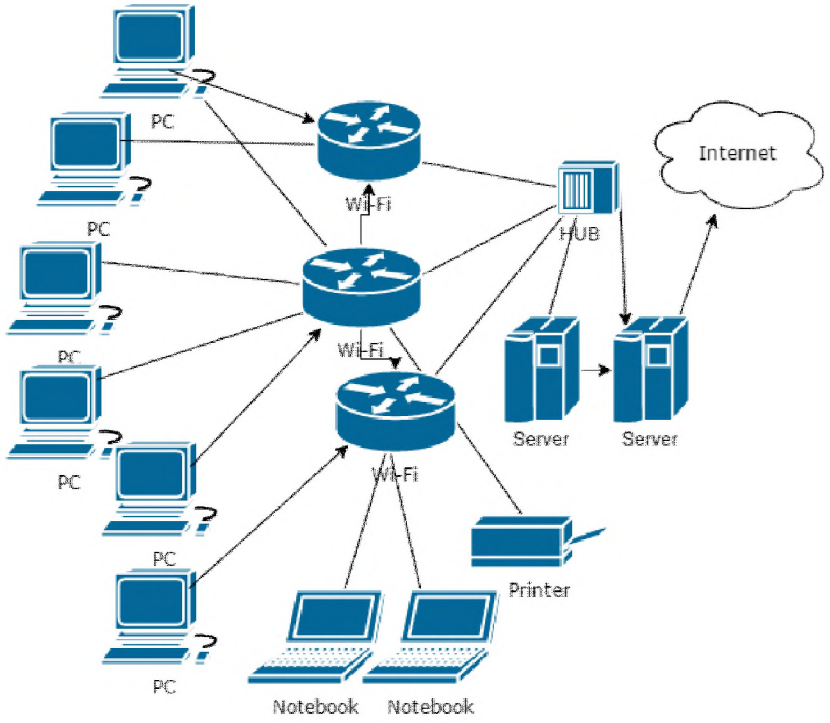

Рисунок 2.3 – Інформаційно-комунікаційна система

В таблиці 2 представлений перелік апаратного, а в таблиці 3 програмного забезпечення мережі ТОВ «Пауер системз».

Таблиця 2.1 – Апаратне забезпечення мережі

№ п/п	Найменування	Модель
	Wi-Fi роутер (4шт.)	TP-LINK WR-710

Продовження таблиці 2.1

№	Найменування	Модель
	Сервер (2шт.)	HP Proliant DL380 G7 2U
	Комутатор	D-Link DGS-1-24-222
	Ноутбук (2шт.)	ASUS K52S
	Робоча станція (6 шт.)	IBM Cartoon W-33-100
	Мережевий принтер	Samsung L-3080
	Монітори (6шт.)	Acer Predator K-33-200
	Мишка(8шт.)	A4Tech Bloody V10
	Клавіатура(6шт.)	Razer Blackwidow
	МФУ	Canon i-SENSYS MF4410
	Телефон(4шт.)	Siemens Gigaset A120 Black006B

Таблиця 2.2 – Програмне забезпечення мережі

№ п/п	Тип ПЗ	Найменування
	Операційна система	Windows 10 Ultimate x64 (ПК)
		Linux R2 Standard Edition VLC (Сервер)
	Прикладне ПЗ	Microsoft Office 2019
		Edge Browser
		Avast (антивірус)
		7Zip (архіватор)
		Thunderbird 24.3.0 (програма для роботи з електронною поштою)
	Бухгалтер	Odoo Enterprise (управління підприємством, бухоблік)
	Спеціальне ПЗ	Система електронного документообігу FossDoc

Продовження таблиці 2.2

№ п/п	Тип ПЗ	Найменування
		File Securer (призначена для блокування несанкціонованого доступу до файлів та програм)
		FileAssurity OpenPGP Lite (призначена для безпечного обміну даними через Інтернет між користувачами)
		Handy Backup Professional (призначена для резервного копіювання даних, забезпечує безпечну передачу даних на віддалений сервер)

2.3 Аналіз ризиків

Згідно Закону України «Про захист інформації» в ІКС ТОВ «Пауер системз» оброблюється і зберігається інформація з обмеженим доступом. На об'єкті захисту немає відомостей, що становлять державну таємницю.

Згідно Законів України «Про захист інформації в інформаційно-комунікаційних системах» та «Про захист персональних даних» порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються власником інформації. Власник інформації та інформаційної системи сам може визначити необхідність створення КСЗІ та КЗЗ, якщо це не суперечить чинному законодавству.

Таблиця 2.3. Перелік інформації, яка циркулює на Об’єкті інформаційної діяльності

№	Назва виду інформації	Режим доступу	Правовий режим	Вид зберігання	К	Ц	Д
1	Інформація про статут організації	відкрита		Паперовий та електронний		+	+

Продовження таблиці 2.3

2	Інформація про займані посади співробітників, ПІБ та їх робочі телефони	З обм.доступом	Служ.інф.	Електронний	+	+	
3	Інформація щодо графіку роботи організації	відкрита		Паперовий		+	+
4	Інформація про діяльність підприємства	відкрита		Паперовий та електронний		+	+
5	Інформація про списки філіалів підприємства регіону, партнерів	відкрита		Електронний		+	+
6	Персональні дані співробітників та їх посадові інструкції	З обм.доступом	ПД	Паперовий та електронний	+	+	
7	Інформація про фінансову діяльність організації (накладні,бухгалтерські звіти і заробітні плати співробітників)	З обм.доступом	Служ.інф.	Паперовий та електронний	+	+	+
8	Інформація про документи організації(службові записки, накази, розпорядження, звіти)	З обм.доступом	Служ.інф.	Паперовий та електронний	+	+	+

Таблиця 2.4 – Матриця доступу до інформації

Посада / Інформація	Директор	Служба безпеки	Бухгалтер	Відділ кадрів	Відділ продажу	Адміністратор системний
1	2	3	4	5	6	7
1	R,W,D	R,W	R	R	R	R
2	R,W,D	R,W	R,W	R	R	R
3	R,W,D	R,W	R	R	R	R
4	R,W,D	R,W	-	-	-	R,W
5	R,W,D	R ,W	-	-	-	-
6	R,W,D	R,W	R	-	-	R,W
7	R,W,D	-	R,W, D	-	-	-
8	R,W,D	R,W	R	-	-	R

В даній таблиці показано права доступу до всіх видів інформації з обмеженим доступом користувачів, які працюють на досліджуваному підприємстві. ОС:

- До принтеру мають доступ усі співробітники.

- До Інтернету працівники мають доступ, але на певні сайти доступ обмежений (вк, однокласники, тощо)

- Зовнішній носій (флешки, CD) мають доступ тільки директор та системний адміністратор.

Зарплата співробітників.

Обробкою інформації зарплати співробітників займається бухгалтер. Спочатку бухгалтер реєструє всю інформацію на комп'ютері про кількість змін, кількість годин, кількість вихідних. Потім для кожного робітника розраховує заробітну плату у спеціальній програмі. За допомогою платіжного поручення на виплату зарплати підприємство перечислює суму зарплати на рахунок банку. Тоді банк на основі

реєстру розподіляє суму, яка поступила на їхній рахунок по картам робітників підприємства. Ця інформація передається через електронну пошту та вона захищена ЕЦП.

Обов’язки персоналу.

Директор:

- Керує відповідно до чинного законодавства господарської та фінансово-економічною діяльністю ТОВ «Пауер системз», несучи всю повноту відповідальності за наслідки прийнятих рішень, збереження та ефективне використання майна.
- Забезпечує виконання компанією всіх зобов'язань перед сторонніми організаціями, замовниками послуг, покупцями, а також господарських, трудових договорів та бізнес-планів.
- Вирішує питання, що стосуються фінансово-економічної та господарської діяльності компанії, в межах наданих йому законодавством прав, доручає ведення окремих напрямків діяльності іншим посадовим особам - головному бухгалтеру.
- Розпоряджається інформацією про документи організації (службові записки, накази, розпорядження, звіти) та інформацією про займані посади співробітників, ПІБ та їх робочі телефони, персональними даними співробітників та їх посадові інструкції.
- Головний бухгалтер:
- Організовує роботу з постановки та ведення бухгалтерського обліку компанії з метою отримання зацікавленими внутрішніми та зовнішніми користувачами повної і достовірної інформації про її фінансово-господарської діяльності та фінансового стану.
- Очолює роботу: по забезпеченню порядку проведення інвентаризації та оцінки майна та зобов'язань, документального підтвердження їх наявності, стану та оцінки; по організації системи внутрішнього контролю за правильністю оформлення господарських операцій, дотриманням порядку документообігу,

технології обробки облікової інформації та її захисту від несанкціонованого доступу.

- Керує формуванням інформаційної системи бухгалтерського обліку та звітності відповідно до вимог бухгалтерського, податкового, статистичного та управлінського обліку, забезпечує надання необхідної бухгалтерської інформації внутрішнім і зовнішнім користувачам. Зараховує заробітну плату.
- Системний адміністратор:
- Знати перелік встановлених в підрозділі РС (АРМ) і перелік завдань, що вирішуються за їх використанням.
- Забезпечувати постійний контроль за виконанням співробітниками підрозділу (охоронці) встановленого комплексу заходів щодо забезпечення безпеки інформації в АС;
- Негайно повідомляти керівництву підрозділу і співробітникам служби забезпечення безпеки інформації (СЗБІ) про які мали місце в підрозділі спробах несанкціонованого доступу до інформації та технічних засобів ЕОМ, а також вживати необхідних заходів щодо усунення порушень.
- Розмежую доступ до інформації, яка циркулює на підприємстві.
- Видавати прості паролі співробітникам для входу в систему.
- Служба безпеки підприємства виконує наступні загальні функції:
- керує роботами по правовому й організаційному регулювання відносин щодо захисту комерційної таємниці;
- розробляє і здійснює спільно з іншими підрозділами заходи щодо забезпечення роботи з документами, що містять відомості, що є комерційною таємницею, при всіх видах робіт, організовує і контролює виконання вимог "ІНСТРУКЦІЇ щодо захисту комерційної таємниці";
- своєчасно виявляє і затримує осіб, які протиправно проникли (які намагаються проникнути) на території які охороняються;
- попереджує події на охоронюваному об'єкті і ліквідує наслідки.

- контролює об'єкт і що охороняється, зокрема території із особливим режимом пропуску, з метою виявлення й запобігання спроб несанкціонованого проникнення туди сторонніх осіб (зловмисників);
- забезпечує конфіденційність і збереження таємних фактів проведення закритих заходів для підприємства (його об'єктах), обговорюваних або розглядаються ними питань;
- супроводжує й охороняє носії конфіденційної комп'ютерної інформації, зокрема службові документи підприємства, ці матеріальні цінності;
- захищає об'єкти і території із особливим режимом пропуску від насильницьких діянь та збройних нападів, що потенційно можуть зашкодити підприємству;
- виконує у необхідних випадках спеціальні завдання щодо забезпечення особистої охорони керівництва підприємства і персоналу підприємства, допущеного до конфіденційної комп'ютерної інформації;

Служба безпеки є самостійною організаційною одиницею, що підкоряється безпосередньо керівнику підприємства. Очолює службу безпеки начальник служби безпеки.

Відділ кадрів:

- Має доступ до персональних даних усіх працівників та редагує усі зміни.
- Вносить до переліку працівників нових співробітників.
- Заповнює і видає відряджувальні листи.

Модель загроз

Джерела загроз поділяються на 3 основні групи:

1. Антропогенні – виступають об’єкти-користувачі, дії яких можуть бути кваліфіковані як умисні чи випадкові злочини. Ця група становить найбільший інтерес з точки зору організації захисту, так як дії об’єкта-користувачів завжди можна оцінити, спрогнозувати і вжити адекватних заходів.

2. Техногенні – спрямовані від технічних засобів, що оточують персонал, компоненти ІКС чи інформаційні ресурси.

3. Стихійні – характеризуються тим, що їх неможливо передбачити, або можливо передбачити, але неможливо уникнути. Такі джерела загроз не піддаються прогнозуванню та заходи, щодо захисту від них повинні застосовуватися завжди.

Таблиця 2.5 – Класифікація джерел загроз

Позначення	Джерело загрози	Рівень загрози
1	2	3
Антропогенні		
ПВн1	простий персонал (оператори, охорона, відділ продажу)	1
ПВн2	привілейований персонал (директор, бухгалтер, служба безпеки)	2
ПВн3	системний адміністратор	3
ПЗв1	Будь які особи, що знаходяться за межами КЗ	1
ПЗв2	Відвідувачі	2
ПЗв3	Конкуренти	3
ПЗв4	Кримінальні структури	3
ПЗв5	Хакери	2
Техногенні		
Т1	засоби зв'язку (телефон, Інтернет)	1
Т2	мережі інженерних комунікацій (система опалення, каналізації, водопостачання, заземлення, вентиляції, кондиціонування)	2
Т3	допоміжні засоби (відеоспостереження, сигналізація, протипожежна система)	2
Т4	неякісні технічні засоби обробки інформації (робочі станції, сервер, комутатор, система кабелів, принтери)	3
Т5	неякісні програмні засоби обробки інформації	3

Продовження таблиці 2.5

Стихійні		
С1	Пожежа	3
С2	Урагани та повені	2
С3	Інші форс-мажорні обставини	1
С4	Інші непередбачувані обставини	1

Модель порушника — абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії і т. ін. По відношенню до АС порушники можуть бути внутрішніми (з числа співробітників, користувачів системи) або зовнішніми

Таблиця 2.6 – Модель порушника

Позначення	Ознаки порушника	Рівень загрози
1	2	3
За мотивами		
Мт1	самоствердження	1
Мт2	безвідповідальність	2
Мт3	корисливий інтерес	3
За кваліфікацією		
К1	не має інформації щодо системи захисту	1
К2	знає особливості систем захисту на об’єкті	2
К3	знає структуру, функції та механізми систем захисту інформації	3
За часом		
Ч1	в неробочій час	1
Ч2	під час функціонування підприємства	2

Продовження таблиці 2.6

1	2	3
Ч3	в будь-який час	3
За місцем		
М1	без доступу до контрольованої зони	1
М2	з доступом до контрольованої зони, але без доступу до приміщень	2
М3	усередині приміщень, але без доступу до АС	3
М4	від робочих станцій співробітників компанії	3

Таблиця 2.7 – Специфікація порушників

Специфікація порушника	Загроза							
	ПВн1	ПВн2	ПВн3	ПЗв1	ПЗв2	ПЗв3	ПЗв4	Зв5
Мотив	Мт1,2	Мт2,3	Мт2,3	Мт3	Мт3	Мт3	Мт3,4	Мт3,4
Кваліфікація	К1	К2	К2	К1	К1	К1	К1	К2,3
Час дії	Ч1	Ч2	Ч2	Ч3	Ч2	Ч3	Ч3	Ч3
Місце дії	М2,3	М4	М4	М1,2	М3,4	М3,4	М1	М1

Згідно таблиці 2.6 – Модель порушника, можна зробити висновок, що загрози для підприємства становлять: простий персонал (оператори, охорона, відділ продажу), привілейований персонал (директор, бухгалтер, служба безпеки), системний адміністратор та хакери. У них підсумок становить вище 10 балів. Всі інші (відвідувачі, кримінальні структури, конкуренти) не становлять загрозу, так як підсумок менше 10 балів, тому далі їх можна не розглядати.

Основні вразливості

Перелік основних вразливостей ІКС на підприємстві ТОВ «Пауер системз» вказана у таблиці.

Таблиця 2.8 – Перелік вразливостей

Залишені без нагляду документи та незаблоковані робочі станції
Залишені без нагляду мобільні робочі станції
Розголошення, передача атрибутів розмежування доступу
Пошкодження мережевих кабелів
Вплив на співробітників (шантаж, погрози, методи соціальної інженерії)
Випадкові помилки співробітників
Пошкодження носіїв інформації внаслідок пожару
Мережеві кабелі перетинаються з іншими провідними лініями
Відмова зовнішніх джерел електроживлення
Несвоєчасне оновлення ОС та прикладного ПО
Несвоєчасне оновлення системи антивірусного захисту
Несвоєчасна профілактика роботи робочих станцій
Помилки при розмежуванні доступу до інформації
Несвоєчасне оновлення ОС
Відсутність фільтрування пакетів та NAT
Використання ненадійних протоколів передачі даних

Таблиця 2.9 – Аналіз загроз

Джерело загрози	Вразливість	Загроза	Ресурс, який піддається впливу	Ступінь впливу	Імовірність	Рівень небезпеки
1	2	3	4	5	6	7
Антропогенні						

Продовження таблиці 2.9

1	2	3	4	5	6	7
ПВн1, ПВн2, ПВн3	Відсутність системи контролю доступу співробітників до чужих робочих місць	порушення режиму розмежування доступу	інформація, до якої співробітник має доступ	С	В	В
ПВн1, ПВн2, ПВн3	помилки співробітників при роботі з інформацією	модифікація інформації, знищення інформації	інформація, що обробляється в даний момент	С	С	В
ПВн3	помилки при розмежуванні доступу до інформації	порушення режиму розмежування доступу	інформація, що обробляється на носії	В	С	В
ПВн3	Відсутність резервного копіювання	Знищення усієї інформації без доступу повернення	Інформація, що зберігається в системі	В	В	В
ПВн1, ПВн2, ПВн3, ПЗв2, ПЗв3	Залишені без нагляду документи та незаблоковані робочі станції	порушення режиму розмежування доступу	інформація, до якої має доступ користувач	С	С	В

Продовження таблиці 2.9

1	2	3	4	5	6	7
ПВн3	несвоєчасне оновлення системи антивірусного захисту	знищення, втрата доступності до інформації	інформація, що обробляється в системі	С	Н	С
ПВн1, ПВн2, ПВн3, ПЗв2 ПЗв4	Залишені без нагляду мобільні робочі станції	Крадіжка ноутбуків (Порушення режиму розмежування доступу)	Інформація, що зберігається на даній мобільній робочій станції	В	Н	С
ПЗв3 ПЗв4 ПЗв5	Вплив на співробітників (шантаж, погрози, фізичні розправи)	Порушення режиму розмежування доступу, блокування чи модифікація інформації	Інформація до якої мав доступ цей користувач	В	С	В
ПВн2, ПВн3	Розголошення, передача атрибутів розмежування доступу	Порушення режиму розмежування доступу	Інформація, до якої мав доступ користувач	В	С	В
Т4	Несвоєчасна профілактика роботи робочих станцій	Відмова в обслуговуванні ОС чи прикладного ПО	Інформаціящо зберігається та оброблюється на робочій станції			

Продовження таблиці 2.9

1	2	3	4	5	6	7
Техногенні та стихійні						
Т4	пошкодження носіїв інформації або мережевого обладнання	порушення доступності, цілісності інформації	інформація, що передається, зберігається	С	С	С
Т1, Т2	перетин мережевих кабелів з іншими провідними лініями	модифікація, знищення інформації	інформація, що передається	С	Н	Н
Т5	неякісні програмні засоби обробки інформації	порушення режиму розмежування доступу, знищення, втрата доступності до інформації	інформація, що обробляється на даному пристрої	С	Н	Н
Т4	неякісні технічні засоби обробки інформації	порушення режиму розмежування доступу, знищення, втрата доступності до інформації	інформація, що обробляється на даному пристрої	С	Н	Н

Продовження таблиці 2.9

1	2	3	4	5	6	7
Т2	залежність від зовнішніх джерел електроживлення (відсутність безперебійника)	порушення доступності інформації	інформація, що обробляється на даному пристрої	В	С	В
С3	близько розташовані виробництва, які можуть нанести загрозу підприємству	знищення, втрата доступності до інформації	інформація, що обробляється в системі	Н	Н	Н
С1, С2	пошкодження носіїв інформації або мережевого обладнання	порушення доступності інформації	інформація, що обробляється на носії	С	Н	Н

2.4 Обґрунтування необхідності створення КСЗІ

Згідно НД ТЗІ 3.7-003 -2005:

1. Підставою для визначення необхідності створення КСЗІ є норми та вимоги чинного законодавства, які встановлюють обов'язковість обмеження доступу до певних видів інформації або забезпечення її цілісності чи доступності, або прийняте власником інформації рішення щодо цього, якщо нормативно-правові акти надають йому право діяти на власний розсуд.

2. Вихідні дані для обґрунтування необхідності створення КСЗІ у загальному випадку одержуються за результатами:

- аналізу нормативно-правових актів (державних, відомчих та таких, що діють в межах установи, організації, підприємства), на підставі яких може встановлюватися обмеження доступу до певних видів інформації чи заборона такого обмеження, або

визначатися необхідність забезпечення захисту інформації згідно з іншими критеріями;

- визначення наявності у складі інформації, яка підлягає автоматизованій обробці, таких її видів, що потребують обмеження доступу до неї або забезпечення цілісності чи доступності відповідно до вимог нормативно-правових актів;
- оцінки можливих переваг (фінансово-економічних, соціальних і т.п.) експлуатації ІКС у разі створення КСЗІ.

3. На підставі проведеного аналізу приймається рішення про необхідність створення КСЗІ.

Згідно Законів України «Про захист інформації в інформаційно-комунікаційних системах» та «Про захист персональних даних» порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються власником інформації. Власник інформації та інформаційної системи сам визначає необхідність створення КСЗІ, якщо це не суперечить чинному законодавству

2.5 Розробка положень політики безпеки ІКС ТОВ «Пауер системз»

2.5.1 Вибір профілю захищеності

Відповідно до документів: «НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» та «НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» встановимо клас АС, функціональний профіль захищеності та критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

Клас «3» — розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу.

Стандартний профіль захищеності АС – 3.КЦД.1 функціональний профіль захищеності в КС, що входить до складу АС класу 3, з підвищеними вимогами до забезпечення властивостей інформації:

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 }

2.5.1.1 Критерії конфіденційності

Для того, щоб КС могла бути оцінена на предмет відповідності критеріям конфіденційності, КЗЗ оцінюваної КС повинен надавати послуги з захисту об'єктів від несанкціонованого ознайомлення з їх змістом (компрометації). Конфіденційність забезпечується такими послугами: довірча конфіденційність, адміністративна конфіденційність, повторне використання об'єктів, аналіз прихованих каналів, конфіденційність при обміні.

1. Довірча конфіденційність

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

1.1 КД-2. Базова довірча конфіденційність

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

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

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

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

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

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

Необхідні умови: НИ-1.

2. Повторне використання об'єктів

Ця послуга дозволяє забезпечити коректність повторного використання розділюваних об'єктів, гарантуючи, що в разі, якщо розділюваний об'єкт виділяється новому користувачу або процесу, то він не містить інформації, яка залишилась від попереднього користувача або процесу.

2.2 КО-1. Повторне використання об'єктів

Політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС.

Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані.

Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною.

Необхідні умови: немає.

3. Конфіденційність при обміні

Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжуються на підставі повноти захисту і вибірковості керування.

3.1 КВ-1. Мінімальна конфіденційність при обміні

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

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

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

НЕОБХІДНІ УМОВИ: НЕМАЄ.

2.5.1.2 Критерії цілісності

Для того, щоб КС могла бути оцінена на предмет відповідності критеріям цілісності, КЗЗ оцінюваної КС повинен надавати послуги з захисту оброблюваної інформації від несанкціонованої модифікації. Цілісність забезпечується такими послугами: довірча цілісність, адміністративна цілісність, відкат, цілісність при обміні.

1. Довірча цілісність

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

1.1 ЦД-1. Мінімальна довірча цілісність

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

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

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

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

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої цілісності

мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту.

Необхідні умови: НІ-1.

2. Відкат

Ця послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкатити) захищений об'єкт до попереднього стану. Рівні даної послуги ранжуються на підставі множини операцій, для яких забезпечується відкат.

2.1 ЦО-1. Обмежений відкат

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

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

Необхідні умови: НІ-1.

3. Цілісність при обміні

Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжуються на підставі повноти захисту і вибірковості керування.

3.1 ЦВ-1. Мінімальна цілісність при обміні

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

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

Необхідні умови: немає.

2.5.1.3 Критерії доступності

Для того, щоб КС могла бути оцінена на відповідність критеріям доступності, КЗЗ оцінюваної КС повинен надавати послуги щодо забезпечення можливості використання КС в цілому, окремих функцій або оброблюваної інформації на певному проміжку часу і гарантувати спроможність КС функціонувати у випадку відмови її компонентів. Доступність може забезпечуватися в КС такими послугами: використання ресурсів, стійкість до відмов, гаряча заміна, відновлення після збоїв.

1. Використання ресурсів

Ця послуга дозволяє користувачам керувати використанням послуг і ресурсів. Рівні даної послуги ранжуються на підставі повноти захисту і вибірковості керування доступністю послуг КС.

1.1 ДР-1. Квоти

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

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

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

Необхідні умови: НО-1.

2. Відновлення після збоїв

Ця послуга забезпечує повернення КС у відомий захищений стан після відмови або переривання обслуговування. Рівні даної послуги ранжуються на підставі міри автоматизації процесу відновлення.

2.1 ДВ-1. Ручне відновлення

Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов КС і переривань обслуговування, після яких можливе повернення у відомий

захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція КС.

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

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

Необхідні умови: НО-1.

2.5.1.4 Критерії спостереженості

Для того, щоб КС могла бути оцінена на предмет відповідності критеріям спостереженості, КЗЗ оцінюваної КС повинен надавати послуги з забезпечення відповідальності користувача за свої дії і з підтримки спроможності КЗЗ виконувати свої функції. Спостереженість забезпечується в КС такими послугами: реєстрація (аудит), ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність КЗЗ, самотестування, ідентифікація і автентифікація при обміні, автентифікація відправника, автентифікація отримувача.

1. Реєстрація

Реєстрація дозволяє контролювати небезпечні для КС дії. Рівні даної послуги ранжуються залежно від повноти і вибірковості контролю, складності засобів аналізу даних журналів реєстрації і спроможності вияву потенційних порушень.

1.1 НР-2. Захищений журнал

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

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

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

КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування.

Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації.

Необхідні умови: НІ-1, НО-1.

2. Ідентифікація і автентифікація

Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до КС. Рівні даної послуги ранжуються залежно від числа задіяних механізмів автентифікації.

2.1 НІ-2. Одиночна ідентифікація і автентифікація

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

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

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

Необхідні умови: НК-1.

3. Достовірний канал

Ця послуга дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ. Рівні даної послуги ранжуються залежно від гнучкості надання можливості КЗЗ або користувачу ініціювати захищений обмін.

3.1 НК-1. Однонаправлений достовірний канал

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

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

Необхідні умови: немає.

4. Розподіл обов'язків

Ця послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Рівні даної послуги ранжуються на підставі вибірковості керування можливостями користувачів і адміністраторів.

4.1 НО-2. Розподіл обов'язків адміністраторів

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

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

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

Необхідні умови: НІ-1.

5. Цілісність комплексу засобів захисту

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

5.1 НЦ-2. КЗЗ з гарантованою цілісністю

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

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

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

Необхідні умови: немає.

6. Самотестування

Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Рівні даної послуги ранжуються на підставі можливості виконання тестів у процесі запуску або штатної роботи.

6.1 НТ-2. Самотестування при старті

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

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

Необхідні умови: НО-1.

7. Ідентифікація і автентифікація при обміні

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

7.1 НВ-1. Автентифікація вузла

Політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ.

КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму.

Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації.

Необхідні умови: немає.

2.5.6 Фізична безпека та безпека навколишнього середовища

За для покращення фізичного захисту на підприємстві повинні бути введені додаткові засоби фізичного захисту.

2.5.6.1 Механізми контролю фізичного входу

Захищаємі області будуть захищені механізмами контролю входу, що забезпечують можливість доступу тільки для авторизованого персоналу. Тому на вході до КЗ будуть встановлені електронні замки із зчитувальним пристроєм контроля доступу.

2.5.6.2 Захист офісів, кімнат та обладнання

Були спроєктовані і будуть використовуватися механізми забезпечення фізичної безпеки офісів, кімнат та обладнання. За для цього у офісі компанії не повинно бути «мертвих зон», де унеможливлюється контроль за сторонніми особами(окрім зон указаних у законі). Для виконання цієї задачі буде встановлено додаткові датчики руху і камери внутрішнього спостереження.

2.5.6.3 Захист від зовнішніх загроз і загроз навколишнього середовища

За для фізичного захисту від стихійних небезпек, стіни підприємства ТОВ «Пауер системз» будуть посилені армованою сіткою та обшиті негорючими облицювальними матеріалами.

2.5.6.4 Допоміжні служби та захист кабелів

За для захисту від збоїв електропостачання, а також забезпечення захисту від прослуховування та пошкодження кабелів, усі кабелі будуть ізольовані спеціальними оболонками, а на підприємстві встановлено додаткові мережеві фільтри та автономний електрогенератор.

2.5.6.5 Комп’ютерна база

За для забезпечення безпеки інформації повинні використовуватися якісні пристрої. У багатьох пристроїв на підприємстві вже вийшов термін їх експлуатації, а тому було вирішено обновити матеріальну базу комп’ютерної техніки.

2.6 Аналіз ризиків інформаційної безпеки після впровадження політики безпеки

Таблиця 2.10 – Аналіз загроз після впровадження політики безпеки

Джерело загрози	Вразливість	Загроза	Ресурс, який піддається впливу	Ступінь впливу	Імовірність	Рівень небезпеки
1	2	3	4	5	6	7
Антропогенні						
ПВн1, ПВн2, ПВн3	Відсутність системи контролю доступу співробітників до чужих робочих місць	порушення режиму розмежування доступу	інформація, до якої співробітник має доступ	С	Н	В
ПВн1, ПВн2, ПВн3	помилки співробітників при роботі з інформацією	модифікація інформації, знищення інформації	інформація, що обробляється в даний момент	С	Н	В
ПВн3	помилки при розмежуванні доступу до інформації	порушення режиму розмежування доступу	інформація, що обробляється на носії	В	Н	В

Продовження таблиці 2.10

1	2	3	4	5	6	7
ПВн1, ПВн2, ПВн3, ПЗв2, ПЗв3	Залишені без нагляду документи та незаблоковані робочі станції	порушення режиму розмежування доступу	інформація, до якої має доступ користувач	С	Н	В
ПВн3	несвоєчасне оновлення системи антивірусного захисту	знищення, втрата доступності до інформації	інформація, що обробляється в системі	С	Н	С
ПВн1, ПВн2, ПВн3, ПЗв2 ПЗв4	Залишені без нагляду мобільні робочі станції	Крадіжка ноутбуків (Порушення режиму розмежування доступу)	Інформація, що зберігається на даній мобільній робочій станції	В	Н	С
ПЗв3 ПЗв4 ПЗв5	Вплив на співробітників (шантаж, погрози, фізичні розправи)	Порушення режиму розмежування доступу, блокування чи модифікація інформації	Інформація до якої мав доступ цей користувач	В	Н	В

Продовження таблиці 2.10

1	2	3	4	5	6	7
ПВн2, ПВн3	Розголошення, передача атрибутів розмежування доступу	Порушення режиму розмежування доступу	Інформація, до якої мав доступ користувач	В	Н	В
Т4	Несвоєчасна профілактика роботи робочих станцій	Відмова в обслуговуванні ОС чи прикладного ПО	Інформація, що зберігається та оброблюється на робочій станції			
Техногенні та стихійні						
Т4	пошкодження носіїв інформації або мережевого обладнання	порушення доступності, цілісності інформації	інформація, що передається, зберігається	С	Н	С
Т1, Т2	перетин мережевих кабелів з іншими провідними лініями	модифікація, знищення інформації	інформація, що передається	С	Н	Н
Т5	неякісні програмні засоби обробки інформації	порушення режиму розмежування доступу, знищення, втрата доступності до інформації	інформація, що обробляється на даному пристрої	С	Н	Н

Продовження таблиці 2.10

1	2	3	4	5	6	7
Т2	залежність від зовнішніх джерел електроживлення (відсутність безперебійника)	порушення доступності інформації	інформація, що обробляється на даному пристрої	С	С	В
С3	близько розташовані виробництва, які можуть нанести загрозу підприємству	знищення, втрата доступності до інформації	інформація, що обробляється в системі	Н	Н	Н
С1, С2	пошкодження носіїв інформації або мережевого обладнання	порушення доступності інформації	інформація, що обробляється на носії	С	Н	Н

Завдяки впровадженню політики безпеки нам вдалося значно знизити ризика майже за усіма показниками.

Висновки до другого розділу

В наш час завдяки розвиненим технологіям і міцній правовій базі можна з легкістю забезпечити захист на підприємстві. Чим я і займався у цьому розділі написавши рекомендації до покращення системи захисту на підприємстві ТОВ «Пауер системз».

Проаналізувавши загрози після впровадження політики безпеки ми можемо зробити висновок, що її впровадження значно підвищить захист системи і дозволить не хвилюватися за те, що інформація буде втрачена.

РОЗДІЛ 3
ЕКОНОМІЧНА ЧАСТИНА

Метою виконання економічного розділу є визначення того, чи буде використання запропонованих засобів та заходів інформаційної безпеки в ТОВ «Пауер системз» вигідним для підприємства.

3.1 Необхідність обґрунтування витрат на реалізацію політики безпеки.

Для цього визначено економічну ефективність використання основних результатів, що отримані в результаті виконання роботи.

Економічна доцільність визначається розрахунками:

- капітальних витрат, що потребує розроблена політика безпеки;
- експлуатаційних витрат;
- річного економічного ефекту від впровадження інформаційної політики безпеки.

Запропонована політика інформаційної безпеки передбачає необхідність витрат на її реалізацію. Заходами, що потребують витрат, є:

- оновлення ліцензій програмного забезпечення;
- навчання персоналу в питаннях інформаційної безпеки.

3.2 Визначення трудомісткості розробки політики безпеки інформації

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

Де $t_{тз}$ = 6 год - тривалість складання технічного завдання на розробку політики безпеки інформації;

$t_{в}$ = 4 год - тривалість розробки концепції безпеки інформації у організації;

$t_{а}$ = 2 год – тривалість процесу аналізу ризиків;

tвз = 4 год – тривалість визначення вимог до заходів, методів та засобів захисту;

tозб = 3 год – тривалість вибору основних рішень з забезпечення безпеки інформації;

товр = 2 год – тривалість організації виконання відновлювальних робіт забезпечення неперервного функціонування організації;

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

t = 6 год + 4 год + 2 год + 4 год + 3 год + 2 год + 4 год = 25 год

3.3 Розрахунок витрат на створення політики безпеки

$$Крп = Ззп + Змч, \quad (3.3)$$

де Крп – витрати на створення політики безпеки;

Ззп – заробітна плата спеціаліста з інформаційної безпеки;

Змч – вартість витрат машинного часу, що необхідні для створення політики безпеки.

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

$$Ззп = t * Зіб = 25 * 200 = 5000 \text{ грн}$$

де t – загальна тривалість розробки політики безпеки, год;

Зіб – средньогодинна заробітна плата спеціаліста з інформаційної безпеки становить 200 грн/год.

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

$$Змч = t * Смч, \text{грн}$$

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

Смч – вартість 1 години машинного часу ПК, грн/год.

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = Р * tнал * Се + \frac{Фзал * На}{Fp} + \frac{Клпз * Напз}{Fp} =$$

$$= 0{,}2 * 2 * 1{,}68 + \frac{(6000 * 0{,}2)}{1920} + \frac{7000 * 0{,}2}{1920} =$$

$$= 0{,}67 + 0{,}63 + 0{,}73 = 2{,}03 \text{ грн/год},$$

Де Р- встановлена потужність апаратури інформаційної безпеки, 0.3 кВт - середня потужність одного комп'ютера;

tнал – кількість машин на яких розроблюється політика безпеки;

Се – тариф на електричну енергію, 1,68 грн/кВт·год;

Фзал – залишкова вартість ПК на поточний рік, 6000 грн;

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

Напз – річна норма амортизації на ліцензійне програмне забезпечення, 0,2 частки одиниці;

Клпз – вартість ліцензійного програмного забезпечення, 7000 грн;

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

$$Змч = t * Смч = 25 * 2{,}03 = 50{,}75 \text{ грн}$$

$$Крп = Ззп + Змч = 5000 + 50{,}75 = 5050{,}75 \text{ грн}$$

3.4 Розрахунок (фіксованих) капітальних витрат.

Оновлення ліцензії системного, прикладного і спеціалізованого ПЗ: Avast Antivirus Pro Plus - 525 грн (вартість ліцензії для одного ПК на рік), Windows 11 Pro

— 1150 грн на рік, MS Office 2019 – 2210 грн на рік, Odoo Enterprise – 1000 грн на рік. Необхідно оновлення ПЗ для 4 комп'ютерів.

Загальна вартість закупівель ліцензійного ПЗ:

$$Кзпз = 4 * 4885 \text{ грн} = 19540 \text{ грн} \quad (3.4)$$

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

$$К = Кпр + Кзпз + Крп + Каз + Кнавч + Кн,$$

де Кпр – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, 9000 грн;

Кзпз – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), 19540 грн;

Каз – вартість закупівель апаратного забезпечення та допоміжних матеріалів відсутня, оскільки за розробленими політики безпеки закупівля апаратного забезпечення не є необхідною.

Кнавч - витрати на навчання адміністратора безпеки, становлять 3000 грн.

Крп – вартість розробки політики безпеки інформації, 5050,75 грн;

Кн – витрати на встановлення обладнання та налагодження системи інформаційної безпеки відсутні, оскільки не закуповується апаратне забезпечення.

$$К = Кпр + Кзпз + Крп + Каз + Кнавч + Кн =$$
$$= 9000 + 19540 + 5050,75 + 3000 = 36590,75 \text{ грн}$$

3.5 Розрахунок поточних (експлуатаційних) витрат.

- навчання персоналу в питаннях інформаційної безпеки;
- витрати на керування системою інформаційної безпеки.

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

Со = 1300 грн – витрати на навчання персоналу.

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

$$Сз = Зк + Заб = 1666{,}67 + 1666{,}67 = 3333{,}34 \text{ грн (за 1 місяць)} \qquad (3.5)$$

$$Сз = 3333{,}34 * 12 = 40000{,}08 \text{ грн (за 1 рік)}$$

де Зк – додаткова заробітна плата керівника, 20000 грн на рік.

Заб – додаткова заробітна плата адміністратора безпеки, 20000 грн. на рік.

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

$$Се = Р * Fp * Це$$

де Р – встановлена потужність апаратури інформаційної безпеки (0,3 кВт*4 комп'ютерів = 1,2 кВт)

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

Це = 1,68 грн за 1 кВт/год – тариф на електроенергію на 01.01.2023 року.

$$Се = 1{,}2 * 7680 * 1{,}68 = 15482{,}88 \text{ грн}$$

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

$$\text{Стос} = \text{К} * 0{,}02 = 36590{,}75 * 0{,}02 = 731{,}82 \text{ грн}$$

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

$$\text{С} = \text{Со} + \text{Сз} + \text{Се} + \text{Стос} =$$

$$= 1300 + 40000{,}08 + 15482{,}88 + 731{,}82 = 57514{,}78 \text{ грн.}$$

Розрахунок оцінки величини збитку:

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

Таблиця 3.1 Заробітні плати працівників за місяць

Посада	**Розмір зар. плати**	**Кількість співробітників**	**Витрати на зар. плату на міс., грн**
Директор	30000	1	30000
Заступник директора	20000	1	20000
Бухгалтер	15000	1	15000
Менеджер відділу продажу	15000	4	60000
Менеджер відділу кадрів	15000	2	30000
Системний адміністратор	14000	2	28000
Працівник служби інформаційної безпеки	15000	2	30000
		Сума:	213000

Місячний фонд робочого часу складає 160 годин. Річний – 1920 годин. Час простою внаслідок атаки tп = 4 год.

$$Пп = (Зс/Fр) * tв = (213000/160) * 4 = 5325 \text{ грн}$$

Витрати на відновлення працездатності системи включають кілька складових:

Пви – витрати на повторне введення інформації, грн;

Ппв – витрати на відновлення системи, грн;

Пзч – вартість заміни частин системи, грн.

Витрати на повторне введення інформації розраховуються виходячи з розміру заробітної плати співробітників системи Зс, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу tви = 8 год:

$$Пви = (213000/160) * 8 = 10650 \text{ грн}$$

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

$$Ппв = (14000/160) * 4 = 350$$

Витрати на відновлення працездатності системи:

$$Пв = Пви + Ппв + Пзч = 10650 + 350 + 7000 = 18000 \text{ грн}$$

Пзч = 7000 грн - вартість для витрат на заміну частин;

О = 1900000 грн - обсяг чистого прибутку за рік.

Втрати від зниження працездатності атакованої системи:

$$V = О/Fр * (tп + tв + tви) = 1900000/1920 * (3 + 4 + 8) = 14843{,}75 \text{ грн}$$

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

tп – 4 годин простою після атаки;

tв – 4 годин відновлення після атаки;

tви – 8 годин повторного введення загубленої інформації під час атаки;

Таким чином, загальний збиток від атаки на ІКС відділення при реалізації загрози складе:

$$U = Пп + Пв + V = 5325 + 18000 + 14843{,}75 = 38168{,}75 \text{ грн}$$

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

$$B = \sum_i \sum_n * U = 3 * 4 * 38168{,}75 \ = 458025 \text{ грн}$$

де: і- число атакованих вузлів, 3 комп'ютери;

n – середнє число атак на рік, 4 рази.

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

Ймовірність R (0…1). Якщо реалізація загроз найімовірніша 1 раз на 3 місяці, тобто 4 рази на рік, то R=0,25.

Загальний ефект від впровадження політики безпеки:

$$E = B * R - C = 458025 * 0{,}25 - 57514{,}78 = 56991{,}47 \text{ грн}$$

Визначення та аналіз показників економічної ефективності системи інформаційної безпеки:

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

- коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI (Return on Investment for Security);
- термін окупності капітальних інвестицій То.

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

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

Коефіцієнт ROSI розраховують за допомогою показників:

Е – загальний ефект від впровадження системи інформаційної безпеки, грн;

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

$$\text{ROSI} = \text{E}/\text{K} = 56991{,}47/36590{,}75 = 1{,}56$$

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

$$\text{To} = \text{K}/\text{E} = 1/\text{ROSI} = 1 / 1{,}56 = 0{,}64 \text{ років} = 7{,}68 \text{ місяців}.$$

Висновки до третього розділу

Розробка і впровадження політики інформаційної безпеки для ТОВ «Пауер системз» можна назвати економічно доцільними, так як витрати на її створення значно менші за суму збитків, завдяки невеликій вартості комплектуючих, необхідних для відновлення системи та її інформаційних ресурсів у разі успішних атак порушників.

Тому в результаті:

- капітальні витрати на впровадження інформаційної політики безпеки становлять 36590,75 грн;
- експлуатаційні витрати на впровадження інформаційної політики безпеки становлять 57514,78 грн.;
- загальний збиток від атаки на вузол складає 458025 грн;
- ефект від впровадження системи інформаційної безпеки становить 56991,47 грн;
- термін окупності капітальних інвестицій складатиме 7,68 місяців.

Отже, економічна доцільність обґрунтована і впровадження інформаційної політики безпеки може бути ефективним та успішним.

ВИСНОВКИ

В кваліфікаційній роботі було проаналізовано ризики на підприємстві та приведені рекомендації щодо покращення системи захисту.

В наш час неможливо уявити підприємство на якому б не циркулювала інформація з обмеженим доступом. І багато підприємств у наш час не дотримується простих правил по їх захисту. Хоча у нашій державі існує достатня правова база для забезпечення безпеки інформації.

Було розглянуто статистику, загрози та ризики в інформаційній сфері, Ці дані дали зрозуміти, що захист інформації в сучасному світі є необхідною складовою. Для цього існує нормативно-правова база, яка допоможе на всіх рівнях забезпечити захист інформації.

В наш час завдяки розвиненим технологіям і міцній правовій базі можна з легкістю забезпечити захист на підприємстві. Щодо цього були надані рекомендації для покращення системи захисту на підприємстві ТОВ «Пауер системз».

Проаналізувавши загрози після впровадження політики безпеки ми можемо зробити висновок, що її впровадження має економічну доцільність.

У економічній частині кваліфікаційної роботи була запропонована політика безпеки інформації та було розраховано витрати на її створення в ТОВ «Пауер системз». Також було розраховано і обґрунтовано ефект від впровадження системи інформаційної безпеки та термін окупності капітальних інвестицій.

СПИСОК ЛІТЕРАТУРИ

1 НД ТЗІ 3.7-003-05 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі" [Електронний ресурс]. – 2005. – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46074.

2 Закон України "Про захист персональних даних" [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2297-17.

3 НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу" [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: www.dsszzi.gov.ua/dsszzi/doccatalog/.

4 НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу" [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/.

5 НД ТЗІ 1.1-002-99 "Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу" [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: www.dsszzi.gov.ua/dsszzi/.

6 Закон України "Про інформацію" [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2657-12.

7 Закон України "Про захист інформації в інформаційно-комунікаційних системах" [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.

8 НД ТЗІ 1.1-003-99 "Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу" [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: https://tzi.com.ua/downloads/1.1-003-99.pdf.

9 ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ Захист інформації. Технічний захист інформації. Терміни та визначення. ДСТУ 3396.2-97 [Електронний ресурс]. – 1998. – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/.

10 НД ТЗІ 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі" [Електронний ресурс]. – 2012. – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/.

11 ЕКСПЛУАТАЦІЯ СИСТЕМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ [Електронний ресурс]. – 2013. – Режим доступу до ресурсу: https://lektsii.org/15-1903.html.

12 Віхорєв С. В. КЛАСИФІКАЦІЯ ЗАГРОЗ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ [Електронний ресурс] / Сергій Вікторович Віхорєв. – 2001. – Режим доступу до ресурсу: https://elvis.ru/upload/iblock/f60/f602ee2337fcc7250c71c2a138fe9ecc.pdf.

13 ІНСТРУКЦІЯ з порядку обліку і зберігання знімних носіїв конфіденційної інформації [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: http://www.mpsu-yar.ru/images/mpsu/docs/polozheniya/.

14 Рекомендації щодо захисту Active Directory: Частина 1. Бекап контролера домену [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://www.veeam.com/blog/ru/backing-up-domain-controller-best-practices-for-ad-protection.html.

15 Крижанівський В. Б. КОНСПЕКТ ЛЕКЦІЙ з курсу «Безпека інформаційних систем» [Електронний ресурс] / В'ячеслав Борисович Крижанівський. – 2012. – Режим доступу до ресурсу: https://learn.ztu.edu.ua/mod/resource/view.php?id=201.

ДОДАТОК А. Список файлів на оптичному носії

- Данюк_125-19-1.docx
- Данюк_125-19-1.pptx

ДОДАТОК Б. Інструкція з користування бездротовою мережею

1 Мета політики безпеки

Встановити правила користування бездротовою мережею підприємства ТОВ «Пауер системз», необхідні вимоги для безпечної роботи з конфіденційною інформацією та безпечної роботи мережі в цілому. Всі користувачі, що використовують бездротову мережу для доступу до інформаційних ресурсів мають виконувати вимогу даної інструкції.

2 Область дії

Область дії даної інструкції є бездротова мережа підприємства та всі користувачі, що користуються нею.

3 Відповідальні особи політики безпеки

Відповідальною особою за виконання інструкції системним адміністратором є заступник директора.

4 Інструкція

Перед підключенням до бездротової мережі, на мобільній робочій станції мають бути встановлені критичні оновлення ОС та ПО, що використовується для обробки чи доступу до інформації, мають бути встановлені актуальні бази даних антивірусних систем.

При обробленні інформації, що є конфіденційною, користувач має контролювати щоб сторонні особи, що не мають доступу до цієї інформації, не мали можливості несанкціоновано ознайомитися з екрану монітору.

Після включення адаптеру бездротової мережі, користувач має бути ввести свої автентифікаційні дані.

Паролі для доступу до бездротової мережі видаються адміністратором мережі.

Після проходження процедури автентифікації користувач отримує право доступу до інформації.

Мобільна робоча станція, що використовується для доступу до ІКС підприємства повинна бути перевірена системним адміністратором та на неї повинні бути встановлені обмеження, що забезпечують достатню охорону інформації.

Заборонено залишати мобільну робочу станцію без нагляду.

При необхідності залишити робоче місце, мають бути:

– збережені всі зміни;

– завершені всі програми для обробки інформації;

– зроблено відключення від мережі;

– заблокована мобільна робоча станція.

Після виконання необхідної роботи з інформацією, користувач має відключитись від бездротової мережі

5 Затвердження політики

Політика безпеки розробляється системним адміністратором та підписується директором підприємства при прийнятті усіх розділів політики.

6 Дії з виконання інструкції інформаційної безпеки

Системний адміністратор контролює підключення до бездротової мережі, та має засоби моніторингу та виконання політики доступу. Заступник директор контролює виконання інструкції шляхом регулярного обходу приміщень.

7 Відповідальність

Системний адміністратор та заступник директору несуть відповідальність за виконання інструкції.

ДОДАТОК В. Політика використання паролів

1 Опис

Паролі – один з найважливіших аспектів інформаційної безпеки, так як погано підібраний пароль підвищує потенційний ризик несанкціонованого доступу в інформаційну систему компанії. Всі користувачі ІКС ТОВ «Пауер системз» (включаючи підрядників і третю сторону) несуть відповідальність за виконання вимог цієї політики.

2 Мета

Мета цієї політики встановити стандарти створення сильних паролів, їх захист, збереження і частоту зміни.

3 Область застосування

Ця політика належить до всього персоналу, хто має або відповідальний за доступ до конфіденційної інформації усіх рівнів (або будь-яка форма доступу, яка підтримує або вимагає пароля) на будь-якій системі, обладнанні, що має доступ (або що зберігає конфіденційну інформацію) до Вашої корпоративної мережі.

4. Політика

4.1 Паролі системних облікових записів (адміністратора домену, локального адміністратора, root і т. д.) повинні змінюватися щокварталу.

4.2 Всі паролі системних облікових записів, а також паролі додатків і активного обладнання необхідно зберігати в базі даних в зашифрованому вигляді, доступ до якої обмежений.

4.3 Термін дії паролів облікових записів домену повинен становити не більше 9 місяців. Рекомендований інтервал зміни пароля 6 місяців.

4.4 Пароль облікового запису користувача, який має адміністративні привілеї, отримані за допомогою членства в групі або за допомогою програм, таких як sudo, повинен бути унікальний по відношенню до інших паролів облікових записів даного користувача.

4.5 Забороняється передача паролів користувачам за допомогою поштових повідомлень або іншим відкритим способом через Інтернет.

4.6 Пароль отриманий користувачем, необхідно змінити при першому вході в систему.

4.7 При використанні SNMP протоколу, необхідно використовувати відмінні від стандартних значень рядків підключень (Community Name) «public», «private», «system» і відмінними від пароля використовуваного для входу в систему.

4.8 Всі паролі користувачів, а також системні паролі повинні відповідати даній політиці.

5 Інструкції

Інструкція по створенню пароля. ТОВ «Пауер системз» використовує паролі для різних цілей. Серед них: доступ до облікового запису користувача, до веб-інтерфейсів, до електронної пошти, для захисту зберігача екрану, паролі голосової пошти та доступ до маршрутизаторів. Оскільки дуже мало систем підтримують токени з одноразовими паролями (динамічні паролі, які використовуються тільки один раз), слід знати як вибрати стійкий пароль.

Погані, слабкі паролі володіють наступними ознаками:

– містять менше восьми символів;

– є словом, яке міститься в словниках (українців або іноземних);

– є найбільш вживаним словом.;

– містять прізвище, кличку тварини, імена друзів, співробітників, вигаданих персонажів і т. д.;

– містять комп'ютерні терміни і назви, команди, назви сайтів, компаній, обладнання, програмного забезпечення;

– містять назву вашої компанії і географічні найменування, наприклад «Москва», «Саратов» або їх похідні;

– містять дати народження та іншу особисту інформацію, наприклад, адреси і номери телефонів;

– слово або число за шаблоном типу аааббб, qwerty, zyxwvuts, 12345 і т.д.;

– попередній приклад, що вводиться в зворотній послідовності.

– два попередні прикладу з цифрою на початку або кінці пароля (наприклад, Київ1, 1Петро).

6 Параметри сильних паролів:

– містить поєднання букв верхнього та нижнього регістрів (наприклад, az, AZ);

– включає цифри і знаки пунктуації, наприклад, 0-9,! @ # $% ^ & * () _ + | ~ - = \ ` {} []:"; '<>?,. /);

– складається з восьми і більше символів;

– не є словом на будь-якій мові, діалекті, сленгу, жаргоні і т.д.;

– не ґрунтується на персональній інформації, наприклад прізвища, дату народження і т.д.;

– ніколи не записується і не зберігається on-line.

Створюйте паролі, що легко запам'ятовуються. Одним із способів створення таких паролів, використовувати пісні, вірші та інші фрази, що легко запам'ятовуються. Наприклад з фрази: "This May Be One Way To Remember" можна отримати такі паролі: "TmB1w2R!" або "Tmb1W> r ~" та інші варіанти.

Увага: Не використовуйте жоден з попередніх прикладів в якості пароля!

7 Правила парольного захисту

7.1 Не використовуйте один і той же пароль для доступу до облікових записів ТОВ «Пауер системз» і до інших ресурсів (наприклад, доступ в інтернет з дому, систем електронної комерції і т. д.). По можливості не використовуйте один і той же пароль для доступу до різних ресурсів всередині компанії. Наприклад, використовуйте один пароль для прикладних програм та іншої для адміністрування ресурсів. Використовуйте різні паролі для облікових записів Windows і Unix-систем.

7.2 Не повідомляйте ваш пароль нікому, навіть вашому секретареві або обслуговуючому персоналу. Всі паролі є конфіденційною інформацією ТОВ «Пауер системз».

7.3 Список заборонених дій:

– не повідомляйте нікому свій пароль по телефону;

– не відправляйте свій пароль по електронній пошті;

– не повідомляйте свій пароль начальнику;

– не кажіть про свій паролі поруч з сторонніми;

– не згадуйте про вміст пароля (наприклад, "мій день народження");

– не вказуйте свій пароль в анкетах або опитувальниках;

– не повідомляйте свій пароль членам своєї сім'ї;

– не повідомляйте свій пароль товаришам по службі перед відходом у відпустку;

– чи не записуйте пароль і не зберігайте його на робочому місці;

– не зберігайте паролі у файлі на комп'ютері, включаючи переносний, без шифрування;

– не використовуйте функцію "Запам'ятати пароль" в таких додатках як Eudora, Outlook або Netscape Messenger.

Якщо хто-небудь вимагає повідомити ваш пароль, пошліться на цей документ або попросіть зателефонувати у відділ інформаційної безпеки.

Якщо ви вважаєте, що обліковий запис або пароль скомпрометовані, повідомте про це системного адміністратора ТОВ «Пауер системз» і змініть всі паролі.

Уповноважені особи ТОВ «Пауер системз» можуть регулярно проводити підбір або спроби злому паролів. Якщо пароль буде вгаданий або зламаний під час таких заходів, вас попросять змінити пароль.

Стандарт розробки додатків

Розробники додатків повинні забезпечити в своїх програмах таких заходів безпеки:

– додатки повинні підтримувати автентифікацію окремих користувачів, а не груп;

– додатки не повинні зберігати паролі у відкритому вигляді або такому, що легко відкривається;

– додатки повинні забезпечувати свого роду передачу прав, щоб один користувач міг виконувати функції іншого не знаючи його пароль;

– додатки повинні по можливості завжди підтримувати TACACS +, RADIUS, та / або X.509 на основі LDAP.

9 Використання паролів і парольних фраз для віддаленого доступу

Для контролю віддаленого доступу до мереж ТОВ «Пауер системз» використовуйте або одноразові паролі або асиметричну ключову систему зі стійкою парольною фразою.

Парольні фрази відрізняються від паролів. Парольний фраза більш довга версія пароля і, таким чином, більш надійна. Парольні фрази зазвичай використовуються для автентифікації в асиметричних системах шифрування. Асиметрична ключова система визначає математичну зв'язок між відкритим ключем, відомим всім і закритим ключем, відомим тільки його власнику. Без парольного фрази, що дає доступ до закритого ключа, користувач не отримає доступ.

Парольна фраза зазвичай складається з декількох слів, будучи більш стійкою до атак за словником. Хороша парольна фраза відносно довга і містить комбінацію букв у верхньому і нижньому регістрі, а також цифри і розділові знаки. Ось приклад хорошої парольної фрази: "The *? #> * @ TrafficOnThe101Was * & #! # ThisMorning" Всі правила створення стійких паролів відносяться і до парольних фраз.

Відповідальність

Будь-який співробітник, який порушив справжню політику, може бути підданий стягненню аж до звільнення.

ДОДАТОК Г. Інструкція з організації антивірусного захисту

1 Вступ

Ця Інструкція визначає вимоги до організації антивірусного захисту в ІКС ТОВ «Пауер системз» та встановлює відповідальність керівників і співробітників ТОВ «Пауер системз», що експлуатують та супроводжуючих ІКС, за виконання вимог цієї Інструкції.

2 Загальні положення

Для забезпечення інформаційної безпеки до використання в ІКС ТОВ «Пауер системз» допускаються тільки ліцензійні антивірусні засоби, централізовано закуплені ТОВ «Пауер системз» у розробників (постачальників) зазначених коштів, рекомендовані до застосування СІП.

Установка засобів антивірусного контролю на ПК здійснюється системним адміністратором на всі ПК ІКС ТОВ «Пауер системз». Налаштування параметрів використання антивірусного ПЗ виконується системним адміністратором.

3 Застосування засобів антивірусного контролю

Обов'язковому антивірусному контролю підлягають усі ПК, а також будь-яка інформація, одержувана і передана по телекомунікаційним каналам, а також інформація на знімних носіях.

Антивірусний контроль ПК повинен проводитися щоденно в автоматичному режимі при початковій завантаженні ПК (для серверів ІКС ТОВ «Пауер системз» - при перезапуску).

Оновлення баз антивірусних засобів повинно проводитися регулярно в автоматичному режимі, для чого спеціалістом служби техпідтримки повинен бути налаштований доступ до серверів оновлень розробника антивірусного засобу.

Встановлення (зміна) системного та прикладного програмного забезпечення повинна здійснюватися тільки в присутності спеціаліста служби безпеки. Встановлюване (змінюване) програмне забезпечення повинне бути попередньо перевірено спеціалістом служби безпеки на відсутність вірусів. Безпосередньо після

встановлення (зміни) системного програмного забезпечення ІКС ТОВ «Пауер системз».

При виникненні підозри на наявність у системі комп'ютерного вірусу (нетипова робота програм, перекручення даних, постійна поява повідомлень про системні помилки тощо) співробітником підрозділу ТОВ «Пауер системз» повинен бути проведений позачерговий антивірусний контроль ПК (самостійно або разом з відповідальним за забезпечення безпеки інформації підрозділу). При необхідності для визначення факту наявності або відсутності вірусу можуть бути залучені фахівці служби безпеки.

У разі виявлення при проведенні антивірусної перевірки наявності в системі комп'ютерного вірусу співробітники ТОВ «Пауер системз» зобов'язані:

– негайно поставити до відома адміністратора і припинити будь-які дії на персональному комп'ютері призупинити роботу;

У разі виявлення наявності в системі комп'ютерного вірусу адміністратори зобов'язані:

– спільно з власником заражених вірусом файлів провести аналіз необхідності подальшого їх використання;

– провести локалізацію вірусу в системі;

– забезпечити видалення вірусу із системи;

– у разі виявлення нового вірусу, що не піддається лікуванню застосовуваними антивірусними засобами, спеціаліст служби техпідтримки повинен направити заражений вірусом файл системному адміністратору для подальшої передачі його в організацію, з якою укладено договір на антивірусну підтримку;

– за фактом виявлення вірусу повинна бути складена службова записка системному адміністратору, в якій потрібно вказати Можливий джерело (відправника, власника і т.д.) вірусу, тип зараженого файлу, характер міститься у файлі інформації, тип вірусу і виконані антивірусні заходи.

Користувачеві ІКС забороняється без схвалення системного адміністратора:

– змінювати налаштування і конфігурацію засобів антивірусного захисту;

– видаляти або додавати в систему будь-які інші засоби антивірусного захисту;

– використовувати на ПК знімні носії інформації без попередньої перевірки встановленими засобами антивірусного захисту;

– запускати невідомі додатки, які прийшли по електронній пошті.

Користувач зобов'язаний:

– щодня при початковій завантаженні ПК переконатися в наявності резидентного антивірусного монітора і в разі його відсутності повідомити про це системного адміністратора;

– самостійно запускати позапланову антивірусну перевірку ПК при отриманні від системного адміністратора повідомлення про наявність в системі вірусу, а також при виникненні підозри на наявність вірусу.

4 Відповідальність

Відповідальність за організацію антивірусного контролю в ТОВ «Пауер системз», що експлуатує ІКС, відповідно до вимог цієї Інструкції покладається на керівника ТОВ «Пауер системз». Відповідальність за проведення заходів з антивірусного контролю та дотримання вимог цієї Інструкції покладається на відповідального за забезпечення інформаційної безпеки і всіх співробітників підрозділів ТОВ «Пауер системз», які є користувачами ІКС ТОВ «Пауер системз».

Періодичний контроль за станом антивірусного захисту в ІКС ТОВ «Пауер системз», а також за дотриманням встановленого порядку антивірусного контролю та виконанням співробітниками підрозділів ТОВ «Пауер системз» вимог цієї Інструкції здійснюється системним адміністратором.

Співробітники ТОВ «Пауер системз», які порушили вимоги цього документа, притягуються до відповідальності відповідно до чинного законодавства України.

ДОДАТОК Ґ. Інструкція з використання електронних ресурсів комп’ютерної мережі

1 Загальні положення

1.1 Метою цієї інструкції є регулювання роботи системного адміністратора і користувачів, розподілу мережевих ресурсів колективного користування та підтримки необхідного рівня захисту інформації, її збереження, і дотримання прав доступу до інформації. Більш ефективного використання мережевих ресурсів і зменшення ризику навмисного чи ненавмисного неправильного їх використання.

1.2 До роботи в системі допускаються особи, призначені начальником відповідного відділу, які пройшли інструктаж та реєстрацію.

1.3 Робота в системі кожному працівникові дозволена тільки на певних комп'ютерах і тільки з дозволеними програмами і мережевими ресурсами. Якщо потрібно працювати на інших комп'ютерах і з іншими програмами, необхідно отримати дозвіл системного адміністратора.

1.4 За рівнем відповідальності і прав доступу до КМ користувачі поділяються на такі категорії: системний адміністратор і користувачі.

1.5 Користувач підключеного до мережі комп'ютера - обличчя, за яким закріплена відповідальність за даний комп'ютер. Користувач повинен вживати всі необхідні заходи щодо захисту інформації та контролю за дотриманням прав доступу до неї.

1.6 Кожен користувач користується індивідуальним ім'ям користувача для своєї ідентифікації в мережі, що видаються системним адміністратором.

1.7 Кожен користувач створює пароль для входу в комп'ютерну мережу. При цьому пароль повинен містити мінімум 8 символів, містити букви і цифри.

1.8 Кожен користувач повинен користуватися лише своїм іменем користувача та паролем для входу в локальну мережу та мережу Інтернет, передача їх будь-кому заборонено.

1.9 Для роботи на комп'ютері окрім користувача необхідний дозвіл системного адміністратора. Ніхто не може давати дозвіл на навіть тимчасову роботу на комп'ютері, без дозволу системного адміністратора або начальника відділу.

1.10 У разі порушення правил користування мережею, користувач повідомляє системного адміністратора, який проводить розслідування причин і виявлення винуватців порушень і вживає заходи щодо припинення подібних порушень. Якщо винуватцем порушення є користувач даного комп'ютера, адміністратор має право відсторонити винуватця від користування комп'ютером або вжити інші заходи.

1.11 У разі появи у користувача комп'ютера відомостей або підозр про факти порушення цих правил, а особливо про факти несанкціонованого віддаленого доступу до інформації, розміщеної на контрольованому ним комп'ютері чи якомусь іншому, користувач повинен негайно повідомити про це системного адміністратора.

1.12 Системний адміністратор - особа, що обслуговує сервер і стежить за правильним функціонуванням мережі. Системний адміністратор дає дозвіл на підключення комп'ютера до мережі, видає IP-адреса комп'ютера, створює обліковий запис електронної пошти для користувача. Самовільне підключення є серйозним порушенням правил користування мережею.

1.13 Системний адміністратор інформує користувачів про всі планові профілактичні роботи, що можуть призвести до часткової або повної непрацездатності мережі на обмежений час, а також про зміни сервісів та обмеження, що накладаються на доступ до ресурсів мережі.

1.14 Системний адміністратор має право відключити комп'ютер користувача від мережі у випадку, якщо з даного комп'ютера проводилися спроби несанкціонованого доступу до інформації на інших комп'ютерах, і у випадках інших серйозних порушень цієї інструкції.

1.15 Користувач повинен ознайомитися з цією інструкцією. Обов'язок ознайомлення користувача з інструкцією лежить на системному адміністраторі.

2 Обов’язки користувачів мережі

2.1 Дотримуватися правил роботи в мережі, обумовлені цією інструкцією.

2.2 При доступі до зовнішніх ресурсів мережі, дотримуватися правил, встановлених системними адміністраторами для використовуваних ресурсів.

2.3 Негайно повідомляти системного адміністратора про виявлені проблеми у використанні наданих ресурсів, а також про факти порушення цієї інструкції ким-

небудь. Адміністратор, при необхідності, за допомогою інших фахівців, повинен провести розслідування зазначених фактів і вжити відповідних заходів.

2.4 Не розголошувати відому їм конфіденційну інформацію (імена користувачів, паролі), необхідну для безпечної роботи в мережі.

2.5 Негайно відключати від мережі комп'ютер, який підозрюється в зараженні вірусом. Комп'ютер не повинен підключатися до мережі до тих пір, поки системний адміністратор не переконаються у видаленні вірусу.

2.6 Забезпечувати безперешкодний доступ до мережевого обладнання та комп'ютерів користувачів.

2.7 Виконувати приписи, спрямовані на забезпечення безпеки мережі.

2.8 У разі виявлення несправності комп'ютерного обладнання або програмного забезпечення, користувач повинен звернутися до системного адміністратора.

3 Права користувачів мережі

3.1 Використовувати в роботі надані їм мережеві ресурси в обумовлених у цій інструкції рамках. Системний адміністратор вправі обмежувати доступ до деяких мережевих ресурсів аж до їх повного блокування, змінювати розподіл трафіку і проводити інші заходи, спрямовані на підвищення ефективності використання мережевих ресурсів.

3.2 Звертатися до адміністратора з питань, пов'язаних з розподілом ресурсів комп'ютера. Будь-які дії користувача, що ведуть до зміни обсягу використовуваних їм ресурсів, або впливають на завантаженість або безпеку системи (наприклад, установка на комп'ютері колективного доступу), повинні санкціонуватися системним адміністратором.

3.3 Звертатися за допомогою до системного адміністратора при вирішенні задач використання ресурсів мережі.

3.4 Вносити пропозиції щодо поліпшення роботи з ресурсом.

4 Заборонено

4.1 Дозволяти стороннім особам користуватися довіреним їм комп'ютером.

4.2 Використовувати мережеві програми, не призначені для виконання прямих службових обов'язків без узгодження з системним адміністратором.

4.3 Самостійно встановлювати або видаляти встановлені системним адміністратором мережеві програми на комп'ютерах, змінювати налаштування операційної системи та програм, що впливають на роботу мережевого обладнання та мережевих ресурсів.

4.4 Пошкоджувати, знищувати або фальсифікувати інформацію, що не належить користувачу.

4.5 Розкривати комп'ютери, мережеве і периферійне устаткування, підключати до комп'ютера додаткове обладнання без відома системного адміністратора, змінювати налаштування BIOS, а також робити завантаження робочих станцій з дискет.

4.6 Самовільно підключати комп'ютер до мережі, а також змінювати IP-адресу комп'ютера, виданий системним адміністратором.

4.7 Одержувати і передавати в мережу інформацію, що суперечить законодавству та нормам моралі суспільства, що представляє комерційну або державну таємницю, поширювати через мережу інформацію, зачіпає честь і гідність громадян, а також розсилати обманні, що турбують або загрозливі повідомлення.

4.8 Обходження облікової системи безпеки, системи статистики, її пошкодження або дезінформація.

4.9 Використовувати інші форми доступу до мережі Інтернет, за винятком дозволених системним адміністратором.

4.10 Здійснювати спроби несанкціонованого доступу до ресурсів мережі, проводити або брати участь в мережевих атаках і мережевому зломі.

4.11 Використовувати мережу для здійснення комерційних угод, розповсюдження реклами, комерційних оголошень, порнографічної інформації, закликів до насильства, розпалювання національної або релігійної ворожнечі, образ, погроз тощо.

4.12 Користувачі повинні поважати право інших користувачів на особисту інформацію. Це означає, що користувач (системний адміністратор) не має права користуватися чужими іменами і паролями для входу в мережу, читати чужу пошту,

заподіювати шкоду даними (крім випадків, зазначених вище), що належать іншим користувачам.

4.13 Забороняється проводити дії, спрямовані на злом (несанкціоноване отримання привілейованого доступу) робочих станцій і сервера мережі.

4.14 Закривати доступ до інформації паролями без узгодження з системним адміністратором.

5 Правила роботи з веб-ресурсами

5.1 Користувачі використовують програми для пошуку інформації тільки у випадку, якщо це необхідно для виконання своїх посадових обов'язків.

5.2 Використання ресурси мережі Інтернет дозволяється тільки в робочих цілях, використання її ресурсів не має потенційно загрожувати підприємству.

5.3 Щодо використання Інтернет ведеться статистика і надходить до архіву підприємства.

5.4 Дії будь-якого користувача, підозрюваного в порушенні правил користування Інтернетом, можуть бути запротокольовані і використовуватися для прийняття рішення про застосування до нього санкцій.

5.5 Користувачам організації, які користуються Інтернетом, заборонено передавати або завантажувати на комп'ютер матеріал, який є непристойним, порнографічним, фашистським чи расистським і не належать до діяльності підприємства.

5.6 Усі програми, що використовуються для доступу до мережі Internet, повинні бути затверджені адміністратором і на них повинні бути налаштовані необхідні рівні безпеки.

5.7 Усі файли, якими користуються за допомогою мережі Internet, повинні перевірятися на віруси за допомогою затверджених антивірусних програм.

5.8 В організації має вестися список заборонених сайтів. Програми для роботи з Internet повинні бути налаштовані так, щоб до цих сайтів можна було отримати доступ.

5.9 Заборонено розміщувати в гостьових книгах, форумах, конференціях повідомлення, що містять грубі та образливі вирази.

5.10 Заборонено одержувати і передавати через мережу інформацію, що суперечить законодавству та нормам моралі суспільства, що представляє комерційну таємницю, поширювати інформацію, а також розсилати обманні, що турбують або загрозливі повідомлення.

5.11 Заборонено отримувати доступ до інформаційних ресурсів мережі або мережі Інтернет, які не є публічними, без дозволу їх власника.

6 Відповідальність

6.1 Користувач комп'ютера відповідає за інформацію, що зберігається на його комп'ютері, технічно справний стан комп'ютера і ввіреній техніки.

6.2 Системний адміністратор відповідає за безперебійне функціонування мережі.

6.3 Користувач несе особисту відповідальність за весь інформаційний обмін між його комп'ютером та іншими комп'ютерами в мережі і за її межами.

6.4 За порушення цієї інструкції користувач може бути відсторонений від роботи з мережею.

6.5 Порушення даної інструкції, що призвело до знищення, блокування, модифікації або копіювання охороняється законом комп'ютерної інформації, порушення роботи комп'ютерів користувачів, системи або комп'ютерів, може спричинити адміністративну або кримінальну відповідальність відповідно до чинного законодавства.

ДОДАТОК Д. ВІДГУК КЕРІВНИКА ЕКОНОМІЧНОГО РОЗДІЛУ

Керівник економічного розділу к.е.н., доц. Пілова Д.П.

Дата: _____ Підпис: _____

ДОДАТОК Е. ВІДГУК КЕРІВНИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ

«Розробка політики безпеки інформації інформаційно-комунікаційної системи ТОВ «Пауер системз» студента групи 125-19-1 Данюка І.І.

Кваліфікаційна робота представлена пояснювальною запискою на 81 с., 3 рис., 12 табл., 7 додатків, 15 джерел.

Мета кваліфікаційної роботи – підвищення рівня безпеки інформації в ІКС ТОВ «Пауер системз», розробка рішень для захисту від загроз інформаційної безпеки. Тема і зміст дипломної роботи повністю відповідає технічному завданню на дипломну роботу.

У ході виконання дипломного проекту були вирішені наступні питання: аналіз існуючих загроз, обґрунтування необхідності створення комплексної системи захисту інформації для ОІД ТОВ «Пауер системз», приведена модель загроз та порушника для підприємства, прийняті проектні рішення щодо захисту інформації.

У економічному розділі були розраховані витрати на впровадження політики безпеки.

До недоліків проекту слід віднести окремі незначні невідповідності вимогам оформлення.

В цілому дипломний проект виконано у відповідності до вимог, які пред'являються до кваліфікаційної роботи бакалавра і заслуговує оцінки «_____», а Данюк Ілья Ігорович – присвоєння йому кваліфікації «бакалавр з кібербезпеки».

Керівник кваліфікаційної роботи к.т.н., доц. Ковальова Ю.В.

Дата: _____Підпис: _____