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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента ***Волкова Андрія Віталійовича***
академічної групи ***125-20-1***
спеціальності ***125 Кібербезпека***
спеціалізації[1]
за освітньо-професійною програмою ***Кібербезпека***
на тему ***Розробка політики безпеки інформації інформаційно комунікаційної системи ТОВ «ЛендінгСистем»***

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	проф. Кагадій Т.С			
розділів:				
спеціальний	ас. Мілінчук Ю.А			
економічний	к.е.н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2024

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____д.т.н., проф. Корнієнко В.І.
«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Волкову А.В*** **академічної групи** ***125-20-1***
(прізвище ім'я по-батькові) (шифр)

спеціальності ***125 Кібербезпека***
(код і назва спеціальності)

на тему ***Політика безпеки інформації інформаційно-комунікаційної системи ТОВ «ЛендінгСистем»***

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

Розділ	Зміст	Термін виконання
Розділ 1	Дослідити стан питання, постановку задачі	15.03.2024
Розділ 2	Провесті обстеження ОІД, побудувати модель порушника, модель загроз, виявити вразливості на підприемстві, визначити профіль захищеності, розробити елементи політики безпеки	10.05.2024
Розділ 3	Пояснити витрати на впровадження політики безпеки інформації	11.06.2024

Завдання видано _____ Тетяна КАГАДІЙ
(підпис керівника) (ім'я, прізвище)

Дата видачі: 20.04.2024р.
Дата подання до екзаменаційної комісії: 28.06.2024р.
Прийнято до виконання _____ Андрій ВОЛКОВ
(підпис студента) (ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 75 с., 3 рис., 10 табл., 4 додатки, 8 джерел.

Предмет розробки: політики безпеки інформації інформаційно-комунікаційної системи приватного підприємства ТОВ «ЛендінгСистем».

Об`єкт розробки: інформаційно-комунікаційна система ТОВ «ЛендінгСистем» - підприємство, яке займається послугами просування продуктів.

Мета роботи: підвищення рівню захищеності інформації в ІКС приватного підприємства ТОВ «ЛендінгСистем».

В першому розділі розглянуто стан питання, нормативно-правову базу, основи і етапи створення КСЗІ та ПБ, види загроз для малих підприємств.

В спеціальній частині була визначена загальна характеристика підприємства. Виконано дослідження інформаційної системи, фізичної середи та середи користувачів. Описана технологія обробки інформації та функціональний стан захисту. Зроблено поділ на категорії інформації, обробленої в ІКС та визначені основні загрози, вразливості, джерело, та зроблена модель порушника. Були розроблені основні положення політики безпеки

В економічному розділі розраховані основні затрати на впровадження політики безпеки інформації та щорічні експлуатаційні витрати на підтримку. Було доведено економічну доцільність впровадження політики безпеки інформації.

ПОЛІТИКА БЕЗПЕКИ , НОРМАТИВНО-ПРАВОВІ АКТИ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ЕКОНОМІЧНА ДОЦІЛЬНІСТЬ, ВРАЗЛИВОСТІ, ПРОФІЛЬ ЗАХИЩЕНОСТІ.

ABSTRACT

Explanatory note: 75 p., 3 figures, 10 tables, 4 appendices, 8 sources.

Subject of development: information security policy of the information and communication system of the private enterprise LLC "LandingSystem".

Object of development: information and communication system of LLC "LandingSystem" - an enterprise that provides services of product promotion.

Purpose: to increase the level of information security in the ICS of the private enterprise LLC "LandingSystem".

The first section discusses the state of the art, the regulatory framework, the basics and stages of creating an IPSS, and the types of threats to small enterprises.

In the special part, the general characteristics of the enterprise were determined. A study of the information system, physical environment and user environment is carried out. The information processing technology and functional state of protection are described. The categories of information processed in the ICS are divided into categories and the main threats, vulnerabilities, sources are identified, and a model of the offender is made. The main provisions of the security policy were developed

The economic section calculates the main costs of implementing the information security policy and annual operating costs for support. The economic feasibility of implementing the information security policy was proved.

SECURITY POLICY, REGULATIONS, THREAT MODEL, OFFENDER MODEL, ECONOMIC FEASIBILITY, VULNERABILITIES, SECURITY PROFILE.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС - автоматизована система;

ДСТУ - державний стандарт України;

ВК - відділ кадрів;

ВПН - віртуальна приватна мережа;

ЗУ - закон України;

ІБ - інформаційна безпека;

ІД – інформаційна діяльність;

ІзОД – інформація з обмеженим доступом;

КЗЗ - комплекс засобів захисту;

ІКС – інформаційно-комунікаційні системи;

ІТ - інформаційні технології ;

КЗЗ – комплекс засобів захисту;

МЗД- мережа зберігання даних;

ОІД – об’єкт інформаційної діяльності;

ОС - операційна система;

ПЗ – програмне забезпечення;

СВВ- система виявлення вторгнень;

СЗВ- система запобігання вторгненням;

СЗІ – служба захисту інформації;

СКУД - система контролю та управління доступом;

ТС - технологічне середовище

ТЗІ – технічний захист інформації.

ТОВ - товариство з обмеженою відповідальністю;

ЗМІСТ

ВСТУП

У час цифрової епохи інформаційно-комунікаційні системи відіграють важливу роль у роботі державних установ, компаній і суспільства. Збільшення кількості та складності кіберзагроз, спрямованих на ці системи, вимагає розроблення та впровадження ефективних стратегій і політик інформаційної безпеки. Сфера інформаційних технологій не стоїть на місті, та все більше і більше автоматизуються звичайні процеси.

Об`єктом в кваліфікаційній роботі являється інформаційно-комунікаційна система ТОВ «ЛендінгСистем» - підприємство, яке займається послугами просування рекламних продуктів.

Предметом розробки кваліфікаційної роботи є політика безпеки інформації.

Мета кваліфікаційної роботи є підвищення рівня безпеки інформації на підприємстві. Ця тема є актуальною та сучасною у нинішніх реаліях, оскільки зовнішній вплив на безпеку (злом, пограбування) підприємства дає справжню загрозу витоку інформації. Зовнішньої безпеки недостатньо. З'являються велика кількість фірм, які виробляють однакові послуги, відповідно росте і конкуренція.

Основою задачею для кожного зацікавленого керівника, забезпечення цілісності, доступності та конфіденційності інформації, що є частиною підприємства.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1. Стан питання

За даними статистики урядової команди реагування на комп'ютерні надзвичайні події CERT-UA кількість кібератак за 2023 рік зросла на 16% порівняно з 2022 роком.

В середньому, 45% листів на електронну пошту містять заражені формати типу .docx, приблизно 15,5% включають формат .exe і .png

Кібератаки стали звичним явищем для бізнесів і підприємств, адже впровадження нових рішень, продуктів або технологій є їх головною цілю.

Сьогодні головне завдання власників компаній - захищати дані бізнесу.

Експерти провели межу між порушенням хакерів, і порушенням, результат якого став виток інформації через помилку робітників при обробці інформації.

Частішим випадком стають інциденти з вірусами-вимагачами, а ніж вразливості системи, шкідливі програми або фішингові атаки.

Кіберзлочинці запускають до системи огранізації програму-вимагач завдяки фішинговим атакам. Після цього організація стає об’єктом спостереження з боку злочинців, це перша складова інциденту безпеки.

Виток інформації в організації викликає внутрішні помилки, які займають близько - 78%. Але такі випадки трапляються коли співробітники надсилають інформацію не тій людині, залишають важливі фізичні та інформаційні файли в загальнодоступному місці або не встановлюють оновлення.

Внутрішні помилки частіше за все призводять до ситуацій, коли складно сказати, що співробітник сторонній, бо задачею керівників є інформування всіх працівників про ризики безпеки, які можуть бути стати вони самі, і демонструвати уникнення помилок, задля збереження коштів компанії. Однією з причин витоку інформації можуть стати інсайдери в середині компанії.

Рисунок 1.1 - Типи порушень

Компанія, яка спеціалізується на розробці антивірусного ПЗ, кожного року проводить дослідження динаміки DDoS-атак за даними системи моніторингу DDoS Intelligence. В результаті досліджень, у 3 кварталі 2023 року, кількість атак по всьому світу зросла на 24% порівняно з попереднім кварталом (див.рис. 1.2).

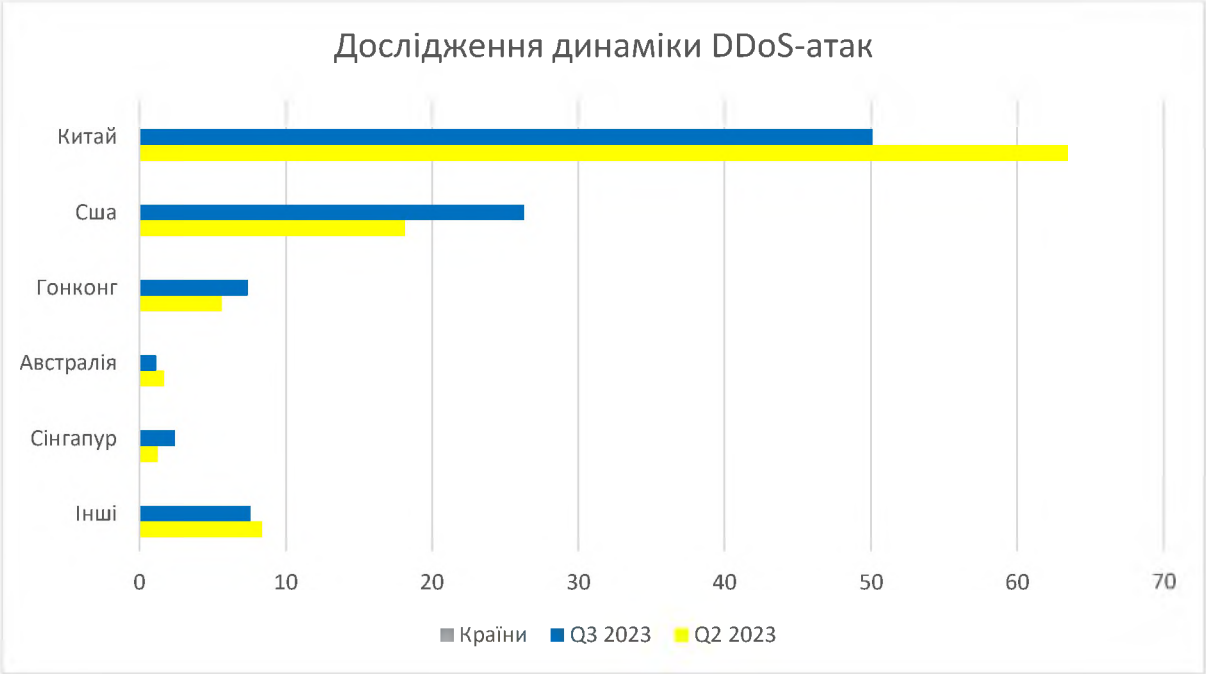


Рисунок 1.2 - Порівняння кількості атак у 2 та 3 кварталі 2023 року

У 89% кібератак фішинг є однією з перших, у той час як традиційні фішинг-атаки розсилають листи електронною поштою тисячам адресатів, спрямованих на невелику групи людей, приклад, співробітники компаній.

Злочинець, який планує фішинг атаку, може створити фальшиву електронну адресу співробітника, через яку, задаючи питання дізнається інформацію про компанію. Інші співробітники, вважаючи що вони спілкуються з колегою, можуть надати цю інформацію без побоювань.

Однією з таких може бути використання стратегії атаки типу «Watering Holes» хакери розміщують шкідливі програми в коді вебресурсів, які з високою ймовірністю відвідують співробітники компанії, яка є цілю кіберзлочину. Працівник, заходячи на цей сайт, ставить під загрозу мережу всієї компанії, вона може піддатися вірусу, що викрадає дані.

Внутрішні загрози компанії - результат ситуацій, які відбуваються всередині. У корпораціях бувають свої можливості та загрози бізнесу. Якщо розглянути основні внутрішні ризики компанії малого та середнього бізнесів, то можна віднести такі загрози:

– співробітник може передавати конфіденційну інформацію конкурентам. У разі звільнення, менеджер частіше йде до конкурента, у якого

він може проводити дзвінки до власної клієнтської бази, пропонуючи співпрацювати. Щоб звести подібні ризики до мінімуму, компанії впроваджують CRM-систему, у якій зберігають дані в централізованій базі сервервів компанії;

— двоє друзів вирішили відкрити свою справу. Бізнес почав набирати обертів, настав період розподілу прибутку. Друзі починають сваритися, акцентуючи увагу що кожен з них заслуговує на більший прибуток ніж інший.

В результаті може дійти до конфлікту, який перейде до розладу у бізнесі. Фахівці радять починати бізнес поодинці, без співзасновників або партнерів, у необхідності працівники наймаються. Звільнити його можна в будь-який момент, а співзасновник залишається за будь-яких обставин.

— результат недостатньої кваліфікації управлінського персоналу, неправильних рішень, помилок при плануванні. Проблеми з менеджментом та низького рівня управління можуть призвести до краху підприємства;

— фінансові загрози для бізнесу можуть бути віднесені як до зовнішніх, так і внутрішніх. Така загроза виникає через стрибки валюти, борги за оплатою, невірного фінансового планування, економічної ситуації в країні.

Зовнішні загрози, які діють на безпеку бізнесу - ситуація, що склалася поза підприємством, не прив'язуючи до цього діяльність компанії. В таких випадках керівник може лише мінімізувати наслідки. До такого типу загрози відносять:

— макроекономічні кризи, впливаючи на діяльність компанії , через які знижується можливість клієнтів купувати або замовляти продукти компанії, що спостерігається зростанням вартості кредитів та рівня інфляції;

— дії від конкурентів, які мають загрозу у вигляді аналогічних товарів;

— несанкціоноване отримання доступу до комерційної інформації;

— різка зміна політичної ситуації у країні або світі;

– неочікувані ситуації природного характеру у вигляді урагану, граду або пожежі;

– ситуації технічного характеру;

– клієнти, які відносяться недобросовісно до компанії несвоєчасно сплачуючи товар або послугу, відмовитися забирати товар або повернути його через день після отримання;

– постачальники, які з невідомих причин починають завищувати ціни на товар, поставляти його у неналежній якості або відправляє товар не в обмежені терміни. Якщо у компанії один постачальник, то є велика загроза з реалізацією цього товару та збитків через це.

1.2 Аналіз нормативно-правової бази в сфері захисту інформації

Проведення аналізу та ефективне використання правової бази допомагає компаніям забезпечити надійний захист інформації, зберегти довіру клієнтів і відповідати вимогам законодавства у сфері інформаційної безпеки.

Візьмемо основні нормативно-правові акти, що діють у сфері захисту інформації в Україні:

Закон України "Про інформацію" встановлює основні засади регулювання інформаційних відносин, включно із захистом конфіденційності та запобіганням несанкціонованому доступу до даних;

Закон України "Про електронні документи та електронний документообіг" визначає правові аспекти використання електронних документів і заходи щодо захисту від змін або підробок;

Закон України "Про кібербезпеку" може містити положення про необхідність забезпечення безпеки критично важливих інформаційних систем від кібератак та інших загроз;

Закон України "про персональні дані" документ, що визначає правила збору, зберігання та обробки персональних даних громадян;

Указ президента України «Про положення про технічний захист інформації в Україні»;

НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу розглянуто поняття політики безпеки. Термін "політика безпеки" буде застосовуватися щодо організації, АС, послуг, ОС, що реалізується набором функцій.

Політика безпеки інформації АС є частиною більш загальної політики безпеки інформації і може успадковуватись, до положення державної політики у формі захисту безпеки. Для АС кожна політика безпеки інформації може бути індивідуальною в залежності від технологій обробки інформації, особливостей ОС та фізичного середовища. Тоді політика безпеки інформації в такій АС буде складена, а її частини, будуть відповідати різним технологіям.

Частина політики безпеки, що регламентує правила для доступу користувачів та процесів до КС, компонує правила розмежування доступу.

НД ТЗІ 3.7-003-2005 наводить обґрунтування необхідності створення КСЗІ та основні етапи створення КСЗІ : підставою для визначення необхідності створення КСЗІ вступають норми та вимогу чинного законодавства, які позначають обов'язковість обмеження доступу до певних видів інформації, забезпечення цілісності та доступності, або прийняте рішення власником інформації до цього, якщо нормативно-правові акти надають право діяти на власний розсуд.

Дані для обґрунтування необхідності створення КСЗІ отримується за результатами:

— дослідження законодавчих актів (державних, відомчих та тих, що діють у межах установи, організації, підприємства), які можуть обмежувати доступ до певних видів інформації або забороняти такі обмеження, або встановлювати необхідність забезпечення безпеки інформації за іншими критеріями;

— визначення наявності в інформації, що підлягає автоматизованому

опрацюванню, таких типів даних, які потребують обмеження доступу або забезпечення цілісності та доступності відповідно до вимог законодавства;

– Оцінка можливих переваг (фінансових, економічних, соціальних тощо) використання ІТС при створенні КСЗІ.

На основі проведеного аналізу робиться висновок про необхідність створення КСЗІ.

Обстеження середовища функціонування ІКС.

Під час проведення цих робіт ІТ-систему розглядають як комплексну систему, що об'єднує обчислювальне обладнання, фізичне середовище, користувачів, інформацію, що обробляється, та технології її обробки (далі - оточення функціонування ІКС-системи).

Метою інспекції є підготовка основних даних для визначення вимог до засобів захисту інформації шляхом опису кожного елемента оточення функціонування ІКС-системи та виявлення нових компонентів, що можуть негативно вплинути на безпеку інформації як напряму, так і опосередковано. Також необхідно враховувати взаємодію різних елементів різних середовищ, документувати результати інспекції для використання на наступних етапах робіт. Інспекція проводиться після розроблення концепції ІКС-системи(основні принципи та побудови), визначені основні завдання та характеристики ІКС, функціональних комплексів ІКС та варіант реалізації.

Під час проведення перевірки інформаційно-обчислювальної системи ІКС необхідно проаналізувати та описати такі аспекти:

– загальна структурна схема і склад (перелік обладнання, технічних і програмних засобів, зв'язки між ними, особливості конфігурації, архітектури і топології, програмні та апаратні засоби захисту інформації, взаємне розміщення засобів та інше);

– види та характеристики каналів зв'язку;

– особливості взаємодії окремих компонентів системи, їхній вплив один на одного;

– можливі обмеження щодо використання ресурсів тощо. Необхідно виявити компоненти ІТС, які мають або не мають захист інформації, потенційні можливості цих засобів захисту, характеристики цих механізмів, зокрема стандартні параметри.

Мета подібного аналізу полягає в узагальненні потенційних можливостей щодо забезпечення безпеки даних, визначенні компонентів ІКС, які потребують додаткової безпеки.

Під час перевірки інформаційного середовища підлягають аналізу всі дані, що обробляються або зберігаються в ІКС (дані та програмне забезпечення). Властивості безпеки для кожного типу даних, що перебувають на об'єкті КС, мають бути відповідні вимоги (конфіденційність, цілісність, доступність), або КС має визначити, якою мірою рішення відповідають цим вимогам. Під час вивчення електронних документів необхідно виявити особливості їхнього обігу, визначити інформаційні потоки та середовища, через які вони передаються, джерела формування потоків та їхні кінцеві пункти призначення. Також важливо встановити принципи управління інформаційними потоками, розробити структурні схеми потоків. Необхідно визначити типи носіїв інформації та способи їх використання в процесі функціонування ІТ-системи. Для кожного елемента структурної схеми інформаційних потоків потрібно зафіксувати склад інформаційних об'єктів, режим доступу до них, можливий вплив на них з боку користувачів або фізичного середовища в контексті збереження властивостей інформації.

На етапі формування завдання на розроблення комплексної системи захисту інформації (КСЗІ):

– визначаються цілі забезпечення безпеки інформації в інформаційно-телекомунікаційній системі (ІКС) і призначення створення комплексної системи захисту інформації (КСЗІ), варіанти розв'язання завдань із забезпечення безпеки (відповідно до національного стандарту ДСТУ 3396.1), основні напрями забезпечення безпеки (згідно з пунктом 5.8);

– проводиться аналіз загроз (вивчення моделі загроз і профілю порушника, можливих наслідків від реалізації потенційних загроз, оцінка можливих збитків та інше) і визначається список значущих загроз;

– описується загальна структура і склад комплексної системи захисту інформації, вимоги до можливих заходів, методів і засобів захисту інформації, допустимі обмеження щодо використання певних заходів і засобів захисту (наприклад, обмеження на використання активних засобів захисту від витоку інформації каналами шляхом використання обчислювальної техніки в захищеному виконанні та інше), інші обмеження щодо умов функціонування ІКС, обмеження щодо використання ресурсів ІКС для виконання завдань безпеки, допустимі витрати на забезпечення безпеки ІКС, оцінка можливих збитків, оцінка можливих збитків тощо.

Оформлюється звіт про виконання робіт цієї стадії та подається заявка на розроблення КСЗІ.

У Законі України "Про інформацію" містяться визначення термінів "захист інформації" та "інформація". "Захист інформації - це комплекс заходів правового, адміністративного, адміністративно-організаційного, технічного характеру та інших заходів для збереження даних цілісністю даних цілісністю даних. Інформація - це будь-які відомості та дані, які можна записати на різних носіях або відобразити в цифровому вигляді".

У постанові Кабінету Міністрів України "Про Прийняття Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-комунікаційних системах" наведено визначення таких понять:

Автентифікація - процедура встановлення належності користувачеві наданого ним облікового запису в системі.

Ідентифікація - процедура розпізнавання користувача в системі, як правило, за заздалегідь визначеним ім'ям (обліковим записом) або іншою відомою про нього інформацією, яку система розпізнає."

Також в цьому документі описані типи інформації, що підлягає захисту:

Публічна інформація належить до державних ресурсів інформації, а також до відкритої інформації про діяльність суб'єктів публічної влади та військових формувань, що публікується через Інтернет, інші глобальні мережі та передається комунікаційними засобами (далі - відкрита інформація).

Конфіденційна інформація перебуває під контролем керівників даних, визначених частиною першою статті 13 Закону України "Про доступ до публічної інформації".

Службова інформація. Це дані державного або іншого закритого характеру (далі - секретна інформація).

Інформацію потрібно захистити згідно із законодавством.

Відкрита інформація під час опрацювання повинна зберігати свою цілісність завдяки заходам безпеки від несанкціонованих дій, що можуть призвести до випадкових або навмисних змін чи видалення даних.

Усім користувачам має бути доступ для ознайомлення з відкритою інформацією. Модифікація або видалення відкритих даних та доступ до інформації дозволено тільки зареєстрованим і авторизованим користувачам, які мають відповідні права доступу. Будь-яким спробам зміни або видалення відкритої інформації користувачами без відповідних повноважень, а також неавторизованими або користувачами, у яких не підтверджено достовірність їхніх облікових даних у момент автентифікації, мають запобігти. Під час обробки конфіденційної та секретної інформації необхідно забезпечити її захист від несанкціонованого доступу, змін, знищення, копіювання та поширення. Доступ до конфіденційної інформації надається тільки зареєстрованим і авторизованим користувачам. Будь-які спроби доступу до такої інформації з боку незареєстрованих осіб або користувачів з непідтвердженими обліковими даними в момент автентифікації мають бути заблоковані.

У стандарті НД ТЗІ 1.1-002-00 "Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу" міститься визначення політики безпеки: "Під політикою безпеки інформації

розуміється набір правил, обмежень, рекомендацій та іншого, що визначають порядок обробки інформації та спрямовані на захист її від певних загроз. Термін політика безпеки' може застосовуватися до організацій, автоматизованих систем (АС), операційних систем (ОС), послуг або функціональних блоків системи, що реалізується, тощо. Чим більш деталізований об'єкт застосування цього терміну, тим більш конкретними і формалізованими стають правила".

Політика безпеки інформації в автоматизованих системах (АС) є частиною всієї політики безпеки організації та може наслідувати, зокрема, принципи державної політики щодо захисту інформації. Для кожної конкретної АС політика безпеки інформації може бути унікальною і залежати від використовуваних технологій оброблення даних, особливостей операційних систем, фізичного оточення та інших чинників. Ба більше, одна й та сама АС може використовувати кілька різних технологій обробки інформації. У такому разі політика безпеки інформації для цієї АС буде збірною, і її складові частини, що відповідають різним технологіям, можуть значно відрізнятися.

Політика безпеки має визначити ресурси АС, що потребують захисту, включно з категоріями оброблюваної в них інформації. Необхідно явно вказати основні загрози для операційних систем, персоналу та інформації різних категорій, а також встановити вимоги щодо захисту від цих загроз.

Особиста відповідальність співробітників за дотримання вимог політики безпеки має бути виділена. Підходи до реалізації політики безпеки інформації в різних комп'ютерних системах відрізнятимуться не тільки тому, що функції захисту можуть надавати захист від різного роду загроз, а й через суттєві відмінності в ресурсах комп'ютерних систем. Наприклад, якщо операційна система працює з файлами, то бази даних мають справу з даними розподіленими по різних файлах.

Один з аспектів політики безпеки - це правила доступу користувачів і процесів до ресурсів комп'ютерних систем (КС) - формує правила обмеження

доступу.".

У стандарті ДСТУ ISO/IEC 27005:2015 містяться рекомендації з управління ризиками інформаційної безпеки, що охоплюють управління інформацією та ризиками інформаційної безпеки в галузі телекомунікаційних технологій. Методи, викладені в цьому стандарті, відповідають основним принципам, моделям і процесам, зазначеним у ДСТУ ISO/IEC 27001:2015.

1.3 Постановка задачі

З огляду на важливість питань забезпечення інформаційної безпеки на підприємстві, вивчення динаміки загроз у світі за останні роки та актуальних ризиків для малого бізнесу, необхідно гарантувати належний рівень захисту інформації. Шляхом аналізу нормативно-правової бази можна досягти необхідного рівня інформаційної безпеки шляхом створення комплексної системи захисту інформації (КСЗІ). Під час розроблення КСЗІ на основі законодавчих актів слід провести аналіз і описати:

- вид діяльності підприємства;
- інформаційну систему підприємства;
- створити модель зловмисника і модель загроз;
- виявити вразливості;
- розробити елементи політики безпеки інформації.

Висновок до розділу 1

У висновку першого розділу кваліфікаційної роботи було проаналізовано темпи зростання кіберзлочинності у світі, основні загрози кіберпростору. Також було описано основні види внутрішніх і зовнішніх загроз для малих підприємств. Базуючись на аналізі нормативно-правової бази, сформульовано завдання для наступної частини кваліфікаційної роботи.

РОЗДІЛ 2. СПЕЦІАЛЬНИЙ РОЗДІЛ

2.1 Загальні відомості про діяльність підприємства.

Об'єктом інформаційної діяльності (далі ОІД) є офіс приватного підприємства - ТОВ «ЛендінгСистем».

Підприємство знаходиться за юридичною адресою: 01004, м. Київ, вулиця Євгена Чикаленка, 28.

Основна діяльність підприємства визначена, як налаштування таргету на рекламні кампанії різних видів бізнесів.

Часи роботи: понеділок-п'ятниця (9:00-18:00);

субота (9:00-20:00);

неділя - вихідний.

Структура працівників підприємства: директор, директор з консультацій, менеджер з консультацій, директор з продажів, менеджер з продажів, бухгалтер, системний адміністратор, кадровий працівник.

2.2 Обстеження ОІД

2.2.1 Обстеження фізичного середовища

Об'єктом інформаційної діяльності є офіс приватного підприємства - ТОВ «ЛендінгСистем».

Підприємство знаходиться за адресою вул. Євгена Чикаленка, 28.

ОІД знаходиться у п'ятиповерховій будівлі на 3 поверсі. Має 5 вікон з виходом на головну вулицю біля будівлі.

Стіни будівлі, в якій знаходиться ОІД створені з газо-бетонних блоків (30х40х60). Фундамент - стовпчастий, дах - профнастил, для цього беруть гофровану листову сталь, що пройшла оцинкування або покриття полімерами, територія навколо будівлі частково покрита плиткою і асфальтом.

Зовнішні стіна будівлі - газо-бетонні. Товщина зовнішність стін - 480 мм (2 шари газо-бетонних із цементом та штукатуркою).

Внутрішні стіну зроблені з аналогічного матеріалу, товщина 250 мм (1 шар газо-бетонного блоку із цементом та штукатуркою). Внутрішні стіни зведені з використанням гіпсокартону та металоконструкцій, загальною товщиною - 80мм.

Вікна - металопластикові, подвійні, 2300 х 1500 мм.

Вхідні двері - металеві, 1600 мм ширина і 2200 мм висота.

Замок - врізаний зі сталі, зачиняється вбудованім циліндром під ключ з перфорацією.

Міжкімнатні двері виготовлені з комбінованого переклеєного масиву дерева і МДФ, розмірами 40х2000х100х.

Офіс має висота 3,5 м (від підлоги до стелі), стеля - підвісна, з конструкцією кріплення Грільято. Підлога - ламінат і плитка (у вбиральні).

Навпроти будівлі знаходиться готель.

Область, обмежена стінами будівлі, піддається контролю. Для доступу використовується система управління доступом (СУД). Згідно з класифікацією рівнів автоматизації СУД підприємства є повністю автоматизованою, що означає, що весь процес перевірки та прийняття рішень здійснюється комп'ютером.

Електропостачання підключено до трансформаторної підстанції №8, яка обслуговує сторонніх споживачів і розташована за межами центральної зони.

Опалення працює на міській системі опалення і теж знаходиться за межами центральної зони. Каналізація та водопостачання підключені до міських мереж і також виходять за межі центральної зони.

Усі пристрої приєднані до загальної системи заземлення, яка має контур заземлення, що виходить за межі центральної зони.

Система вентиляції працює за припливно-витяжним принципом.

Інтернет проведено за допомоги оптично-волокнистого кабелю, від обладнання провайдеру «Телеміст» та «Київстар».

Встановлена система охоронної та пожежної сигналізації підключена до чергового пульта охоронної компанії «Протект» за допомогою GSM зв’язку.

Ситуаційний та генеральний план наведено у ДОДАТКУ Д та Е

2.2.2 Обстеження обчислювальної системи ОІД

ІКС ОІД являє собою мережу типу "зірка", оснащену виділеним сервером і побудовану на базі одного комутатора.

Ця система містить у собі багатокористувацький комплекс, здатний обробляти інформацію різних рівнів конфіденційності, а також має доступ до Інтернету через ADSL.

Основне обладнання складають:

- 10 ПЕОМ під управлінням операційної системи Microsoft Windows 10 Home (білд 19044);
- сервери для управління доступом до інтернету з централізованим оновленням антивірусних баз і системних оновлень;
- активне мережеве обладнання (включно з комутаторами першого і другого рівня), програмне забезпечення для управління мережевим обладнанням;
- набір прикладного ПЗ (Microsoft Office, Total Commander, 7-zip, Adobe Reader, Kaspersky Antivirus, BitDefender TotalSecurity). Крім того, до складу системи входить периферійний пристрій для введення/виведення даних - Nikon 5100.

Схема мережі наведена на рисунку 2.1

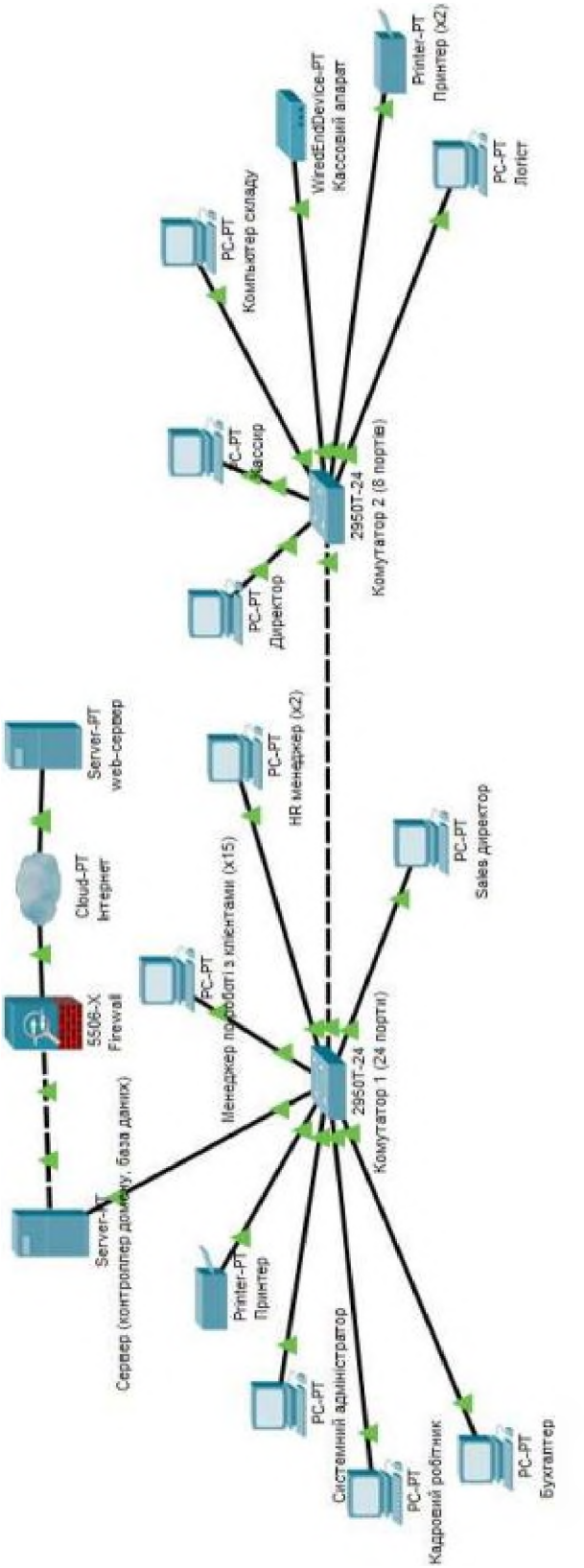


Рисунок 1.1 - Структурна схема мережі підприємства

2.2.3 Інформаційне середовище

Інформація про підприємство зберігається у електронному та паперовому вигляді.

Дані наведено в таблиці 2.1.

Таблиця 2.1 - Інформація, що циркулює на підприємстві

№	Інформація	Режим доступу	Правовий режим	Працівники, що мають доступ	Зберігання
1	Загально-організаційна	З обмеженим доступом	Конфіденційна інформація	Директор, сис. а дмін.	ПК директора
2	Облік внутрішніх документів	З обмеженим доступом	Конфіденційна інформація	Директор, сис. а дмін.,кадровий працівник	Сервер
3	Інформація про послуги, тарифи, конткати підприємства	Відсутній	Відкрита	Всі	Сайт компанії
4	БД працівників	З обмеженим доступом	Конфіденційна інформація	Директор, сис.адмін.,кадровий працівник, бухгалтер, менеджер з продажів	Сервер
5	Огляд послуг	Відсутній	Відкрита	Всі	Сайт компанії або сервер
6	Інформація про клієнтів	З обмеженим доступом	Конфіденційна інформація	Директор, сис.адмін., бухгалтер, менеджер з продажів та менеджер з консультацій	Сервер
7	БД замовлень	З обмеженим доступом	Конфіденційна інформація	Директор, сис.адмін, менеджер з продажів	Сервер

Продовження таблиці 2.1

№	Інформація	Режим доступу	Правовий режим	Працівники, що мають доступ	Зберігання
8	Фінансова звітність	З обмеженим доступом	Комерційна таємниця	Директор, сис.адмін., бухгалтер	Сервер, паперові носії, ПК директора або бухгалтера
9	Дані про обладнання підприємства, система охорони	З обмеженим доступом	Комерційна таємниця	Директор, сис.адмін., менеджер з продажів	Сервер, паперові носії, ПК сис.адміна

Таблиця 2.2 - Визначення рівня конфіденційності, цілісності та доступності інформації

№	Інформація	Рівень Конфіденційності	Рівень цілісності	Рівень доступу
1	Загально-організаційна	К1	Ц2	Д1
2	Облік внутрішніх документів	К2	Ц2	Д2
3	Інформація про послуги, тарифи, конткати підприємства	К1	Ц3	Д4
4	БД працівників	К2	Ц3	Д2
5	Огляд послуг	К1	Ц4	Д4
6	Інформація про клієнтів	К2	Ц4	Д3
7	БД замовлень	К3	Ц5	Д4
8	Фінансова звітність	К4	Ц5	Д3
9	Дані про обладнання підприємства, система охорони	К4	Ц3	Д2

Для поділу інформації використовувалися рівні секретності, описані нижче.

Рівні конфіденційності:

- рівень 1 (К1) - інформація, за якої можливі незначні втрати в разі її розкриття особам без доступу або коли інформація не є конфіденційною;
- рівень 2 (К2) - інформація, за якої компанія зазнає невеликих збитків від розкриття особам без доступу;
- рівень 3 (К3) - інформація, за якої організація зазнає значних збитків від розкриття особам без доступу;
- рівень 4 (К4) - інформація, розкриття якої може призвести до серйозних матеріальних втрат для компанії;
- рівень 5 (К5) - критичний рівень конфіденційності, який може призвести до банкрутства компанії в разі витоку конфіденційної інформації.

Рівні збереження інформації:

- рівень 1 (Ц1) - інформація, втрата цілісності якої не має серйозних наслідків;
- рівень 2 (Ц2) - інформація, втрата цілісності якої призведе до невеликих фінансових втрат для компанії;
- рівень 3 (Ц3) - інформація, втрата цілісності якої спричинить значні фінансові втрати для організації;
- рівень 4 (Ц4) - інформація, втрата цілісності якої може призвести до суттєвих матеріальних збитків;
- рівень 5 (Ц5) - критичний рівень збереження інформації, втрата цілісності якої може призвести до банкрутства компанії.
- рівні доступності:
- рівень 1 (Д1) - інформація, доступність якої не має великого значення;
- рівень 2 (Д2) - недоступність інформації може призвести до незначних фінансових втрат для компанії;

- рівень 3 (Д3) - неприпустимість доступу до інформації спричинить відчутні фінансові втрати для організації;
- рівень 4 (Д4) - відсутність доступу до інформації може спричинити значні матеріальні втрати;
- рівень 5 (Д5) - критичний рівень доступності інформації, відсутність якої може призвести до банкрутства компанії.

2.2.4 Технології обробки інфомації

Загально-організаційна інформація зберігається на комп'ютері директора і створюється ним. За необхідності вона поширюється серед співробітників через електронну пошту тим, хто потребує доступу до неї.

Облік внутрішніх документів здійснюється на сервері підприємства, де реєструються паперові носії інформації, як-от угоди та накладні від постачальників. Цим займається співробітник відділу кадрів.

Інформація про послуги, тарифи і контакти підприємства доступна на його сайті для загального ознайомлення. Редагування здійснює системний адміністратор за вказівкою директора підприємства або директора з продажу з попередньою згодою керівництва.

База даних працівників містить особисті дані кожного співробітника компанії, як-от ПІБ, паспортні дані та ІПН, кадровим робітником або самим директором.

Каталоги послуг розміщені на сайті компанії та сервері піддаються редагуванню зі сторони системного адміністратора за вказівкою керівництва з відповідним дозволом. Особисті дані клієнтів зберігаються в спеціальній базі даних на сервері компанії: ПІБ, паспортні дані, ІПН, адреси та інформація про замовлення. Зазвичай ці дані оновлюють менеджери під час оформлення замовлень, але якщо клієнт уже робив замовлення раніше, його дані вже присутні в базі. Менеджер оновлює інформацію в історії замовлень, додаючи нові дані. Коли новий клієнт робить замовлення вперше, його дані

реєструються в базі даних, де кожному клієнту присвоюється особистий ідентифікаційний номер для зберігання інформації.

Фінансові звіти формуються бухгалтером або директором на основі інформації з бази даних замовлень і друкуються за необхідності, після чого зберігаються на робочих місцях бухгалтера і директора.

Інформація про технічне обладнання компанії та систему безпеки часто використовуються системними адміністраторами для перевірки цілісності та наявності обладнання на підприємстві, а також як інвентаризаційний список.

2.2.5 Середовище користувачів

В офісі, у робочі будні, зазвичай знаходяться наступні люди:

- директор;
- системний адміністратор;
- менеджер з консультацій;
- помічник менеджера з консультацій;
- менеджер з продажів;
- помічник менеджера з продажів;
- бухгалтер;
- кадровий робітник.

Для того щоб детальніше вивчити доцільність надання доступу до інформації всім співробітникам компанії, ми розглянемо основні обов'язки кожного працівника. Дані посадових обов’язків описані у таблиці 2.3.

Таблиця 2.3 - Основні посадові обов’язки працівників

№	Посада	Кількість	Посадові обов’язкі
1	Директор	1	Ведення всіх операцій на підприємстві, реєстрація угод між виконавцями та замовниками, також усі юридичні процедури, пов'язані з діяльністю компанії.
2	Бухгалтер	1	Фінансовий облік і аудит компанії, розрахунок і видача заробітної плати робітникам
3	Системний адміністратор	1	Управління роботою інформаційної системи, усунення технічних проблем, спостереження за віртуальними серверами, технічна підтримка всіх компонентів системи, опрацювання запитів про несправності, забезпечення контролю доступу до інформації згідно з політикою безпеки компанії та корпоративними документами підприємства.
4	Директор з продажів	1	Контроль роботи менеджерів з продажів, супровід допродажів
5	менеджер з продажів	5	Пропозиція знижок або цікавих пропозиції, які можуть бути потрібні клієнту
6	Директор з консультацій	1	Контроль роботи менеджерів з консультації, супровід у складних питаннях
7	Помічник менеджеру з консультацій	4	Обговорення актуальності послуги для клієнту, підбір більш вигідної або унікальної
8	Кадровий робітник	1	Облік документації компанії та реєстрація нових працівників

Таблиці 2.4 - Матриця керування доступом

	1	2	3	4	5	6	7	8	9	10
Директор	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ
Директор з продажів	ЧЗ	-	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ	-	ЧРЗВ	ЧРЗВ
Бухгалтер	-	-	ЧЗ	ЧРЗВ	ЧЗ	ЧЗ	ЧЗ	ЧРЗВ	ЧРЗВ	-
Директор з консультацій	-	-	ЧЗ	-	ЧЗ	ЧРЗВ	ЧРЗВ	-	-	-
Сис.адмін.	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ
Менеджер з продажів	-	-	ЧЗ	ЧЗ	ЧЗ	ЧЗ	ЧЗ	-	ЧЗ	ЧЗ
Менеджер з консультацій	-	-	ЧЗ	-	ЧЗ	ЧЗ	ЧЗ	-	-	-
Кадровий робітник	-	ЧРЗВ	ЧЗ	ЧРЗВ	ЧЗ	-	-	-	-	-

Вказані літери мають абревіатуру: ч - читання, р - редагування, з - зберігання, в - видалення. Оцінкою від 1 до 10 вказано інформацію згідно таблиці 1.1

2.3 Аналіз загроз та вразливостей

2.3.1 Модель загроз та вразливостей

Визначено як найістотніші для даної ІКС загрози, які виникають від дій людей, таких як конкуренти та співробітники.

Створюємо детальний перелік загроз та вразливостей взявши до уваги джерела загроз.

Таблиця 2.5 - Модель загроз та вразливостей

Джерело	Загроза	Вразливість
Конкуренти	Викрадення інформації (отримання та копіювання без дозволу)	— Можливість доступу до корпоративної мережі з будь-якого пристрою — Відсутність ефективної політики встановлення паролів для перевірки автентичності
	Зміна інформації	
	Видалення інформації	
	Несанкціонований доступ до корпоративної мережі	— Можливість підключення до корпоративної мережі з будь-якого пристрою.
	Статистичний аналіз мережевого трафіку	

	Перехоплення інформації	

Продовження таблиці 2.5

Джерело	Загроза	Вразливість
Персонал (системний адміністратор є виключенням)	Неавторизована зміна інформації	— Можливість використовувати будь-які зовнішні носії даних. — Відсутність належної політики щодо створення паролів для перевірки автентичності.
	Неавторизоване знищення інформації	
	Неавторизований друк і копіювання інформації	
	Неавторизована зміна та/або знищення та/або встановлення ПЗ	
	Помилки в роботі програмного забезпечення, технічних засобів	— Недостатній рівень підготовки персоналу з питань безпеки — Некомпетентність співробітників — Недостатня інформаційна грамотність — Відсутність організаційних методів захисту від розкриття інформації.
	Ненавмисне розкриття конфіденційної або комерційної таємниці	
	Навмисне розкриття конфіденційної або комерційної таємниці	
Персонал (з системним адміністратором)	Несанкціоновані зміни інформації	— Зберігання інформації без захисту — Недолік правильного обмеження доступу та "квот" — Можливість підключення до корпоративної мережі з будь-якого пристрою
	Несанкціоноване видалення інформації	
	Несанкціоновані друк і копіювання інформації	
	Помилки під час роботи з ПЗ, ТЗ	— Недостатній рівень підготовки персоналу в галузі безпеки — Некомпетентність працівників — Відсутність організаційних методів захисту від розкриття інформації.
	Ненавмисне розголошення конфіденційної або комерційної таємниці	
	Умисне розголошення конфіденційної або комерційної таємниці	
	Зміна журналу подій	

	Умисне або ненавмисне вимкнення антивірусного захисту	— Зберігання без захисту — Некомпетентність працівників — Відсутність правильної політики створення паролів для аутентифікації — Відсутність організаційних методів захисту від розкриття інформації. — Умисне або ненавмисне вимкнення антивірусного захисту
	Розкриття даних аутентифікації користувачів системи	
	Умисне або ненавмисне знищення програмного забезпечення або технічних засобів	— Зберігання без захисту — Відсутність правильного обмеження доступу та "квот" — Відсутність організаційних методів захисту від розкриття інформації

Продовження таблиці 2.5

Порахуємо коефіцієнт небезпеки для кожної з вразливостей за формулою (К1*К2*К3)/125=$К_н$

де К1 - фатальність;

К2 - можливість/зручність впровадження;

К3 - кількість компонентів, схильних до вразливості, і визначення найбільш критичних загрози.

Таблиця 2.6 - Коефіцієнт небезпеки

Вразливість	К1	К2	К3	$К_н$
Відсутність систем захисту інформації організації	3	2	3	0,144
Можливість доступу до корпоративної мережі з будь-якого пристрою	3	4	5	0,48
Зберігання даних без захисту	4	3	3	0,288
Відсутність правильної політики для створення паролів ідентифікації	3	4	3	0,288
Недостатнє розмежування доступу та "квот"	3	4	3	0,288
Недостатній рівень підготовки персоналу з безпеки	3	2	4	0,192
Недосвідченість співробітників у сфері ІТ	4	4	3	0,384
Недоступність сторонніх носіїв даних для підключення	4	2	2	0,128
Можливість доступу до корпоративної мережі з будь-якого пристрою	3	2	4	0,192

Рівні групи К1:

— 1 - наслідки, які можна ігнорувати;

— 2 - незначні наслідки;

— 3 - помітні наслідки;

— 4 - значні наслідки;

— 5 - повний крах підприємства.

Рівні групи К2:

— 1 - уразливість дуже складно або неможливо експлуатувати;

— 2 - для використання вразливості потрібні спеціальні умови, обладнання та/або досвідчений інсайдер;

— 3 - уразливість може бути використана тільки досвідченим інсайдером з мінімальним обладнанням;

— 4 - вразливість може бути використана тільки досвідченим інсайдером;

— 5 - уразливість доступна для всіх.

Рівні групи К3:

— 1 - відсутній або присутній лише один елемент;

— 2 - від двох до дев'яти елементів;

— 3 - від десяти до чотирнадцяти елементів;

— 4 - від п'ятнадцяти до дев'ятнадцяти елементів;

— 5 - понад двадцять елементів.

Отже, найвищий рівень ризику становлять:

— можливість підключення до корпоративної мережі з будь-якого пристрою;

— зберігання даних без належного захисту;

— недостатня кваліфікація співробітників.

Крім загроз, створюваних людиною, існують загрози техногенного і стихійного характеру. Зробимо перерахунок цих двох видів загроз, вказавши властивості інформації, що порушуються. А саме - конфіденційність (К), цілісність (Ц) і доступність (Д).

Таблиця 2.7 - Техногенні та стихійні загрози

Загроза	Інформаційні властивості, які порушуються		
	К	Ц	Д
Техногенні загрози			
Проблеми, які можуть вплинути на роботу системи: — швидкість обробки даних; — пропускна здатність мережевих каналів; — доступна оперативна пам'ять; — доступне місце на жорсткому диску; — електроживлення обладнання; — кібератаки через інтернет.	-	-	+
Перехоплення інформації (несанкціоноване): — з використанням ПЕМВ від технічних пристроїв; — під час підключення до каналів передавання даних; — порушення встановлених правил доступу; — впровадження вірусів на робочі станції; атаки хакерів	+	+	-
Помилки: — під час встановлення ПЗ, ОС, СУБД; — під час використання ПЗ; — під час експлуатації технічних пристроїв; — недбале ставлення співробітників до документації; — помилки під час введення даних.	-	+	+
Порушення нормальної роботи: — порушення працездатності системи обробки інформації; — порушення працездатності зв'язку; — старіння носіїв інформації та засобів її обробки; обробка; — порушення встановлених правил доступу; електромагнітний вплив на технічне обладнання.	-	+	+

Продовження таблиці 2.7

Загроза	Інформаційні властивості, які порушуються		
	К	Ц	Д
Знищення (пошкодження): — програмного забезпечення, операційних систем, систем управління базами даних; пристроїв обробки інформації.	-	+	+
Модифікація (зміна): — програмного забезпечення, операційних систем, систем керування базами даних; даних під час передавання засобами зв'язку і телекомунікацій.	+	+	+
Стихійні Загрози			
інциденти, пожежі, стихійні лиха; - несподівані ситуації, незрозумілі феномени та інші форс-мажорні обставини.	-	+	+

2.3.2 Визначення переліку порушників

Інформація, що циркулює в підприємстві, може бути викрадена зловмисниками - особами, які помилково, через незнання, або навмисне, зі злим наміром чи без нього, намагалися виконати операції, що порушують властивості інформації, визначені політикою безпеки. Порушники ІКС можуть бути як внутрішніми (співробітники або користувачі системи), так і зовнішніми (зовнішні особи). Метою порушника може бути:

— отримання необхідної інформації в потрібному обсязі та різноманітності;

— можливість змінювати інформаційні потоки відповідно до своїх намірів (інтересів, планів);

— заподіяння шкоди шляхом знищення матеріальних та інформаційних цінностей.

Створимо модель порушника, враховуючи можливий мотив, кваліфікацію, місце і час дій порушників.

Таблиця 2.8 - Модель порушника

Посада	Мотив	Кваліфікація	Місце дії	Час дії
Внутрішні порушники				
Директор	М1, М2,М3	К4	Д5	Ч3
Директор з продажів	М1, М2,М3	К1	Д5	Ч3
Директор з консультацій	М1, М2,М3	К1	Д5	Ч3
Менеджер з продажів	М1, М2,М3	К1	Д4	Ч3
Менеджер з консультацій	М1, М2,М3	К1	Д4	Ч3
Бухгалтер	М3	К1	Д5	Ч3
Сис.адмін.	М1, М2,М3	К5	Д6	Ч4
Кадровий робітник	М1, М3	К1	Д4	Ч3
Зовнішні порушники				
Представники компаній, що займаються сферою технічної підтримки	М3	К5	Д2	Ч1
Представники компаній, що працюють у сфері програмного забезпечення	М3	К4	Д3	Ч1
Кіберзлочинці	М2, М3	К3	Д1	Ч3

Специфікація характеристик порушника, заснованих на мотивах вчинення правопорушень:

- М1 - Відсутність відповідальності
- М2 - Бажання самоствердитися
- М3 - Егоїстичні мотиви

Специфікація характеристик порушника за рівнем кваліфікації та знань про інформаційно-технічні системи (ІТС):

- К0 - не має знань про функціональні особливості системи, принципи формування даних і потоків запитів, володіє базовими навичками використання стандартних інструментів системи.
- К1 - знає функціональні особливості системи, принципи формування даних і потоків запитів, володіє навичками використання стандартних інструментів системи.
- К2 - має високий рівень знань і практичні навички в роботі з технічними засобами системи та їх обслуговуванні.
- К3 - володіє глибокими знаннями в галузі програмування та комп'ютерної техніки, проектування та експлуатації автоматизованих інформаційних систем.
- К4 - знає структуру, функції та недоліки засобів захисту.
- К5 - вивчив недоліки та вразливості механізмів захисту, вбудованих у програмне забезпечення або його не задокументовані можливості.
- К6 - є розробником програмного або апаратного забезпечення для захисту або системного програмного забезпечення.

Специфікація характеристик порушника за місцем розташування дій:

- Д1 - без доступу до контрольованої території організації.
- Д2 - на контрольованій території без доступу до будівель або споруд.
- Д3 - у приміщенні без доступу до технічного обладнання АС.
- Д4 - з урахуванням робочих місць користувачів інформаційної системи.
- Д5 - З доступом до даних (включно з базами даних, архівами та іншим).
- Д6 - з можливістю управління засобами безпеки інформаційної системи.

Опис дій порушника за часовими критеріями:

- Ч1 - до впровадження інформаційної системи або її компонентів.
- Ч 2 - у період неактивності компонентів системи (у неробочий час, під час планових перерв, обслуговування та ремонту тощо).
- Ч3 - під час роботи інформаційної системи (або її компонентів).
- Ч4 - під час роботи інформаційної системи та при неактивних компонентах.

2.3.3 Встановлення каналів несанкціонованого доступу до ІКС

Несанкціонований доступ до даних - це отримання інформації таким чином, що порушуються встановлені правила і закони. Це може бути отримання доступу до конфіденційної інформації співробітником, який не має відповідних повноважень, або особою без дозволу на доступ до цієї інформації.

Іноді несанкціонованим доступом також називають отримання інформації особою, яка має право на доступ до неї, але в обсязі, що перевищує необхідний для виконання службових обов'язків. Витік інформації - це поширення даних без контролю, що може призвести до їх несанкціонованого використання.

Основні способи витоку даних у системі ІКС на ОІД включають:

- змінні диски та інші пристрої для зберігання даних;
- комп'ютери співробітників відділів;
- робочі станції адміністраторів системи;
- пристрої для введення/виведення даних;
- засоби передачі інформації в інформаційно-телекомунікаційній системі;
- комутаційне обладнання.

2.4 Вживання заходів захисту

Система автоматизації - це організаційно-технічна система, що об'єднує операційну систему, фізичне середовище, персонал і оброблювану інформацію. Для спрощення процесу зіставлення вимог до обчислювальної системи автоматизованої системи з характеристиками автоматизованих систем було запроваджено класифікацію та визначено кілька стандартних профілів безпеки. Таким чином, інформаційна система підприємства належить до класу "3".

Це означає, що це розподілений комплекс із безліччю машин і користувачами, який обробляє інформацію різних рівнів доступу. Для даної інформаційної системи класу "3" було обрано відповідний профіль безпеки.

3.КЦД.1=[КД-2, КО-1, КВ-1, ЦД-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1, НР-2, НИ2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1]

Таблиця 2.9 – Профіль захищеності ІКС

Критерії	Послуги безпеки	Вимоги до рівнів послуг безпеки
	1	2
Конфіденційність	Базовий рівень конфіденційності	КД-2 (базовий)
	Повторне використання об'єктів	КО1 (повторне)
	Конфіденційність під час обміну	КВ1 (мінімальна)
Цілісність	Довірча цілісність	ЦД1 (мінімальна)
	Відкат	ЦО1 (обмежений)
	Цілісність при обміні	ЦВ1 (минімальна)
Доступність	Відновлення після збою	ДВ1 (у ручну)
	Використання ресурсів	ДР1 (норми)
Спостережність	Реєстрація в журналі	НР2 (журнал охорони)
	Ідентифікація	НИ2 (перевірка автентичністості)
	Цілісність комплексу засобів захисту	НЦ2 (КЗЗ)
	Самодіагностика	НТ2 (самодіагностика старту)
	Ідентифікація та перевірка автентичності під час обміну даними	НВ1 (перевірка автентичності)

Базова політика конфіденційності (КД-2) призначена для управління доступом користувачів до захищених об'єктів і забезпечує можливість користувачам контролювати потік інформації в автоматизованій системі в межах своїх захищених об'єктів, передаючи доступ до інших користувачів.

Положення про конфіденційність застосовуються до об'єктів і забезпечують взаємодію між такими сутностями:

– користувачами всіх рівнів;

– об'єктами, що містять конфіденційну інформацію;

– групами користувачів в АС з однаковими правами щодо такої інформації і тільки в межах цих груп;

– усіма іншими об'єктами, під заступництвом яких перебуває інформація, але які не належать до перелічених вище видів.

Положення про конфіденційність, що реалізується КЗЗ (комлекс засобів захисту), може бути застосовано до об'єктів, які були захищені користувачем під час виконання ним функціональних завдань.

КЗЗ повинна здійснювати розмежування доступу на основі атрибутів доступу користувача і об'єкта, що захищається. Запити на зміну прав доступу до об'єкта мають бути авторизовані КЗЗ (контрольною зоною захисту) на основі атрибутів доступу користувача, який запитує доступ, і самого об'єкта.

КЗЗ повинна забезпечити можливість визначення конкретних користувачів або групи користувачів із правом запуску цієї програми. Права доступу до кожного об'єкта, що охороняється, мають бути встановлені в момент його створення або ініціалізації.

Цей сервіс гарантує, що під час передачі об'єкта новому користувачеві або процесу не залишиться слідів інформації попереднього користувача або процесу. Він стосується лише конфіденційної інформації, якою діляться користувачі та додаткові процеси в системах управління доступом. Вимоги цієї послуги поширюються на сегменти оперативної пам'яті.

Механізм скасування певних операцій і повернення захищеного об'єкта в попередній стан дозволяє користувачам відкочувати зміни. Політика обмеження відкату керує взаємодією різних об'єктів, включно з користувачами всіх рівнів, об'єктами з конфіденційною інформацією та технологічною інформацією. Зазвичай під терміном "ступінь захищеності" експортованих об'єктів мається на увазі високий ступінь надійності алгоритмів шифрування, що використовуються.

Повторне використання об'єктів (КО-1) - це сервіс, який гарантує правильність повторного використання спільних об'єктів. Він забезпечує, що під час передачі спільного об'єкта новому користувачеві або процесу він не містить інформацію, що залишилася від попереднього використання цього об'єкта іншим користувачем або процесом.

Політика повторного використання об'єктів, що реалізується КЗЗ, застосовується тільки до тих об'єктів ЛОМ, які містять конфіденційну інформацію і використовуються різними користувачами та прикладними процесами в ЛОМ. Вимоги до цього сервісу поширюються на оперативну пам'ять робочих станцій і серверів (усіх типів) та носії інформації на жорстких магнітних дисках (ЖД), що використовуються системними та функціональними процесами під час роботи з конфіденційною інформацією, а також на певні периферійні пристрої з власною пам'яттю, які задіяно під час передання конфіденційної інформації до ЛОМ та створення резервних копій.

Перш ніж новий користувач або процес отримають доступ до об'єкта, що звільняється іншим користувачем або процесом, права доступу попереднього користувача або процесу до цього об'єкта мають бути анульовані. Ця вимога повністю поширюється на процеси, які одночасно використовуються кількома користувачами.

Мінімальний рівень конфіденційності під час обміну (КВ-1):

– політика конфіденційності під час обміну, яку реалізує (КЗЗ), повинна визначати набір об'єктів і процесів взаємодії, до яких вона застосовується;

– політика конфіденційності під час обміну, яку впроваджує КЗЗ, повинна визначити рівень захищеності, що забезпечується використовуваними механізмами, а також здатність користувачів та/або процесів керувати цим рівнем захищеності;

– КЗЗ повинен гарантувати захист від прямого доступу до інформації, що міститься в об'єкті, що передається.

Мінімальний ступінь довіри до цілісності (ЦД-1):

Цей сервіс використовується для забезпечення захисту оброблюваної інформації від несанкціонованих змін і надає користувачам будь-якої категорії можливість контролю потоків інформації від інших користувачів до захищених об'єктів з його домену.

Політика довірчої цілісності, що реалізується КЗЗ, поширюється на слабко і тісно пов'язані об'єкти, що створюються користувачами в процесі виконання функціональних обов'язків. Творець об'єкту має право визначити конкретних користувачів або групи користувачів із правом модифікації цього об'єкта.

КЗЗ повинен проводити розмежування доступу на основі атрибутів доступу користувача і об'єкта, що захищається.

Запити на зміну прав доступу до об'єкта мають бути опрацьовані в КЗЗ з урахуванням атрибутів доступу користувача, який ініціює запит, і самого об'єкта. Права доступу до кожного захищеного об'єкта мають бути встановлені в момент його створення або ініціалізації.

Обмежений відкат (ЦО-1) надає можливість скасувати виконання окремої операції або послідовності операцій і повернути захищений об'єкт до попереднього стану, визначеного заздалегідь. Політика обмеженого відкату може бути застосована до всіх категорій користувачів і пов'язаних об'єктів, що

містять конфіденційну інформацію. Компоненти повинні мати автоматизовані засоби для скасування виконання операцій над об'єктами за певний період часу. Використання послуги має фіксуватися в системному журналі, а видалення з журналу записів про операції, що були скасовані, не допускається.

Мінімальна цілісність під час обміну (ЦВ-1) забезпечує захист об'єктів від несанкціонованої модифікації інформації під час їх експорту або імпорту через незахищене середовище. Зазвичай ця послуга використовує криптографічні механізми, такі як цифровий підпис і коди автентифікації повідомлень. Рівні цієї послуги залежать від рівня захисту та вибірковості управління. За повноту захисту розуміється здатність забезпечити захист від різних видів загроз.

Зазвичай ступінь захищеності експортованих об'єктів визначається тим, наскільки криптостійкі алгоритми шифрування використовуються.

Використання ресурсів (ДР-1)

Цей сервіс дає змогу керувати використанням послуг і ресурсів користувачами. Політика використання ресурсів, що впроваджується КЗЗ, застосовується до зазначених об'єктів і забезпечує взаємодію між ними, передбачаючи можливість встановлення обмежень на використання ними користувачами всіх категорій.

Системний адміністратор або користувачі з відповідними правами інших адміністраторів можуть встановлювати обмеження на використання обчислювальних ресурсів АС або кількість об'єктів для окремих користувачів або процесів. Запити на зміну цих обмежень повинні оброблятися КЗЗ тільки при надходженні від адміністраторів.

Спроби користувачів перевищити встановлені ліміти з використання ресурсів мають бути зареєстровані в системному журналі.

Ручне відновлення після збоїв (ДВ-1)

Ця політика відновлення після збоїв, що здійснюється (КЗЗ), поширюється на зазначені об'єкти та забезпечує їхню взаємодію:

– програмне та функціональне обладнання;

– засоби захисту інформації та інструментарій для управління комплексною системою захисту інформації;

– засоби адміністрування та управління обчислювальною системою;

– периферійні пристрої (наприклад, принтери, накопичувачі інформації, змінні носії даних), що використовуються для роботи з конфіденційною інформацією.

Цей сервіс гарантує повернення АС до відомого безпечного стану після відмови або тимчасового припинення роботи, спричинених помилками користувачів, неврахованими функціональними дефектами програмного або апаратного забезпечення (наприклад, можлива поява невиявлених на етапі проєктування функцій) або іншими непередбачуваними обставинами.

Важливо визначити та задокументувати різні види збоїв і переривань у роботі локальної обчислювальної мережі (ЛОМ) або окремих її компонентів, щоб мати змогу повернути систему до відомого захищеного стану, дотримуючись політики безпеки. Для кожного типу збою необхідно чітко визначити рівні, при досягненні яких потрібне повторне встановлення автоматизованої системи. Відновлення роботи окремих компонентів зі стану, що характеризується низькою якістю обслуговування, у нормальний режим має здійснюватися шляхом використання ручних процедур, а не автоматично.

Журнал безпеки (НР-2)

Сервіс реєстрації рівня НР-2 дає змогу відстежувати потенційно небезпечні дії користувачів усіх категорій щодо процесів та об'єктів інформаційної системи.

Політика реєстрації поширюється на всіх користувачів і сприяє взаємодії між ними.

Система захисту має фіксувати всі події, пов'язані безпосередньо з її безпекою. Серед таких подій слід виділити:

– вхід/вихід або спроби входу/виходу із системи користувачами різних категорій;

– реєстрація, видалення або спроби реєстрації та видалення користувачів будь-якої категорії із системи;

– зміна пароля користувача будь-якої категорії;

– отримання доступу або спроби його отримання користувачем будь-якої категорії до процесів і об'єктів інформаційної системи, що мають обмеження доступу на рівні конфіденційної інформації;

– виведення конфіденційних документів або інформації на принтер, здійснене користувачем будь-якої категорії, а також спроби такого виведення;

– копіювання конфіденційних даних на запам'ятовуючі пристрої з можливістю запису інформації та спеціально призначені для цього цілі; на пристроях зберігання даних, що не призначені для цього згідно з правилами безпеки:

– виявлення і реєстрація порушень цілісності інформаційної системи;

– інші події, для яких обов'язкова реєстрація відповідно до політики забезпечення безпеки інформації.

Реєстрація всіх подій, пов'язаних із безпекою, здійснюється в журналі реєстрації. У ньому міститься інформація про дату, час, місце (адресу робочої станції в АС), ім'я користувача, тип і успішність або невдачу кожної зареєстрованої події. Журнал має містити достатню інформацію для однозначної ідентифікації робочої станції, користувача, процесу та/або об'єкта, пов'язаних із кожною подією.

Адміністратор з безпеки та користувачі з відповідними правами повинні мати доступ до перегляду та аналізу журналу реєстрації. Інформаційна система повинна гарантувати захист журналу від несанкціонованого доступу (НСД), змін або знищення.

Ідентифікація та перевірка автентичності однієї особи (НІ-2)

Процеси ідентифікації та автентифікації дають змогу встановити особу користувача різних категорій, який бажає отримати доступ до інформаційної системи або захищених ресурсів, і повинні гарантувати, що доступ надається тільки авторизованим особам.

Політика ідентифікації та автентифікації застосовується до зазначених об'єктів з метою забезпечення їхньої взаємодії.

Кожен користувач, який намагається отримати доступ до інформаційної системи, має бути впізнаний контрольно-системним обладнанням на основі унікального імені. Після успішної аутентифікації користувача контрольно-системне обладнання на основі введеного пароля надає йому право на виконання дій, контрольованих контрольно-системними зонами.

Механізм реалізації послуги має забезпечувати надійне і точне виконання процесів ідентифікації та аутентифікації. Контрольно-системне обладнання повинно гарантувати захист даних автентифікації від несанкціонованого доступу, змін або пошкоджень.

Односпрямований достовірний канал (НК-1)

Послуга повинна забезпечити можливість користувача різних категорій безпосередньої взаємодії з контрольно-системним обладнанням, при цьому гарантуючи неможливість модифікування цієї взаємодії іншим користувачем або процесом. Послуга також повинна визначити вимоги до механізму створення безпечного зв'язку між користувачем і контрольно-системним обладнанням.

Політика безпечного каналу поширюється на всіх користувачів, окремі компоненти програмного забезпечення системи, задіяні для реалізації функцій контрольно-системного обладнання, з метою забезпечення взаємодії зазначених об'єктів.

Достатньо використовувати безпечний канал для початкової перевірки особи та автентичності. Взаємодія через цей канал може бути запущена тільки самим користувачем.

Розподіл завдань між адміністраторами (АЛЕ-2)Сервіс дає змогу визначити різні рівні доступу до системи, встановлюючи певні ролі для кожної категорії користувачів. Метою послуги є зниження можливих втрат від втручання або помилок користувачів та обмеження централізованого контролю над автоматизованою системою.

Політика розподілу обов'язків, поширюється на всіх користувачів і має включати такі ролі як мінімум:

– адміністратора безпеки;

– як мінімум одного іншого адміністратора (наприклад, адміністратор баз даних, адміністратор мережевого обладнання, адміністратор сервісів тощо);

– користувачів із доступом до конфіденційної інформації.

Ролі адміністраторів можуть бути доручені іншим користувачам у разі потреби, але кількість таких випадків має бути мінімальною.

Системний адміністратор повинен мати доступ до технічної інформації про систему захисту інформації та програмного забезпечення для її реалізації. Іншому адміністратору потрібен доступ до технічної інформації про функціонування автоматизованої системи та програмного забезпечення для її управління. Усім іншим користувачами забороняється доступ до цих даних.

Доступ адміністраторів до об'єктів з конфіденційною інформацією має бути обмежений, за винятком випадків об'єднання оперативних повноважень і повноважень на роботу з конфіденційними даними в рамках своїх функціональних завдань.

Достовірний односторонній канал (НК1)

Сервіс має гарантувати користучаву можливість будь-якої взаємодії з КЗЗ, а також що використання ЛОМ не буде модифікованою іншими користувачами.

Сервіс повинен встановлювати вимоги до створення надійного каналу зв'язку між користувачем і КЗЗ. Політика надійного каналу застосовується до

всіх користувачів, різних компонентів системного та функціонального програмного забезпечення, що використовуються для реалізації механізмів КЗЗ, і гарантує взаємодію цих об'єктів. Надійний канал має використовуватися для початкової ідентифікації та автентифікації. З'єднання через цей канал має бути запущено тільки користувачем.

Розподіл обов'язків адміністраторів (НО-2) дає змогу визначити повноваження користувачів шляхом виділення категорій із відповідними функціями для кожної з них. Цей сервіс спрямований на зниження потенційних збитків від навмисних або випадкових дій користувачів і обмеження авторитарності управління Автоматизованими Системами (АС). Політика розподілу обов'язків, що реалізується КЗЗ, охоплює всіх користувачів і повинна визначати щонайменше такі ролі:

— системний адміністратор;

— не менше одного іншого адміністратора (наприклад, адміністратор баз даних, адміністратор мережевого обладнання, адміністратор сервісів);

— користувачі з доступом до конфіденційної інформації.

Ролі адміністраторів можуть бути доручені іншим користувачам. Кількість таких користувачів має бути мінімальною.

Адміністратор безпеки отримує доступ до технічної інформації, що захищається КСЗІ, і програмного забезпечення системного управління та функціонального ПЗ, що реалізує механізми захисту. Інший адміністратор має доступ до технічної інформації щодо управління автоматизованими системами та програмного забезпечення системного управління і функціональних можливостей цієї системи.

Доступ до цих об'єктів має бути обмежений для всіх інших користувачів. Дозвіл адміністраторам на доступ до об'єктів з високою та низькою зв'язністю, що містять конфіденційну інформацію, має бути виключним, за винятком випадків, коли їхні обов'язки потребують комбінування адміністративних повноважень із повноваженнями з обробки конфіденційної інформації.

Послуга з гарантованим забезпеченням цілісності (НЦ-2)

Цей сервіс оцінює здатність системи контролю за секретністю КЗЗ забезпечувати свій захист і підтримувати управління захищеними об'єктами. Для досягнення рівня НЦ-2 потрібно, щоб КЗЗ працював у своїй власній області виконання, відокремленій від усіх інших процесів, що допомагає їй захиститися від зовнішніх впливів. Ця вимога є одним з основних критеріїв для системи контролю доступу. Зазвичай реалізація цієї вимоги має бути забезпечена апаратними можливостями операційної системи.

Самоперевірка під час запуску (НТ-2)

Процедура самоперевірки дає змогу КЗЗ перевірити і гарантувати правильне функціонування і цілісність безлічі функцій локальної обчислювальної мережі, які забезпечують безпеку.

Політика самоперевірки поширюється на такі об'єкти і регламентує їхню взаємодію:

- адміністратор безпеки;
- компоненти системного та функціонального програмного забезпечення, необхідні для реалізації механізмів КЗЗ;
- інструменти захисту інформації та технічну інформацію про КСЗІ.

У складі КСЗІ має бути набір тестових процедур, достатній для оцінки правильності виконання всіх критичних для безпеки конфіденційних даних і технічної інформації за допомогою ЛОМ, а сама КСЗЗ повинна мати можливість контролювати це виконання. Тестування має виконуватися під час запуску КСЗІ за запитом адміністратора безпеки.

Якщо в процесі виконання одного з тестів КСЗІ виникнуть проблеми, необхідно перевести інформаційну систему АС у режим, коли оброблення конфіденційної інформації заборонено повністю або з використанням послуг безпеки, для яких тест не було проведено. Відновити працездатність АС може лише адміністратор безпеки після відновлення КСЗІ та повторного проведення всіх необхідних тестів.

Автентифікація вузла (НВ-1) - це сервіс, який забезпечує захист об'єктів від незаконної зміни інформації, що міститься в них, під час їхнього передавання через незахищені мережі. Зазвичай цей сервіс реалізується за допомогою криптографічних методів захисту, таких як цифровий підпис і коди автентифікації повідомлень. Система може бути оцінена на цей рівень, якщо вона дозволяє проводити перевірку цілісності програмного забезпечення на комп'ютері на основі цифрового підпису або забезпечує цифровий підпис повідомлень в електронній пошті.

2.5 Розробка політики безпеки інформації

Необхідно розробити елементи політики безпеки інформації знідно таблиці 2.9, що зможуть знизити рівень впливу тих загроз, що мають найбільший степінь небезпечності, а саме:

- читання даних, що виводяться на екран;
- несанкціонований перегляд інформації на паперових носіях;
- пошкодження носіїв інформації;
- ураження шкідливим програмним забезпеченням.

Виходячи з переліку найнебезпечніших загроз, розроблено політики безпеки інформації.

2.5.1 Політика безпеки «чистого столу»

Політика "чистого столу" покликана забезпечити, що всі паперові документи, які можуть містити конфіденційну інформацію, будуть прибрані з поля зору.

Також у цій політиці передбачено приховування інформації на моніторах за відсутності співробітника за робочим столом.

Основна мета політики полягає у встановленні вимог щодо зберігання паперових носіїв інформації та забезпечення їхньої недоступності для сторонніх осіб. Ці правила поширюються на всіх співробітників компанії.

Інструкції з політики:

– співробітники повинні гарантувати захист конфіденційної інформації на робочому місці весь робочий день.

– за відсутності співробітника за робочим столом, ноутбук має бути заблокований.

– після закінчення робочого дня всі ноутбуки компанії мають бути вимкнені.

– паперові документи з конфіденційною інформацією слід прибирати в шухляду і замикати її ключем до кінця робочого дня або за відсутності працівника за столом.

– не рекомендується залишати ключі від шухляд без нагляду або передавати їх будь-кому.

– забороняється записувати паролі на папері або зберігати їх на ноутбуках.

– у разі друку документів із конфіденційною інформацією необхідно одразу після друку забирати їх із принтера.

– для знищення паперових документів з конфіденційною інформацією кожен аркуш слід розірвати на 10 частин.

Інформацію на знімних носіях слід зберігати в закритих ящиках робочих столів. Співробітник, який порушив цю політику, може бути підданий дисциплінарним заходам у вигляді штрафу або звільнення залежно від серйозності порушення.

2.5.2 Політика безпеки інформації для резервного копіювання

Мета політики полягає у встановленні процедур резервного копіювання для подальшого відновлення працездатності інформаційної системи в разі повної або часткової втрати даних через збої в апаратному або програмному забезпеченні, помилки користувачів, стихійні лиха та інші надзвичайні ситуації.

Також метою є визначення процедур відновлення інформації за необхідності та забезпечення захисту від випадкового видалення файлів. Інструкція з політики наказує створення регулярних резервних копій для інформації, яку використовують користувачі та система організації. Носії з даними мають зберігатися в безпечному місці з відповідними умовами навколишнього середовища.

Частота та обсяг резервного копіювання повинні відповідати значущості інформації та рівню прийнятого ризику, визначеному власником даних. Процес створення резервних копій і відновлення інформаційних ресурсів має бути документований і періодично перевірятися.

Системи, що надають можливість створення резервних копій за межами основного місцезнаходження, мають бути очищені від конфіденційної інформації високого рівня. Фізичні механізми контролю доступу до сховищ даних мають відповідати або перевищувати рівень контролю доступу до основних систем.

Крім того, носії даних мають бути захищені на найвищому рівні конфіденційності інформації, що зберігається на них. Процес підтвердження успішності створення резервної копії електронної інформації також є необхідним.

Резервні копії операційних систем та іншого важливого програмного забезпечення слід зберігати окремо від самого ПЗ. Для захисту інформації в резервній копії системи необхідно передбачити захист від несанкціонованих змін і впливу зовнішнього середовища. Перевірка резервних копій повинна проводитися щомісяця, щоб переконатися, що вони придатні для відновлення.

Для підтвердження надійності носія і збереження даних слід регулярно перевіряти резервну інформацію. Резервні копії даних повинні містити певні характеристики, які можна легко впізнати за мітками або штрих-кодами: назву системи, дату створення, класифікацію та контактну інформацію.

Процес резервного копіювання має відповідати методу "3-2-1", за якого створюють три копії необхідної інформації:

- дві з них мають зберігатися на різних носіях
- третю - за межами офісу (наприклад, у хмарному сховищі або на знімному носії).

Співробітники, які порушили положення цієї політики, підлягають дисциплінарним заходам - штрафу або звільненню - залежно від серйозності порушення.

2.5.3 Політика безпеки з антивірусного захисту

Мета цієї політики безпеки - поліпшити безпеку інформації в компанії шляхом розроблення системної політики зі створення, впровадження та обслуговування комплексних засобів антивірусного захисту. Ці засоби встановлюють основні правила і вимоги для захисту інформаційних ресурсів організації від загроз, пов'язаних з діями програм, спеціально створених або змінених для несанкціонованого видалення, блокування, зміни або копіювання інформації, а також порушення роботи організації.

Ця політика обов'язкова для всіх співробітників компанії, які використовують комп'ютери в робочій діяльності. Вона доповнює інші політики безпеки.

Відповідальність за виконання політики безпеки лежить на системному адміністраторі.

Засоби захисту від шкідливих програм мають бути встановлені, налаштовані й активовані на всіх програмах і технічних пристроях до початку використання для роботи з інформаційними ресурсами організації.

Дозволяється використовувати тільки ліцензійні антивірусні засоби, рекомендовані системним адміністратором. Якщо необхідно використовувати інші антивірусні програми, крім рекомендованих, це слід попередньо обговорити з фахівцем із системного адміністрування.

Встановлення засобів захисту від шкідливого ПЗ на комп'ютерах і налаштування параметрів проводиться системним адміністратором відповідно до інструкцій із застосування конкретних програм-антивірусів.

Контролю за виявленням шкідливих програм має піддаватися вся інформація, що створюється або обробляється через ПЗ, а також передається через переносні носії даних і телекомунікаційні канали.

Оновлення баз даних антивірусів має відбуватися автоматично не рідше ніж один раз на день - це залежить від можливостей використовуваного ПЗ.

Для запобігання проблемам із вірусами слід дотримуватися таких рекомендацій:

– не відкривайте файли або макроси, вкладені в електронні листи від незнайомих відправників. Якщо такі файли виявлено, рекомендується негайно видалити їх з вашого комп'ютера.

– видаляйте спам та інші непотрібні електронні листи без пересилання, згідно з правилами використання.

– не завантажуйте файли з недовірених джерел, це суворо заборонено.

– перед використанням будь-якого знімного носія рекомендується перевіряти його на наявність шкідливого ПЗ щоразу.

– регулярно створюйте резервні копії критичних даних і конфігурацій системи, зберігайте їх відповідно до політики безпеки щодо резервного копіювання.

Співробітники, які недотримуються цієї політики, піддаються дисциплінарним заходам - починаючи від штрафів до звільнення залежно від серйозності порушень. Будь-який відступ від політики має бути схвалений директором компанії.

2.5.4 Політика безпеки інформації до паролів

Мета цієї політики полягає у встановленні правил використання паролів для доступу до баз даних, електронних документів і підключення до бездротової мережі підприємства. Користувачі системи зобов'язані дотримуватися вимог, описаних у цій політиці. Дотримання цих правил щодо

використання паролів сприяє підвищенню рівня безпеки інформаційних ресурсів, які ходять і обробляються на підприємстві.

Дія політики безпеки щодо паролів поширюється на всіх користувачів, які мають доступ до баз даних або електронних документів, а також тих, хто підключається до корпоративної автоматизованої системи через бездротову мережу.

Відповідальним за дотримання правил щодо використання паролів користувачами системи є системний адміністратор.

Паролі на рівні системи:

– створюються адміністратором системи, директор компанії встановлює додатковий пароль для доступу до системи в разі надзвичайних ситуацій;

– кожен користувач повинен мати унікальні ідентифікатори та паролі;

– паролі мають складатися не менше ніж із 8 символів, включно із символами з 3 із наступних 4 категорій:

– великі латинські літери (A-Z); - малі латинські літери (a-z); - цифри (0-9);

– спеціальні символи, відмінні від літер і цифр (наприклад: ! $,%,#);

– пароль не повинен містити ім'я облікового запису завдовжки понад п'ять символів;

– заборонено передавати паролі третім особам, вставляти їх у текст програм або записувати на папері чи зберігати незашифрованими;

– паролі повинні регулярно змінюватися кожні 6 місяців (або раніше в разі можливої загрози витоку пароля або його втрати; у разі зміни системного адміністратора);

– забороняється повторювати одні й ті самі паролі мінімум 3 рази поспіль;

– не можна використовувати однаковий символ більше двох разів поспіль.

Правила безпеки розробляє системний адміністратор і директор організації підписує її за умови прийняття всіх пунктів політики.

Дотримання правил безпеки контролюється системним адміністратором підприємства з використанням стандартних методів автентифікації операційної системи. Під час введення нової політики безпеки кожен співробітник має бути проінформований не пізніше, ніж за 5 робочих днів до її набуття чинності. Підтвердження ознайомлення з даною політикою безпеки має бути підписано користувачем, який зобов'язується дотримуватися правил, встановлених у цьому документі.

Політика безпеки переглядається заступником директора щорічно. У разі виникнення непередбачених обставин політика безпеки може бути переглянута раніше встановленого року.

Співробітники, які прочитали політику безпеки, несуть відповідальність за зберігання своїх паролів. Порушники цієї політики будуть піддані дисциплінарним заходам залежно від тяжкості порушення.

Висновок розділу 2

У спеціальній частині було виконано обстеження ОІД, а саме:

– класифіковано інформацію, яка циркулює на підприємстві та потребує захисту;

– побудовано модель порушника і загроз, які можуть бути присутні у ІКС.

Проаналізувавши моделі загроз, були наведені найактульніші загрози і політики безпеки інформації проти них:

– політика безпеки з антивірусного захисту

– політика безпеки інформації для резервного копіювання

– політика безпеки «чистого столу»

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

Головна ціль захисту інформаційних ресурсів є мінімізація збитків від порушень, тому метою аналізу є економічне обґрунтування необхідності впровадження стратегії безпеки інформації.

Для цього оцінюється економічна ефективність використання ключових результатів, отриманих у процесі дослідження.

Економічна обґрунтованість визначається такими розрахунками:

– капітальні витрати, необхідні для реалізації розроблених елементів політики безпеки;

– операційні витрати;

– річний економічний ефект від впровадження інформаційної політики безпеки.

Капітальні витрати

Пропоновані елементи політики безпеки потребують фінансування для їх здійснення. Серед заходів, що потребують витрат, можна виділити:

– політика "чистого столу";

– олітика антивірусного захист.

3.1 Визначення трудомісткості розробки політики безпеки інформації

В першу чергу необхідно розрахувати витрти на розробку політики безпеки.

Тривалість створення політики безпеки інформації рахуеться за формуло:

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

де $t_{\text{тз}}$ – тривалість складання технічного завданння на розробку політики безпеки інфомації, 9 год.

$t_{\text{в}}$ – тривалість розробки концепції безпеки інформації підприємстві, 7 год.;

$t_а$ – тривалість процесу аналізу ризиків, 4 год.;

$t_{вз}$ – тривалість визначення вимог до заходів, методів та засобів захисту, 4 год.;

$t_{озб}$ – тривалість вибору основних рішень з забезпечення безпеки інформації, 7 год.;

$t_{овр}$ – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування підприємства, 8 год.;

$t_д$ – тривалість документального оформлення політики безпеки, 6 год.;

t = 9год+7год+4год+4год+7год+8год+6год = 45 год (3.1)

Розрахунок витрат на створення політики безпеки інформації

Візьмемо $К_{рп}$ як витрати на розробку безпеки інформації, $З_{зп}$ як витрати на заробітню плату працівника, а $З_{мч}$ як вартість витрат машинного часу, що необхідно для розробки політики безпеки інформації. За формулу візьмемо:

$$К_{рп} = З_{зп} + З_{мч}, грн \quad (3.2)$$

Заробітня плата для виконавці політики безпеки розраховується, формулою:

$$З_{зп} = t \cdot З_{іб}, грн \quad (3.3)$$

де t – загальна тривалість розробки політики безпеки, грн;

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

$$З_{зп} = 45 * 190 = 8550 грн$$

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

$$З_{мч} = t \cdot С_{мч}, грн \quad (3.3)$$

де t – трудоємкість розробки політики безпеки іфнормації на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу на ноутбуку визначається за формулою.

$$Смч=Р*tнал*Се+(Фзал*На/Fр)+(Клпз*На/Fр), грн \quad (3.4)$$

де Р -втановлена потужність ноутбуку, кВт

tнал – кількість станцій під час написання політики безпеки

Се – тариф на електричну енергію, грн/кВт година

Фзал – залишкова вартість ноутбуку на поточний рік, грн

На – річна норма амортизації на ноутбуці, частки рік

Напз – річна норма амортизації на ліцензійне ПЗ, частки одиниці

Клпз – вартість ліцензійного ПО, грн

Fр – річний фонд робочого часу (у 40-годинній робочій неділі, Fр=1920).

Потужність підприємства 0.4, тариф на електричну енергію дорівнює 4,32 грн/кВт година, тому:

$$С_{мч}=0,4*4,32*11+(15600*0,5\ /1920)+(4042*0,5/1920)=24,12грн$$

$$З_{мч} = t \cdot С_{мч} = 45 \cdot 24,12 = 1085грн$$

3.2 Розрахунок капітальних витрат

Капітальні витрати розраховуються таким методом:

$$К = К_{пр} + К_{зпз} + К_{рп} + К_{аз} + К_{навч} + К_{кн} \quad (3.5)$$

де Кпр – вартість розробки проекту інформаційної безпеки. Інші організації не були задіяні;

Кзпз – вартість ліцензійного ПЗ;

Таблиця 3.1 – Перелік ліцензійного ПЗ, яке було придбане

Назва	Кількість	Вартість (грн)
Windows 10 Home	12	30000
Total Commander	12	15300
Kaspersky	12	3200
Вього		48500

Крп – вартість розробки політики безпеки, 9635 грн;

Каз – вартість закупівлі апаратного забезпечення, та додаткових матеріалів (врізний замок = 800грн);

Кнавч – витрати на навчання персоналу та технічних фахівців, тис.грн (навчання системного адміністратора = 2300грн);

Кн – витрати на встановлення обладнання та налагодження системи, тис.грн;

Так як підприємство не закуповує обладнання для інформаційної безпеки, але є додаткові матеріли, враховуємо тільки його.

$$К = 48500 + 9635 + 1300 + 2300 + 800 = 62535 \text{ грн}$$

3.3 Розрахуной поточних (операційних) витрат

Річні (операційні) витрати на функціонування системи інформаційної безпеки розраховуються:

$$С = С_в + С_к + С_{ак}, \text{тис. грн} \quad (3.6)$$

де Св – витрати на оновлення системи;

Сак – витрати на допомогу користувачам системи, які сладають 850 грн (розробка додатків - 200 грн, робота з даними – 200 грн, неформальне навчання – 150 грн, формальне навчання - 300 грн);

Ск – витатри на керування інформаційною безпекою, відбувається за формулою:

$$С_к = С_н + С_а + С_з + С_{єв} + С_{ел} + С_о + С_{тос} \quad (3.7)$$

де Сн - витрати на навчання адміністративного персоналу та кінцевих користувачів визначають на основі даних про проведення тренінгів і курсів підвищення кваліфікації, які становлять 5500 гривень.

Са - річний фонд амортизаційних відрахувань розраховується як відсоток від загальної суми інвестицій в основні фонди та нематеріальні активи. На підприємстві використовується дванадцять ноутбуків загальною вартістю 192000 гривень, а вартість програмного забезпечення для них становить 48500 гривень. Разом - 240500 гривень. Мінімальний строк амортизації - два роки. Ліквідаційна вартість дванадцяти комп'ютерів становить 45000 гривень, а програмного забезпечення для них - 7000 гривень.

$$Са = (240500 – 52000)/2 = 94250 \text{ грн}$$

Сз – річний фонд заробітної плати персоналу, що обслуговує систему фніормаційної безпеки, розраховується:

$$Сз = Зосн + Здод, грн \quad (3.8)$$

де Зосн – заробітня плата 7500 грн на місяць, 90000 на рік;

Здод – додаткова заробітня плата, складає 1474 грн на місяць, 17688 грн на рік. В 2024 році ЄСВ складає 22% від фонду заробітної плати і розраховується:

$$Сєв = 107688 * 22\% = 23691 грн$$

$$Сз = 90000 + 17688 + 23691 = 131\ 379 грн$$

Сел – вартість електроенергії, що споживається робочими станціями системи інформаційної безпеки прятом року:

$$С_{ел} = Р \cdot Fр \cdot Це, грн \quad (3,10)$$

де Р – потужність робочих станцій інформаційної безпеки 0.36 кВт для одного ноутбуку, для всього підприємс тва 12 ноутбуків споживають 4.32 кВт.

де Fр – потужність роботи станцій інформаційної безпеки складає 12 місяців * 25 робочих днів/місяць * 9 робочх годин * 12 комп'ютерів = 38800;

Це – тариф на електроенергію, 4,32 грн/кВт годин;

Сел = 4.8 * 38800 * 4,32 = 804445 грн;

Со – витрти на залучення сторонніх спеціалістів з обслуговування і сертифікації персоналу, залучення не відбувається;

Стос – витрати на технічне і оганізаційне адмінастрування та серсів системи інформаційної безпеки визначається за відсотками від вартості капітальних витрат, які складають 1% і мають вигляд 625 грн.

$$Ск = 5500+94250+131379+23691+709171+625 = 940925 грн$$

Маючи всі необхідні дані розрахуємо річні експплуатаційні витрати:

$$С = 940925 + 850 = 941775$$

Оцінка величини збиту

Посада	Розмір заробітної плати, грн
Директор	65000
Директор з продажів	45000
Менеджер з продажів (3 особи)	75000
Директор з консультацій	40000
Менеджер з консультацій (3 особи)	60000

Бухгалтер	30000
Кадровий працівник	15000
Системний адміністратор	30000
Всього	360000

Витрати від зниження продуктивності співробітника атакованої системної мережі, моють наслідки простою та втрату іхньої заробітної плати за час (Пп).

Втрачна вигода від простою атакованої мережі:

$$U = П_п + П_в + V \quad (3.10)$$

де Пп – оплачуванні витрати робочого часу та простою співробітників атакованої мережі, грн;

Пв – вартість відновлення вузла корпоративної мережі, грн;

V – витрати від зниження обсягу продажів за час простою атакованої мережі, грн;

Місячний фонд робочго часу 235 годин. Час простою внаслідок атаки 7 годин:

$$П_п = \left(\frac{З_с}{F}\right) * t_a, грн \quad (3.11)$$

де Зс – загальна кількість витрат на заробітню плату співробітникам за місяць;

F – місячний фонд робочого часу;

tп – час простою внаслідок атаки.

Маємо такі розрахунки:

Пп = (36000/235)*7 = 1072 грн.

Витарати на відновлення працездатності (Пв) включать декілька складових:

Пви – витрати на введення інформації, грн;

Ппв – витрати на відновлення системи, грн;

Пзч – вартість заміни частини системи, грн.

Витрати на повторне введення інформації розраховуються:

$$П_{ві} = \left(\frac{З_с}{F}\right) * t_{ві}, грн \quad (3.12)$$

де Зс – загальна кількість витрат на заробітню плату співробітникам за місяць;

F – місячний фонд робочого часу;

tві – час повторного введення інформації співробітниками.

Пві = (360000/235)*6 = 9185грн

Витрати на відновлення Ппв розраховуються:

$$П_{пв} = \left(\frac{З_о}{F}\right) * \ t_в, грн \quad (3.13)$$

де Зо - заробітня плата системного адміністратора;

F – місячний фонд робочого часу;

tві – час відновлення мережі після атаки.

Ппв = (30000/235)*8 = 1021 грн

Пзч – вартість витрат на запасні частини складає 2500грн.

$$П_в = П_{ві} + П_{пв} + П_{зч}, грн \quad (3.14)$$

Пв = 9185+1021+2500 = 12706 грн

Витрати від зниження працездатності атакованої мережі:

$$V = \left(\frac{О}{F_р}\right) * (t_п + t_в + t_{ві}) \quad (3.15)$$

де О – обсяг продажів атакованої мережі, 12000000 грн за рік;

Fр – річний фонд часу роботи за рік, 2820 год.;

tп – 7 годин простою внаслідок атаки;

tв – 8 повторне введення інформації;

tві – 6 годин відновлення після атаки;

V = (12000000/2820)*21 = 89652 грн

Маючи всі потрібні дані, потрібно розрахувати втрачену вигоду від атаки ІКС організації:

U= 1072+12706+89652 = 103430 грн

Таким чином, загальний збиток від атаки на мережу має вигляд:

$$B = \sum i \sum n \ U \quad (3.16)$$

В = 6 * 7 * 103430 = 4344060 грн

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахування ризиків порушення інформаційної безпеки, та має вигляд:

$$E = B * R - C \quad (3.17)$$

де В – загальний збиток від атаки на мережу, 4344060 грн;

R – очікувана імовірність атаки на мережу становить приблизно 0,5(при умові загрозі раз у 6 місяців);

С – щорічні витрати на експлуатацію системи інформаційної безпеки складають 941775.

$$E = (4344060 * 0,5) – 941775 = 1239265$$

Аналіз показників економічної доцільності

Коефіцієнт повернення інвестицій ROSI показує, який додатковий прибуток приносить кошти копітальних інвестицій на врповадження системи інформаційної безпеки. Простіше кажучи, це показник запобігання можливих витрат на атаку копроративної мережі, тому він має вигляд:

$$ROSI=E/K \quad (3.18)$$

де Е – загальний ефект від провадження системи інформаційної безпеки, 1239265 грн;

К – капітальни витрати, 62535 грн.

$$ROSI = 1239265/62535 = 19,8$$

Термін окупності капітальних інвестицій То показує, за який час капітальні інвестиції окупляться за рахунок загально ефекту від впровадження системи інформаційної безпеки:

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

$$To = 1/19,8 = 0,1 \text{ (менше місяця)}$$

Висновок до розділу 3

При виконанні розрахунку економічної частини була проаналізована доцільність впровадження політики безпеки інформації. Визначено економічну ефективність використання основних результатів. Капітальни

витрати на впровадження політики інформаційної безпеки становлять 62535 грн., операційних витрати складають 941775 грн., а загальні збитки від атаки 4344060 грн., ефект від впровадження системи інформаційної безпеки становить 1239265 грн.. Термін окупності капітальних інвестицій складає меньше місяця. Отримані дані говорять про те, що впровадження створених елементів політики безпеки інформації є економічно доцільними.

ВИСНОВКИ

Під час кваліфікаційної роботи було вивчено тенденції зростання кіберзлочинності на світовому та українському рівнях, включно з аналізом порушень інформаційної безпеки у сфері малого бізнесу. Також було оцінено законодавчу базу щодо захисту інформації, проведено обстеження об'єктів інформаційної діяльності.

Було проведено класифікацію збереженої та переданої інформації на підприємстві, яка потребує захисту.

Було розроблено модель загроз і потенційних порушників в ІКС для визначення необхідного рівня безпеки з урахуванням актуальних ризиків.

Проведено аналіз інформаційних ризиків, розроблено політики безпеки для запобігання їх реалізації із застосуванням відповідних методів захисту.

Було виконано розрахунок доцільності впровадження політик безпеки інформації.

Отримані дані підтверджують ефективність впровадження створених елементів політик безпеки інформації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України». URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text (дата звернення: 06.06.2024)
2. Закон України «Про захист персональних даних». URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 06.06.2024)
3. ПРІОРИТЕТИ УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ. URL: https://ippi.org.ua/sites/default/files/solodka.pdf (дата звернення: 06.06.2024)
4. Закон України «Про електронні документи та електронний документообіг» URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 06.06.2024)
5. Закон України «Про захист інформації в інформаційно-комунікаційних системах». URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 06.06.2024)
6. Обстеження середовищ функціонування ІТС. URL: https://studfile.net/preview/5367203/page:2/ (дата звернення: 06.06.2024)
7. Інфомація про кібератаки. URL: https://www.epravda.com.ua/news/2024/01/31/709355/#:~:text=%D0%97%D0%B0%20%D0%B4%D0%B0%D0%BD%D0%B8%D0%BC%D0%B8%20%D1%83%D1%80%D1%8F%D0%B4%D0%BE%D0%B2%D0%BE%D1%97%20%D0%BA%D0%BE%D0%BC%D0%B0%D0%BD%D0%B4%D0%B8%20%D1%80%D0%B5%D0%B0%D0%B3%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F,%D0%BE%D0%B1%D0%BE%D1%80%D0%BE%D0%BD%D0%B8%2C%20127%20%E2%80%93%20%D0%BA%D0%BE%D0%BC%D0%B5%D1%80%D1%86%D1%96%D0%B9%D0%BD%D1%96%20%D0%BE%D1%80%D0%B3%D0%B0%D0%BD%D1%96%D0%B7%D0%B0%D1%86%D1%96%D1%97.

8. Порядок проведення робіт з КСЗІ. URL: https://tzi.com.ua/downloads/3.7-003-2005.pdf

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	1	
4	А4	Вступ	1	
5	А4	Стан питання. Постановка задачі	11	
6	А4	Спеціальна частина	37	
7	А4	Економічна частина	8	
8	А4	Висновки	1	
9	А4	Перелік посилань	1	
10	А4	ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи	1	
11	А4	ДОДАТОК Б. Перелік документів на оптичному носії	1	
12	А4	ДОДАТОК В. Відкуг керівника економічного розділу	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1. Кваліфікаійна робота – Волков Андрій 125-20-1.docx
2. Презентація – Волков Андрій 125-20-1.pptx

ДОДАТОК В. Відкуг керівника економічного розділу

Керівник розділу _____ к.е.н. доц. Пілова Д.П
(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК

на кваліфікаційну роботу бакалавра
студента групи 125-20-1
Волкова Андрія Віталійовича
на тему: розробка політики безпеки інформації інформаційно-комунікаційних систем

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 76 сторінках та містить 3 рисунка, 10 таблиць, 8 джерел та 4 додатка.

Об`єктом в кваліфікаційній роботі являється інформаційно-комунікаційна система ТОВ «ЛендінгСистем» - підприємство, яке займається послугами просування рекламних продуктів.

Предметом розробки кваліфікаційної роботи є політика безпеки інформації.

Мета кваліфікаційної роботи полягає у підвищення рівня безпеки інформації на підприємстві. Ця тема є актуальною та сучасною у нинішніх реаліях, оскільки зовнішній вплив на безпеку (злом, пограбування) підприємства дає справжню загрозу витоку інформації. Зовнішньої безпеки недостатньо. З'являються велика кількість фірм, які виробляють однакові послуги, відповідно росте і конкуренція.

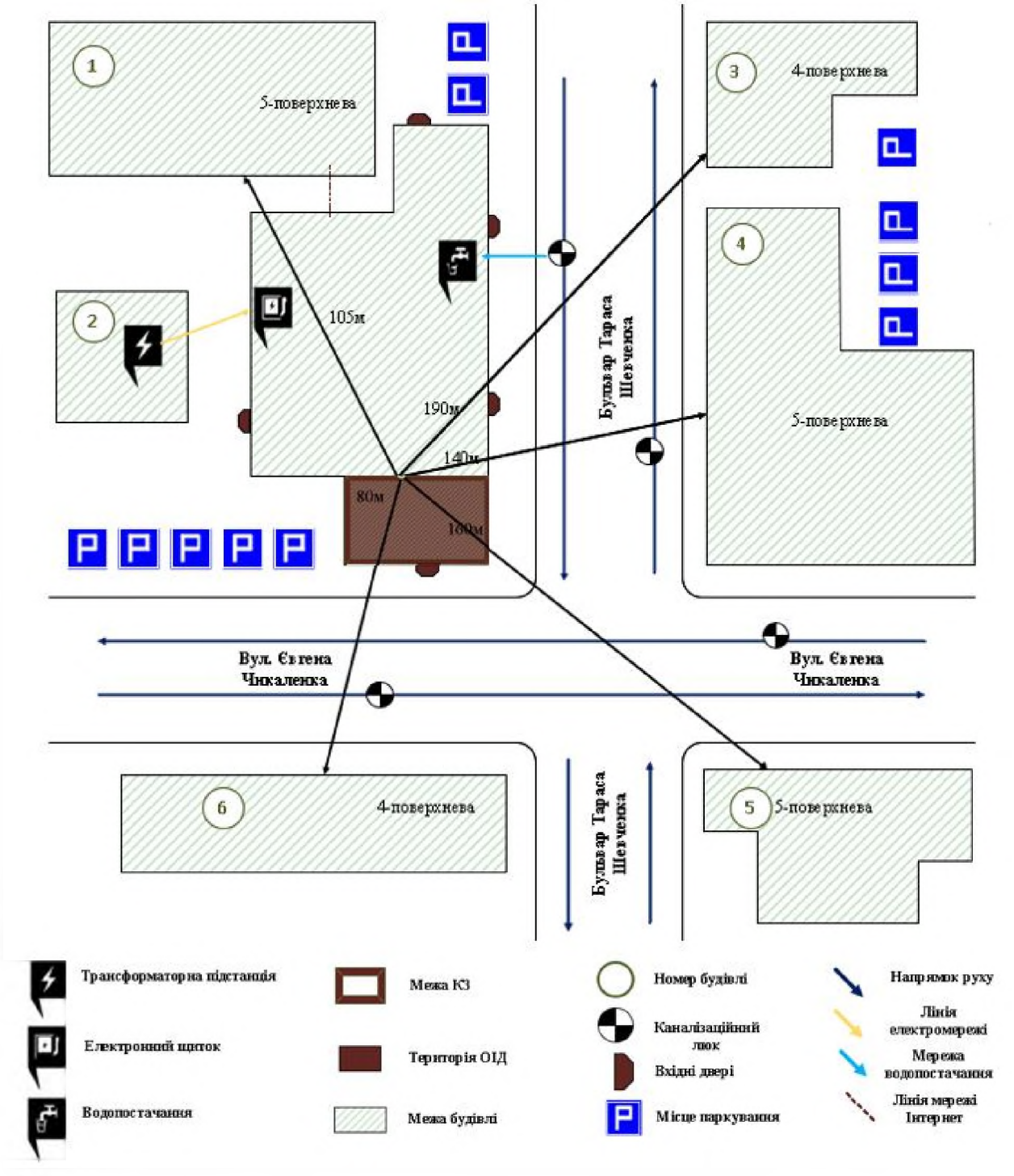
Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота оформлена та написана грамотною мовою, відповідає вимогам положення про систему запобігання та виявлення плагіату у Національному технічному університеті «Дніпровська політехніка». Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

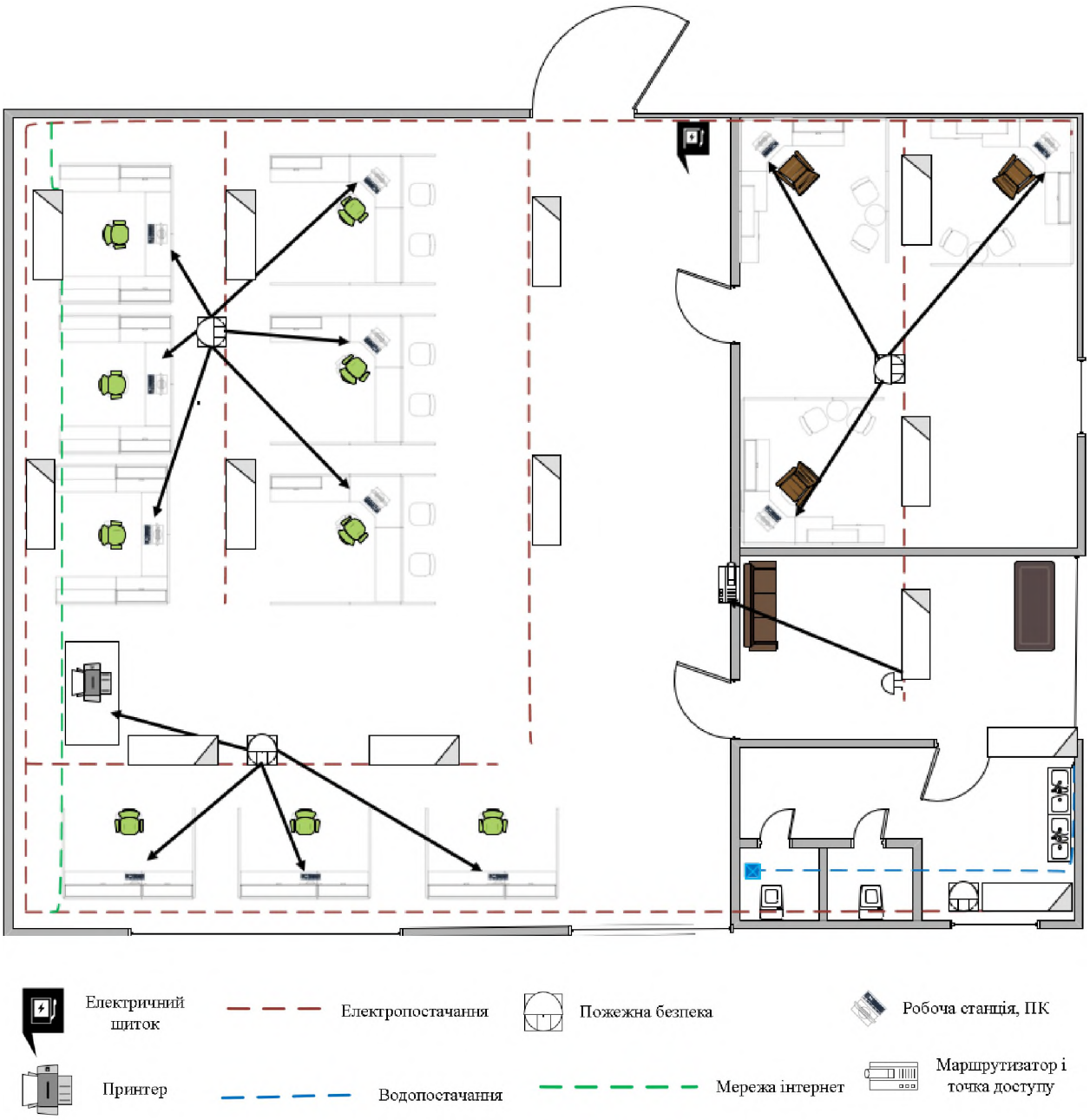
В цілому робота задовольняє усім вимогам і може бути допущена до захисту, а його автор заслуговує на оцінку «_____».

Керівник:

ДОДАТОК Д. Ситуаційний план ОІД



ДОДАТОК Г. Генеральний план ОІД


Електричний щиток
Електропостачання
Пожежна безпека
Робоча станція, ПК
Принтер
Водопостачання
Мережа інтернет
Маршрутизатор і точка доступу