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

студентки ***Каркан Анастасії Володимирівни***
академічної групи ***УБіт-15-1***
спеціальності ***6.170103 Управління інформаційною безпекою***
спеціалізації[1]
за освітньо-професійною програмою ***бакалавр***

на тему ***Розробка політики безпеки інформації інформаційно-телекомунікаційної системи приватного підприємства ТОВ «IntercarsUA Dnipro»***

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	к.т.н., доц. Герасіна О.В.			
розділів:				
спеціальний	ас. Чебаненко О.В.			
економічний	к.е.н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2019

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студентці ***Каркан Анастасії Володимирівні*** **академічної групи** ***УБіт-15-1***
(прізвище ім'я по-батькові) (шифр)

напряму підготовки ***6.170103 Управління інформаційною безпекою***
(код і назва спеціальності)

на тему ***Розробка політики безпеки інформації інформаційно-телекомунікаційної системи приватного підприємства ТОВ «IntercarsUA Dnipro»***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 21.05.2019 № 771-л.

Розділ	Зміст	Термін виконання
Розділ 1	*Стан питання. Постановка задачі*	20.03.2019
Розділ 2	*Обстеження інформаційно-телекомунікаційної системи. Аналіз загроз та вразливостей. Аналіз стану захищеності інформаційно-телекомунікаційної системи приватного підприємства ТОВ «IntercarsUA Dnipro». Розробка політики безпеки інформації.*	30.05.2019
Розділ 3	*Техніко-економічне обґрунтування доцільності запровадження запропонованих в роботі рішень.*	15.06.2019

Завдання видано: _____ Герасіна О.В.
(підпис керівника) (прізвище, ініціали)

Дата видачі: 08.01.2019р.

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання: _____ Каркан А.В.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: ___ ст., ___ рис., ___ табл., ___ додатків, ___ джерел.

Об'єкт розробки: політика безпеки інформації інформаційно-телекомунікаційної системи приватного підприємства ТОВ «IntercarsUA Dnipro».

Мета проекту: підвищення рівня захищеності інформації в ІТС приватного підприємства ТОВ «IntercarsUA Dnipro».

Перший розділ кваліфікаційної роботи описує стан питання, нормативно-правову базу, підстави та етапи створення КСЗІ та ПБ, види інформації та доступ до неї.

У другому розділі наведено основні відомості про підприємство. Виконано обстеження інформаційної системи, фізичного середовища, середовище користувачів. Описано технологію обробки інформації та функціональний профіль захисту. Виконано категоріювання інформації, що обробляється в ІТС та визначено основні загрози та вразливості, їх джерела та складено модель порушника. Розроблено положення політики безпеки.

В третьому розділі було розраховано витрати на впровадження політики безпеки інформації та щорічні експлуатаційні витрати на її підтримку. Також було доведено економічну доцільність введення в експлуатацію політики безпеки інформації, розробленої в другому розділі.

Практичне значення проекту полягає в підвищенні рівня інформаційної безпеки приватного підприємства ТОВ «IntercarsUA Dnipro».

ПОЛІТИКА БЕЗПЕКИ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ІНФОРМАЦІЙНА БЕЗПЕКА, ВРАЗЛИВОСТІ, ФУНКЦІОНАЛЬНИЙ ПРОФІЛЬ ЗАХИЩЕНОСТІ.

РЕФЕРАТ

Пояснительная записка: ___ с., ___ рис., ___ табл., ___ приложений, ___ источников.

Объект разработки: политика безопасности информации информационно-телекоммуникационной системы частного предприятия ООО «IntercarsUA Dnipro».

Цель проекта: повышение уровня защищенности информации в ИТС частного предприятия ООО «IntercarsUA Dnipro».

Первый раздел квалификационной работы описывает состояние вопроса, нормативно-правовую базу, основания и этапы создания КСЗИ и ПБ, виды информации и доступ к ней.

Во втором разделе приведены основные данные про предприятие. Выполнено обследование информационной системы, физической среды, среды пользователей. Описано технологию обработки информации и функциональный профиль защиты. Выполнено категорирование информации, которая обрабатывается в ИТС и определено основные угрозы и уязвимости, их источники и составлено модель нарушителя. Разработано положения политики безопасности.

В третьем разделе было рассчитано затраты на внедрение политики безопасности информации и ежегодные эксплуатационные затраты на её поддержку. Также было доказано экономическую целесообразность введения в эксплуатацию политики безопасности информации, разработанной во втором разделе.

Практическое значение проекта состоит в повышении уровня информационной безопасности частного предприятия ООО «IntercarsUA Dnipro».

ПОЛИТИКА БЕЗОПАСНОСТИ, МОДЕЛЬ УГРОЗ, МОДЕЛЬ НАРУШИТЕЛЯ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТИ, УЯЗВИМОСТИ, ФУНКЦИОНАЛЬНЫЙ ПРОФИЛЬ ЗАЩИЩЕННОСТИ.

ABSTRACT

Explanatory note: ___ p., ___ fig., ___ tables, ___ applications, ___ sources.

Object of elaboration: Information Security Policy for information and telecommunication system of the private enterprise «IntercarsUA Dnipro» LLC.

Project Objective: increasing the level of information security in the ITS of the private enterprise «IntercarsUA Dnipro» LLC.

The first section of the qualification project describes the state of the issue, the regulatory framework, the grounds and stages of creating the CRPP and the PB, the types of information and access to it.

The second section provides basic information about the company. A survey of the information system, the physical environment, the user environment. Information processing technology and functional protection profile are described. The information has been categorized, which is processed in the ITS and the main threats and vulnerabilities have been identified, their sources and the violator model have been compiled. Developed a security policy.

In the third section, the costs of implementing the information security policy and the annual operating costs of its support were calculated. The economic feasibility of introducing the information security policy developed in the second section was also proved.

The practical significance of the project is to increase the level of information security of the private enterprise «IntercarsUA Dnipro» LLC.

SECURITY POLICY, THREAT MODEL, INTRUDERS MODEL, INFORMATION SECURITY, VULNERABILITIES, FUNCTIONAL SECURITY PROFILE.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ДСТУ – державний стандарт України;

ЕОМ – електронно-обчислювальна машина;

ЖМД – жорсткий магнітний диск;

ЗУ – закон України;

ІБ – інформаційна безпека;

ІТС – інформаційно-телекомунікаційна система;

КЗЗ – комплекс засобів захисту;

КСЗІ – комплексна система захисту інформації;

ЛОМ – локальна обчислювальна мережа;

НД ТЗІ – нормативний документ в галузі технічний захист інформації.

НСД – несанкціонований доступ;

ОІД – об'єкт інформаційної діяльності;

ОС – операційна система;

ПБ – політика безпеки;

ПЕМВ – побічне електромагнітне випромінювання;

ПЕОМ – персональна електронно-обчислювальна машина;

ПЗ – програмне забезпечення;

ПЗП – постійний записуючий пристрій.

СКУД – система контролю та управління доступом;

СУБД – система управління базами даних;

ТОВ – товариство з обмеженою відповідальністю;

ЗМІСТ

ВСТУП

В сучасному світі інформація стрімко набуває своєї значимості. Із розвитком технологій процес інформатизації охоплює більшість сфер діяльності такі як економічна, соціальна, культурна, організаційна, освітня; сфери діяльності усіх ланок соціального управління та господарювання, тощо.

В Україні процес інформатизації здійснюється згідно до ЗУ «Про національну програму інформатизації». Національна програма інформатизації визначає стратегію розв'язання проблеми забезпечення інформаційних потреб та інформаційної підтримки соціально-економічної, екологічної, науково-технічної, оборонної, національно-культурної та іншої діяльності у сферах загальнодержавного значення.

Із стрімким розвитком рівня інформатизації, нині в кожній інформаційній системі (ІС) циркулює інформація, розголошення якої призведе до значних збитків власнику інформації або особі, якої стосується інформація. Тому, на сьогоднішній день, питання створення заходів захисту інформації підприємств та держави є актуальним.

Для забезпечення безпеки інформації під час її обробки в автоматизованій системі (АС) створюється комплексна система захисту інформації (КСЗІ), що запобігає витоку тих чи інших видів інформації, а також політика безпеки, що регламентує порядок захисту інформації.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

Із набуттям інформацією високої важливості для функціонування підприємства, значимим стає питання захисту інформації в ІТС, адже нині в кожній інформаційній системі (ІС) циркулює інформація, розголошення якої призведе до значних збитків власнику інформації або особі, якої стосується інформація.

Для захисту різних видів інформації розробляється комплексна система захисту інформації та політика безпеки інформації.

Метою кваліфікаційної роботи є виявлення вразливостей в інформаційній системі ОІД. А також складення додаткових політик безпеки до існуючих ПБ підприємства, техніко-економічне обґрунтування доцільності впровадження розроблених політик безпеки.

1.2 Аналіз нормативно-правової бази у сфері інформаційної безпеки

Із стрімкими розвитком інформаційних технологій, на державному рівні створюються закони, нормативні документи, державні стандарти, тощо задля регулювання інформаційних відносин. В Україні існує достатньо велика кількість нормативно-правових документів, що стосуються інформації, її безпеки, та регулювання інформаційних відносин. Окрім створення власних нормативних документів, широкою є практика застосування міжнародних стандартів.

1.3 Види інформації. Порядок доступу до інформації

Задля побудови КСЗІ та створення ПБ перш за все необхідно чітко усвідомлювати що таке інформація та які її види існують.

Згідно з [1] інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

За порядком доступу інформація поділяється на відкриту та інформацію з обмеженим доступом. Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом.

Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація [1].

Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом [1].

Порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються володільцем інформації. Порядок доступу до державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, перелік користувачів та їх повноваження стосовно цієї інформації визначаються законодавством. У випадках, передбачених законом, доступ до інформації в системі може здійснюватися без дозволу її володільця в порядку, встановленому законом [3].

1.4 Об’єкт інформаційної діяльності

Згідно з [2] об’єкт інформаційної діяльності – інженерно-технічна споруда (приміщення), транспортний засіб, де здійснюється озвучення та/або обробка технічними засобами інформації з обмеженим доступом.

Об’єкти, на яких здійснюватиметься обробка технічними засобами та/або озвучуватиметься інформація з обмеженим доступом, що не становить державної таємниці, підлягають обов’язковому категоріюванню.

Категоріювання може бути первинним, черговим або позачерговим.

Категоріювання здійснюється для визначення необхідного (зі встановлених нормативно-правовими актами та нормативними документами системи

технічного захисту інформації рівнів) рівня захисту інформації, що обробляється технічними засобами та/або озвучується на об’єкті.

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

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

Категоріювання здійснюється за ознакою: ступінь обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на ОІД.

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

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

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

1.5 Підстави створення КСЗІ

Згідно з [5] комплексна система захисту інформації (КСЗІ) – сукупність організаційних заходів і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС.

Відповідно до [6] підставою для визначення необхідності створення КСЗІ є норми та вимоги чинного законодавства, які встановлюють обов’язковість обмеження доступу до певних видів інформації або забезпечення її цілісності чи доступності, або прийняте власником інформації рі-

шення щодо цього, якщо нормативно-правові акти надають йому право діяти на власний розсуд.

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

– аналізу нормативно-правових актів (державних, відомчих та таких, що діють в межах установи, організації, підприємства), на підставі яких може встановлюватися обмеження доступу до певних видів інформації чи заборона такого обмеження, або визначатися необхідність забезпечення захисту інформації згідно з іншими критеріями;

– визначення наявності у складі інформації, яка підлягає автоматизованій обробці, таких її видів, що потребують обмеження доступу до неї або забезпечення цілісності чи доступності відповідно до вимог нормативно-правових актів;

– оцінки можливих переваг (фінансово-економічних, соціальних і т.п.) експлуатації ІТС у разі створення КСЗІ.

На підставі проведеного аналізу приймається рішення про необхідність створення КСЗІ.

1.6 Процеси створення КСЗІ

1.6.1 Процес обстеження ОІД

Відповідно до [6] метою обстеження є підготовка засадничих да-них для формування вимог до КСЗІ у вигляді опису кожного середовища функціонування ІТС та виявлення в ньому елементів, які безпосередньо чи опосередковано можуть впливати на безпеку інформації, виявлення взаємного впливу елементів різних середовищ, документування результатів обстеження для використання на наступних етапах робіт.

Під час виконання цих робіт ІТС розглядається як організаційно-технічна система, яка поєднує обчислювальну систему, фізичне середовище, середовище користувачів, оброблювану інформацію і технологію її обробки (далі – середовища функціонування ІТС).

При обстеженні обчислювальної системи ІТС повинні бути проаналізовані й описані:

– загальна структурна схема і склад (перелік і склад обладнання, технічних і програмних засобів, їхні зв'язки, особливості конфігурації, архітектури й топології, програмні і програмно-апаратні засоби захисту інформації, взаємне розміщення засобів тощо);

– види і характеристики каналів зв'язку;

– особливості взаємодії окремих компонентів, їх взаємний вплив один на одного;

– можливі обмеження щодо використання засобів та ін.

Мають бути виявлені компоненти обчислювальної системи, які містять і які не містять засобів і механізмів захисту інформації, потенційні можливості цих засобів і механізмів, їхні властивості і характеристики, в тому числі ті, що встановлюються за умовчанням та ін.

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

При обстеженні інформаційного середовища аналізу підлягає вся інформація, що обробляється, а також зберігається в ІТС (дані і програмне забезпечення). Під час аналізу інформація повинна бути класифікована за режимом доступу, за правовим режимом, визначені й описані види (в термінах об’єктів КС) її представлення в ІТС.

Для кожного виду інформації і типу об’єкта, в якому вона міститься, ставляться у відповідність властивості захищеності інформації (конфіденційність, цілісність, доступність) чи КС (спостережність), яким вони повинні задовольняти.

Аналіз технології обробки інформації повинен виявити особливості обігу електронних документів, мають бути визначені й описані інформаційні потоки і середовища, через які вони передаються, джерела утворення потоків

та місця їх призначення, принципи та методи керування інформаційними потоками, складені структурні схеми потоків. Фіксуються види носіїв інформації та порядок їх використання під час функціонування ІТС.

Для кожного структурного елемента схеми інформаційних потоків фіксуються склад інформаційних об’єктів, режим доступу до них, можливий вплив на нього (елементу) елементів середовища користувачів, фізичного середовища з точки зору збереження властивостей інформації.

При обстеженні фізичного середовища здійснюється аналіз взаємного розміщення засобів обробки інформації ІТС на об’єктах інформаційної діяльності, комунікацій, систем життєзабезпечення і зв’язку, а також режим функціонування цих об’єктів.

Аналізу підлягають такі характеристики фізичного середовища:

– територіальне розміщення компонентів ІТС (генеральний план, ситуаційний план);

– наявність охорони території та перепускний режим;

– наявність категорійованих приміщень, в яких мають розміщуватися компоненти ІТС;

– режим доступу до компонентів фізичного середовища ІТС;

– вплив чинників навколишнього середовища, захищеність від засобів технічної розвідки;

– наявність елементів комунікацій, систем життєзабезпечення і зв’язку, що мають вихід за межі контрольованої зони;

– наявність та технічні характеристики систем заземлення;

– умови зберігання магнітних, оптико-магнітних, паперових та інших носіїв інформації;

– наявність проектної та експлуатаційної документації на компоненти фізичного середовища.

При обстеженні середовища користувачів здійснюється аналіз:

– функціонального та кількісного складу користувачів, їхніх функціональних обов’язків та рівня кваліфікації;

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

– повноважень користувачів щодо управління КСЗІ;

– рівня можливостей різних категорій користувачів, що надаються (можуть бути доступними) їм засобами ІТС.

– наявності СЗІ в ІТС.

1.6.2 Процес аналізу загроз та побудови моделі порушника

За результатами обстеження розробляється модель загроз та вразливостей, модель порушника.

Відповідно до [5] загроза – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків АС.

Згідно з [10] загрози для інформації, що обробляється в АС, залежать від характеристик ОС, фізичного середовища, персоналу, технологій обробки та інших чинників і можуть мати об'єктивну або суб'єктивну природу. Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні. Мають бути визначені основні види загроз для безпеки інформації, які можуть бути реалізовані стосовно АС і повинні враховуватись у моделі загроз, наприклад:

– зміна умов фізичного середовища (стихійні лиха і аварії, як землетрус, повінь, пожежа або інші випадкові події);

– збої і відмови у роботі обладнання та технічних засобів АС;

– наслідки помилок під час проектування та розробки компонентів АС (технічних засобів, технології обробки інформації, програмних засобів, засобів захисту, структур даних тощо);

– помилки персоналу (користувачів) АС під час експлуатації;

– навмисні дії (спроби) потенційних порушників.

Випадковими загрозами суб'єктивної природи (дії, які здійснюються персоналом або користувачами по неуважності, недбалості, незнанню тощо, але без навмисного наміру) можуть бути:

– дії, що призводять до відмови АС (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв'язку, видалення даних, програм та ін.);

– ненавмисне пошкодження носіїв інформації;

– неправомірна зміна режимів роботи АС (окремих компонентів, обладнання, ПЗ тощо), ініціювання тестуючих або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації);

– неумисне зараження ПЗ комп'ютерними вірусами;

– невиконання вимог до організаційних заходів захисту чинних в АС розпорядчих документів;

– помилки під час введення даних в систему, виведення даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо;

– будь-які дії, що можуть призвести до розголошення конфіденційних відомостей, атрибутів розмежування доступу, втрати атрибутів тощо;

– неправомірне впровадження і використання забороненого політикою безпеки ПЗ (наприклад, навчальні та ігрові програми, системне і прикладне забезпечення та ін.);

– наслідки некомпетентного застосування засобів захисту;

– інші.

Навмисними загрозами суб'єктивної природи, спрямованими на дезорганізацію роботи АС (окремих компонентів) або виведення її з ладу, проникнення в систему і одержання можливості несанкціонованого доступу до її ресурсів, можуть бути:

– порушення фізичної цілісності АС (окремих компонентів, пристроїв, обладнання, носіїв інформації);

– порушення режимів функціонування (виведення з ладу) систем життєзабезпечення АС (електроживлення, заземлення, охоронної сигналізації, вентиляції та ін.);

– порушення режимів функціонування АС (обладнання і ПЗ);

– впровадження і використання комп'ютерних вірусів, закладних (апаратних і програмних) і підслуховуючих пристроїв, інших засобів розвідки;

– використання засобів перехоплення побічних електромагнітних випромінювань і наводів, акусто-електричних перетворень інформаційних сигналів;

– використання (шантаж, підкуп тощо) з корисливою метою персоналу АС;

– крадіжки носіїв інформації, виробничих відходів (роздруків, записів, тощо);

– несанкціоноване копіювання носіїв інформації;

– читання залишкової інформації з оперативної пам'яті ЕОМ, зовнішніх накопичувачів;

– одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача ("маскарад");

– неправомірне підключення до каналів зв'язку, перехоплення даних, що передаються, аналіз трафіку тощо;

– впровадження і використання забороненого політикою безпеки ПЗ або несанкціоноване використання ПЗ, за допомогою якого можна одержати доступ до критичної інформації (наприклад, аналізаторів безпеки мереж);

– інші.

Основою для проведення аналізу ризиків і формування вимог до КСЗІ є розробка моделі загроз для інформації та моделі порушника.

Для створення моделі загроз необхідно скласти перелік суттєвих загроз, описати методи і способи їхнього здійснення.

Модель порушника – абстрактний формалізований або неформалізований опис порушника. Модель порушника відображає його практичні та потенційні можливості, апріорні знання, час та місце дії тощо.

1.7 Процес створення політики безпеки інформації

Інформація, процеси, що її підтримують, інформаційні системи та мережева інфраструктура, які є істотними активами сучасних фірм, підприємств та організацій, все частіше зштовхуються із різними загрозами безпеки, такими як комп’ютерне шахрайство, шпіонаж, шкідництво, вандалізм. Тому актуальною є задача інформаційного захисту підприємств. Наявність політики інформаційної безпеки свідчить про зрілість та компетентність підприємства у питаннях забезпечення інформаційної безпеки.

Згідно з [10] під політикою безпеки інформації (далі - політика безпеки) слід розуміти набір вимог, правил, обмежень, рекомендацій і т. ін., які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз. Термін "політика безпеки" може бути застосовано щодо АС, окремого її компонента, послуги захисту, що реалізується системою і т. ін. Політика безпеки інформації в АС є частиною загальної політики безпеки організації і повинна успадковувати основні її принципи.

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

Політика інформаційної безпеки виступає як документ або багаторівнева система документів, які визначають вимоги безпеки, систему заходів або порядок дій, відповідальність співробітників та механізми контролю задля забезпечення інформаційної безпеки підприємства.

1.8 Постановка задачі

Беручи до уваги вищезазначені пункти, задля доцільної розробки політики безпеки підприємства виконати обстеження об’єкта інформаційної діяльності, проаналізувати загрози та вразливості, виявити їх джерела.

Розробити положення політики безпеки.

Техніко-економічно обґрунтувати доцільність впровадження розроблених політик безпеки.

1.9 Висновки

Перший розділ кваліфікаційної роботи описує:

– стан питання;
– аналіз нормативно-правової бази;
– види інформації, порядок доступу до неї, а також описує ОІД;
– підстави для створення КСЗІ та процеси її створення;
– процес створення політики безпеки;
– постановку задачі.

Таким чином визначено необхідність здійснення обстеження об'єкту та виявлення основних загроз та вразливостей, реалізація яких призведе до порушення властивостей інформації, що циркулює в ІТС підприємства.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальні відомості про підприємство

Об’єктом інформаційної діяльності (далі ОІД) є офіс приватного підприємства – ТОВ «IntercarsUA Dnipro».

Адреса: 14000, м. Дніпро, вул. Княгині Ольги 22.

Специфікація діяльності ОІД:

Реалізація автозапчастин, інструментів та ремонтного обладнання.

Працює 6 днів на тиждень. З понеділка по п’ятницю з 9:00 до 18:00 без перерви, у суботу – з 9:00 до 14:00 без перерви. Неділя – вихідний.

Штат працівників: директор(1 особа), бухгалтер(1 особа), системний адміністратор(1 особа), sales директор(1 особа), менеджери по роботі з клієнтами(15 осіб), кадровий робітник(1 особа), HR менеджер(2 особи), касир (1 особа), логіст(1 особа), комірник(3 особи), водій(5 осіб).

2.2 Обстеження ОІД

2.2.1 Обстеження фізичного середовища

Об’єктом інформаційної діяльності є офіс приватного підприємства – ТОВ «IntercarsUA Dnipro».

Офіс знаходиться за адресою вул. Княгині Ольги 22.

ОІД знаходиться в одноповерховій будівлі. Має 3 вікна, що виходять на дорогу біля будівлі.

Стіни будівлі, в якій знаходиться ОІД зроблені з газо-бетонних блоків (20х30х60 см). Фундамент — стовпчастий, дах — покритий руберойдом з грубозернистим посипанням з лицьового боку і полімерною плівкою з направленого боку полотна, територія навколо будівлі частково покрита плиткою та асфальтом.

Зовнішні стіни офісу — газо-бетонні. Товщина зовнішніх стін — 480 мм (2 шари газо-бетонних блоків із цементом та штукатуркою).

Внутрішні несучі стіни також газо-бетонні, товщина — 250 мм (1 шар газо-бетонного блоку із цементом та штукатуркою). Внутрішні перегородки зведені за допомогою металоконструкцій та гіпсокартону, загальною товщиною — 65 мм.

Вікна – металопластикові, подвійні, 2100 х 1500 мм.

Вхідні двері – металопластикові двустулкові з подвійним армованим склом – 2000 мм шириною і висотою 2500 мм.

Замок - врізний зі сталі, закривається вбудованим циліндром під ключ з перфорацією.

Міжкімнатні двері виготовлені з МДФ плити, розмірами 40х2000х800 мм.

Офіс має висоту 3 м (від підлоги до стелі), стеля – підвісна, з конструкцією кріплення Армстронг. Підлога на підприємстві – лінолеум і плитка (у туалеті).

Ліворуч від будівлі ОІД знаходиться будівля авто мийки, праворуч — станція технічного обслуговування автомобілів, навпроти — автосалон.

Контрольована зона обмежена стінами будівлі. Контроль доступу здійснюється через систему контроля та управління доступом (СКУД). Згідно з класифікацією за рівнями автоматизації СКУД підприємства автоматична, тобто вся процедура перевірки та прийняття рішення здійснюється комп’ютером.

Система електропостачання підключена до трансформаторної підстанції №5, яка має сторонніх споживачів і знаходиться за межами КЗ.

Система опалення підключена до міської системи опалення та знаходиться за межами КЗ.

Системи каналізації та водопостачання підключені до міської системи, знаходяться за межами КЗ.

Усі пристрої заземлені на загальний контур заземлення, що замкнут та виходить за межі КЗ.

Система вентиляції використовується приточно-витяжна.

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

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

Генеральний план та план комунікацій наведено у ДОДАТКУ __ та ситуаційний план наведено у ДОДАТКУ__.

2.2.2 Обстеження обчислювальної системи ОІД

ІТС ОІД являє собою мережу типу «зірка», з виділеним сервером, побудовану з використанням одного комутатору.

ІТС являє собою багатомашинний багатокористувацький комплекс, який обробляє інформацію різних категорій конфіденційності, а також має ADSL доступ до мережі Інтернет, який забезпечує ВАТ «Телемост». Відноситься до третього класу.

Обчислювальна система у складі:

1 двадцять п'ять ПЕОМ Microsoft Windows 10 Professional (білд 9600);

2 сервер управління доступом до мережі Інтернет з централізованим оновленням антивірусних баз і управлінням системними оновленнями;

3 активне мережеве обладнання (1 комутатор першого рівня на 24 порти і 1 комутатор на 8 портів);

4 програмні засоби активного мережевого обладнання, що реалізують спеціальні алгоритми управління мережею;

5 прикладне ПЗ (Microsoft Office, Total Commander, WinRAR, Adobe Reader, Avast Endpoint Protection Suite Plus, Norton Personal Firewall 2004);

6 периферійні пристрої вводу\виводу даних Canon 1100 (3 шт.);

Структурна схема мережі наведена на рисунку 1.1.

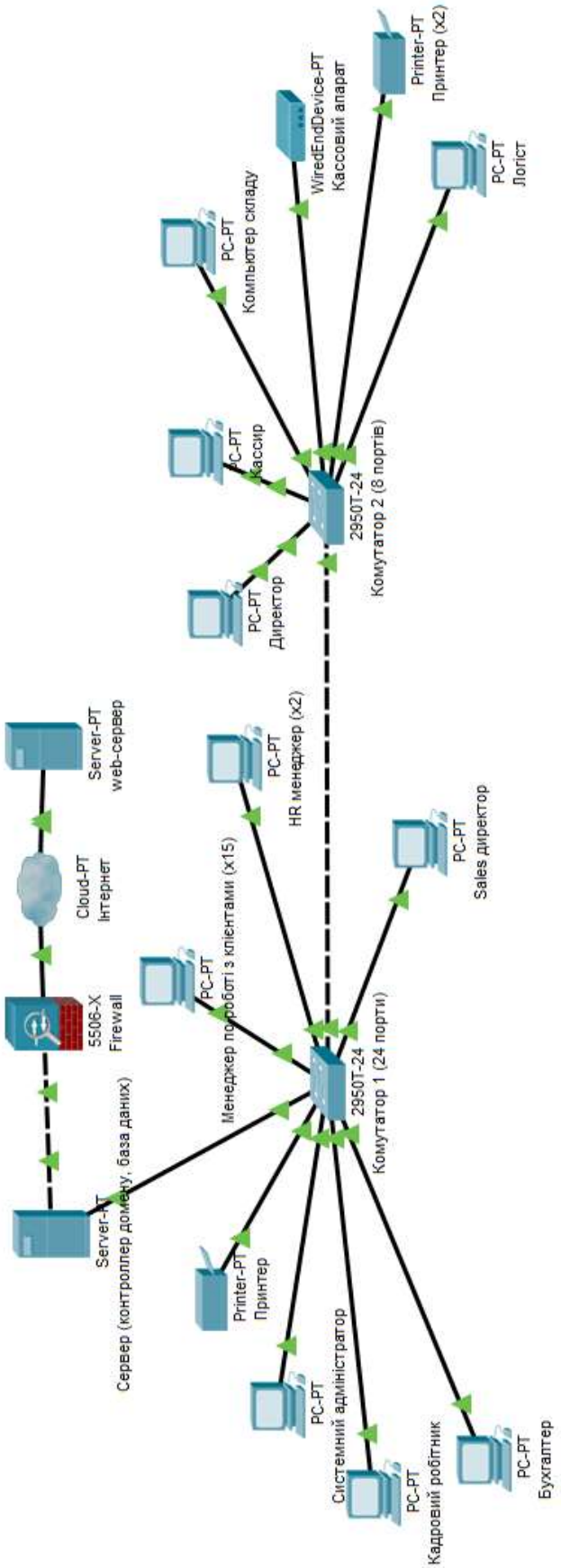


Рисунок 1.1 – Структурна схема мережі підприємства

2.2.3 Інформаційне середовище

Інформація підприємства зберігається на електронних та паперових носіях.

Детально данні наведено в таблиці 2.1.

Таблиця 2.1 – Інформація, що циркулює на підприємстві

№	Інформація	Режим доступу	Правовий режим	Працівники, що мають доступ	Місце зберігання
1	Організаційно-розпорядча	З обмеженим доступом	Конфідеційна інформація	Директор підприємства, sales директор, сис.админ	ПК директора
2	Облік внутрішніх документів	З обмеженим доступом	Конфідеційна інформація	Директор підприємства, сис.админ кадровий працівник	Сервер
3	Інформація про послуги, тарифи, контакти підприємства	Відсутній	Відкрита	Всі	Сайт компанії
4	Інформація про працівників (БД працівників)	З обмеженим доступом	Конфідеційна інформація	Директор підприємства, сис.админ кадровий працівник, HR-manager, бухгалтер, sales директор	Сервер
5	Каталоги товарів	Відсутній	Відкрита	Всі	Сайт компанії, сервер
6	Інформація про клієнтів	З обмеженим доступом	Конфідеційна інформація	Директор, сис.админ, бухгалтер, sales директор, менеджер	Сервер
7	База даних замовлень	З обмеженим доступом	Конфідеційна інформація	Директор, сис.админ, бухгалтер, sales директор, менеджер, логіст, касир, комірник	Сервер

Продовження таблиці 2.1

№	Інформація	Режим доступу	Правовий режим	Працівники, що мають доступ	Місце зберігання
8	Фінансова звітність	З обмеженим доступом	Комерційна таємниця	Директор, сис.админ, бухгалтер	На паперових носіях, сервер, ПК директора і/або бухгалтера
9	База даних постачальників товару	З обмеженим доступом	Комерційна таємниця	Директор, сис.админ, бухгалтер, sales директор	Сервер
10	Данні про обладнання підприємства, охоронна система	З обмеженим доступом	Комерційна таємниця	Директор, сис.админ, sales директор	На паперових носіях, сервер і/або ПК сис.адміна

Визначення рівня конфіденційності, цілісності та доступності інформації описане у таблиці 2.2.

Таблиця 2.2 – Визначення рівня конфіденційності, цілісності та доступності інформації

№	Інформація	Рівень конфіденційності	Рівень цілісності	Рівень доступності
1	Організаційно розпорядча	К1	Ц2	Д1
2	Облік внутрішніх документів	К2	Ц2	Д2
3	Інформація про послуги та товари	К1	Ц3	Д4
4	БД працівників	К2	Ц3	Д2
5	Каталог товарів	К1	Ц4	Д4
6	БД клієнтів	К2	Ц4	Д3
7	БД замовлень	К3	Ц5	Д4
8	БД постачальників	К3	Ц4	Д2
9	Фінансова звітність	К4	Ц5	Д3
10	Данні про обладнання підприємства, охоронна система	К4	Ц3	Д2

Для класифікації інформації були використані рівні властивостей, що описані далі.

Рівні конфіденційності:

– К1 – рівень конфіденційності інформації, при якому можна знехтувати збитками у разі розкриття інформації особам, що не мають допуску до неї, або при якому інформація не є конфіденційною;

– К2 – рівень конфіденційності інформації, при якому компанія зазнає незначних збитків у разі розкриття інформації особам, що не мають допуску до неї;

– К3 – рівень конфіденційності інформації, при якому організація зазнає відчутних збитків у разі розкриття інформації особам, що не мають допуску до неї;

– К4 – рівень конфіденційності інформації, що може призвести до значних матеріальних втрат у разі розкриття інформації особам, що не мають допуску до неї;

– К5 – критичний рівень конфіденційності інформації, що може призвести до краху компанії у разі втрати конфіденційності інформації.

Рівні цілісності:

– Ц1– рівень цілісності інформації, при якому можна знехтувати втратою цілісності інформації;

– Ц2 – рівень цілісності інформації, при якому компанія зазнає незначних збитків у разі втрати цілісності інформації;

– Ц3 – рівень цілісності інформації, при якому організація зазнає відчутних збитків у разі втрати цілісності інформації;

– Ц4 – рівень цілісності інформації, що може призвести до значних матеріальних втрат у разі втрати цілісності інформації;

– Ц5 – критичний рівень цілісності інформації, що може призвести до краху компанії у разі втрати цілісності інформації.

Рівні доступності:

– Д1– рівень доступності інформації, при якому можна знехтувати втратою доступності інформації;

– Д2 – рівень доступності інформації, при якому компанія зазнає незначних збитків у разі втрати доступності інформації;

– Д3 – рівень доступності інформації, при якому організація зазнає відчутних збитків у разі втрати доступності інформації;

– Д4 – рівень доступності інформації, що може призвести до значних матеріальних втрат у разі втрати доступності інформації;

– Д5 – критичний рівень доступності інформації, що може призвести до краху компанії у разі втрати доступності інформації.

2.2.4 Технологія обробки інформації

Організаційно-розпорядча інформація зберігається на ПК директора. Створюється директором. Серед працівників поширюється за необхідністю через електронну пошту та тим працівникам, яких стосується.

Облік внутрішніх документів зберігається на сервері підприємства. Реєструються паперові носії інформації такі як угоди, накладні від постачальників, тощо. Реєстрацією документів займається кадровий робітник.

Інформація про послуги, тарифи, контакти підприємства знаходиться на сайті підприємства у відкритому доступі. Редагується системним адміністратором за наказом директора підприємства, або sales директора, за попередньою згодою директора підприємства.

Інформація про працівників (БД працівників). До неї (бази) додаються і/або редагуються матеріали HR-менеджером, кадровим робітником або директором. Містить в собі данні про кожного працівника компанії, їх особисті данні такі як ПІБ, паспортні данні, ІНН тощо.

Каталоги товарів розміщені на сайті компанії та сервері. Редагуються системним адміністратором за наказом директора підприємства, або sales директора, за попередньою згодою директора підприємства.

Інформація про клієнтів зберігається в спеціальній базі даних на сервері компанії, містить в собі особисті дані клієнтів такі як ПІБ, паспортні дані, ІНН, адреса, історія замовлень тощо. В основному редагується менеджерами, які оформлюють замовлення. Якщо клієнт вже робив замовлення, то його данні вже є в базі. Менеджер лише додає до історії замовлень нову інформа-

цію. Якщо клієнт раніше не робив замовлень, то менеджер реєструє клієнта в базі. Кожному клієнту присвоєно особистий ID номер, під яким його данні зберігаються в базі, а також здійснюється процес видачі товару на складі компанії, або оформлення доставки, якою займається логіст.

База даних замовлень. Клієнт оформлює замовлення на сайті компанії, данні про замовлення автоматично потрапляють у базу даних замовлень. За персональним ID клієнта, менеджер заносить в базу невистачаючі данні, перевіряє наявність товарів та вірність персональних даних клієнта. Якщо замовлення клієнт забирає особисто, касир формує чек, а комірник збирає товари і видає їх клієнту після оплати. Якщо клієнт замовив доставку, то логіст включає замовлення до маршрутного листа водія, засновуючись на даних клієнта з бази замовлень.

Фінансова звітність. Формується бухгалтером і/або директором, згідно до даних з баз даних замовлень. Друкується за необхідністю. Паперові носії зберігаються на робочих місцях бухгалтера та директора.

База даних постачальників. Містить персональні данні про постачальників та товари, що вони надають підприємству. Замовлення постачальникам формує директор підприємства і/або sales директором. Інформація вилучається, якщо вона застаріла або неактуальна. Нова інформація додається із появою нових постачальників.

Данні про обладнання підприємства, охоронна система. Використовуються в більшості випадків системним адмістратором для контролю цілісності та наявності обладнання на підприємстві, а також як інвентаризаційна відомість.

2.2.5 Середовище користувачів

В офісі, впродовж робочого дня, знаходяться наступні особи:

– Директор;
– Бухгалтер;
– Системний адміністратор;

– Sales директор;
– Менеджери по роботі з клієнтами;
– Кадровий робітник;
– HR менеджер
– Касир;
– Логіст;
– Комірник;
– Водій;
– Клієнти компанії.

Для подальшого аналізу доцільності прав доступу до інформації усіх працівників підприємства, визначимо основні посадові обов'язки кожного працівника. Зібрані данні представлені у таблиці 2.3.

Таблиця 2.3 – Основні посадові обов'язки працівників

№	Посада	Кількість	Посадові обов'язки
1	Директор	1	Контроль всіх робочих процесів, облік угод між підрядними компаніями та клієнтами, всі юридичні процеси пов'язані з діяльністю компанії.
2	Бухгалтер	1	Фінансовий облік та аудит компанії, розрахунок та видача заробітної плати працівникам
3	Системний адміністратор	1	Контроль роботи інформаційної системи, усунення технічних несправностей, моніторинг роботи віртуальних серверів, технічна підтримка всіх елементів системи, обробка заяв про несправності, забезпечення розмежування доступів до інформації згідно до політики безпеки компанії та установчих документів підприємства
4	Sales директор	1	Контроль роботи менеджерів по роботі з клієнтами, супровід замовлень.
5	Менеджери по роботі з клієнтами	15	Консультування та супровід існуючих клієнтів компанії, підбір товарів серед асортименту товарів підприємства, оформлення замовлень, обробка електронних замовлень.
6	Кадровий робітник	1	Облік внутрішніх документів, реєстрація нових працівників
7	HR менеджер	2	Підбір нових працівників
8	Касир	1	Прийом оплати за товари та послуги.

Продовження таблиці 2.3

№	Посада	Кількість	Посадові обов’язки
9	Логіст	1	Створення маршрутів та маршрутних листів для водіїв компанії.
10	Комірник	3	Збір та видача замовлень клієнтам або водіям підприємства.
11	Водій	5	Доставка товарів замовникам.

Матриця керування доступом працівників підприємства до інформації описана у таблиці 2.4.

Таблиця 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
Sales директор	ЧЗ	-	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ	-	ЧРЗВ	ЧРЗВ
Бухгалтер	-	-	ЧЗ	ЧРЗ	ЧЗ	ЧЗ	ЧЗ	ЧРЗВ	ЧРЗВ	-
Сис.адмін	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ	ЧРЗВ
HR менеджер	-	-	ЧЗ	ЧРЗ	ЧЗ	-	-	-	-	-
Менеджер по роботі з клієн-тами	-	-	ЧЗ	-	ЧЗ	ЧРЗВ	ЧРЗВ	-	-	-
Кадровий робітник	-	ЧРЗВ	ЧЗ	ЧРЗВ	ЧЗ	-	-	-	-	-
Касир	-	-	ЧЗ	-	ЧЗ	ЧРЗВ	ЧРЗВ	-	-	-
Логіст	-	-	ЧЗ	-	ЧЗ	ЧЗ	ЧРЗ	-	-	-
Комірник	-	-	ЧЗ	-	ЧЗ	ЧЗ	ЧЗР	-	ЧРЗВ	-
Водій	-	-	ЧЗ	-	ЧЗ	-	-	-	-	-

де Ч – читання, Р – редагування, З – зберігання, В – видалення. Цифрами від 1 до 10 позначено інформацію згідно до таблиці 1.1.

2.3 Аналіз загроз та вразливостей

2.3.1 Модель загроз та вразливостей

Найбільш критичними для даної ІТС визначені антропогенні загрози, джерелами яких є конкуренти та персонал.

Складемо детальний перелік загроз та вразливостей беручи до уваги джерела загроз (антропогенні). Перелік наведено у вигляді 2.5.

Таблиця 2.5 – Антропогенні загрози та вразливості

Джерело	Загроза	Вразливість
Конкуренти	Крадіжка інформації (читання та несанкціоноване копіювання)	– Можливість підключення до корпоративної мережі з будь-якого пристрою – Відсутність коректної політики створення паролів для автентифікації
	Модифікація інформації	
	Знищення інформації	
	Несанкціонований доступ до корпоративної мережі	– Можливість підключення до корпоративної мережі з будь-якого пристрою.
	Статистичний аналіз мережевого трафіку	
	Перехват інформації	
Персонал (*окрім* системного адміністратора)	Несанкціонована модифікація інформації	– Можливість підключення до корпоративної мережі з будь-якого пристрою. – Можливість підключати будь-які сторонні електронні носії. – Відсутня коректна політика створення паролів для автентифікації.
	Несанкціоноване знищення інформації	
	Несанкціонований друк та копіювання інформації	
	Несанкціонована модифікація та/або знищення та/або встановлення ПЗ	
	Помилки при експлуатації ПЗ, технічних засобів	– Недостатній рівень підготовки персоналу з питань безпеки – Некомпетентність працівників – Інформаційна безграмотність – Відсутні організаційні методи захисту від розголошення інформації.
	Ненавмисне розголошення конфіденційної інформації або інформації, що становить комерційну таємницю	
	Навмисне розголошення конфіденційної інформації або інформації, що становить комерційну таємницю	

Продовження таблиці 2.5

Джерело	Загроза	Вразливість
Персонал (системний адміністратор)	Несанкціонована модифікація інформації	– Незахищене зберігання – Відсутність коректного розмежування доступу та «квот» – Можливість підключення до корпоративної мережі з будь якого пристрою
	Несанкціоноване знищення інформації	
	Несанкціонований друк та копіювання інформації	
	Помилки при експлуатації ПЗ, технічних засобів	– Недостатній рівень підготовки персоналу з питань безпеки – Некомпетентність працівників – Відсутні організаційні методи захисту від розголошення інформації.
	Ненавмисне розголошення конфіденційної інформації або інформації, що становить комерційну таємницю	
	Навмисне розголошення конфіденційної інформації або інформації, що становить комерційну таємницю	
	Модифікація журналу подій	– Незахищене зберігання – Некомпетентність працівників – Відсутня коректна політика створення паролів для автентифікації – Відсутні організаційні методи захисту від розголошення інформації.
	Навмисне або ненавмисне вимкнення антивірусного захисту	
	Розголошення даних автентифікації користувачів системи	
	Навмисне або ненавмисне знищення ПЗ або технічних засобів	– Незахищене зберігання – Відсутність коректного розмежування доступу та «квот» – Відсутні організаційні методи захисту від розголошення інформації.

Розрахуємо коефіцієнт небезпеки для кожної вразливості за формулою (К1*К2*К3)/125=К_небезпеки,

де К1 – фатальність;

К2 – можливість/зручність реалізації;

К3 – кількість елементів, котрим притаманна вразливість і визначимо, які з загроз найкритичніші.

Результати розрахунків наведені у таблиці 2.6.

Таблиця 2.6 – Коефіцієнти небезпеки

Вразливість	К1	К2	К3	$К_{небезпеки}$
Відсутність організаційних методів захисту від розголошення інформації	3	2	2	0,096
Можливість підключення до корпоративної мережі з будь якого пристрою	3	3	5	0,36
Незахищене зберігання	4	3	4	0,384
Відсутня коректна політика створення паролів для автентифікації	3	4	2	0,192
Відсутність коректного розмежування доступу та «квот»	3	4	2	0,192
Недостатній рівень підготовки персоналу з питань безпеки	3	2	3	0,144
Некомпетентність працівників	4	3	3	0,288
Інформаційна безграмотність працівників	4	2	3	0,192
Можливість підключати сторонні електронні носії	3	2	4	0,192

Рівні К1:

– 1 – наслідки, якими можна знехтувати;

– 2 – незначні наслідки;

– 3 – відчутні наслідки;

– 4 – значні наслідки;

– 5 – крах компанії.

Рівні К2:

– 1 – вразливість дуже складно або неможливо використати;

– 2 – для використання вразливості потрібні спеціальні умови, обладнання і/або висококваліфікований порушник;

– 3 – вразливість може використати лише кваліфікований порушник з мінімальним набором обладнання;

– 4 – вразливість може використати лише кваліфікований порушник;

– 5 – вразливість може використати будь хто;

Рівні К3:

– 1 – 0-1 елемент;

– 2 – 2-9 елементів;

– 3 – 10-14 елементів;

– 4 – 15-19 елементів;

– 5 – 20+ елементів.

Таким чином, найвищий коефіцієнт небезпеки мають:

– можливість підключення до корпоративної мережі з будь якого пристрою;

– незахищене зберігання;

– некомпетентність працівників.

Окрім антропогенних загроз, існують техногенні та стихійні загрози. Складемо перелік цих двох видів загроз із зазначенням властивостей інформації, що порушуються. А саме конфіденційність(К), цілісність(Ц), доступність(Д). Детально данні наведено у таблиці 2.7.

Таблиця 2.7 – Техногенні та стихійні загрози

Загроза	Властивості інформації, що порушуються		
	К	Ц	Д
Техногенні загрози			
Порушення нормальної роботи (переривання): – швидкості обробки інформації; – пропускної здатності каналів зв'язку; – обсягів вільної оперативної пам'яті; – обсягів вільного дискового простору; – електроживлення технічних засобів; – хакерські атаки через глобальну мережу Інтернет.	-	-	+

Продовження таблиці 2.7

Загроза	Властивості інформації, що порушуються		
	К	Ц	Д
Перехоплення інформації (несанкціоноване): – за рахунок ПЕМВ від технічних засобів; – при підключенні до каналів передачі інформації; – за рахунок порушення встановлених правил доступу; – занесення вірусу в робочі станції; – хакерські атаки.	+	+	-
Помилки: – при інсталяції ПЗ, ОС, СУБД; – при експлуатації ПЗ; – при експлуатації технічних засобів; – недбале ставлення співробітників до документації; – помилки при введенні даних.	-	+	+
Порушення нормальної роботи: – порушення працездатності системи обробки інформації; – порушення працездатності зв'язку; – старіння носіїв інформації і засобів її обробки; – порушення встановлених правил доступу; – електромагнітний вплив на технічні засоби.	-	+	+

Продовження таблиці 2.7

Загроза	Властивості інформації, що порушуються		
	К	Ц	Д
Знищення (руйнування): – програмного забезпечення, ОС, СУБД; засобів обробки інформації.	-	+	+
Модифікація (зміна): – програмного забезпечення, ОС, СУБД; інформації при передачі по каналах зв'язку і телекомунікацій.	+	+	+
Стихійні загрози			
– аварії, пожежі, урагани; – непередбачувані ситуації, нез'ясовні явища, інші форс-мажорні обставини.	-	+	+

2.3.2 Визначення переліку порушників

Інформацією, що циркулює на підприємстві, можуть заволодіти порушники – особа або особи, що помилково внаслідок необізнаності, цілеспрямовано, за злим умислом або без нього здійснили спробу виконати операції, які призвели або можуть призвести до порушення властивостей інформації, що визначені політикою безпеки.

Відносно ІТС порушники можуть бути: внутрішніми (з числа персоналу або користувачів системи), або зовнішніми (сторонніми особами).

Метою порушника можуть бути:

– отримання необхідної інформації у потрібному обсязі та асортименті;

– мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами (інтересами, планами);

– нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

Складемо модель порушника беручи до уваги можливий мотив, кваліфікаційні ознаки, місце та час дії порушників.

Детально дані наведено у таблиці 2.8.

Таблиця 2.8 – Модель порушника

Посада	Мотив	Кваліфікаційні ознаки	Місце дії	Час дії
Внутрішні порушники				
Директор	М1, М2, М3	К4	Д5	Ч3
Sales директор	М1, М2, М3	К1	Д5	Ч3
Бухгалтер	М3	К1	Д5	Ч3
Сис.адмін	М1, М2, М3	К5	Д6	Ч4
HR менеджер	М1, М3	К1	Д4	Ч3
Менеджер по роботі з клієнтами	М1, М2, М3	К1	Д4	Ч3
Кадровий робітник	М1, М3	К1	Д4	Ч3
Логіст	М1, М3	К1	Д4	Ч3
Комірник	М1, М3	К1	Д4	Ч3
Водій	М1, М2, М3	К1	Д3	Ч2
Зовнішні порушники				
Представники організацій, що взаємодіють з питань технічного забезпечення	М3	К5	Д2	Ч1
Представники організацій, що взаємодіють з питань ПЗ	М3	К4	Д3	Ч1
Хакери	М2, М3	К3	Д1	Ч3

Специфікація моделі порушника за мотивами здійснення порушень:

– М1 – Безвідповідальність

– М2 – Самозатвердження

– М3 – Корисливий мотив

Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС:

– К0 – Не знає функціональні особливості системи, основні закономірності формування масивів даних та потоків запитів до них, має навички щодо користування штатними засобами системи.

– К1 – Знає функціональні особливості системи, основні закономірності формування масивів даних та потоків запитів до них, має навички щодо користування штатними засобами системи.

– К2 – Володіє високим рівнем знань та практичними навичками роботи з технічними засобами системи та їх обслуговування.

– К3 – Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації автоматизованих інформаційних систем.

– К4 – Знає структуру, функції й механізми дії засобів захисту, їх недоліки.

– К5 – Знає недоліки та “вади” механізмів захисту, які вбудовані у системне програмне забезпечення та його не документовані можливості.

– К6 – Є розробником програмних та програмно-апаратних засобів захисту або системного програмного забезпечення.

Специфікація моделі порушника за місцем дії:

– Д1 – Без доступу на контрольовану територію організації.

– Д2 – З контрольованої території без доступу у будинки та споруди.

– Д3 – Усередині приміщень, але без доступу до технічних засобів АС.

– Д4 – З робочих місць користувачів АС.

– Д5 – З доступом у зони даних (баз даних, архівів й т.ін.).

– Д6 – З доступом у зону керування засобами забезпечення безпеки АС.

Специфікація моделі порушника за часом дії:

– Ч1 – До впровадження АС або її окремих компонентів.

– Ч2 – Під час бездіяльності компонентів системи (в неробочий час, під час планових перерв у роботі, перерв для обслуговування і ремонту і т.д.).

– Ч3 – Під час функціонування АС (або компонентів системи).

– Ч4 – Як у процесі функціонування АС, так і під час зупинки компонентів системи.

2.3.3 Визначення каналів несанкціонованого доступу до ІТС

Несанкціонований доступ до інформації - доступ до інформації, за якого порушуються встановлений порядок його здійснення та (чи) правові норми.

Доступ порушенням посадових повноважень співробітника, доступ до закритої для публічного доступу інформації з боку осіб, котрі не мають дозволу на доступ до цієї інформації. Також іноді несанкціонованим доступом називають одержання доступу до інформації особою, що має право на доступ до цієї інформації в обсязі, що перевищує необхідний для виконання службових обов'язків.

Витік інформації – неконтрольоване поширення інформації, яке призводить до її несанкціонованого одержання [4].

Основними каналами витоку інформації в ІТС на ОІД є :

– змінні носії, та носії на які здійснюється архівування;
– робочі станції працівників відділів;
– робоча станція адміністратора системи;
– засоби вводу\виводу інформації;
– канали передачі інформації в ІТС;
– комутатор.

2.4 Вибір заходів захисту інформації в ІТС підприємства

Автоматизована система являє собою організаційно-технічну систему, що об’єднує ОС, фізичне середовище, персонал і оброблювану інформацію. Задля полегшення задачі співставлення вимог до КЗЗ обчислювальної системи АС з характеристиками АС введено класифікацію АС, а також визначено декілька стандартних профілів захищеності.

Таким чином, АС підприємства – АС «3» класу. Тобто, це розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу. Для даної АС «3» класу обрано наступний профіль захищеності:

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

Опис послуг безпеки наведено у таблиці 2.1.

Таблиця 2.9 – Профіль захищеності ІТС

Критерії	Послуги безпеки	Вимоги до рівнів послуг безпеки
	1	2
Конфіденційності	Довірча конфіденційність	КД-2 (базова довірча конфіденційність)
	Повторне використання об'єктів	КО-1 (повторне використання об'єктів)
	Конфіденційність при обміні	КВ-1(мінімальна конфіденційність при обміні)
Цілісності	Довірча цілісність	ЦД-1 (мінімальна довірча цілісність)
	Відкат	ЦО-1 (обмежений відкат)
	Цілісність при обміні	ЦВ-1 (мінімальна цілісність при обміні)

Продовження таблиці 2.9

Критерії	Послуги безпеки	Вимоги до рівнів послуг безпеки
	1	2
Доступності	Використання ресурсів	ДР-1 (квоти)
	Відновлення після збоїв	ДВ-1 (ручне відновлення)
Спостережності	Реєстрація	НР-2 (захищений журнал)
	Ідентифікація і автентифікація	НИ-2 (одиночна ідентифікація і автентифікація)
	Цілісність комплексу засобів захисту	НЦ-2 (КЗЗ з гарантованою цілісністю)
	Самотестування	НТ-2 (самотестування при старті)
	Ідентифікація і автентифікація при обміні	НВ-1(автентифікація вузла)

Базова довірча конфіденційність (КД-2)

Послуга застосовується для розмежування доступу користувачів до захищених об'єктів і дозволяє користувачу керувати потоками інформації в АС від захищених об'єктів, що належать його домену, до інших користувачів.

Політика довірчої конфіденційності поширюється на об’єкти і забезпечує взаємодію зазначених об’єктів:

– користувачів усіх категорій;

– об’єкти, які містять конфіденційну інформацію;

– визначення в АС груп користувачів з однаковими повноваженнями стосовно такої інформації і тільки в межах цих груп;

– всі інші об’єкти, які підлягають захисту, але не належать до зазначених вище видів.

Політика довірчої конфіденційності, що реалізується КЗЗ, стосується об’єктів, які створюються користувачем у процесі виконання ним функціональних обов’язків.

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

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

КЗЗ повинен надавати користувачу, як власнику процесу, можливість визначати конкретних користувачів і/або групи користувачів, які мають право ініціювати цей процес.

Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації.

Повторне використання об’єктів (КО-1)

Послуга дозволяє забезпечити коректність повторного використання розділюваних об'єктів, гарантуючи, що в разі, якщо розділюваний об'єкт виділяється новому користувачу або процесу, він не містить інформації, яка залишилась від використання його попереднім користувачем або процесом.

Політика повторного використання об'єктів, що реалізується КЗЗ, стосується тільки тих об'єктів ЛОМ, які містять конфіденційну інформацію і ресурси яких поділяються між користувачами ЛОМ та прикладними процесами, що виконуються в ЛОМ.

Вимоги цієї послуги поширюються на сегменти оперативної пам'яті робочих станцій та серверів (усіх без виключення типів) та носії інформації на жорстких магнітних дисках (ЖМД), якими укомплектовані робочі станції й сервери, і використовуються системними та функціональними процесами під час оброблення конфіденційної інформації, а також на окремі види периферійних пристроїв, які мають власну пам’ять і задіяні під час експорту (імпорту) конфіденційної інформації з (в) ЛОМ та створенні «твердих» копій тощо.

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

Вимога цієї послуги в повному обсязі поширюється і на розділювані одночасно декількома користувачами процеси.

Мінімальна конфіденційність при обміні (КВ-1):

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

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

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

Мінімальна довірча цілісність (ЦД-1)

Послуга застосовується для захисту оброблюваної інформації від несанкціонованої модифікації і дозволяє користувачу будь-якої категорії керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену.

Політика довірчої цілісності, що реалізується КЗЗ, поширюється на слабо- та сильнозв’язані об’єкти, які створюються користувачем у процесі виконання ним функціональних обов’язків. Користувач, який створив об’єкт, має право визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати цей об'єкт.

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

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

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації.

Обмежений відкат (ЦО-1)

Послуга забезпечує можливість відмінити окрему операцію або послідовність операцій й повернути захищений об'єкт, з яким маніпулював користувач, до попереднього наперед визначеного стану.

Політика обмеженого відкату забезпечує взаємодію нижчезазначених об’єктів і поширюється на:

– користувачів усіх категорій;

– сильно та слабозв’язані об’єкти, які містять конфіденційну інформацію і в процесі обробки яких передбачається можливість їхньої модифікації користувачем, а також технологічну інформацію КСЗІ.

Компоненти КЗЗ повинні мати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити певну множину операцій, що вже виконані над захищеним об'єктом за певний проміжок часу.

Факт використання користувачем послуги має реєструватись в системному журналі. Відміна операції не повинна призводити до видалення з журналу запису про операцію, яка пізніше була відмінена, якщо остання підлягала реєстрації відповідно до вимог послуги безпеки .

Мінімальна цілісність при обміні (ЦВ-1)

Дана послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Найчастіше ця послуга реалізується з використанням таких механізмів криптографічного захисту, як цифровий підпис і коди автентифікації повідомлень. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування. Під повнотою захисту, як і для послуги конфіденційність при обміні, треба розуміти множину типів загроз, від яких забезпечується захист. Під ступенем захищеності об'єктів, що експортуються, як правило, слід розуміти крипостійкість використовуваних алгоритмів шифрування.

Використання ресурсів (ДР-1)

Послуга дозволяє керувати використанням користувачами послуг та ресурсів. Політика використання ресурсів, що реалізується КЗЗ, поширюється на нижчезазначені об’єкти і забезпечує взаємодію цих об’єктів, передбачаючи можливість встановлення обмежень на їх використання користувачами всіх категорій.

Обмеження щодо використання окремим користувачем та/або процесом обсягів обчислювальних ресурсів АС або кількості об’єктів встановлюються адміністратором безпеки або користувачами, яким надано повноваження інших адміністраторів. Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів.

Спроби користувачів перевищити встановлені обмеження на використання ресурсів повинні реєструватися в системному журналі.

Ручне відновлення після збоїв (ДВ-1)

Політика відновлення після збоїв, що реалізується КЗЗ, поширюється на нижчезазначені об’єкти та забезпечує їх взаємодію:

– системне та функціональне ПЗ;
– засоби захисту інформації та засоби управління КСЗІ;
– засоби адміністрування та управління обчислювальною системою;
– окремі периферійні пристрої (принтери, накопичувачі інформації, змінні носії інформації і т.і.), які задіяні для обробки конфіденційної інформації.

Послуга гарантує повернення АС у відомий захищений стан після відмов або переривання обслуговування, спричинених помилковими діями користувачів, неврахованою функціональною недостатністю програмного та апаратного забезпечення (наприклад, можливою наявністю не виявлених під час проектування незадекларованих функцій), іншими непередбачуваними ситуаціями.

Політикою відновлення після збоїв повинна бути визначена й задокументована множина типів відмов і переривань обслуговування ЛОМ або окремих її компонентів, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Для кожної з відмов повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція автоматизованої системи.

Повернення АС (окремих компонентів) із режиму, що визначається погіршеними характеристиками обслуговування, в режим нормального функціонування повинно здійснюватися за допомогою ручних (не автоматизованих) процедур.

Захищений журнал (НР-2)

Послуга реєстрації рівня НР-2 дозволяє контролювати небезпечні для АС дії зі сторони користувачів будь-яких категорій відносно процесів і об'єктів.

Політика реєстрації поширюється та забезпечує взаємодію користувачів усіх категорій.

КЗЗ повинен забезпечувати реєстрацію всіх подій, які мають безпосереднє відношення до його безпеки. До таких відносяться наступні класи подій:

– вхід/вихід або намагання входу/виходу в/із системи користувачів будь-яких категорій;

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

– зміна паролю користувачем будь-якої категорії;

– отримання або намагання отримання доступу користувачем будь-якої категорії до будь-яких процесів і об'єктів АС, що мають ступінь обмеження доступу на рівні конфіденційної інформації;

– виведення користувачем будь-якої категорії документа або інформації конфіденційного характеру на призначений для цього при-

стрій друку, або намагання виведення користувачем будь-якої категорії документа або інформації конфіденційного характеру на пристрій друку;

– копіювання наборів даних із інформацією конфіденційного характеру на запам’ятовуючих пристроях, які працюють зі змінними носіями, що здатні записувати інформацію, і виділені спеціально для виконання процесів копіювання, або намагання копіювання інформації конфіденційного характеру на запам’ятовуючих пристроях, які згідно з політикою безпеки для цього не призначені;

– виявлення і реєстрація фактів порушення цілісності КЗЗ;

– інші події, обов’язковість реєстрації яких передбачена політикою

– реалізації окремих послуг безпеки інформації.

Реєстрація всіх подій, що мають безпосереднє відношення до безпеки, здійснюється в журналі реєстрації, який містить інформацію щодо дати, часу, місця (адреси робочої станції в АС), імені користувача, типу й успішності чи неуспішності кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію достатню для однозначної ідентифікації робочої станції, користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події.

Адміністратор безпеки і користувачі, яким надано повноваження інших адміністраторів, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації, а КЗЗ повинен забезпечувати захист журналу реєстрації від НСД, модифікації або руйнування.

Одиночна ідентифікація та автентифікація (НИ-2)

Ідентифікація та автентифікація дозволяють визначити й перевірити особу користувача будь-якої категорії, що намагається одержати доступ до АС або до захищених об’єктів, та повинні гарантувати, що доступ може бути надано тільки авторизованому користувачу.

Політика ідентифікації та автентифікації поширюється на нижчезазначені об’єкти і забезпечує їх взаємодію .

Кожний користувач, що отримує доступ до АС, повинен ідентифікуватися КЗЗ на підставі присвоєного йому імені. Дозвіл на виконання будь-яких дій, що контролюються КЗЗ, користувач отримує тільки після автентифікації його КЗЗ на підставі введеного ним пароля.

Механізм реалізації послуги повинен відповідати умовам надійного та однозначного виконання ідентифікації та автентифікації.

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

Однонаправлений достовірний канал (НК-1)

Послуга повинна гарантувати користувачу будь-якої категорії можливість безпосередньої взаємодії з КЗЗ, а також те, що ніяка взаємодія користувача з ЛОМ не може бути модифікованою іншим користувачем або процесом. Послуга повинна визначати вимоги до механізму встановлення достовірного зв'язку між користувачем і КЗЗ.

Політика достовірного каналу поширюється на користувачів усіх категорій, окремі компоненти системного та функціонального ПЗ, які задіяні для реалізації механізмів КЗЗ, і забезпечує взаємодію зазначених об’єктів.

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

Розподіл обов’язків адміністраторів (НО-2)

Послуга дозволяє розмежувати повноваження користувачів, визначивши категорії користувачів із певними й притаманними для кожної з категорій функціями. Послуга призначена для зменшення потенційних збитків від навмисних або помилкових дій користувачів й обмеження авторитарності керування АС.

Політика розподілу обов’язків, що реалізується КЗЗ, поширюється на користувачів усіх категорій і повинна визначати щонайменше такі ролі:

– адміністратора безпеки;

– не менше, ніж одного іншого адміністратора (адміністратора баз даних, адміністратора мережевого обладнання, адміністратора сервісів та ін.);

– користувачів, яким надано право доступу до конфіденційної інформації.

Ролі адміністраторів можуть дублюватися уповноваженими на це користувачами. Кількість таких користувачів повинна бути мінімальною.

Адміністратор безпеки повинен мати доступ до технологічної інформації КСЗІ та системного й функціонального ПЗ, яке реалізує механізми захисту. Інший адміністратор повинен мати доступ до технологічної інформації щодо управління автоматизованої системи та системного й функціонального ПЗ, яке реалізує ці функції. Усім іншим користувачам доступ до цих об’єктів повинен бути заборонений.

Повинен заборонятися доступ адміністраторів до сильно- та слабозв'язаних об'єктів, що містять конфіденційну інформацію, за виключенням випадків, коли їхніми функціональними обов’язками передбачено суміщення адміністративних повноважень та повноважень щодо обробки конфіденційної інформації.

КЗЗ з гарантованою цілісністю (НЦ-2)

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

Для рівня НЦ-2 необхідно, щоб КЗЗ підтримував власний домен виконання, відмінний від доменів виконання всіх інших процесів, захищаючи себе від зовнішніх впливів. Дана вимога є однією з вимог до реалізації диспетчера доступу. Як правило, реалізація даної вимоги повинна забезпечуватися можливостями апаратного забезпечення ОС.

Самотестування при старті (НТ-2)

Самотестування дозволяє КЗЗ перевірити й на підставі цього гарантувати правильність функціонування і цілісність множини функцій ЛОМ, що забезпечуються захистом.

Політика самотестування поширюється на нижчезазначені об’єкти і забезпечує їх взаємодію:

– адміністратора безпеки;

– компоненти системного та функціонального ПЗ, які задіяні для реалізації механізмів КЗЗ;

– засоби захисту інформації, а також технологічну інформацію КСЗІ.

До складу КЗЗ повинен входити набір тестових процедур, достатній для оцінки правильності виконання в ЛОМ всіх критичних для безпеки конфіденційної інформації та технологічної інформації КСЗІ функцій, а сам КЗЗ повинен бути здатним контролювати їх виконання.

Тести повинні виконуватися при ініціалізації КЗЗ за запитом адміністратора безпеки.

У разі некоректного виконання якогось із тестів КЗЗ повинен перевести АС до стану, в якому забороняється обробка конфіденційної інформації взагалі, або до стану, в якому забороняється обробка конфіденційної інформації з використанням послуг безпеки, для яких тест не було виконано. Повернути АС до нормального функціонування може тільки адміністратор безпеки після відновлення працездатності КЗЗ і повторного виконання повного набору тестів.

Автентифікація вузла (НВ-1)

Дана послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Найчастіше ця послуга реалізується з використанням таких механізмів криптографічного захисту, таких як цифровий підпис і коди автентифікації повідомлень. На включення даного рівня в свій рейтинг може претендувати система, що дозволить на підставі цифрового підпису перевіряти цілісність функціонуючого на ЕОМ ПЗ, або система електронної пошти, що забезпечує цифровий підпис повідомлень.

2.5 Політика інформаційної безпеки

На даний час, на підприємстві вже розроблено та діють політики безпеки, що стосуються прав доступу до інформації, правила розмежування доступу до певних приміщень підприємства; політика безпеки щодо захисту web-сторінок підприємства, а також політика використання зовнішніх електронних носіїв інформації та правила зберігання та знищення інформації.

Дані політики безпеки були розроблені системним адміністратором та директором підприємства. Затверджені були директором компанії.

Усі працівники були ознайомлені із розробленими політиками безпеки за п’ять робочих днів до дати набуття чинності політик безпеки. Відповідальність за виконання вище зазначених ПБ несе системний адміністратор.

2.6 Організаційні заходи щодо забезпечення політики безпеки

Були визначені наступні організаційні заходи щодо забезпечення політики безпеки:

1 розробити та впровадити посадові інструкції користувачів та персоналу ІТС, а також інструкції, якими регламентується порядок виконання робіт іншими особами з числа тих, що мають доступ до ІТС;

2 розробити та впровадити розпорядчі документи щодо використання робочих станцій користувачами та зазначити в них що користувач несе матеріальну відповідальність за цілісність робочої станції;

3 визначити правила обліку, зберігання, розмноження, знищення носіїв конфіденційної інформації, яка обробляється на ОІД згідно матриці доступу;

4 створити на програмному рівні системи розпізнавання й розмежування доступу до інформації засобами ідентифікації й автентифікації користувачів даної ІТС;

5 розмежувати права користувачів ІТС у групи користувачів, згідно з матрицею доступу, програмними методами ОС;

6 блокувати облікові записи користувачів після певного числа невдалих спроб входу в систему, що зменшить вірогідність підбору паролю неав-

торизованим користувачем за допомогою функції менеджера облікових записів, до якої входить підтримка механізму ідентифікації і перевірки дійсності користувачів при вході в систему, блокувати ПЕОМ на час відсутності користувача;

7 створити набір прав, що дозволяє надавати користувачеві доступ на виконання окремих операцій та використання окремих програм за допомогою програмного продукту DeviceLock;

8 організувати захист атрибутами файлів. При цьому передбачена можливість встановлювати, чи може індивідуальний файл бути змінений або розділений визначеним користувачем. Захист атрибутами файлів використовується для запобігання випадкових змін або видалення окремих файлів. При захисті даних використовуються файлові атрибути: «модифікація, читання, копіювання, друкування, знищення» програмними засобами;

9 контролювати доступ користувачів до CD-і DVD-дисководів, жорстких дисків, зовнішніх USB-носіїв, USB-портів за допомогою програмного продукту DeviceLock, чим забезпечиться мінімізація занесення вірусу з боку зовнішніх носіїв та зменшиться вірогідність копіювання інформації;

10 знищувати інформацію (або створити резервну копію), що зберігається в ПЗП, при списанні або відправці ПЕВМ в ремонт;

11 захищати локальні розділи диску від випадкового або навмисного форматування;

12 ідентифікувати зовнішні носії на які здійснюється архівування даних, ідентифікувати периферійні засоби вводу\виводу інформації (клавіатури, миші, принтери), надаючи користувачеві доступ до пристрою з відповідним ідентифікатором (драйвером або серійним номером) програмним методом;

13 протоколювати всі дії користувачів з пристроями і файлами згідно матриці доступу (копіювання, читання, знищення і т.п);

14 встановити нове антивірусне програмне забезпечення та налаштування між сітьового екрану;

15 зберігати конфіденційну інформацію на окремому спеціально виділеному локальному диску та обмежити до нього мережевий доступ програмними засобами.

16 обмежувати доступ до соціальних мереж та засобів миттєвого обміну повідомленнями, а також до сайтів, які не зв'язані з робочим процесом програмними засобами;

17 заборонити користувачам скачування та встановлення будь-яких програм програмними засобами;

18 налаштувати поштовий антивірусний монітор, який сканuватиме кожне повідомлення і доставить на поштову скриньку листи які не містять ні вбудованого шкідливого коду, ні інфікованих вкладень;

19 заблокувати невживані порти комутатора програмними засобами.

20 роздати обов'язки системних адміністраторів програмними засобами, а також ввести в експлуатацію для віддаленої роботи системних адміністраторів програмного додатку ScreenConnect.

21 встановити на об'єкті, де обробляється конфіденційна інформація, відео спостереження (встановлення камер відео спостереження).

22 впровадити підписання договорів про заборону розголошення конфіденційної інформації, що обробляється в ІТС для всіх категорій працівників, що мають доступ до ІТС.

23 створення гостьової мережі для виходу в Інтернет задля унеможливлення несанкціонованого доступу до АС підприємства.

24 впровадити квартальні семінари та навчання персоналу (користувачів АС), що спрямоване на покращення навичок роботи з ІТС.

2.7 Розроблення елементів політики безпеки

2.7.1 Політика безпеки відносно паролів

Мета політики безпеки:

Встановити правила використання паролів для доступу до баз даних, електронних документів, а також використання паролів для підключення до

безпровідної мережі підприємства. Користувачі системи повинні дотримуватися вимог, що висвітлюються в даній політиці. Виконання вимог даної політики відносно паролів підвищує рівень захищеності інформаційних ресурсів, що циркулюють та обробляються на підприємстві.

Область дії:

Область дії політики безпеки відносно паролів розповсюджується на всіх користувачів, що мають доступ до баз даних чи електронних документів або підключаються до АС підприємства за допомогою безпровідної мережі.

Відповідальні особи політики безпеки:

Відповідальною особою за виконання політики паролів користувачами системи є системний адміністратор підприємства.

Політика безпеки:

Паролі системного рівня:

– паролі створюються системним адміністратором. Директором підприємства встановлюється резервний пароль доступу до системи на випадки надзвичайних подій;

– ідентифікатори та паролі користувачів мають бути унікальними;

– паролі мають бути довжиною не менше ніж 8 символів, що відносяться до 3 з 4 наступних категорій:

  – латинські заголовні букви (A-Z);

  – латинські прописні букви (a-z);

  – цифри (0-9);

  – символі відмінні від букв чи цифр (наприклад: !,$,%,#);

– пароль не має містити ім’я облікового запису, довжиною більше п’яти символів;

– паролі заборонено передавати третім особам, не мають вставлятися до тексту програм, чи записуватися на папері або зберігатися в незашифрованому вигляді деінде;

– паролі мають змінюватися кожні 6 місяців (чи раніше при виникненні загрози розголошення пароля чи його втрати; зміні особи, що займає посаду системного адміністратора);

– паролі не мають повторюватися принаймні 3 рази;

– забороняється використовувати один і той самий символ більше двох разів підряд.

Паролі рівня користувачів:

– паролі генеруються користувачами особисто та вони мають відповідати приведеним нижче критеріям;

– ідентифікатори та паролі користувачів мають бути унікальними;

– паролі мають бути довжиною не менше ніж 8 символів, що відносяться до 3 з 4 наступних категорій:

– латинські заголовні букви (A-Z);

– латинські прописні букви (a-z);

– цифри (0-9);

– символі відмінні від букв чи цифр (наприклад: !,$,%,#);

пароль не має містити ім’я облікового запису, довжиною більше двох символів;

– паролі заборонено передавати третім особам, не мають вставлятися до тексту програм, чи записуватися на папері чи зберігатися в незашифрованому вигляді деінде;

– паролі мають змінюватися кожні 3 місяці (чи раніше при виникненні загрози розголошення пароля чи його втрати; зміні осіб на посадах передбачених на підприємстві);

– забороняється використовувати один і той самий символ більше двох разів підряд;

– паролі не мають повторюватися принаймні 3 рази.

Паролі для доступу до безпровідної мережі:

– паролі генеруються користувачами особисто та вони мають відповідно приведеним нижче критеріям;

– ідентифікатори та паролі користувачів мають бути унікальними;

– паролі мають бути довжиною не менше ніж 8 символів, що відносяться до 3 з 4 наступних категорій:

– латинські заголовні букви (A-Z);

– латинські прописні букви (a-z);

– цифри (0-9);

– символі відмінні від букв чи цифр (наприклад: !,$,%,#);

– пароль не має містити ім’я облікового запису, довжиною більше двох символів;

– паролі заборонено передавати третім особам, не мають вставлятися до тексту програм, чи записуватися на папері чи зберігатися в незашифрованому вигляді деінде;

– паролі мають змінюватися кожні 6 місяців (чи раніше при виникненні загрози розголошення пароля чи його втрати);

– забороняється використовувати один і той самий символ більше двох разів підряд;

– паролі не мають повторюватися принаймні 3 рази.

Затвердження політики:

Політика безпеки розробляється системним адміністратором та підписується директорам закладу при прийнятті усіх розділів політики.

Дії з виконання політики:

Виконання політики безпеки контролює системний адміністратор підприємства за допомогою вбудованих засобів автентифікації в ОС. При прийнятті (зміні) політики безпеки кожен працівник має бути ознайомлений не пізніше, чим за 5 робочих днів до прийняття нової редакції даної політики. При ознайомленні з даною політикою безпеки користувач має підписатися, що він ознайомлений з нею, та зобов’язується виконувати встановлені цим документом правила.

Порядок та періодичність перегляду:

Політики безпеки переглядається раз у рік заступником директора. У разі виникнення форс-мажорних ситуацій політика безпеки може бути переглянута раніше вказаного терміну.

Відповідальність:

Співробітники, що ознайомились з політикою безпеки несуть повну відповідальність за збереження паролів. До співробітників, що порушили дану політику безпеки, будуть прийняті дисциплінарні міри.

2.7.2 Політика антивірусного захисту

Мета політики безпеки:

Підвищити інформаційну безпеку підприємства шляхом розробки системної політики по створенню, впровадженню і супроводу комплексних засобів антивірусного захисту, які визначають основні правила і вимоги по захисту інформаційних ресурсів організації від загроз, пов'язаних з дією програм, спеціально розроблених або модифікованих для несанкціонованого знищення, блокування, зміни або копіювання інформації, а також порушення процесу функціонування організації.

Область дії:

Політика поширюється на всіх працівників підприємства, які в своїй професійній діяльності використовують комп'ютери, і є обов'язковою для виконання. Дана політика безпеки не відміняє інші політики.

Відповідальні особи політики:

Відповідальним за виконання політики безпеки є системний адміністратор.

Політика:

Засоби захисту від шкідливих програм мають бути встановлені, налагоджені і активізовані на всіх програмно-технічних засобах до початку їх використання для роботи з інформаційними ресурсами організації.

До використання допускаються лише ліцензійні антивірусні засоби, рекомендовані до використання системним адміністратором. У разі потреби

використання антивірусних засобів, що не увійшли до переліку рекомендованих, їх вживання необхідно погоджувати з системним адміністратором.

Установка засобів антивірусного захисту на комп'ютерах і налаштування їх параметрів здійснюється системним адміністратором відповідно до керівництва по вживанню конкретних антивірусних засобів.

Контролю на предмет виявлення шкідливих програм повинна піддаватися вся інформація, що створюється або обробляється програмно-технічними засобами, а також інформація, що приймається або передається по знімних носіях і засобам телекомунікації.

Оновлення антивірусних баз повинне виконуватися не рідше одного разу на добу автоматично, згідно з можливостями програмного забезпечення.

Заходи антивірусного захисту:

Профілактику вірусів :

1 щоденна автоматична перевірка наявності вірусів при включенні комп'ютера;

2 регулярна (не рідше за один раз в квартал) вибіркова перевірка комп'ютерів на наявність вірусів, навіть за відсутності зовнішніх проявів вірусів.

3 перевірка наявності вірусів в комп'ютерах, що повернулися з ремонту (у тому числі гарантійного);

4 ретельна перевірка всіх програм, що поступають, а також куплених програм і баз даних.

Вживання засобів антивірусного захисту:

– якщо вірус уразив які-небудь програми, то знищення вірусу виконується шляхом знищення програми на диску, або на дискеті. Після знищення зараженої програми необхідно відновити програму, використовуючи резервну копію програми;

– якщо вірус уразив файли, то вірус знищується, або шляхом стирання цих файлів, або шляхом використання спеціальних програм, що лікують.

Використання програм, що лікують, не дає повної гарантії відновлення файлу. Тому після лікування необхідна перевірка відновлення даного файлу. Програми, що лікують, використовуються лише в тих випадках, коли відсутня резервна копія зараженої програми або файлу з даними, або відновлення знищеного файлу за допомогою резервної копії дуже трудомістко;

– після знищення вірусів і відновлення заражених програм і файлів з даними необхідно ще раз виконати перевірку наявності вірусів, використовуючи антивірусні програми. Перед повторною перевіркою необхідно перезавантажити комп'ютер через виключення і подальше включення комп'ютера.

Відповідальність:

Відповідальність за виконання заходів антивірусного контролю і дотримання вимог даної політики покладається на всіх співробітників закладу, що є користувачами системи.

Відповідальність за проведення профілактичних заходів щодо забезпечення антивірусного захисту, а також знищення виявлених вірусів покладається на системного адміністратора.

Періодичний контроль за станом антивірусного захисту, а також за дотриманням встановленого порядку антивірусного контролю і виконанням вимог даної політики співробітниками здійснюється системним адміністратором.

Виключення:

Усі виключення з політики мають бути погоджені з директором. Неузгоджені відступи від політики розцінюються як інциденти інформаційної безпеки і можуть служити підставою для прийняття адміністративних заходів відповідно до законодавства.

Порядок і періодичність перегляду:

Політика антивірусного захисту передивляється з періодичністю раз на рік. При виникненні частих ситуацій, що порушують інформаційну безпеку підприємства, періодичність перегляду політики може змінюватися.

Після внесення змін до політики безпеки кожен співробітник закладу має бути ознайомлений з новою версією політики і підписатися в угоді про обов'язковість виконання вимог даної політики.

2.7.3 Політика забезпечення доступу до серверу закладу

Мета політики безпеки:

Встановити правила та порядок доступу до серверів та у серверне приміщення. Дотримання вимог даної політики підвищує захищеність інформації, що зберігається та обробляється на сервері.

Область дії:

Дана політика розповсюджується на системного адміністраторів та директора

Відповідальні особи політики безпеки:

Відповідальною особою за виконання політики доступу до серверу є директор підприємства.

Політика безпеки:

Право доступу до серверної кімнати та знаходження у ньому без нагляду мають системний адміністратор та директор, ключі від приміщення зберігаються у системного адміністратора та директора.

Право доступу до серверної кімнати під наглядом системного адміністратора чи директора надається тільки співробітникам підприємства, що мають доступ до АС.

Доступ до апаратної частини серверів має системний адміністратор. Доступ надається при:

- проведенні профілактичних робіт;
- ремонті обладнання;
- заміни комплектуючих;
- модернізації апаратної частини.

Порядок доступу до апаратної частини:

– на ім’я директора оформлюється заява на відкриття серверу з зазначенням мети доступу;

– після прийняття заяви, при наявності директора знімаються пломби системного адміністратора та заступника директора;

– системний адміністратор виконує необхідний обсяг роботи;

– по закінченню роботи встановлюються пломби системного адміністратора та директора;

– оформлюється звіт з зазначенням початку(з моменту зняття пломб) до закінчення (встановлення нових пломб) із зазначення виду та обсягу проведених робіт.

Логічний доступ (віддалений доступ з використанням свого облікового запису) системний адміністратор використовує для налаштування, проведення профілактичних робіт, інсталяції чи видалення програмного забезпечення, усунення несправностей, модернізації ПЗ, оновлення антивірусних баз. Доступ реалізується засобами віддаленого адміністрування з необхідними для авторизації системного адміністратора даних зі свого робочого місця.

Логічний доступ користувачів виконується віддалено з їх робочих станцій. Згідно з їх правами доступу.

Логічний доступ директор виконує віддалено з його робочого місця для аналізу захищеного журналу та перевірки працездатності КЗЗ.

Затвердження політики:

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

Дії з виконання політики інформаційної безпеки:

Виконання політики безпеки користувачами контролює системний адміністратор підприємства за допомогою вбудованих засобів аудиту в ОС. Виконання політики безпеки користувачами, в тому числі й системним адміністратором контролюється заступником директора за допомогою вбудованих засобів аудиту в ОС. При прийнятті (зміні) політики безпеки кожен співробі-

тник має бути ознайомлений не пізніше, чим за 5 робочих днів до прийняття нової редакції даної політики.

Порядок та періодичність перегляду:

Політики безпеки переглядається раз на рік системним адміністратором та директором. У разі виникнення форс-мажорних ситуацій політика безпеки може бути переглянута раніше вказаного терміну.

Відповідальність:

Системний адміністратор та директора несуть відповідальність за виконання політики доступу до серверу та серверного приміщення.

2.7.4 Політика використання мережі Інтернет на підприємстві

Мета політики:

Підвищити рівень інформаційної безпеки компанії шляхом введення правил і інструкцій для співробітників, які при виконанні своїх прямих обов'язків використовують Інтернет.

Область дії:

Політика поширюється на співробітників закладу, які при виконанні своїх прямих обов'язків використовують мережу Інтернет. Дана політика безпеки не відміняє інші політики.

Відповідальні особи політики:

Відповідальною особою за виконання політики доступу є системний адміністратор підприємства.

Політика:

Доступ до мережі Інтернет виконувати лише через устаткування і системи підприємства.

Використання мережі Інтернет можливо лише для:

- отримання та обробки замовлень;
- підтримки і розвитку бізнесу і комунікації співробітників фірми;
- досліджень і розробок;

– збору інформації для більшої обізнаності у фінансових, законодавчих питаннях, якщо ці питання безпосередньо впливають на виконання своїх посадових обов'язків.

Забороняється:

– грати на комп'ютері в робочий час і під час обіду;

– вести діяльність не від імені фірми;

– передавати конфіденційну інформацію третім особам;

– здійснювати дії що суперечать статуту ділової етики підприємства, законодавству, політикам і процедурам підприємства;

– доступ до неавторизованої інформації і її копіювання;

– доступ до системи під іншим паролем.

Використання електронної пошти, дошок оголошень, чат-кімнат в робочий час, на устаткуванні фірми і застосовуючи імена користувачів і паролі фірми в особистих цілях, для переговорів з друзями і членами сім'ї розглядається як експлуатація ресурсів компанії в особистих цілях і категорично забороняється. Жодних виключень не робиться з даного питання для обідніх перерв і неробочого часу.

Відповідальність:

У разі явного порушення даної політики працівником підприємства, будуть застосовані дисциплінарні міри.

Порядок і періодичність перегляду

Політики безпеки переглядається раз на рік системним адміністратором та директором. У разі виникнення форс-мажорних ситуацій політика безпеки може бути переглянута раніше вказаного терміну.

2.8 Висновок спеціальної частини

У спеціальній частині наведено:

– рід діяльності підприємства;

– інформаційну систему;

– фізичне середовище;

– середовище користувачів;
– технологію обробки інформації
– функціональний профіль захисту.

Окрім цього, виконано категоріювання інформації, що обробляється в ІТС та визначено основні загрози та вразливості, їх джерела та складено модель порушника.

Отримані результати обстеження були використані для розробки ПБ ІТС приватного підприємства ТОВ «IntercarsUA Dnipro». На їх основі розроблено збірку правил відносно:

– створення паролів;
– антивірусного захисту;
– використання мережі інтернет;
– фізичного доступу до сервера.

Розроблені рекомендації повинні сприяти забезпеченню належного стану захищеності ІТС підприємства.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

Однією з головних цілей захисту інформаційних ресурсів від внутрішніх загроз є мінімізація збитків від порушення інформаційної безпеки підприємства.

Економічно доцільним слід вважати, якщо витрати на забезпечення інформаційної безпеки не перевищують збитків від реалізації загрози її порушення.

Метою виконання економічних розрахунків дипломного проекту є техніко-економічне обґрунтування доцільності запровадження запропонованих в проекті рішень.

3.1 Визначення витрат на розробку політики безпеки

По-перше, необхідно визначити трудомісткості розробки політики безпеки інформації.

Трудомісткість розробки політики безпеки інформації визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного спеціаліста з інформаційної безпеки):

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

де $t_{тз}$ – тривалість складання технічного завдання на розробку політики безпеки інформації;

$t_{в}$ – тривалість розробки концепції безпеки інформації у організації;

$t_{а}$ – тривалість процесу аналізу ризиків;

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

$t_{озб}$ – тривалість вибору основних рішень з забезпечення безпеки інформації;

$t_{овр}$ – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації;

$t_{д}$ – тривалість документального оформлення політики безпеки.

Таким чином трудомісткість розробки політики безпеки дорівнює:

$$t=18+6+15+10+4+10$$

$$t = 63 \text{ год.}$$

Розрахуємо витрати на створення ПБ. Розрахунок проводиться за формулою 3.2:

$$K_{рп} = З_{зп} + З_{мч} \text{ грн.} \quad (3.2)$$

де $K_{рп}$ – витрати на створення політики безпеки;

$З_{зп}$ – заробітна плата спеціаліста з інформаційної безпеки;

$З_{мч}$ – вартість витрат машинного часу, що необхідні для створення ПБ.

Витрати на заробітну плату спеціаліста ІБ розраховуються за формулою 3.3:

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

де t – загальна тривалість розробки політики безпеки, годин;

$З_{іб}$ – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

Средньогодинна заробітна плата спеціаліста з інформаційної безпеки становить – 42 грн/год.

Відповідно до формули 3.3, витрати на заробітну плату спеціаліста ІБ становлять:

$$З_{зп} = 63 \text{ год} \cdot 42 \text{ грн/год},$$

$$З_{зп} = 2646 \text{ грн.}$$

У свою чергу, витрати машинного часу визначаються за формулою 3.4:

$$З_{мч} = t \cdot С_{мч} \text{ грн.} \qquad (3.4)$$

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

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

Вартість 1 години машинного часу ПК визначається за формулою 3.5:

$$С_{мч} = P \cdot t_{нал} \cdot С_е + \frac{Ф_{зал} \cdot Н_а}{F_р} + \frac{К_{лпз} \cdot Н_{апз}}{F_р} \text{ грн,} \qquad (3.5)$$

де P – встановлена потужність ПК, кВт;

$С_е$ – тариф на електричну енергію, грн/кВт·година;

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн.;

$Н_а$ – річна норма амортизації на ПК, частки одиниці;

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

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.;

$F_р$ – річний фонд робочого часу (за 40-годинного робочого тижня $F_р$ = 1920).

Залишкова вартість ПК визначається виходячи з фактичного терміну його експлуатації як різниця між первісною вартістю та зносом за час використання.

$$C_{мч} = 0{,}1 \cdot 1 \cdot 1{,}86 + 80 + 0{,}5 \text{ грн},$$

$$C_{мч} = 80{,}69 \text{ грн}.$$

Отже, витрати на створення ПБ за формулою 3.2 становлять:

$$K_{рп} = 7729{,}47 \text{ грн}.$$

В результаті розрахунків, вартість розробки ПБ становить – 7729,47 гривень.

Повна вартість капітальних витрат розраховується за формулою 3.6:

$$K = K_{рп} + K_{аз} \text{ грн}. \qquad (3.6)$$

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

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

Для впровадження політики безпеки необхідно придбати наступне апаратне забезпечення:

– врізний замок (1100 грн);
– пломби для опечатування (100 грн);
– комплект внутрішніх камер відео-спостереження (8 шт., 16930 грн);
– зовнішня камера відео-спостереження (1 шт., 2370 грн).

Відповідно до цього вартість закупівлі апаратного забезпечення становить 20500 грн.

Таким чином, згідно з формулою 3.6:

$$K = 28223 \text{ грн.}$$

3.2 Розрахунок експлуатаційних (поточних) витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період (наприклад, рік), що виражені у грошовій формі.

Поточні витрати розраховуються за формулою 3.7:

$$C = C_a + C_з + C_е + C_{лпз} \text{ грн}, \quad (3.7)$$

де C_a – річний фонд амортизаційних відрахувань;

$C_з$ – річний фонд заробітної плати інженерно-технічного персоналу;

$C_е$ – вартість електроенергії, що споживається апаратурою;

$C_{лпз}$ – річні витрати на поновлення ліцензії ПЗ.

Річний фонд амортизаційних відрахувань розраховується за формулою 3.8:

$$C_a = Ф_п / T \text{ грн} \quad (3.8)$$

де $Ф_п$ – первісна вартість придбаного обладнання;

T – мінімальний строк корисного використання.

$$C_a = 3860 \text{ грн.}$$

У свою чергу, витрати на заробітну плату інженерно-технічного персоналу розраховуються за формулою 3.9:

$$C_{зпад} = З_{дод1} + З_{дод2} + З_{дод3} \text{ грн}, \quad (3.9)$$

де $З_{дод1}$ – додаткова заробітна плата інженерно-технічного персоналу за проведення квартальних семінарів та навчання персоналу, що спрямоване на покращення навичок роботи з ІТС;

$З_{дод2}$ – додаткова заробітна плата інженерно-технічного персоналу за додаткові обов'язки – відповідальність за виконання впроваджених розділів політики безпеки інформації;

$З_{дод3}$ – додаткова заробітна плата інженерно-технічного персоналу за модернізацію існуючої ПБ підприємства.

За формулою 3.9, можна розрахувати:

$$C_з = (1000 + 800 + 1000) \cdot 12 \text{ місяців},$$

$$C_з = 3360\,0 \text{ грн}.$$

Річні витрати на поновлення ліцензії складаються з:

– замовлення Avast Endpoint Profession Suite Plus на 1 рік для 25 ПК (5075 грн);

– замовлення Screen Connect Control Wise на 1 рік для ІТС підприємства (790 грн);

– замовлення DeviceLock Endpoint DLP Suite на 1 рік (12750 грн).

Загалом, річні витрати на поновлення ліцензії ПЗ становлять:

$$С_{лпз} = 18615 \text{ грн}.$$

Вартість електроенергії, що споживається апаратурою становить:

$$C_е = 77088 \text{ грн}.$$

Отже повна вартість річних експлуатаційних витрат становить:

$$C = 3860 + 33600 + 77088 + 18615 \text{ грн},$$

і, таким чином,

$$C = 133163 \text{ грн}.$$

3.3 Оцінка величини збитку у разі реалізації загроз

Метою цієї оцінки є визначення обсягів матеріальних збитків, виходячи з імовірності реалізації конкретної загрози й можливих матеріальних втрат від неї.

Для розрахунку збитків від реалізації даних загроз потрібно використати формулу 3.7:

$$U = П_п + П_в + V_{грн}, \quad (3.10)$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла, грн;

$П_в$ – вартість відновлення працездатності вузла (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

У свою чергу, для розрахунку $П_п$, $П_в$ і V, використовують формули 3.8, 3.9, 3.10 відповідно.

$$П_п = \frac{\sum Зс \cdot Чс}{F} \cdot t_п \text{ грн}, \quad (3.11)$$

де F – місячний фонд робочого часу;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн/місяць;

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслі-

док атаки, годин;

$Ч_с$ – чисельність співробітників атакованого вузла.

$$П_в = П_{ви} + П_{пв} + П_{зч}\ грн, \tag{3.12}$$

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

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

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

$$V = \frac{O}{F} \cdot (t_п + t_в + t_{ви})\ грн, \tag{3.13}$$

де F – місячний фонд робочого часу;

O – обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн у місяць;

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин;

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

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин.

У свою чергу, $П_{ви}$ і $П_{пв}$ розраховуються за формулами 3.11 і 3.12 відповідно.

$$П_{ви} = \frac{\sum Зс \cdot Чс}{F} \cdot t_{ви}\ \ грн, \tag{3.14}$$

де F – місячний фонд робочого часу;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн/місяць;

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

$Ч_с$ – чисельність співробітників атакованого вузла.

$$П_{пв} = \frac{\sum Зо \cdot Чо}{F} \cdot t_в \ грн, \qquad (3.15)$$

де F – місячний фонд робочого часу;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), грн на місяць;

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

$Чо$ – чисельність обслуговуючого персоналу.

Вихідні дані для розрахунків наведені у таблиці 3.1.

Таблиця 3.1 – Вихідні дані для розрахунку збитків від реалізації загроз

Умовні позначення	Величина
$t_п$	15 год
$t_в$	6 год
$t_{ви}$	4 год
$З_о$	8000 грн
$З_с$	6000 грн
$Ч_о$	1 особа
$Ч_с$	5 осіб
$О$	200000 осіб
$П_{зч}$	3000 грн
I	3 шт
N	15 шт
F	176 год
$F_г$	8760 год

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

$$П_п = 2557 \text{ грн.}$$

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

$$П_в = 5830 \text{ грн,}$$

де $П_{ви} = 2557$ грн, а $П_{пв} = 273$ грн, а $П_{зч}$ наведено у таблиці 3.1.

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

$$V = 570 \text{ грн.}$$

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

$$U = 8958 \text{ грн.}$$

Загальний збиток від атаки на вузол або сегмент корпоративної мережі організації розраховується за формулою 3.16.

$$B = \sum_i \sum_n U . \qquad (3.16)$$

І таким чином:

$$B = 403110 \text{ грн.}$$

3.4 Визначення та аналіз показників економічної ефективності запропонованих в кваліфікаційній роботі проектних рішень

Загальний ефект від впровадження системи інформаційної безпеки розраховується за формулою 3.17:

$$E = B \cdot R - C \text{ грн}, \qquad (3.17)$$

де B – загальний збиток від атаки на вузол корпоративної мережі, грн;

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

C – щорічні витрати на експлуатацію системи інформаційної безпеки, грн.

Тож, економічний ефект становить:

$$E = 108703 \text{ грн}.$$

Оцінка економічної ефективності системи захисту інформації здійснюється на основі визначення та аналізу наступних показників:

– сукупна вартість володіння (ТСО);

– коефіцієнт повернення інвестицій ROSI (Return on Investment for Security);

– термін окупності капітальних інвестицій $T_о$.

У даному випадку ТСО не використовується, оскільки було визначено величину відверненого збитку.

ROSI, у свою чергу, показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки, розраховується за формулою 3.18:

$$ROSI = E / K, \qquad (3.18)$$

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

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

Таким чином,

$$ROSI = 108703 \text{ грн} / 28223 \text{ грн},$$

$$ROSI = 3{,}85.$$

Для остаточної оцінки варіантів і вибору найбільш ефективного з них необхідно порівняти значення ROSI з бажаним значенням показника ефективності $Е_н$.

Організація здійснює фінансування капітальних інвестицій за рахунок реінвестування власних коштів, тому в якості $E_н$ приймається бажана норма прибутковості альтернативних варіантів вкладення коштів К (на депозитний рахунок у банку).

Проект вважається економічно доцільним, якщо розрахунковий коефіцієнт ефективності перевищує річний рівень прибутковості альтернативного варіанта, розраховується за формулою 3.19:

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

де $N_{деп} = 19$ – річна депозитна ставка або прибутковість альтернативного варіанту вкладення коштів, %;

$N_{інф} = 8$ – річний рівень інфляції, %.

Оскільки 3,85 > 0,11, проект є економічно доцільним.

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупаються за рахунок загального ефекту від впровадження системи інформаційної безпеки, розраховується за формулою 3.20:

$$T_o = E / K = 1 / ROSI = 0{,}26 \text{ року.} \quad (3.20)$$

3.5 Висновок економічного розділу

В цьому розділі були проведені розрахунки:

– капітальних витрат на введення в експлуатацію політики безпеки інформації (28223 грн);

– річних експлуатаційних витрат на підтримку заходів захисту, регламентованих політикою безпеки (133163 грн).

В ході розрахунків з'ясовано, що введення в експлуатацію засобів та заходів захисту вигідне для підприємства. Це підтверджується наступними показниками:

– економічний ефект (108703 грн);

– коефіцієнт ефективності, що перевищує річний рівень прибутковості альтернативного варіанта (3,85 > 0,11);

– термін окупності капітальних інвестицій (0,26 року).

Отже, впровадження та використання обраних проектних рішень повністю доцільне.

ВИСНОВКИ

У першому розділі кваліфікаційної роботи описано стан питання, проаналізовано нормативно-правову базу, на основі якої визначено підстави та етапи створення КСЗІ та ПБ.

Таким чином визначено необхідність здійснення обстеження об'єкту та виявлення основних загроз та вразливостей, реалізація яких призведе до порушення властивостей інформації, що циркулює в ІТС підприємства.

У спеціальній частині наведено основні відомості про підприємство. Виконано обстеження інформаційної системи, фізичного середовища, середовище користувачів. Описано технологію обробки інформації та функціональний профіль захисту.

Окрім цього, виконано категоріювання інформації, що обробляється в ІТС та визначено основні загрози та вразливості, їх джерела та складено модель порушника.

Отримані результати обстеження були використані для розробки ПБ ІТС приватного підприємства ТОВ «IntercarsUA Dnipro». На їх основі розроблено збірку правил відносно створення паролів, антивірусного захисту, використання мережі інтернет, фізичного доступу до сервера.

Розроблені рекомендації повинні сприяти забезпеченню належного стану захищеності ІТС підприємства.

В третьому розділі було проведено розрахунки капітальних витрат на введення в експлуатацію політики безпеки інформації, річних експлуатаційних витрат на підтримку заходів захисту, регламентованих політикою безпеки.

В ході розрахунків з’ясовано, що введення в експлуатацію засобів та заходів захисту вигідне для підприємства.

Отже, впровадження та використання обраних проектних рішень повністю доцільне, і сприяє забезпеченню належного стану захищеності інформації, що циркулює в ІТС підприємства.

ПЕРЕЛІК ПОСИЛАНЬ

1 Закон України "Про інформацію" [Електронний ресурс] // 2657-XII. – 01.01.2017. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2657-12.

2 НД ТЗІ 1.6-005-2013 "Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці" [Електронний ресурс]. – 2013. – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=107993&cat_id=89734&ctime=1366373635138.

3 Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" [Електронний ресурс] // 80/94-ВР. – 19.04.2014. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/80/94-вр.

4 ДСТУ 3396.2-97 "Захист інформації. Технічний захист інформації. Терміни та визначення." [Електронний ресурс]. – 1998. – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38934&cat_id=38836.

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

6 НД ТЗІ 3.7-003-05 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі" [Електронний ресурс]. – 2005. – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=46074&cat_id=38835.

7 НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу" [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106342.

8 НД ТЗІ 1.1-002-99 "Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу " [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106340.

9 НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу" [Електронний ресурс]. – 28.04.1999. – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=101870&cat_id=89734&ctime=1344501089407.

10 НД ТЗІ 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі" [Електронний ресурс]. – 2000. – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106341.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість аркушів	Примітки
Документація				
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	Розділ 1. Стан питання. Постановка задачі	11	
6	А4	Розділ 2. Спеціальна частина	44	
7	А4	Розділ 3. Економічна частина	13	
8	А4	Висновок	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А. Відомість матеріалів дипломної роботи	1	
11	А4	Додаток Б. Перелік документів на оптичному носії	1	
12	А4	Додаток В. Відгук керівника економічного розділу	1	
13	А4	Додаток Г. Відгук керівника дипломної роботи	1	
14	А4	Додаток Д. Ситуаційний план ОІД	2	
15	А4	Додаток Ж. Генеральний план та план комунікацій ОІД	3	

ДОДАТОК Б. Перелік документів на оптичному носії

– Каркан А.В. УБіт-15-1.docx
– Каркан А.В. УБіт-15-1.pptx

ДОДАТОК В. Відгук керівника економічного розділу

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

Дата: _____ Підпис: _____

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

“Розробка політики безпеки інформації інформаційно-телекомунікаційної системи приватного підприємства ТОВ «IntercarsUA Dnipro»”.

студентки групи Убит-15-1 Каркан Анастасії Володимирівни

Кваліфікаційна робота за спеціальністю 6.170103 «Управління інформаційною безпекою» Каркан А.В. представлена пояснювальною запискою на ___ ст., ___ рис., ___ табл., ___ додатків, ___ джерел.

Мета кваліфікаційної роботи є актуальною, адже спрямована на підвищення рівня захисту інформації в ІТС приватного підприємства ТОВ «IntercarsUA Dnipro».

При виконанні роботи продемонстровано задовільний рівень теоретичних

знань та практичних навичок. Виконано аналіз стану питання та нормативно-правової бази, поставлено завдання. На основі цих відомостей виконано обстеження об’єкта інформаційної діяльності, проведено аналіз загроз та вразливостей, розроблено політики безпеки для підприємства.

Практична цінність роботи полягає в розробці політики безпеки та підтвердження доцільності її введення техніко-економічними методами.

До недоліків слід віднести недостатньо глибоке виконання обстеження об’єкта інформаційної діяльності.

Кваліфікаційна робота задовольняє вимогам. Автор Каркан Анастасія Володимирівна заслуговує на оцінку «задовільно» та присвоєння їй кваліфікації фахівця із організації інформаційної безпеки.

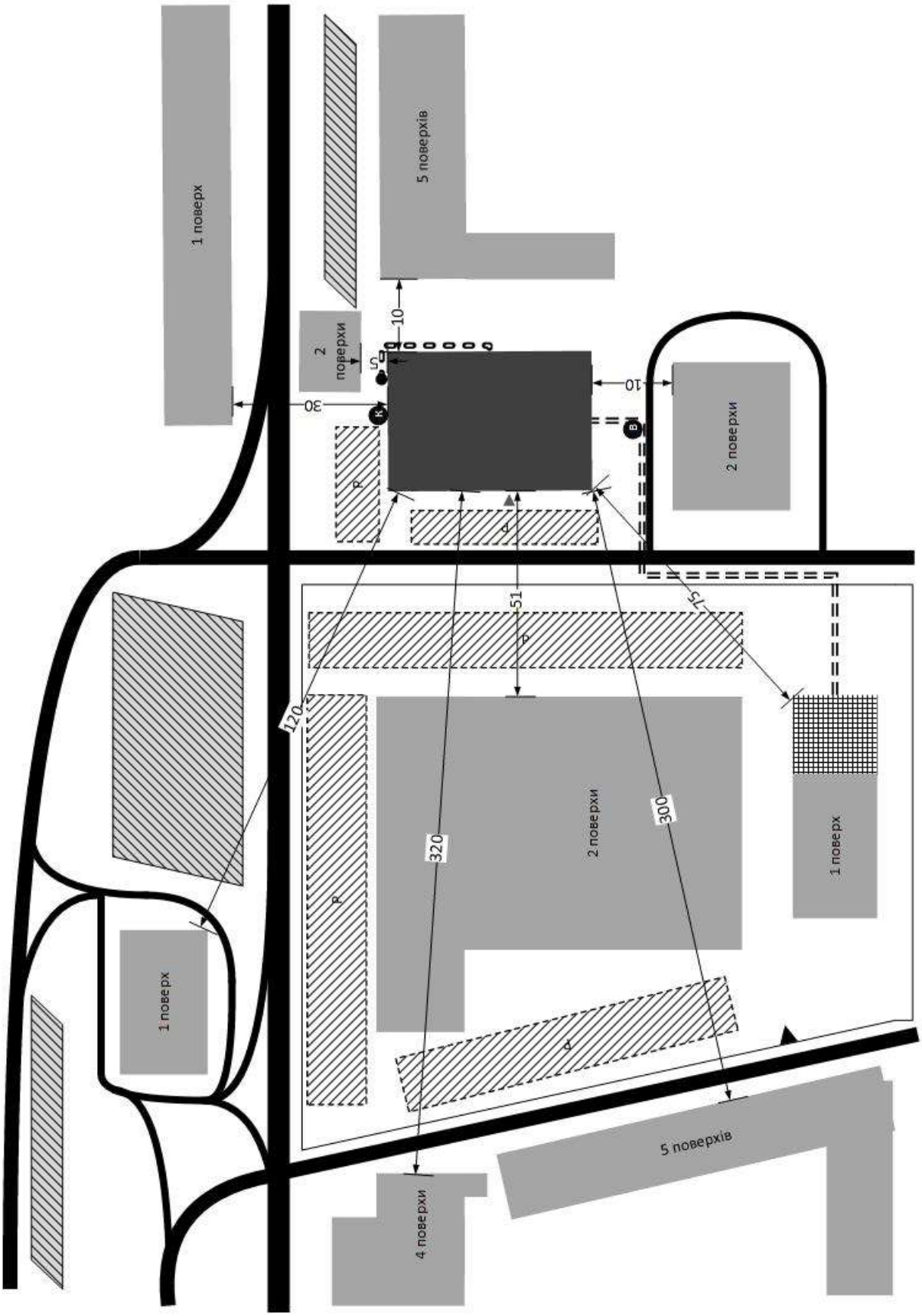
Керівник кваліфікаційної роботи к.т.н., доц. Герасіна О.В.

Дата: _____ Підпис: _____

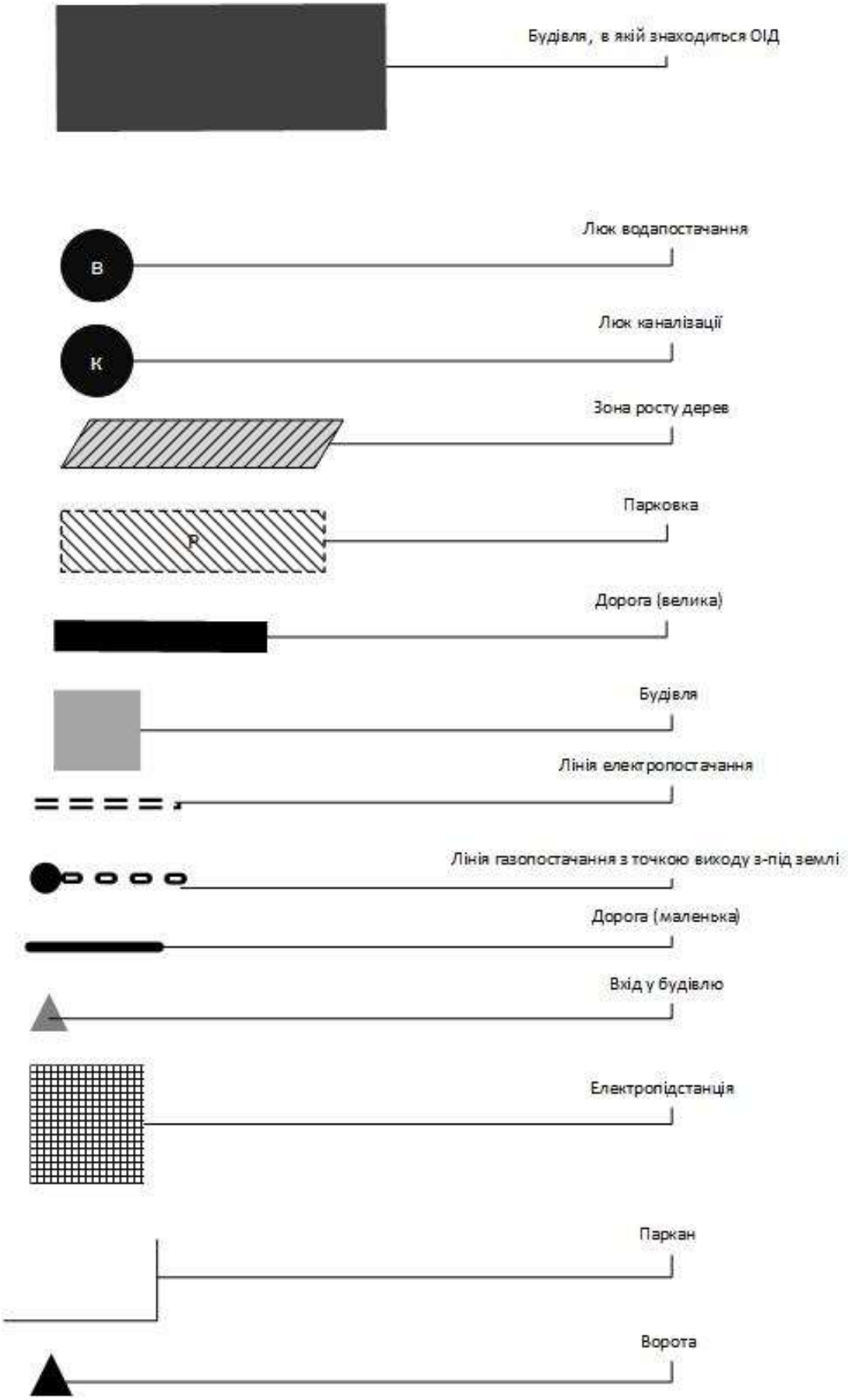
Керівник спеціальної частини ас. каф. БІТ Чебаненко О.В.

Дата: _____ Підпис: _____

ДОДАТОК Д. Ситуаційний план ОІД

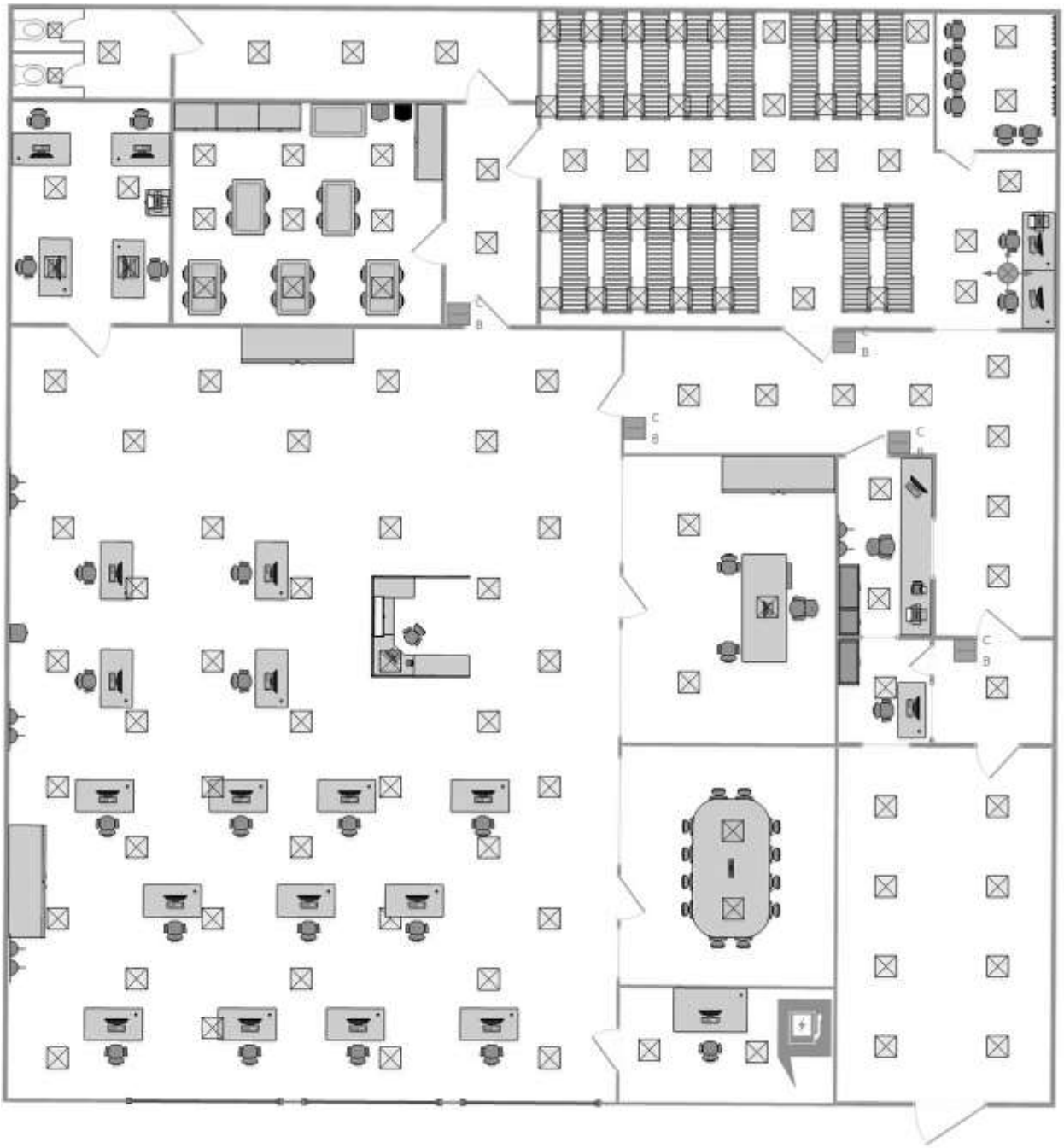


Умовні позначення до ситуаційного плану ОІД:

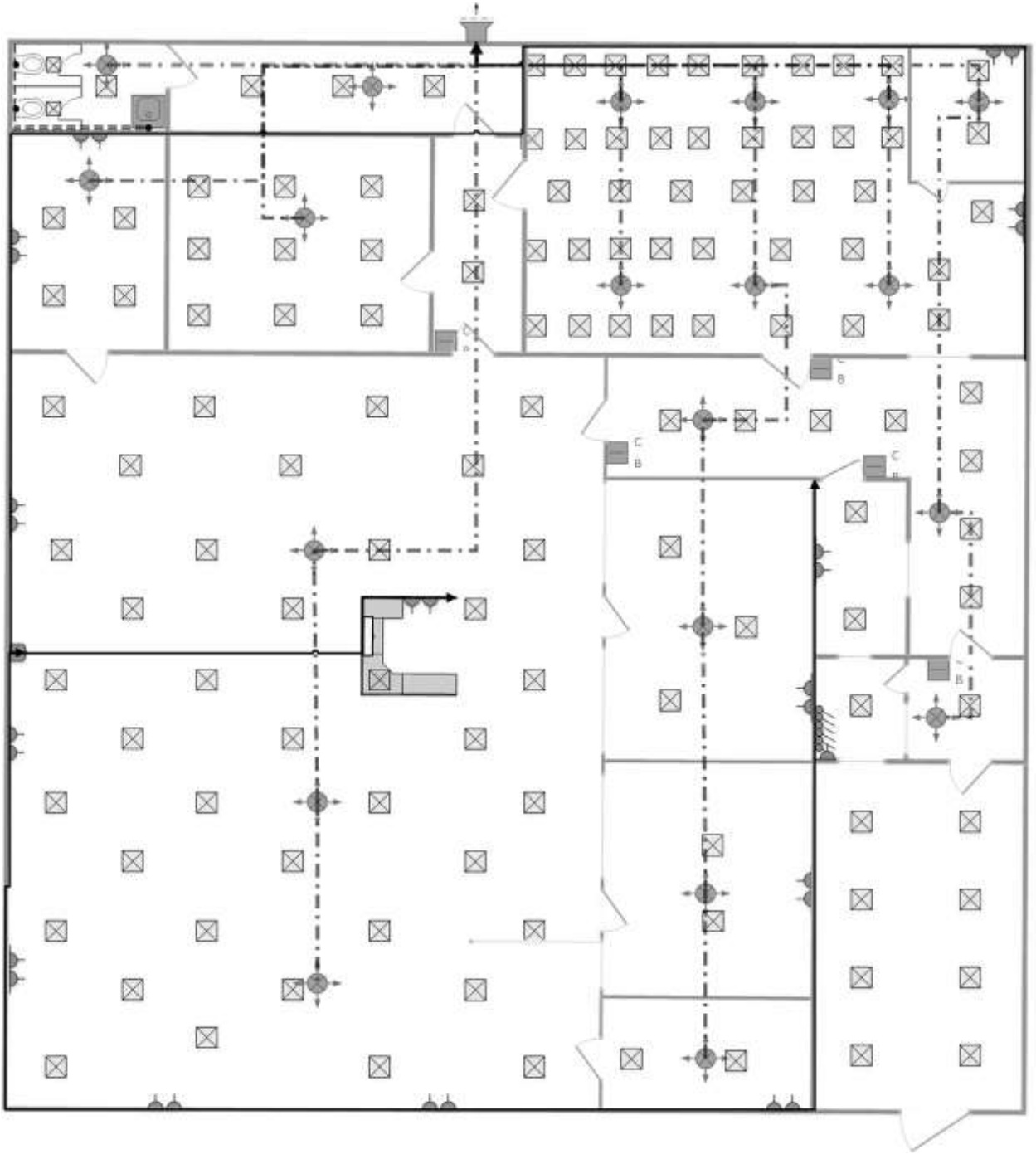


ДОДАТОК Ж. Генеральний план та план комунікацій ОІД

Генеральний план ОІД:



План комунікацій ОІД:



Умовні позначення до генерального плану і плану комунікацій: