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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Скрипніка Андрія Валерійовича*

академічної групи *125-17-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Політика безпеки в інформаційно-телекомунікаційній системі комунального підприємства ТОВ "Експрес Україна"*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	доц. Горєв В.М.			
розділів:				
спеціальний	ст. викл. Святошенко В.О.			
економічний	к.е.н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викл. Тимофєєв Д.С.			

Дніпро
2021

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту *Скрипніка Андрія Валерійовича* **академічної групи** *125-17-2*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

на тему *Політика безпеки в інформаційно-телекомунікаційній системі комунального підприємства ТОВ "Експрес Україна"*

Затверджену наказом ректора НТУ «Дніпровська політехніка» від 07.06.21 № 317-С

Розділ	Зміст	Термін виконання
Розділ 1	Стан питання. Необхідні умови для створення КСЗІ. Постановка задачі	25.04.2021 2.05.2021
Розділ 2	Обстеження об'єкта інформаційної діяльності, аналіз інформаційних потоків на підприємстві, розробка та технічна реалізація політики безпеки	4.05.2021 24.05.2021
Розділ 3	Визначення економічно-технічної доцільності політики безпеки, розрахунки витрат впровадження політики безпеки	25.05.2021 01.06.2021

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

Дата видачі завдання: _____

Дата подання до екзаменаційної комісії: _____

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

РЕФЕРАТ

Пояснювальна записка: 73 сторінки, 7 рисунків, 13 таблиць, 5 додатків, 12 джерел.

Об’єкт дослідження: інформаційно-телекомунікаційна система захисту інформації ТОВ “Експрес Україна”.

Мета проєкту: підвищення рівня безпеки інформації в інформаційно-телекомунікаційній системі (ІТС) підприємства ТОВ ”Експрес Україна”.

У першому розділі знаходиться інформація про стан інформаційної безпеки в Україні та світі. Також надані необхідні умови для створення КСЗІ.

Другий розділ вміщує в себе технічну частину питання. Визначення необхідності реалізації політики безпеки для підприємства. Проведено обстеження ОІД. Також проводиться створення політики безпеки та її технічна реалізація.

Третій розділ має інформацію про економічну частину питання, економічну ефективність елементів створеної політики безпеки на об’єкті інформаційної діяльності.

Практичне значення роботи полягає у підвищенні безпеки інформації за допомогою розробленої політики безпеки для підприємства ТОВ ”Експрес Україна”.

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, МОДЕЛЬ ПОРУШНИКА, ІНФОРМАЦІЙНА БЕЗПЕКА, ПОЛІТИКА БЕЗПЕКИ, МОДЕЛЬ ЗАГРОЗ

РЕФЕРАТ

Пояснительная записка: 73 страницы, 7 рисунков, 13 таблиц, 5 приложений, 12 источников.

Объект исследования: информационно-телекоммуникационная система защиты информации ООО "Экспресс Украина".

Цель проекту: Повышение уровня безопасности информации в информационно-телекоммуникационной системе (ИТС) предприятия ООО "Экспресс Украина".

В первом разделе находится информация о состоянии информационной безопасности в Украине и мире. Также предоставлены необходимые условия для создания КСЗИ.

Второй раздел включает в себя техническую часть вопроса. Определение необходимости реализации политики безопасности для предприятия. Проведено обследование ОИД. Также проводится создания политики безопасности и ее техническая реализация.

Третий раздел содержит информацию об экономической часть вопроса, экономическую эффективность элементов созданной политики безопасности на объекте информационной деятельности.

Практическое значение работы заключается в повышение безопасности информации с помощью разработанной политики безопасности для предприятия ООО "Экспресс Украина".

КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ, МОДЕЛЬ НАРУШИТЕЛЯ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПОЛИТИКА БЕЗОПАСНОСТИ, МОДЕЛЬ УГРОЗ

ABSTRACT

Explanatory note: 73 pages, 7 drawings, 13 tables, 5 appendices, 12 sources.

Object of research: information and telecommunication system of information security LLC "Express Ukraine".

Purpose of the project: Increase the level of information security in the information and telecommunication system (ITS) of the company "Express Ukraine".

The first section contains information on the state of information security in Ukraine and the world. The necessary conditions for the establishment of CIPS are also provided.

The second section contains the technical part of the question. Determining the need to implement a security policy for the enterprise. A survey of IAO was conducted. A security policy and its technical implementation are also being developed.

The third section has information about the economic part of the issue, the economic efficiency of the elements of the security policy created at the object of information activities.

Practical significance of the work Is to increase the security of information with the help of the developed security policy for the company LLC "Express Ukraine".

COMPREHENSIVE INFORMATION PROTECTION SYSTEM, VIOLER MODEL, INFORMATION SECURITY, SECURITY POLICY, MODEL OF THREATS, INFORMATION ACTIVITY OBJECT

ЗМІСТ с.

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

АС – автоматизована система;

ІТС – інформаційно-телекомунікаційна система;

СЗІ – служба захисту інформації;

ІзОД – інформація з обмеженим доступом;

ІБ – інформаційна безпека;

ТОВ – товариство з обмеженою відповідальністю;

ДСТУ – державний стандарт України;

КС – комп'ютерна система;

КЗ – контрольована зона;

КЗЗ – комплекс засобів захисту;

КСЗІ – комплексна система захисту інформації;

НД – нормативний документ;

НД ТЗІ – нормативний документ системи технічного захисту інформації;

НСД – несанкціонований доступ;

ОС – обчислювальна система;

ОІД – об'єкт інформаційної діяльності;

ПЗ – програмне забезпечення.

ВСТУП

У наш час складно уявити світ без інформаційних технологій. Для нормального функціювання кожної галузі зараз використовується багато різного програмного забезпечення (ПЗ). Україна також не залишилась в сторонці та дуже швидко розвивається у цьому напряму. У поточному році прогнозується 3,4 % зростання світового IT-ринку. В результаті, його обсяг досягне майже 3,9 трл доларів. При цьому найбільше збільшення витрат очікується в сегменті програмного забезпечення корпоративного класу - плюс 10,5 %.

Особливо тема про КСЗІ актуальна у наш час. Постійне вдосконалення систем захисту цікава не тільки підприємствам, а також його клієнтам. Бо, любе викрадення або знищення інформації з підприємства може використовуватися для різних маніпуляцій, котрі наддадуть великої шкоди як репутації підприємства, так і фінансовому стану компанії та її клієнтів.

Тому головною ідеєю являє собою створення гарного захисту, для надійності роботи інформаційних систем та зовнішніх інформаційних ресурсів в мережі Інтернет.

Висновок с цього вступу наступний: якою б не була відома компанія/підприємство, без комплексу технічного захисту неможливе існування цієї компанії в цілому. Тому у майже кожній країні світу існують органи котрі займаються питанням захисту інформації. Які існують для покращення роботи всіх галузей у цьому підприємстві і позитивно впливають на економічний стан.

Нижче буде розбір компанії ТОВ ”Експрес Україна”, розглянута її життєдіяльність з точки зору підприємства. З урахуванням усіх вразливостей, буде розроблено комплекс технічного захисту для ІТС. А також буде зроблено висновки зі зробленої роботи.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

Важливість інформаційних технологій у наш час набуває ще більшого сенсу кожний день, бо кожна людина з ними зараз тісно пов’язана. По всьому світу різні підприємства витрачають дуже багато коштів на забезпечення інформаційної безпеки, це зумовлено тим що, кіберзлочинність дуже сильно зростає у наш час. Особливо це можливо побачити у наш час, а саме у час всесвітньої пандемії, тому чимало підприємств страждає від різного роду кіберзлочинів і несуть великих фінансових втрат по всьому світу. Незважаючи на віртуальність злочинів [1], збиток вони завдають цілком справжній. За деякими оцінками експертів, через кіберзлочинців щорічно світова економіка втрачає $ 114 млрд. А США оцінили свої збитки за всі роки існування глобальної мережі у $ 400 млрд. Це у три рази більше щорічних витрат на освіту. Превентивні заходи вже не допомагають, і з кожним роком шкода збільшується, а злочини стають все більш "вишуканими".

На сучасному етапі розвитку України особливої уваги потребує система кібернетичної безпеки як ключовий елемент інформаційної, так і національної безпеки, бо вони тісно пов’язані. За останніми опублікованими даними, якщо порівнювати результати з минулим роком, в Україні за останні 4 місяці, кількість кіберзлочинів зросла на 25%, а це приблизно 1100 інцидентів. Але, однією з головних проблем, чому злочини в сфері IT-технологій мають низький рівень розкриття, є те, що людям не вистачає спеціальних знань у боротьбі з кіберзлочинністю. У зв’язку з тим, що бурхливий розвиток комп’ютерної техніки та телекомунікаційних мереж вимагають постійного оновлення та доопрацьовування. Кожного року змінюються формати даних, операційні системи, протоколи і середовище перенесення даних, технічні засоби, що забезпечують процес передання інформації тощо.

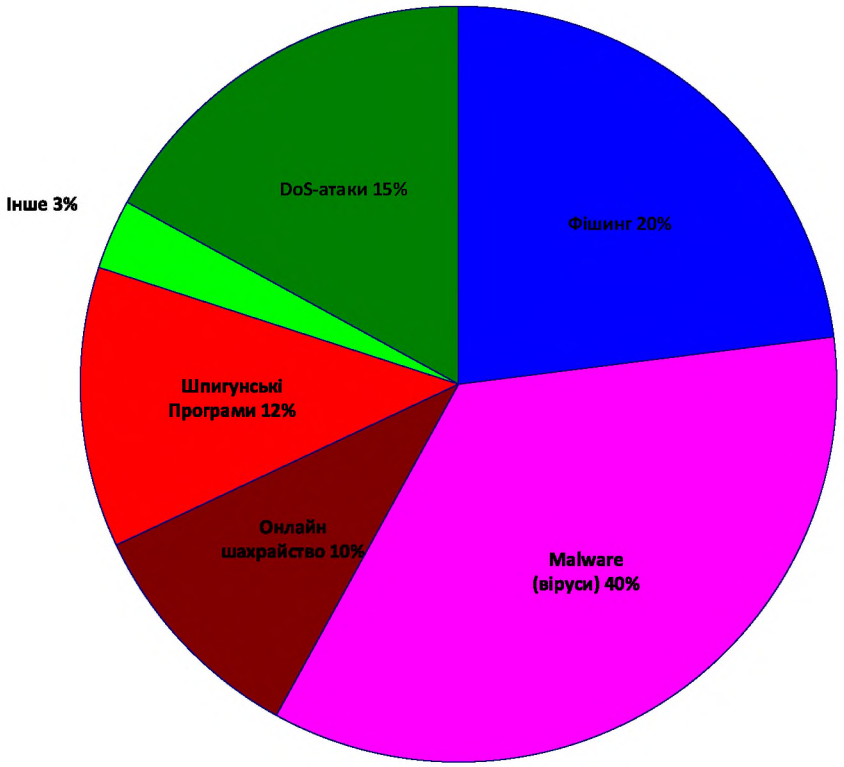


Рисунок 1.1 - Основні види кіберзлочинів в Україні

На рисунку 1.1 зазначені основні види кіберзлочинів в Україні у наші дні. За останні пів року зросла активність DoS-атак в Україні. За статистикою департаменту кіберполіції [2], основні види кіберзлочинів на сьогоднішній день наступні: незаконний доступ, незаконне перехоплення, втручання у дані, зловживання пристроями, шахрайство, пов’язане із комп’ютерами. Кількість кіберзлочинів в Україні щороку зростає на кілька тисяч. Найпоширеніший вид злочину – це шахрайство в мережі інтернет. Шахрайство, як правило, вчиняється з території України. Якщо злочини із використанням шкідливого програмного забезпечення, D-Dos атаки, спам, перекручення інформації, втручання в систему, то тут вже злочинцями можуть бути з усього світу.

Кіберзлочинці також використовують в своїх інтересах пандемію коронавірусу для активізації своєї діяльності не тільки в Україні, но і на всій території ЄС. Замість того, щоб винаходити нові схеми, кіберзлочинці адаптували традиційні фішингові шахрайські розсилки, пов'язуючи їх з коронавірусом. Ризик кіберзлочинності посилюється ще тому, що мільйони

людей працюють віддалено з дому. Деякі з кібератак були ретельно скоординовані, націлені на критично важливу інфраструктуру.

Сьогодні у світі спостерігається постійне збільшення кількості співробітників, які не прив'язані до офісу. З переходом бізнесу в онлайн, активізувалася кіберзлочинність, а витік інформації призводить до суттєвих фінансових та репутаційних втрат.

Тому для захисту від витоку різних типів інформації має бути розроблена комплексна система захисту інформації (далі - КСЗІ), а також політика безпеки інформації підприємства.

В той же час, ефективний захист інформації неможливий без працівників компанії, які являються ключовим ресурсом для прибутковості будь-якої компанії. Працівники, що відповідають за цілісність інформації, мають найважливішу роль у досяганні мети ефективного функціювання підприємства. Цю групу працівників, зазвичай, відносять до підрозділу Служби захисту інформації (далі - СЗІ). До її обов'язків входять:

– забезпечення виконання в автоматизованій системі (далі - АС) послуг конфіденційності, цілісності та доступності інформації, що циркулює в АС;

– дослідження технології обробки інформації в АС з метою виявлення можливих каналів її витоку та інших загроз для безпеки інформації, розробку та внесення змін до моделі загроз;

– дотримання вимог політики безпеки інформації на підприємстві, проведення заходів, спрямованих на реалізацію політики;

– організація та координація робіт, пов'язаних із захистом інформації в АС, підтримка необхідного рівня захищеності інформації, ресурсів і технологій;

– розроблення нормативних і розпорядчих документів, чинних у межах АС, згідно з якими повинен забезпечуватися захист інформації в АС;

– організація та участь у проєктах зі створення та подальшого використання КСЗІ на всіх етапах життєвого циклу АС;

– участь в організації професійної підготовки та підвищенні кваліфікації персоналу АС, донесення до користувачів функціональних підсистем АС базових знань з питань захисту інформації;

– формування у персоналу підприємства та користувачів автоматизованих систем розуміння необхідності виконання вимог нормативно-правових актів, нормативних та розпорядчих документів АС, що стосуються сфери захисту інформації;

– проведення профілактичних заходів, спрямованих на попередження та виявлення загроз інформаційним ресурсам АС;

– забезпечення та контроль виконання персоналом і користувачами вимог нормативно-правових актів, нормативних і розпорядчих документів із захисту інформації АС.

Враховуючи перелічене вище, метою цієї роботи є визначення вразливостей в інформаційній системі ОІД, що стане фундаментом для складання і реалізації додаткових політик безпеки існуючого програмного забезпечення та функцій підприємства ТОВ “Експрес Україна”.

1.2 Необхідні умови для створення КСЗІ

Для створювання КСЗІ в інформаційно-телекомунікаційну систему (далі - ІТС), потрібно використовувати рекомендації щодо його створення. До складу КСЗІ входять заходи та засоби, які реалізують механізми захисту інформації від несанкціонованих дій та несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав’язування хибної інформації, застосування закладних пристроїв чи програм, використання комп’ютерних вірусів та інші можливі загрози. Взагалі створення КСЗІ на об’єкті можна поділити на 5 основних етапів:

– формування загальних вимог до КСЗІ в ІТС;

– розробка політики безпеки інформації в ІТС;

– розробка технічного завдання на створення КСЗІ;

– розробка КСЗІ;

– введення КСЗІ до дії та подальша оцінка захищеності інформації.

Дозволяється комбінувати деякі етапи, а також включати нові етапи робіт. За необхідністю можлива зміна послідовності виконання окремих етапів або виконання одночасно декілька етапів робіт. Окремі етапи потрібно виконувати до завершення попередніх, якщо це не призводить до зниження якості зробленої роботи і не суперечить цілям їх виконання.

1.3 Висновок

Тепер, коли ми розглянули загальний перелік загроз, можна приступати до технічного опису заходів по їх усуненню або мінімізації. Маючи всю інформацію, що була зазначена у попередніх пунктах, а точніше після повного аналізу, обстеження та виявлення усіх можливих загроз, можна починати розробляти КТЗ підприємства.

Тобто, на даному етапі моя задача являє собою розробку та обстеження політики безпеки підприємства ТОВ “Експрес Україна” та технічно правильна реалізація її на ОІД.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Повні відомості про підприємство

Підприємство ТОВ “Експрес Україна” займається відправкою та прийманням посилок по всій Україні та поза її межами. Головний офіс обстеження знаходиться за адресою: проспект Перемоги, 28, місто Запоріжжя, на 3 різних поверхах та в двох суміжних будівлях (далі буде аналізуватись лише 3 поверх будівлі). Компанія була створена ще у 1997 році, та має гарну довіру серед її клієнтів. Тому для нормального функціювання цієї компанії, потрібен якісний та надійний захист від усіх видів витоку інформації. Це має дуже важливу роль, через те що клієнти довіряють цій компанії і користуються її послугами кожний день.

Деякі данні про підприємство були змінені задля конфіденційності.

Характеристика підприємства:

Офіс компанії займає 3 різні поверхи та знаходиться в двох суміжних будівлях.

Адреса: проспект Перемоги 28, Запоріжжя, Запорізька область, 69005

Часи роботи:

понеділок-п'ятниця: 7:30 - 20:00

субота: 7:30 - 18:00

Обідня перерва: з 12:00 до 12:45

Робочі дні: понеділок – субота.

2.2 Об’єкт інформаційної діяльності

Об'єкти, на яких здійснюватиметься обробка технічними засобами та/або озвучуватиметься інформація з обмеженим доступом, що не становить державної таємниці, підлягають обов'язковому категоріюванню. Далі буде зазначено категоріювання на об’єкті відповідно до НД ТЗІ 1.6-005-2013 [3]:

– 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 ОІД;

– 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 III категорія;

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

2.3 Основні критерії обстеження ОІД

Для розробки КСЗІ, потрібно повністю обстежити ОІД. На початку всіх робіт необхідно, щоб директор підприємства затвердив наказ на створення КТЗ, так як він являється власником інформації.

Для того, щоб правильно обстежити ОІД, потрібно детально проаналізувати наступні речі:

– загальні структури та схеми (потрібно перелічити обладнання, технічні та програмні засоби, врахувати всі використані технології, що використовуються на ОІД, тощо;

– потрібно враховувати всі взаємодії окремих компонентів;

– перелічити всі види каналів зв'язку та вказати їх характеристики;

– врахувати всі можливі обмеження щодо використання різних засобів.

Також бажано не забути виявити всі компоненти, які містять або навпаки, не містять в собі спеціальних механізмів захисту інформації.

Метою такого аналізу є складання повної картини захищеності об'єкта, задля виявлення слабких та вразливих місць в системі захисту та подальшого посилення/захисту цих проблемних міст.

По завершенні цього обстеження, наступає черга обстеження фізичного середовища. При цьому аналізується розміщення усіх об'єктів на ОІД (об'єкти інформаційної діяльності, системи зв'язку тощо). Також потрібно не забувати про режим функціонування цих об'єктів.

Наступні об'єкти попадають під аналіз фізичного середовища:

– територіальне розміщення компонентів ОІД (генеральні плани);

– перевірка наявності перепускного режиму;

– перелік режимів доступу до об'єктів на ОІД;

– перевірка всіх систем, які виходять за межі ОІД;

– проводиться обстеження умов зберігання оптико-магнітних, паперових та інших носіїв інформації;

– перевіряються повноваження та рівень можливостей кожного користувача щодо управління КТЗ.

Тільки після цього починається пошук вразливостей на обстеження ОІД та проводиться реалізація вищеназваних пунктів до ІТС підприємства.

2.4 Розташування об'єкту та його пропускний режим

З усіх сторін КЗ обмежена зовнішніми стінами будівлі. Вхід до самого підприємства проходить через пункт охорони на першому поверсі. Для входу кожний співробітник використовує перепустку – друковану картку допуску на підприємство, яку потрібно пред'являти охороннику. До самої території доступ здійснюється через сходи, або через ліфт на 2 поверсі. Охорону здійснює наймана охоронна фірма, яка надає аутсорсингові послуги 24 години на добу, 7 днів на тиждень. До обов'язків охорони входять:

– організація перепускного режиму;
– цілодобовий контроль за територією підприємства;
– реагування на різні інциденти на об'єкті.

Далі на рисунку 2.1 зазначено положення об'єкту інформаційної діяльності (ОІД) відносно інших будівель на місцевості, для подальшого аналізу різних можливостей витоку інформації, також в таблиці 2.1 зазначені назви та характеристики прилеглих будівель.

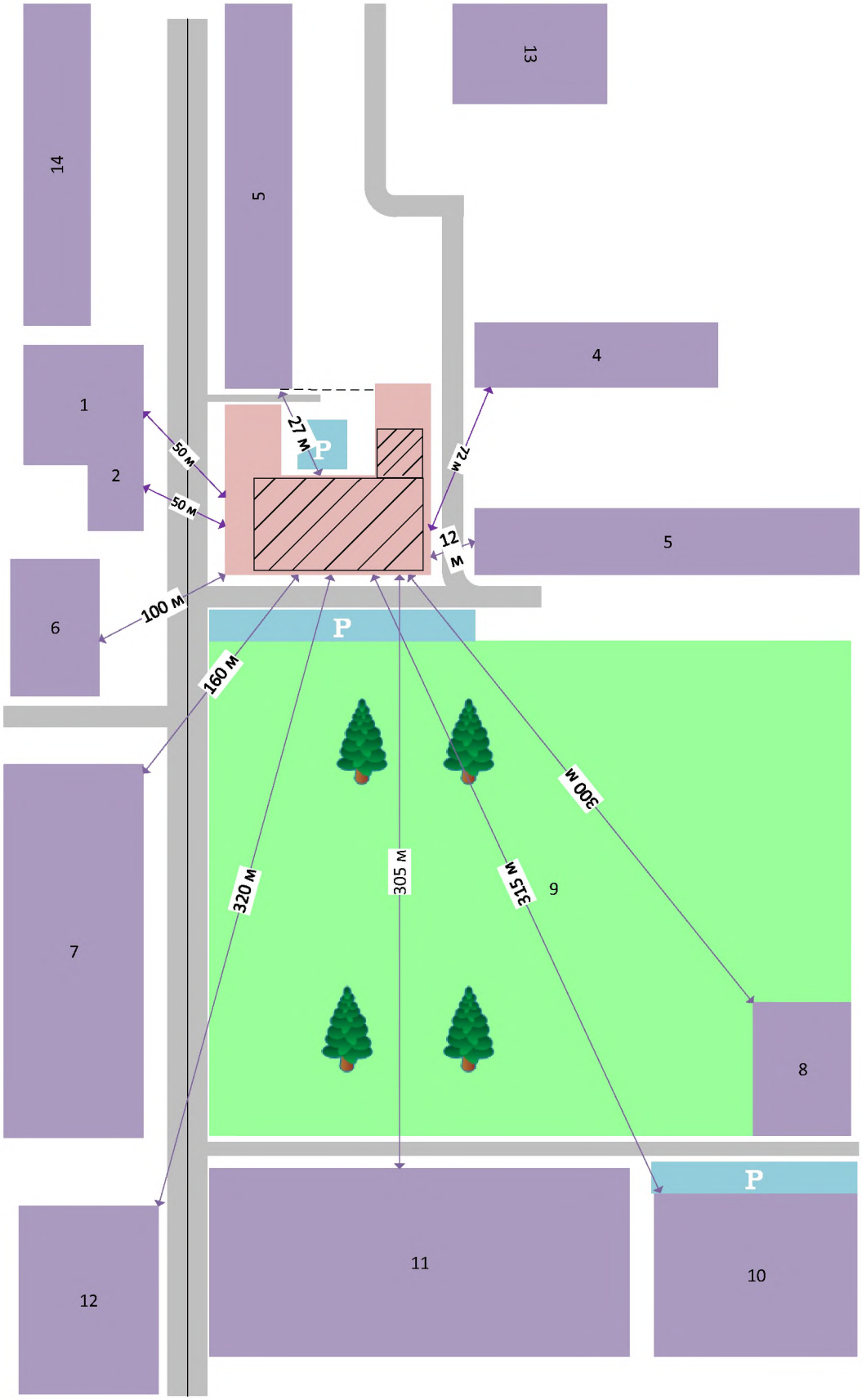
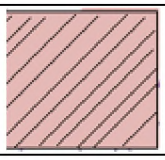


Рисунок 2.1 - Ситуаційний план підприємства з умовними позначеннями

Таблиця умовних позначень до рисунку 2.1

	масив дерев
	центральна дорога (двосторонній рух)
	будівля прилегла до ОІД
	парковка
	паркан
	будівля, де знаходиться ОІД
	межа КЗ

Таблиця 2.1 - Опис будівель, прилеглих до ОІД

Назва будівлі	Короткий опис	Адреса
EcoTower	1 поверх Кафе Monkey Pizza&Bar, 2-18 поверхи бізнес офісів	проспект Перемоги 32, Запоріжжя, Запорізька область, 69005
УкрСібБанк (прибудова до EcoTower)	1 поверх Банк, 2-3 поверх Кафе Coffeelab Tower Bar	проспект Перемоги 32, Запоріжжя, Запорізька область, 69005
Жила будівля	5 поверхів, 1 поверх різні магазини, 2-5 житлові поверхи	проспект Перемоги 30, Запоріжжя, Запорізька область, 69005
Infinity	1 поверх Комп'ютерний клуб	вулиця Шевченко 1Б, Запоріжжя, Запорізька область, 69005
Житлова будівля	1 поверх – різні магазини та кафе, 2-9 житлові поверхи	вулиця Шевченко 3, Запоріжжя, Запорізька область, 69005
Байда	1-2 поверх Кінотеатр	проспект Перемоги 33, Запоріжжя, Запорізька область, 69005

Продовження таблиці 2.1

Назва будівлі	Короткий опис	Адреса
Запорізька обласна державна адміністрація	7 поверхів	проспект Перемоги 34, Запоріжжя, Запорізька область, 69107
Запорізький обласний центр молоді	3 поверхи	вулиця Гусенка 39, Запоріжжя, Запорізька область, 69005
Центральний парк		вулиця Шевченко 3, Запоріжжя, Запорізька область, 69005
Житлова будівля	1 поверх торговий центр, 2-9 житлові поверхи	вулиця Шевченко 4А, Запоріжжя, Запорізька область, 69005
Intourist	1-9 поверх Готель	проспект Перемоги 21, Запоріжжя, Запорізька область, 69005
Житлова будівля	1-9 житлові поверхи	проспект Перемоги 17, Запоріжжя, Запорізька область, 69005

Продовження таблиці 2.1

Назва будівлі	Короткий опис	Адреса
Школа	3 поверхи	проспект Перемоги 21А, Запоріжжя, Запорізька область, 69005
Житлова будівля	1 поверх – різні магазини та кафе, 2-9 житлові поверхи	проспект Перемоги 31, Запоріжжя, Запорізька область, 69005

2.5 Характеристика фізичного середовища ОІД

ОІД, який обстежується, знаходиться на трьох поверхах, має 1 основний вхід та вихід, та 1 - резервний. Територія навколо відкрита і заасфальтована.

Далі визначаються характеристики будівлі, де знаходиться ОІД:

– зовнішні стіни виготовлені з цегли та бетону, товщина стін становить 40 см;

– підлога в будівлі виготовлена з бетону товщиною приблизно 12 см, у коридорах покрита кахельною плиткою;

– на вході встановлені 2 подвійні двері для входу і виходу відвідувачів та персоналу, самі двері зроблені з метало-пластику та мають розміри 4 м · 2,5 м, товщина їх складає 70 см;

– майже по всій будівлі встановленні вікна з металопластику, окрім першого поверху, де разом з металопластиковими вікнами встановлені захисні металеві грати;

Характеристика внутрішніх приміщень:

– стіни виготовлені з бетону та гіпсокартону товщиною 20 см та 10 см відповідно;

– підлога в приміщеннях виготовлена з бетонної стяжки, товщиною приблизно 10 см та покрита лінолеумом;

– міжкімнатні двері зроблені з дерева або в окремих випадках - із заліза, та мають розмір 1,3 м · 2,2 м;

– вікна зроблені с металопластику 1,5 м · 2,4 м;

У таблиці 2.2 вказано усі комунікації, які встановлені та використовуються в ОІД, для подальшого аналізу вразливостей. Також на рисунках 2.2, 2.3, 2.4 та 2,5 надані детальні генеральні плани ОІД.

Таблиця 2.2 - Комунікаційні системи та їх характеристика

Назва комунікації	Виходить за межі КЗ	Характеристика
Система опалення	Так	Централізована міська водяна, яка призначена для отримання, перенесення і передавання необхідної кількості тепла у всі приміщення, які необхідно нагрівати. Послуги надаються ТОВ «Міські теплові мережі»
Система електропостачання	Так	Централізована міська. Призначена для паралельних робіт джерел живлення і розподілу енергії у приміщенні. Послуги надаються ТОВ «Запоріжжяелектропостачання». Наявна система автономного резервного електропостачання для тимчасового живлення серверного обладнання.

Продовження таблиці 2.2

Назва комунікації	Виходить за межі КЗ	Характеристика
Система каналізації	Так	Міська система. Призначена для видалення твердих і рідких продуктів життєдіяльності людини, господарсько-побутових та дощових стічних вод. Послуги надаються ТОВ «Водоканал»
Система водопостачання	Так	Міська господарсько-питна система водопостачання для пиття, приготування їжі і проведення санітарно-гігієнічних процедур. Послуги надаються ТОВ «Водоканал»
Інтернет та телефонні лінії	Так	Інтернет послуги: - ТОВ «Інфоком»,ТОВ «Радіоком» Телефонія: - АТ «Укртелеком»
Система кондиціонування	Так	Нецентралізована. Окрема для кожного приміщення. Окрема для серверної.
Система пожежної сигналізації	Так	Система автоматичного пожежегасіння на базі приладу приймально-контрольного пожежного ПУіЗ "Тірас-1", ПУіЗ "Tiras 1X" з функцією управління автоматичним засобами протипожежного захисту
Система сигналізації	Так	Автономна охоронна сигналізація на базі ППК «Орион-2ТИ.2»

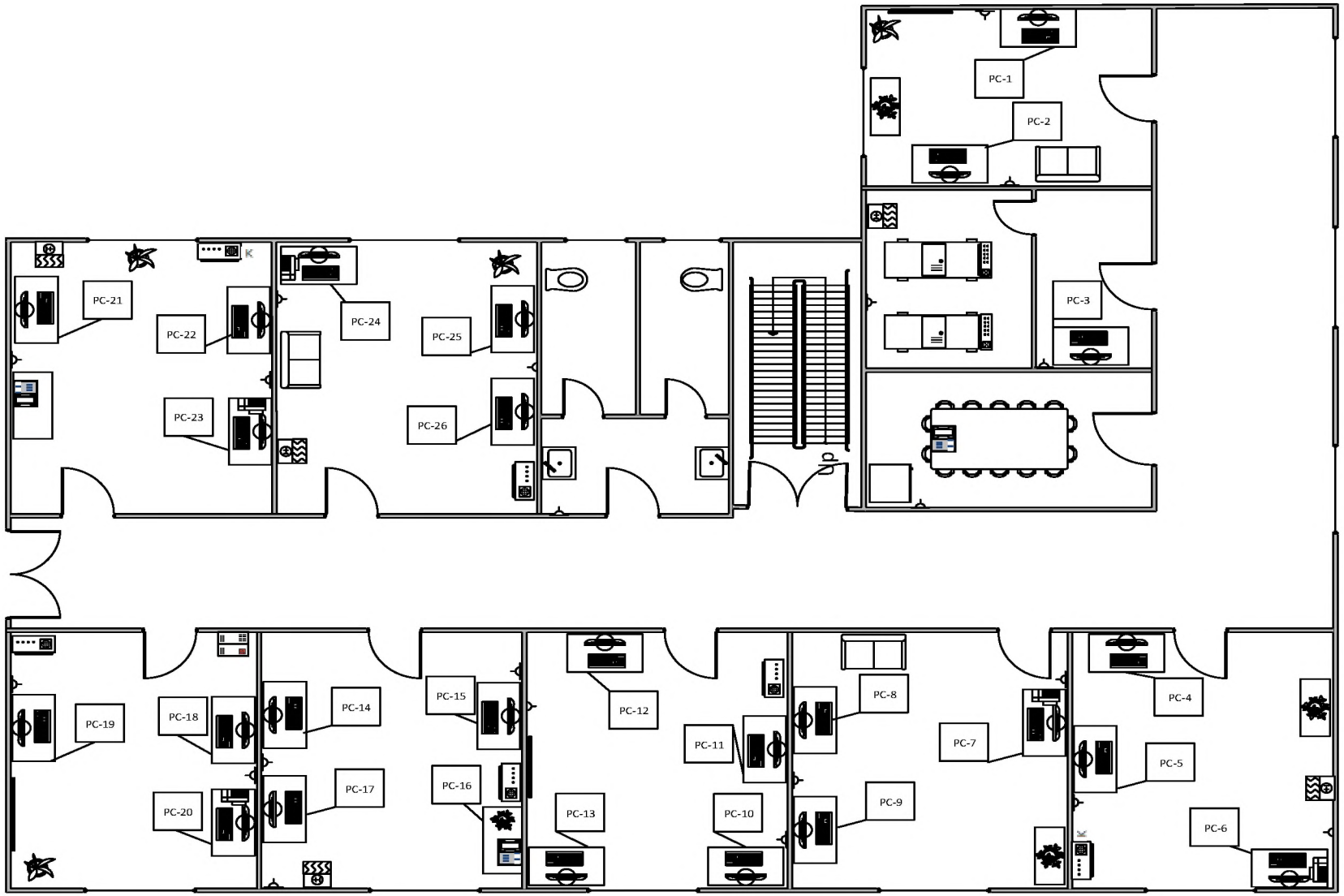
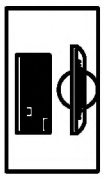
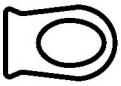
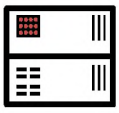
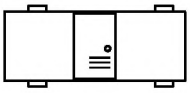
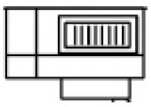


Рисунок 2.2 - Генеральний план підприємства

Таблиця умовних позначень до рисунку 2.2

Умовне позначення на плані	Значення
	Робоче місце (Настільний ПК)
	Кондиціонер
	Санвузол
	Рукомийник
	Розетка
	Електрична щитова офісу
	Некерований комутатор
	Керований комутатор
	48-Pin комутатор
	Сервер
	Принтер
	Робочий телефон

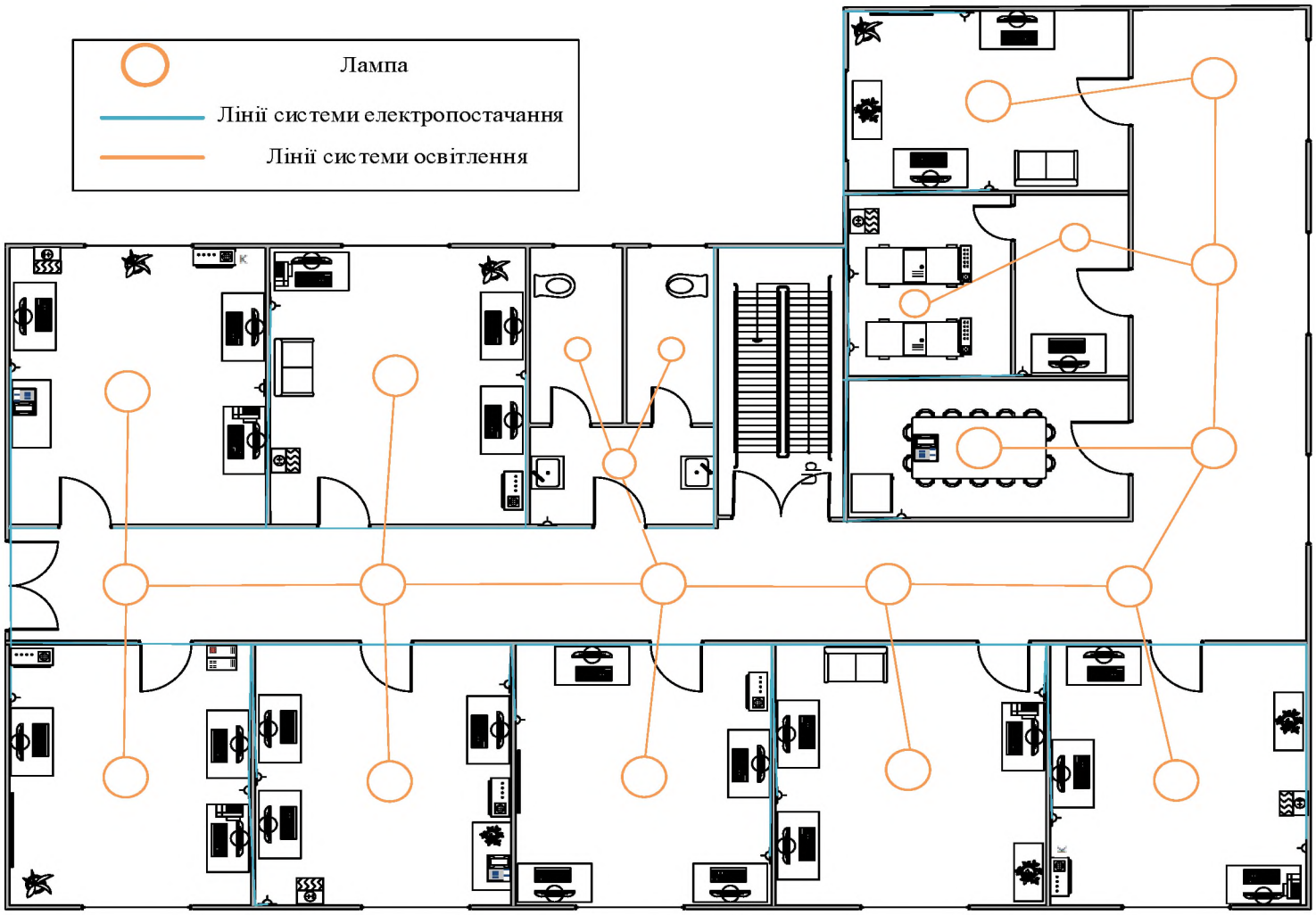


Рисунок 2.3 - Генеральний план підприємства

(Системні лінії освітлення та електропостачання)

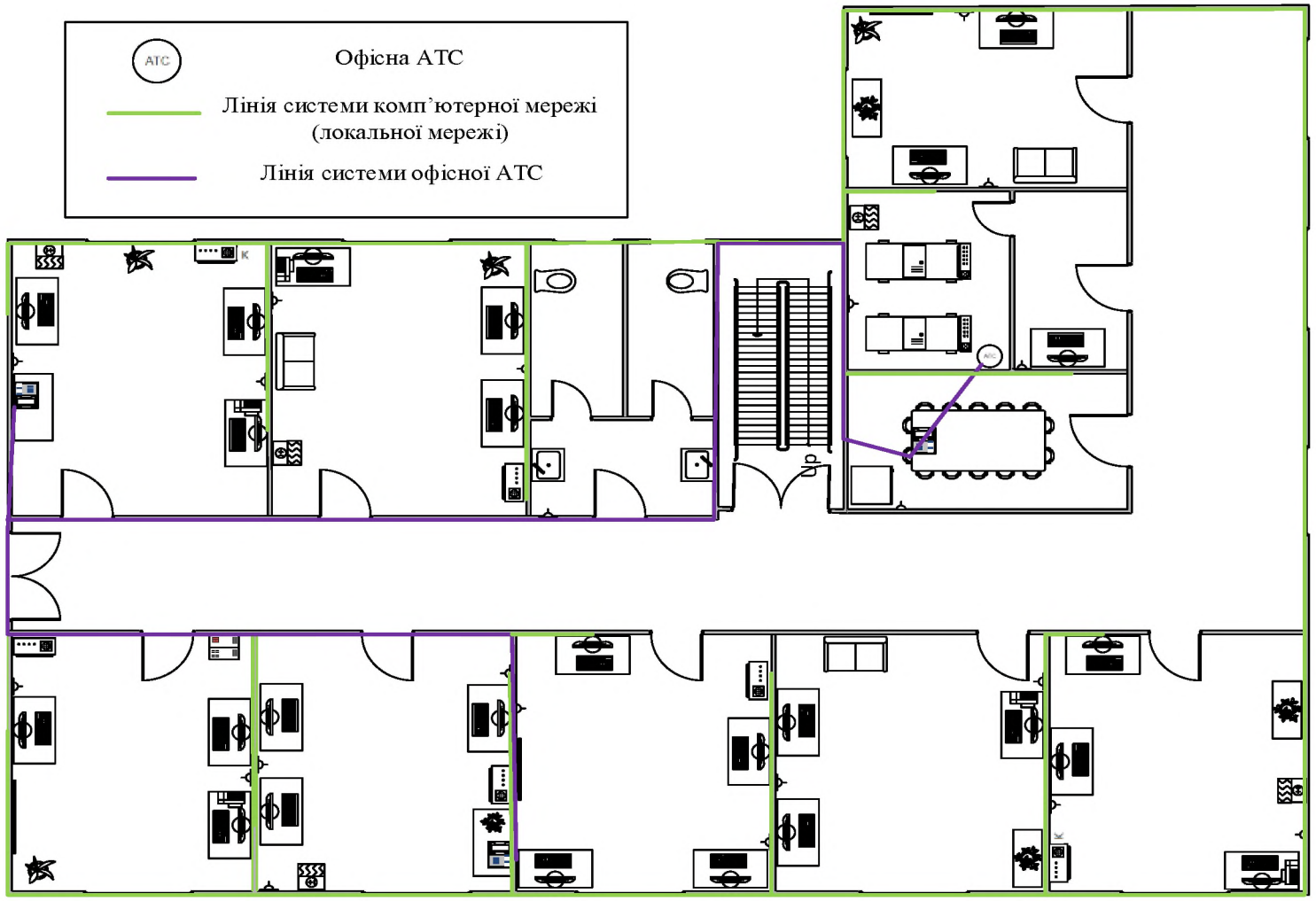


Рисунок 2.4 - Генеральний план підприємства

(Локальна мережа та канал телефонного зв'язку)

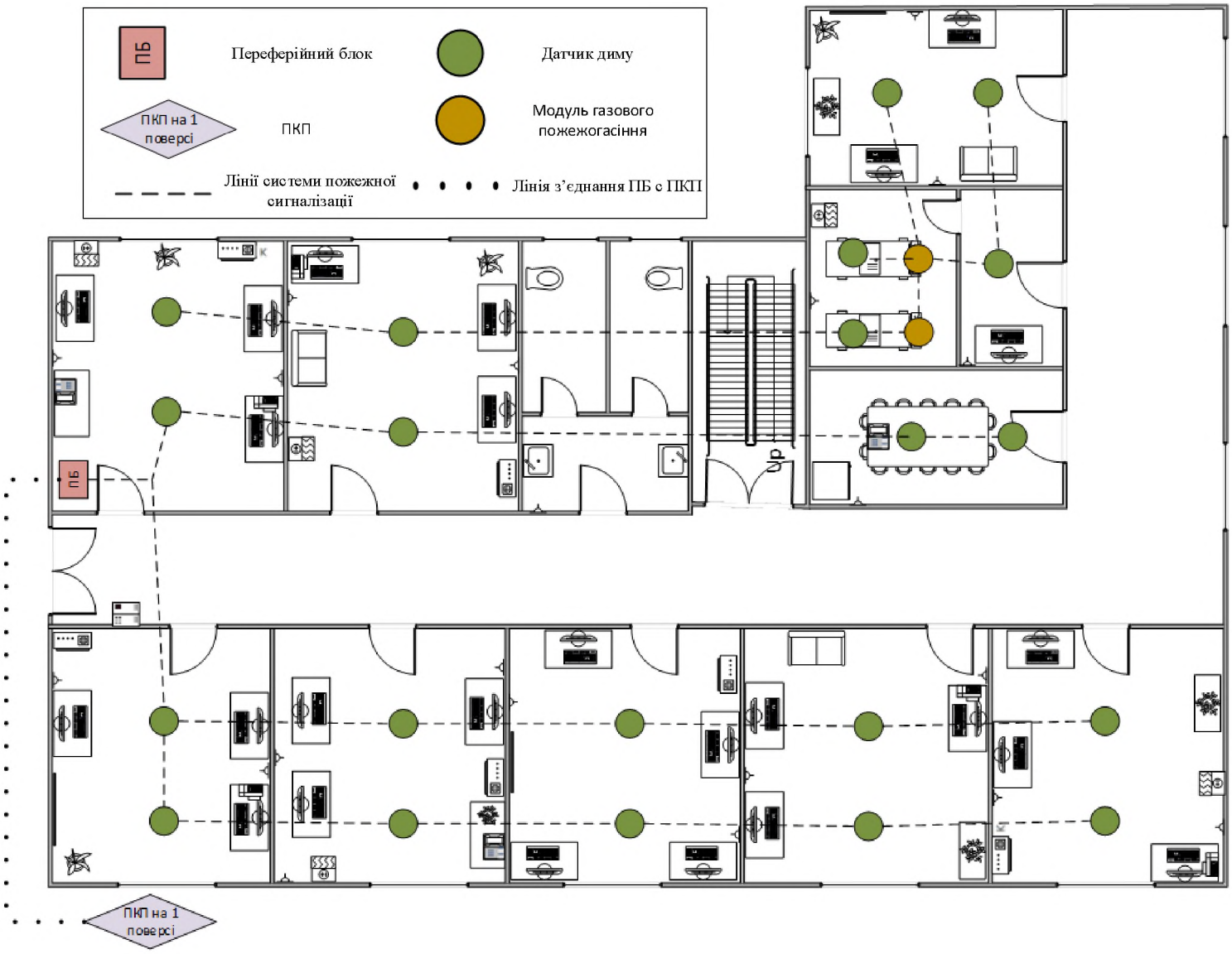


Рисунок 2.5 - Генеральний план підприємства (Лінії системи пожежної та охоронної сигналізації)

2.6 Перелік ОТЗ/ДТЗ на підприємстві

Перелік ОТЗ/ДТЗ Оперативно-технічні (програмні) засоби – це сукупність технічних та/або програмних засобів, спеціально призначених (розроблених, пристосованих, запрограмованих) для негласного одержання інформації під час оперативно-розшукової діяльності, виявлення, запобігання та припинення злочинів. До нього як правило входить:

– мережевий комплект (МК) для здійснення перехоплення телекомунікацій;

– засоби управління системою перехоплення телекомунікацій (сервери, станції, термінали та інші ЗУСП);

– засоби захищеної транспортної мережі (ЗЗТМ);

– програмне забезпечення (ПЗ) технічних засобів;

– експлуатаційна та програмна документація технічних засобів;

– комплект запасних інструментів та приладів (ЗІП).

В якості оперативно-технічних засобів використовуються спеціальні технічні пристрої та обладнання, які дозволяють знімати інформацію з каналів зв'язку, вести візуальне спостереження у громадських місцях, фіксувати дані про окремих осіб, поведінка чиїх є протиправною. Оперативно-технічні засоби можуть бути як загального користування, наприклад, фото, кіно чи відеозйомки, так і спеціального призначення - радіоприлади, оптичні пристрої, засоби проникнення, прослуховування. Будь-яке застосування оперативно-технічних засобів в оперативно-розшуковій діяльності повинно здійснюватися у чіткій відповідності до встановлених законом та відомчими нормативними актами правил.

У складі таких ОТЗ на підприємстві, зокрема на головній касі та у внутрішньому дворі, встановлена система відеоспостереження для спостереження за автотранспортом та персоналом, діючим з товарно-матеріальними цінностями та грошовими коштами. На підприємстві використовуються наступні системи відеоспостереження:

– гібридний відеорегістратор Dahua DHI-XVR5208AN-4KL-X;

– купольна HDCVI камера Dahua DH-HAC-HDBW1200RP-VF (2.8-12 мм);

– зовнішня HDCVI камера Dahua DH-IPC-HFW1120S-W 1.3 МП (3,6 мм).

Ці камері записують на HDD накопичувач відеорегістратора все, що відбувається 24 години на добу, 7 днів на тиждень, для забезпечення повного візуального контролю та моніторингу ситуації на підприємстві. До них мають доступ чергові охоронці.

Крім того, для контролю дій в комп'ютерній мережі на підприємстві використовується спеціальна система моніторингу NetFlow. Завдяки цій технології (Flexible NetFlow або скорочено FNF) та новому сервісному модулю Cisco Service вдається створити систему мережевого моніторингу і виявлення аномалій безпеки. Активація режиму FNF на комутаторі доступу гарантує отримання всіх інформаційних потоків для аналізу. Керовані мережеві комутатори є найбільш логічним та ефективним обладнанням в мережі підприємства для збору статистики і моніторингу. З технологією Netflow можливо один момент отримати MAC- адресу та інформацію про порт доступу, пов'язаного з потоком, щоб вийти безпосередньо до джерела потоку. Таким чином, включаючи опцію FNF на комутаторі доступу, можливо отримати безцінну інформацію про місцезнаходження потоку, що робить її безцінним елементом комплексу оперативно-технічних засобів.

Перед тим, як перелічити все обладнання та програмне забезпечення ОТЗ на підприємстві, визначимо структурну схему мережі зазначену на рисунку 2.6.

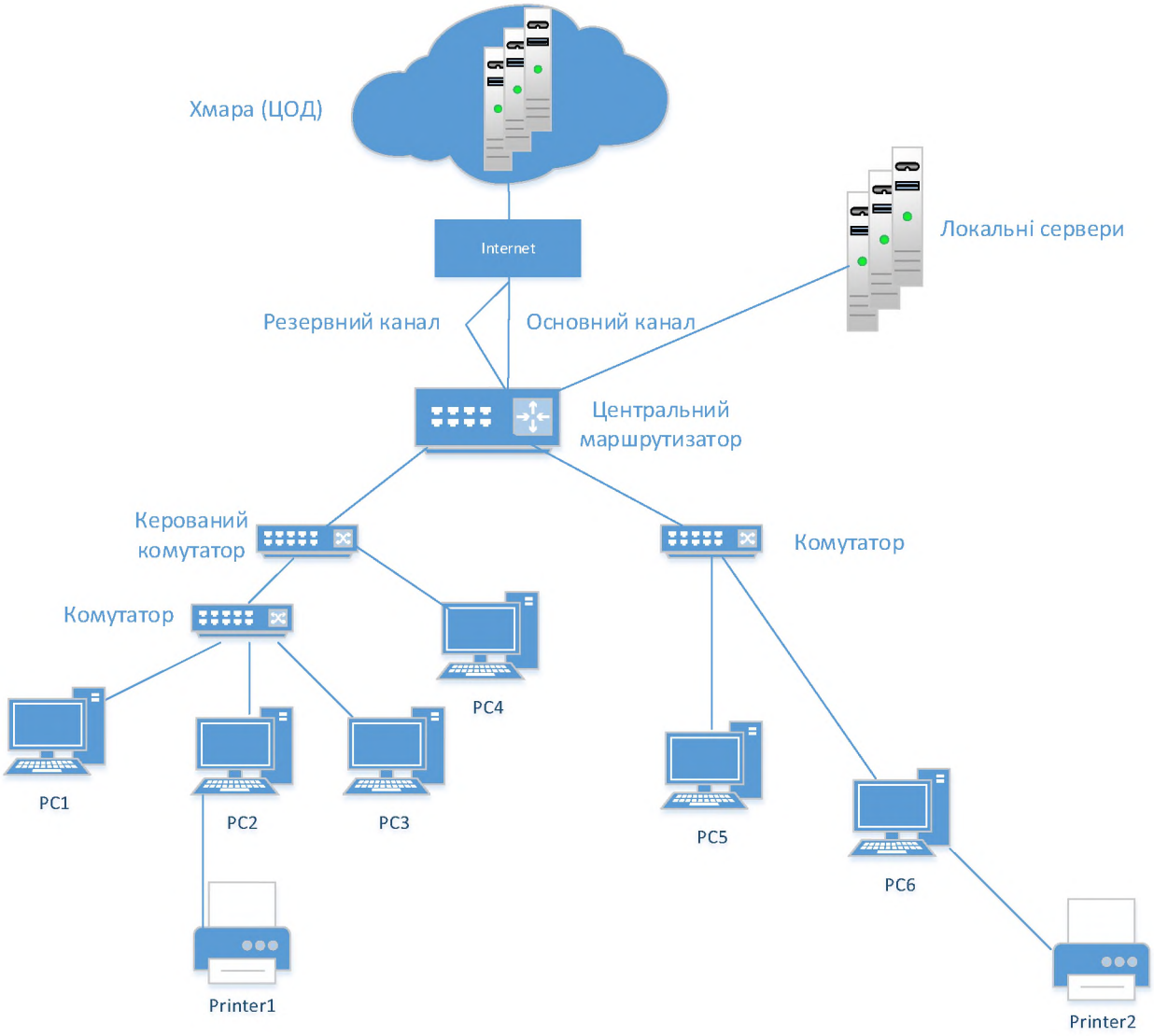


Рисунок 2.6 - Структурна схема мережі

Далі у таблицях 2.3, 2.4 та 2.5 наводиться перелік усього обладнання, ПЗ та ДТЗ, для подальшого аналізу об’єкту, а у таблиці 2.6 зазначено характеристику усього обладнання.

Таблиця 2.3 - Перелік обладнання на підприємстві

Назва обладнання	Марка	Модель	Кількість
Моноблок	HP	Pro 350	16 од.
Моноблок	Asus	Pro AiO	10 од.
PC клавіатура	Logitech	K120 USB	26 од.
PC миша	Logitech	B100 USB	26 од.
БФП (багатофункціональний пристрій)	Xerox	WorkCentre 3215NI	5 од.
Телефон	Cisco	CP-7821-K9	3 од.
Некерований комутатор	D-Link	DES-1008A	2 од.
Некерований комутатор	D-Link	DES-1016A	1 од.
Керований Комутатор	Cisco	Catalyst 3750x-48	2 од.
Керований Комутатор	Edge-core	ECS3510-28T	2 од.
Центральний маршрутизатор	Cisco	ASR 1001	1 од.
Кондиціонер	Sakata	SIH-35SA	12 од.
Кондиціонер (серверна)	Sakata	SIB-140	1 од.
ДБЖ	Mustek	PowerMust 636	26 од.

Продовження таблиці 2.3

Назва обладнання	Марка	Модель	Кількість
ДБЖ (серверна)	APC	MGE Galaxy 3500 20kVA	1 од.
ДБЖ (серверна)	Eaton	Powerware 9125 3000VA	1 од.
Система зберігання даних	EMC	DD160	1 од.
Система зберігання даних	EMC	VNXe3150	1 од.
Сервер	HP	c3000	1 од.
Сервер	HP	Proliant DL360 G6	5 од.

Таблиця 2.4 - Перелік програмного забезпечення на підприємстві

Назва ПЗ	Тип	Опис	Тип ліцензії	ПЗ встановлено
Windows 10 pro(версія 2004)	Системне	Операційна система для ПК	Ліцензія	PC1 – PC26
Microsoft Windows Server 2016	Системне	Серверна операційна система	Ліцензія	PC1 – PC26
Microsoft Office Word 2013	Прикладне	Програми для створення і редагування текстових документів	Ліцензія	PC1 – PC26
Microsoft Office Excel 2013	Прикладне	Програма позволяє виконувати роботу над даними, які знаходять в таблиці	Ліцензія	PC1 – PC26

Продовження таблиці 2.4

Назва ПЗ	Тип	Опис	Тип ліцензії	ПЗ встановлено
Google Chrome (версія 90.0.4430.212)	Прикладне	Програма для роботи в мережі Інтернет	Freeware	PC1 – PC26
Adobe Acrobat Reader (версія 2021.001.20155)	Прикладне	Програма для перегляду і друку pdf-файлів	Ліцензія	PC1 – PC26
7-zip (версія 19.00)	Системне	Архіватор файлів	Freeware	PC1 – PC26
Microsoft Outlook (версія 15)	Прикладне	Програма для використання електронної пошти	Ліцензія	PC1 – PC26
Microsoft Visio 2013	Прикладне	Програма для побудови планів	Ліцензія	PC1, PC2, PC5, PC6, PC7
Skype for Busines	Прикладне	Бізнес месенджер для зв’язку	Ліцензія	PC1 – PC26
TrendMicro ApexOne	Системне	Антивірусна програма	Ліцензія	PC1 – PC26
SAP NetWeaver 2004	Прикладне	Інтегрована технологічна платформа	Freeware	PC7 – PC26
Програмний комплекс ISpro	Прикладне	Система автоматизації обліку та управління	Ліцензія	PC1 – PC26
АС «Передплата» (ПЗ власної розробки)	Прикладне	Система автоматизації обліку передплати	Ліцензія	PC21, PC22, PC23, PC24
АС «Фінансове управління» (ПЗ власної розробки)	Прикладне	Система автоматизації контролю та обліку фінансових потоків	Ліцензія	PC1 – PC26
АС «Ведення мережі» (ПЗ власної розробки)	Прикладне	Система ведення та контролю об’єктів мережі	Ліцензія	PC12, PC13, PC14, PC15

Таблиця 2.5 - Перелік обладнання ДТЗ

Назва обладнання	Марка	Модель	Розміщення
Блок безперервного живлення	Тирас	БЖ 1230	Серверна кімната
Сповіщувач пожежний димовий	Тирас	СПД-2	По всьому ОІД
Пристрій електричний автоматичного контролю і затримки	Тирас-1	ПУиЗ	Серверна кімната
Сповіщувач пожежний ручний	Тирас	СПР	В серверній, та у коридорах
Пристрій ручного запуску	Тирас	ПРЗ	Біля серверної кімнати
Пристрій аварійної запунки	Тирас	ПАЗ	Біля серверної кімнати
Модуль газового пожежогасіння	Импульс	Импульс-20	Серверна кімната
Газ для пожарогасіння (HFC125)	Хладон	Хладон-125	Серверна кімната

Таблиця 2.6 - Характеристика обладнання на ІТС

Назва обладнання	Назва на ІТС	Характеристика	Відповідальні
Моноблок	PC1 – PC15	Дисплей 1600x900 / Процесор Intel Core i3-3220 (2 ядра по 3,30 ГГц) графічною інтегрованою картою Intel HD 2500 / RAM 8 GB / HDD 500 GB / веб-камера / вага 6.08 кг	Інженер-електронники, інженер-програмісти директор, заступники директора, головний бухгалтер, начальники

Продовження таблиці 2.6

Назва обладнання	Назва на ІТС	Характеристика	Відповідальні
Моноблок	PC16 – PC26	Дисплей 1366x768 / Процесор Intel Celeron N4020 (2 ядра по 2,8 ГГц) 2500 / RAM 4 GB / HDD 256 GB / веб-камера / вага 3.12 кг	оператори, інженер-електронники, інженер-програмісти, начальник ЦСПІТ
Комутатор	У різних кімнатах	1,6 Гбіт / Ethernet 10-100 Мбіт/с, 2,19 Вт / 8 портів	інженер-програмісти, начальник Центру супроводу і підтримки ІТ
Комутатор	У різних кімнатах	3,2 Гбіт / Ethernet 10-100 Мбіт/с, 2,28 Вт / 16 портів	інженер-програмісти, начальник Центру супроводу і підтримки ІТ
Комутатор керований	На сервері	160 Гбіт / Ethernet 10-1000 Мбіт/с, 350 Вт / 48 портів	інженер-програмісти, начальник Центру супроводу і підтримки ІТ
Комутатор керований	На сервері	12,8 Гбіт / Ethernet 10-1000 Мбіт/с, від 100 до 200 Вт / 24 портів	інженер-програмісти, начальник Центру супроводу і підтримки ІТ
БФП (багатофункціональний пристрій)	У різних кімнатах	Лазерний друк / 600x600 dpi / 417 Вт / 11.2 кг	Усі робітники
Центральний маршрутизатор	На сервері	Смуга пропускання: 20 Гбіт/ с Продуктивність: 19Mpps Смуга шифрування: 8 Гбіт / с 2 порти 10G (SFP +) 6 портів 1000Base-X (SFP) 1 слот для SPA модулів RAM 8ГБ	інженер-програмісти, начальник Центру супроводу і підтримки ІТ

Продовження таблиці 2.6

Назва обладнання	Назва на ІТС	Характеристика	Відповідальні
Сервер	На сервері	Процесор 2x Intel Xeon X5560 (4 ядра по 2,8 ГГц) / RAM 24 GB / SSD 500ГБ / HDD 2 ТВ	інженер-програмісти, начальник Центру супроводу і підтримки ІТ

2.7 Аналіз статусу нормативно-правової бази на підприємстві

Для подальшого створювання КСЗІ на підприємстві, потрібно розробляти та редагувати всі рішення за допомогою нормативно-правових документів (НД ТЗІ). До них входять як державні нормативні документи, так і документи внутрішньої розробки, побудовані на їх основі, такі як:

– наказ № 337 від 17.02.2017 року «Про впровадження політики інформаційної безпеки ТОВ «Експрес Україна»;

– наказ № 1053 від 31.08.2020 року «Про затвердження Регламенту надання доступу до інформаційних систем та ресурсів ТОВ «Експрес Україна»;

– наказ № 1239 від 19.05.2018 року «Про затвердження Стандарту управління інцидентами інформаційної безпеки в інформаційних системах ТОВ «Експрес Україна»;

– наказ № 653 від 23.10.2017 року «Про затвердження Стандарту з управління життєвим циклом облікових записів та використання паролів при доступі до інформаційних систем та ресурсів ТОВ «Експрес Україна»;

– наказ № 783 від 26.9.2018 року «Політика загальних засад обробки персональних даних у ТОВ «Експрес Україна»;

– наказ № 142 від 21.09.2020 року «Про затвердження Положення про захист персональних даних у ТОВ «Експрес Україна»;

– наказ № 881 від 11.06.2019 року «Про призначення адміністраторів безпеки ТОВ «Експрес Україна»;

– наказ № 484 від 12.12.2017 року «Про затвердження Стандарту антивірусного захисту»;

– наказ № 1839 від 05.03.2017 року «Стандарт з використання VPN»;

– наказ № 1847 від 27.11.2017 року «Стандарт про Інтернет»;

– наказ № 371 року від 27.03.2018 року «Каталог критичності ІС».

Дія цих документів поширюється на ІТС, ТОВ "Експрес Україна", і тільки на неї. Ці положення, регламенти та стандарти є нормативним документом СЗІ і визначають завдання, функції, штатну структуру СЗІ, повноваження та відповідальність співробітників служби, взаємодію з іншими підрозділами та зовнішніми організаціями. Будь які документи СЗІ створюється на підставі наказу директора.

Наступний перелік є переліченням ключових нормативних документів та державних стандартів в сфері інформаційної безпеки, який обов'язковий до виконання на будь якому підприємстві державної власності та рекомендований для виконання приватними компаніями:

– НД ТЗІ 3.7-003-05 [4] «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі»;

– Державний стандарт України [5]. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96;

– НД ТЗІ 1.4-001-2000 [6] «Типове положення про службу захисту інформації в автоматизованій системі»;

– НД ТЗІ 1.6-005-2013 [7] «Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці»;

– НД ТЗІ 2.5-004-99 [8] «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»;

– НД ТЗІ 2.5-005-99 [9] «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу»;

– НД ТЗІ 2.5-008-02 [10] «Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2»;

– НД ТЗІ 2.5-010-03 [11] «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу»;

– НД ТЗІ 3.7-001-99 [12] «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі»;

– НД ТЗІ 3.6-001-2000 [13] «Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу»;

– НД ТЗІ 1.1-002-99 [14] «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу».

Метою створення системи з використанням перелічених нормативних актів є організаційне забезпечення завдань керування КСЗІ над АС та здійснення контролю за її функціонуванням.

2.8 Класифікація інформації та її захищеність

Оскільки в ОІД використовуються сервер і на ньому оброблюється багато інформації, далі має бути визначена інформація, що циркулює на підприємстві, для її подальшої класифікації. Для цього використаємо стандартні рівні властивостей, описані далі.

Рівні конфіденційності

К1 - Рівень конфіденційності інформації, при якому можливо 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. Что-то с интервалом, проверьте по всей работе

К5 - Критичний рівень конфіденційності інформації, що може призвести до краху компанії у разі втрати конфіденційності інформації.

Рівні цілісності

Ц1 - Рівень цілісності інформації, при якому можливо 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 можливо 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.

На ОІД використовується велика кількість інформаційних ресурсів з обмеженим доступом. Кожний працівник компанії має свій доступ до тої чи іншої інформації, яка має свій регламент політики безпеки самої компанії.

В дирекції встановлено центральні сервери, на яких збирається та обробляється інформація з точок присутності по місту та всій Запорізькій області. Через різновидність інформації, яка циркулює на об'єкті, її необхідно поділити на такі категорії:

– інформація про клієнтів компанії;
– інформація про персонал;
– облік технічної та розпорядчої документації;
– інформація про бізнес-показники, фінансову дисципліну;
– інформація про товарно-матеріальні цінності, складські запаси;
– інформація про оперативно-технічні засоби (системи відеоспостереження, охоронні системи та інше обладнання).

Вищеназвані категорії інформації обробляється персоналом компанії, до складу якого входять: директор філії, 2 заступники директора, головний бухгалтер, 4 начальників підрозділів, 4 інженера-програміста, 4 інженер-електронника, 10 операторів.

Уся інформація, що вноситься персоналом (операторами) на власному робочому місці (персональному комп'ютері), зберігається у спеціальному програмному забезпеченні, встановленому на сервері. Заступники та начальники можуть копіювати та друкувати цю інформацію, а працівники загального відділу консолідують всю вхідну та вихідну інформацію в спеціальному електронному репозиторії та зберігають фінансові документи в паперових екземплярах у спеціальному місці (архіві).

2.9 Посадові обов'язки та розмежування інформації

Впродовж усього робочого дня на об'єкті інформаційної діяльності знаходяться наступні особи:

- директор філії;
- заступник директора з операційної діяльності;
- заступник директора з розвитку мережі;
- головний бухгалтер;
- начальник Центру супроводу і підтримки ІТ;
- начальник Центру управління нерухомим майном;
- начальник відділу технологій;
- начальник відділу кадрів;
- оператори 1-2 категорії;
- інженери-програмісти 1-2 категорії;
- інженери-електронники 1-2 категорії.

Для того щоб зробити аналіз доступу до інформації всього персоналу компанії, потрібно визначити його посадові обов'язки. Нижче перелічені основні посадові обов'язки керівництва та персоналу, який має доступ до інформації.

Посадові обов'язки:

- директор філії - Проводить контроль усіх робочих процесів на підприємстві, супроводжує юридичні процеси компанії, виконує представницьку функцію при взаємодії з контрагентами та клієнтами;
- головний бухгалтер - Забезпечує ведення бухгалтерського обліку, дотримуючись єдиних методологічних засад, організовує правильну роботу бухгалтерської служби, контролює відображення на рахунках бухгалтерського обліку всіх операцій на підприємстві;
- заступник директора з операційної діяльності - Здійснює контроль та організує в напрямку операційної діяльності. Забезпечує транспортну логістику та управляння складськими запасами, їх переміщення та облік;

– заступник директора з розвитку мережі - Здійснює контроль за мережею точок присутності. Організовує бізнес-процеси та маркетинг продаж в точках присутності;

– начальник Центру супроводу і підтримки ІТ - Організовує експлуатацію електронно-обчислювального устаткування та пристроїв згідно з технічними умовами і нормами обслуговування, проведення необхідних тестових перевірок, профілактичних оглядів, повне завантаження та безперервну роботу техніки. Організовує обслуговування і надання технічної підтримки користувачам ІТ послуг. Бере участь у прийманні, монтажі та випробуваннях устаткування, яке наново вводиться в експлуатацію, у дослідній перевірці програмного забезпечення оброблення інформації та виконання обчислювальних робіт;

– начальник Центру управління нерухомим майном - Забезпечення безперервної, безпечної та ефективної господарської діяльності підрозділів компанії та точок присутності. Організація управління та обліку нерухомого майна. Взаємодія з орендодавцями та орендарями;

– начальник відділу технологій - Забезпечення організації, впровадження та експлуатації нових технологій обслуговування клієнтів. Ведення обліку об’єктів точок присутності. Оформлення нормативно-правової документації щодо діяльності та режимів роботи підрозділів компаній і точок присутності;

– начальник відділу кадрів - Організацій підбору, перевірки та найму персоналу для підрозділів компанії. Облік кадрових питань. Навчання та перекваліфікація персоналу. Взаємодія з зовнішніми організаціями з питань кадрової політики.

– оператори 1-2 категорії - Одержання та оброблення службової інформації за відповідними супровідними документами. Автоматичне завантаження звітів та реєстрів платежів з точок присутності. Здійснення перевірки завантаженої інформації з первинними прибутковими та видатковими документами.

– інженери-програмісти 1-2 категорії - Виконує роботи під час підготовки програм до налагодження і проводить їх налагодження. Розроблює інструкції на роботи з програмами, оформлює необхідну технічну документацію. Здійснює супроводження впроваджених програм і програмних засобів. Бере участь у проектних роботах. Забезпечує розмежування доступу до інформації згідно політики безпеки інформації

– інженери-електронники 1-2 категорії - Виконання профілактичних та ремонтних робіт по відновленню комп'ютерного, друкуючого та іншого периферійного обладнання.

Облік, приймання та передача в гарантійний ремонт до сервісного центру комп'ютерного обладнання. Облік, обмін, приймання та передача до сервісного центру картриджів на заправку та регенерацію. Ведення обліку та контроль технічного стану ліній фіксованого телефонного зв'язку. Ремонт ліній, АТС та іншого устаткування фіксованого телефонного зв'язку. Взаємодія з оператором зв'язку.

Далі у таблиці 2.7 визначено правові режими та режими доступу до інформації на підприємстві.

Таблиця 2.7 - Правовий режим та доступність інформації на підприємстві

Інформація	Режим доступу	Правовий режим	Мають доступ	Зберігається
Інформація про клієнтів компанії	З обмеженим доступом	Конфіденційна інформація	Всі	На сервері, в складі БД інформаційних систем (АС «Фінансове управління»)
Облік технічної та розпорядчої документації	З обмеженим доступом	Конфіденційна інформація	Загальний відділ, директор, керівники відділів	На сервері (АС «Босс-референт»), в загальному відділі, ПК начальника ЦСПІТ
Інформація про персонал	З обмеженим доступом	Конфіденційна інформація	Директор, начальник та оператори відділу кадрів	На сервері, в базі даних програмного комплексу ISpro, ПК начальника кадрів та підрозділів, ПК директора філії
Інформація про бізнес-показники, фінансову дисципліну	З обмеженим доступом	Комерційна таємниця	Директор, бухгалтерія, економісти	На сервері (АС «Фінансове управління» та ІС «M.E.Doc») ПК директора філії, ПК та паперовий архів головного бухгалтера

Продовження таблиці 2.7

Інформація	Режим доступу	Правовий режим	Мають доступ	Зберігається
Інформація про товарно-матеріальні цінності, складські запаси	З обмеженим доступом	Комерційна таємниця	Заступник директора з операційної діяльності, начальники підрозділів	На сервері (АС «Фінансове управління», на ПК заступника директора з операційної діяльності
Інформація про оперативно-технічні засоби	З обмеженим доступом	Комерційна таємниця	Працівники дільниці фіз. захисту та охоронних засобів, начальник ЦУНМІ та ЦСПІТ	ПК та паперовий архів начальника дільниці фізичного захисту та охоронних засобів, ПК начальника ЦУНМІ, ПК начальника ЦСПІТ

Тепер, коли накопичено інформацію про підрозділи, посади, правові режими та їх доступ до інформації, переходимо до кваліфікації рівнів конфіденційності, цілісності та доступності інформації на підприємстві, які наведені у таблиці 2.8.

Таблиця 2.8 - Рівні конфіденційності, цілісності та доступності інформації

Інформація	Рівень конфіденційності	Рівень цілісності	Рівень доступності
Інформація про клієнтів компанії	К2	Ц4	Д3
Облік технічної та розпорядчої документації	К2	Ц2	Д2
Інформація про персонал	К2	Ц3	Д2
Інформація про бізнес-показники, фінансову дисципліну	К4	Ц5	Д3
Інформація про оперативно-технічні засоби	К4	Ц3	Д2
Інформація про товарно-матеріальні цінності, складські запаси	К3	Ц2	Д2

Виходячи із характеристик рівнів доступності, конфіденційності та цілісності інформації , після складання акту обстеження, потрібно переходити до робот, пов’язаних з можливими вразливостями (помилками та недоліками) у інформаційній системі, які в свій час можуть порушити одну з перелічених властивостей, або взагалі задати дуже великої шкоди усім властивостям. Тому

далі у таблиці 2.9 буде проводитись процедура, яка має на меті визначення всіх негативних факторів, що можуть вплинути на ІТС.

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 підприємству шляхом знищення матеріальних та інформаційних цінностей.

Таблиця 2.9 - Матриця розмежування

Користувач	Рівень кваліфікації	Інформація						Повноваження керувати КСЗІ
		Інф. про клієнтів компанії	Облік технічної та розпорядчої документації	Інф. про персонал	Інф. про бізнес-показники, фінансову дисципліну	Інф. про товарно-матеріальні цінності	Інф. про оперативно-технічні засоби	
Директор філії	Високий	Ч,К,М, Д,З,ЗБ	Ч,К,М, Д,З,ЗБ	Ч,Д	Ч,К,М, Д,З,ЗБ	Ч,К,Д	Ч,К,Д	-
Головний бухгалтер	Високий	Ч,К,Д	Ч,Д	Ч,Д	Ч,К,М, Д,З,ЗБ	Ч,К,М, Д,З,ЗБ	-	-
Заступник директора з операційної діяльності	Високий	Ч,К,Д	Ч,Д	Ч,Д	Ч,Д	Ч,К,М, Д,З,ЗБ	-	Так
Заступник директора з розвитку мережі	Високий	Ч,К,М, Д,ЗБ	Ч,Д	Ч,Д	Ч,К,М, Д,З,ЗБ	Ч,К,Д	-	-
Начальник Центру супроводу і підтримки ІТ	Високий	Ч,К,М, Д,ЗБ	Ч,К,М, Д,З,ЗБ	Ч,Д	Ч,Д	Ч,Д	Ч,К,М, Д,З,ЗБ	Так
Начальник Центру управління нерухомим майном	Середній	Ч,К,Д	Ч,К,М, Д,З,ЗБ	Ч,Д	Ч,К,Д	Ч,К,М, Д,З,ЗБ	-	-
Начальник відділу технологій	Середній	Ч	Ч,К,М, Д,З,ЗБ	Ч,Д	Ч	-	-	-
Начальник відділу кадрів	Середній	Ч	Ч,К,М, Д,З,ЗБ	Ч,К,М, Д,З,ЗБ	-	-	-	-
Оператори 1-2 категорії	Низький	Ч,Д	Ч	-	-	-	-	-
Інженер-програміст 1-2 категорії	Високий	Ч,К,М, Д,З,ЗБ	Ч,К,М, Д,З,ЗБ	Ч,К,М, Д,З,ЗБ	Ч,К,М, Д,З,ЗБ	Ч,К,М, Д,З,ЗБ	Ч,К,Д	-
Інженер-електроник 1-2 категорії	Середній	Ч	Ч	-	-	-	Ч,К,М, Д,З,ЗБ	-

Умовні позначення до таблиці 2.9:

- Ч - Читання інформації;
- К - Копіювання інформації;
- М - Модифікація інформації;
- Д - Друкування інформації;
- З - Запис інформації;
- ЗБ - Зберігання інформації.

2.10 Побудова моделі порушника

Після обстеження об'єкту, потрібно починати розробляти модель загроз та вразливостей, інакше це називається моделлю порушника.

Відповідно до загроз, потрібно розробити перелік суттєвих загроз до об'єкту та описати методи їхнього здійснення задля подальшої мінімізації цих загроз. Насамперед модель порушника повинна визначати:

– можливі цілі порушника та їх градація за ступенями небезпечності для ІТС та інформації, що потребує захисту;

– категорії персоналу, користувачів ІТС та сторонніх осіб, із числа яких може бути порушник;

– припущення про кваліфікацію порушника;

– припущення про характер його дій.

Взагалі порушники поділяються на дві категорії – внутрішні та зовнішні.

Зовнішні особи, що можуть бути порушниками:

– клієнти;

– відвідувачі, запрошені з якогось приводу;

– представники організацій, взаємодіючих з питань забезпечення систем життєдіяльності організації;

– представники конкуруючих організацій, таких як іноземні служби або особи, що діють за їх завданням;

– особи, які випадково або навмисно порушили пропускний режим, тобто не мали мети нічого порушати;

– будь-які особи за межами контрольованої зони.

Серед внутрішніх порушників можливо виділити такі категорії персоналу:

– користувачі системи;

– персонал, що обслуговує технічні засоби;

– співробітники відділів розробки та супроводу програмного забезпечення;

– технічний персонал, що обслуговує будівлю (прибиральниці, електрики, сантехніки та інші співробітники, що мають доступ до будівлі та приміщення, де розташовані компоненти ІТС);

– співробітники служби безпеки;

– керівники різних рівнів та посадової ієрархії.

Усіх порушників можливо класифікувати за такими ознаками:

– за рівнем знань про ІТС;

– за рівнем можливостей;

– за часом дії;

– за місцем дії.

Під час формування моделі порушника обов'язково повинно бути визначено:

– ймовірність реалізації загрози;

– своєчасність виявлення;

– відомості про порушення.

Коли формується модель порушника, потрібно не забувати визначати усі ймовірності реалізації загрози, своєчасно виявляти їх та збирати усі відомості про порушення. Зауважити же треба те, що всі злочини здійснюються людиною. Користувачі ІТС являє собою як складову цієї системи, так і являє собою головною причиною порушень та злочинів. Як факт, питання безпеки захищеності ІТС є питанням людського фактору (відносин та поведінки). Таким чином, основною потенційною загрозою для інформації в ІТС потрібно вважати випадкові або цілеспрямовані дії персоналу, котрі можуть задати великої шкоди, оскільки вони становлять 75 % усіх випадків знищення інформації.

Тепер починаємо будувати модель загроз. Для подальшої оцінки буде використовуватись спеціальна шкала оцінки загроз.

Шкала оцінки загроз:

К1 - визначає ступінь доступності до об'єкта:

– в іншій країні (для техногенних загроз) / немає доступу до об'єкта (для антропогенних загроз);

– в тій самій країні (для техногенних загроз) / віддалений доступ до об'єкта (для антропогенних загроз).

– поблизу будівлі, де знаходиться ОІД, або в тій самій будівлі (для техногенних загроз) / фізичний несанкціонований доступ до об'єкта, несанкціоноване проникнення в приміщення (для антропогенних загроз).

– в тому ж приміщенні (для техногенних загроз) / доступ у приміщення, де знаходиться об'єкт (для антропогенних загроз).

– сам об'єкт (для техногенних загроз) / фізичний дозволенний доступ до об'єкта (для антропогенних загроз).

К2 - присутність необхідних умов, ступінь кваліфікації виконавця та ступінь його бажання реалізувати загрозу:

– виконавець постраждає при реалізації загрози; він не має ніяких відповідних можливостей; техніка та ПЗ постійно оновлюються, встановлюється належним чином та постачається надійним виробником.

– виконавець не постраждає через загрозу, але її виконання не є вигідним для виконавця; він має недостатній рівень знань для реалізації загрози; ПЗ та техніка оновлюється не постійно.

– виконавцю вигідна реалізація загрози; він може навчитися методам, що реалізують загрози; ПЗ та техніка вразливі для деяких атак.

– виконавцю дуже вигідна реалізація загрози; він володіє методами, що реалізують загрози; відсутність оновлень ПЗ або застарілі елементи техніки, ненадійні їх виробники, неякісна техніка.

– мета виконавця; виконавець є експертом у методах, що реалізують загрозу (наприклад, він працює у відповідній сфері); стара або зламана техніка; піратське

ПЗ, тощо.

К3 - фатальність наслідків:

– ОІД нічого не втратить, або наслідки будуть позитивними;

– наслідками можна знехтувати;

– наслідки відчутні, але несуттєві;

– наслідки можуть призвести до проблем, вирішення яких потребуватиме значну кількість матеріальних витрат та значну кількість часу;

– наслідки можуть призвести до втрати репутації компанії, недовіри клієнтів та збитків, що можуть призвести до закриття організації.

Коефіцієнт небезпеки для загроз розраховується за формулою:

$$(К_{неб}) = (К1 \cdot К2 \cdot К3)/125.$$

У таблиці 2.10 описані загрози, проведено аналіз загроз з усіма можливими діями порушників щодо ОІД, або точніше, перелік загроз із констатацією можливих дій порушників щодо конкретних об'єктів, виходячи з пріоритетів безпеки та цінності інформаційних ресурсів які циркулюють на ОІД.

Таблиця 2.10 - Модель загроз

Назва загрози	Вразливість	К1	К2	К3	$К_{неб}$
Загрози внутрішнього характеру					
Викрадення або знищення інформації	Неуважне зберігання документів, різних носіїв інформації	4	3	4	0.38
Викрадення або знищення інформації	Ненавмисне встановлення шкідливого ПЗ, неуважність при використанні Інтернету	5	2	3	0.24
Розголошення конфіденційної інформації	Непоінформованість персоналу про статус службової інформації, якою він користується при виконанні своїх обов'язків	5	2	3	0.24

Продовження таблиці 2.10

Назва загрози	Вразливість	К1	К2	К3	$К_{неб}$
Пожежа, знищення або пошкодження обладнання, інформації та документів	Неправильно встановлена система пожежної сигналізації чи збій у її роботі	4	3	4	0.38
Знищення або пошкодження інформації	Різні відмови систем електропостачання, перепади напруги призводять до некоректної робота обладнання або його пошкодження	4	3	4	0.38
Пошкодження носіїв інформації або серверів	Перенавантаження систем та серверів на підприємстві	3	3	4	0.29
Відсутність або неефективне антивірусне ПЗ	Навмисне розповсюдження вірусного ПЗ, яке може порушити безпеку	5	3	4	0.48
Загрози зовнішнього характеру					
Викрадення або знищення інформації	Копіювання інформації на сторонні носії людьми, які не працюють на підприємстві, через неуважність персоналу.	4	3	4	0.38
Несанкціонований перехват інформації	Неправильне зберігання документів та пристроїв з інформацією	5	3	4	0.48
Хакінг	Виконання злому комп’ютера працівника, з подальшою крадіжкою	5	4	3	0.48
Шпіонаж(неправильний підбір персоналу)	Можлива крадіжка інформації, якщо на підприємстві працює “заслана” людина з іншого підприємства	4	3	4	0.38
Загрози природного характеру					
Катастрофа	Пожежа, землетрус, повінь, техногенні аварії	3	3	4	0.29

Розглянувши цю таблицю, потрібно зробити наступний висновок: однією з найбільш($К_{неб}$=0.48) ймовірних та ризикованих загроз може стати заволодіння/пошкодження інформації одною чи декількома особами, які помилково чи цілеспрямовано можуть провести спробу порушення роботи систем безпеки на ОІД. Це призведе до викрадення, пошкодження інформації або взагалі, до її повного знищення.

Потрібно також розуміти, що випадки витоку інформації можуть як мати, так і не мати якоїсь мети. Проте метою зловмисного порушника може бути щось з наступного переліку:

– отримання в певному обсязі інформації, необхідної для порушника;

– отримання можливості змінювати потоки інформації у відповідності до того, що хоче порушник;

– нанесення великих збитків атакованому підприємству, шляхом знищення інформаційних чи матеріальних цінностей компанії;

– подальше використовування інформації проти підприємства.

Враховуючи вищезгадане, для запобігання можливих вразливостей та зменшення ризиків, нижче побудовані таблиці 2.11 та 2.12 з моделлю порушника та моделлю внутрішнього порушника на підприємстві.

Таблиця 2.11 - Модель внутрішнього порушника

Посада працівника	Мотив порушення	Рівень обізнаності о ІТС	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Директор філії	М1, М2, М3	К4	Ч3	Д5	15
Заступник директора з операційної діяльності	М1, М2, М3	К1	Ч3	Д5	15

Продовження таблиці 2.11

Посада працівника	Мотив порушення	Рівень обізнаності о ІТС	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Заступник директора з розвитку мережі	М1, М3	К1	Ч3	Д4	12
Головний бухгалтер	М3	К1	Ч3	Д4	11
Начальник Центру управління персоналом	М1, М2, М3	К1	Ч3	Д4	14
Начальник Центру супроводу і підтримки ІТ	М1, М2, М3	К5	Ч4	Д6	21
Начальник Центру управління нерухомим майном	М1, М3	К1	Ч3	Д4	12
Начальник відділу технологій	М1, М2, М3	К1	Ч3	Д4	14
Начальник відділу кадрів	М1, М3	К1	Ч3	Д4	12

Продовження таблиці 2.11

Посада працівника	Мотив порушення	Рівень обізнаності о ІТС	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Оператор 1-2 категорії	М1, М3	К1	Ч3	Д4	12
Інженер-програміст 1-2 категорії	М1, М2, М3	К5	Ч4	Д6	21
Інженер-електронник 1-2 категорії	М1, М2, М3	К2	Ч3	Д4	15

Таблиця 2.12 - Модель зовнішнього порушника

Посада працівника	Мотив порушення	Рівень обізнаності о ІТС	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Хакери	М2, М3	К3	Ч3	Д1	12
Діяч організації по питанням технічного забезпечення	М3	К5	Ч1	Д2	11
Діяч організації по питанням програмного забезпечення	М3	К4	Ч1	Д3	11

Специфікація моделі порушника за мотивами здійснення порушень така:

– М1 - безвідповідальність;

– М2 – самоствердження;

– 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 усіх процесів захисту, які вбудовані у системне програмне забезпечення та його не документовані можливості;

Специфікація моделі порушника за місцем дії:

– Д1 - без доступу на контрольовану територію підприємства;

– Д2 - з контрольованої території без доступу до будинку;

– Д3 - в середині приміщень, але без доступу до технічних засобів ІТС;

– Д4 - з робочих місць користувачів ІТС;

– Д5 - з доступом у зони даних (баз даних, архівів);

– Д6 - з доступом у зону керування засобами забезпечення безпеки ІТС.

Специфікація моделі порушника за часом дії:

– Ч1 - до впровадження ІТС або її окремих компонентів;

– Ч2 - під час бездіяльності компонентів системи (в неробочий час, під час перерв для обслуговування і ремонту і т.д.);

– Ч3 - під час функціонування ІТС (або компонентів системи);

– Ч4 - як у процесі функціонування ІТС, так і під час зупинки компонентів системи.

Підводячи висновок до таблиць 1.11 та 1.12 моделі порушника, найбільшу загрозу внутрішнього характеру для інформаційних систем підприємства несуть такі службові особи: начальник Центру супроводу і підтримки ІТ та інженер-програміст 1-2 класу. Це відбувається через те, що вони мають найбільше прав щодо управління інформаційною безпекою на підприємстві. В той же час, найбільшу зовнішню загрозу для інформаційної безпеки несуть хакери.

2.11 Розробка політики інформаційної безпеки

За результатом обстеження на ОІД був обраний профіль захищеності системи 3.КЦД.3 { КД-3, КА-3, КО-1, КК-1, КВ-3, ЦД-2, ЦА-3, ЦО-2, ЦВ-2, ДР-3,ДС-2, ДЗ-2, ДВ-2, НР-4, НИ-3, НК-1, НО-3, НЦ-1, НТ-2, НВ-2, НА-1, НП-1 }.

КД-3. Повна довірча конфіденційність. Частково реалізовано. У КЗЗ підприємства є ресурси, які дозволяють авторизованим користувачам керувати потоками інформації від об'єктів, що належать їх доменам, до інших користувачів системи. (реалізація: авторизація користувачів в Active Directory, доменні групові політики).

КА-3. Повна адміністративна конфіденційність. Не реалізовано. Дана політика не має можливості відноситись до всіх об'єктів КС.

КА-2. Базова адміністративна конфіденційність. Реалізовано. На підприємстві призначено адміністраторів, які на рівні операційних систем можуть керувати потоками інформації від об'єктів до користувачів системи (реалізація: розмежування доступу до мережевих ресурсів засобами серверних ОС та автоматизованих систем).

КО-1. Повторне використання об'єкта. Частково реалізовано. На підприємстві є ресурси для безпечного використання об'єктів, що розділяються, одночасно або послідовно доступних декільком процесам (реалізація: очищення кеш-даних при виході клієнтів із автоматизованих систем, браузерів).

КК-2. Контроль прихованих каналів. Не Реалізовано. В інформаційній системі підприємства відсутні технологічні рішення для виявлення прихованих каналів.

КВ-3. Повна конфіденційність при обміні. Не реалізовано. Відсутні засоби забезпечення повної конфіденційності.

КВ-2. Базова конфіденційність при обміні. Реалізовано. КЗЗ має достатню кількість програмно-апартних ресурсів для забезпечення запитів імпортованих та експортованих ресурсів на підставі атрибутів доступу інтерфейсних процесів (Реалізація: розділення мережі на VLAN, використання VPN тунелей, шифрування даних на мережевому рівні засобами CISCO IOS, розмежування доступу до інформації доменними політиками)

ЦД-2. Базова довірча цілісність. Реалізовано. На підприємстві використовуються засоби забезпечення довірчої цілісності на базовому рівні (реалізація: використання електронного цифрового підпису ЕЦП та кваліфікованого електронного підпису КЕП при електронному документообігу як в компанії так і зовні, ПТК Центр сертифікації ключів CryptoKDC).

ЦА-3. Повна адміністративна цілісність. Не реалізовано. Для повного контролю за цілісністю ресурси відсутні.

ЦА-2. Базова адміністративна цілісність. Частково реалізовано. В системі використовуються програмно-технічні засоби для шифрування інформаційних потоків (реалізація: АС «Криптоавтограф»), що виходять зовні.

ЦО-2. Повний відкат. Частково реалізовано. ІТС має програмно-апаратні ресурси для регулювання відкату за будь-який проміжок часу (реалізація: резервування БД Informix, Microsoft SQL Server, Firebird згідно встановлених графіків).

ЦВ-2. Базова цілісність при обміні. Реалізовано. Адміністратори систем мають можливості на імпорт\експорт даних та присвоєння чи зміни рівня їх захищеності (реалізація: вбудовані в ПЗ власної розробки алгоритми).

ДР-3, ДР-2. Пріоритетність використання ресурсів, недопущення перехоплення ресурсів. Не реалізовано.

ДР-1. Квоти. Реалізовано. В КЗЗ присутні програмно-апаратні механізми, які регулюють циркуляцію IP в КС (реалізація: системні квоти на займане користувачами місце дискового простору на серверах Microsoft).

ДС-2. Стійкість з погіршенням характеристик обслуговування. Реалізовано. В системі присутні програмно-апаратні ресурси, які забезпечують діяльність інформаційних систем у погіршених умовах у результаті відмови компонентів (реалізація: основний та резервний DNS, резервний канал зв'язку, декілька проксі, віртуальні сервери).

ДЗ-3, ДЗ-2. Заміна будь-якого компонента, обмежена гаряча заміна. Частково реалізовано. КЗЗ має можливості модернізації або заміни деяких компонентів без переривання обслуговування (резервування HDD в RAID масивах).

ДЗ-1. Модернізація. Реалізовано. КЗЗ підприємства має IT підрозділ, в посадових обов'язках якого прописане право переривати діяльність інформаційних систем з метою виконання робіт по відновленню роботи обладнання або його модернізації.

ДВ-3, ДВ-2. Вибіркове, автоматичне відновлення. Частково реалізовано. КЗЗ має обмежений перелік програмно-апаратних ресурсів для відновлення і приведення до нормального стану КС у автоматичному режимі (також резервування HDD в RAID масивах).

ДВ-1. Ручне відновлення. Реалізовано. На підприємстві є персонал, який відновлює роботу КС до нормального стану у ручному режимі. У результаті виконання даної процедури КС може бути тимчасово недоступний.

НР-5. Аналіз у реальному часі. Частково реалізовано. КЗЗ має деякі програмно-апаратні механізмів для реєстрації НСД або інших подій у реальному часі (наприклад: моніторинг антивірусного комплексу TrendMicro ApexOne).

НР-4. Детальна реєстрація. Реалізовано. В КЗЗ присутні програмно- апаратні ресурси, які забезпечують захист журналу подій від НСД або іншого негативного впливу на даний продукт. Інженери-програмісти Центру IT мають доступ до журналу подій операційних систем серверів та користувачів (реалізація: журнал

подій Microsoft Server, централізована система моніторингу, управління та звітності TrendMicro ApexOne).

НИ-3. Множинна ідентифікація та автентифікація. Частково реалізовано. Система має декілька програмно-апаратних механізмів для перевірки користувача при вході в інформаційні системи. (реалізація: система ідентифікації ОС через ресурси Microsoft Active Directory, алгоритми власної розробки в ПЗ підприємства).

НК-1. Однонаправлений достовірний канал. Реалізовано. В системі присутні ресурси, які забезпечують процедуру з боку користувача (реалізація: локальна обчислювальна мережа).

НО-3. Розподіл обов'язків на підставі привілеїв. Частково реалізовано. Політика розподілу в системі в деяких програмних продуктах власної розробки та SAP NetWeaver 2004, програмний комплекс ISpro визначають множину користувачів, надають їм ролі з матрицею обов1язків.

НО-2. Розподіл обов'язків адміністраторів. Реалізовано. В системі присутні механізми, які керують діяльністю обов'язків адміністраторів. АС має декілька осіб, визначених розпорядчими документами, які виконують функції адміністраторів систем, програмних комплексів, антивірусного захисту та безпеки.

НЦ-1. КЗЗ з контролем цілісності. Реалізовано. Система має програмні ресурси, які спрямовані на оповіщення адміністратора системи і блокування КС від негативного втручання до тих пір, доки адміністратор не приведе ресурс до нормального стану власноруч (реалізація: антивірусний комплекс TrendMicro ApexOne, ПЗ керованих комутаторів).

НТ-3. Самотестування у реальному часі. Реалізовано. Система має програмно-апаратні механізми для тестування КС у реальному часі (наприклад: програмне забезпечення ДБЖ серверної MGE Galaxy 3500 20kVA проводить тестування батарей згідно графіку).

НТ-2. Самотестування при старті. Реалізовано. В КЗЗ присутні механізми, які реалізують дану політику (реалізація: антивірусне ПЗ, RAID-контролер серверів).

НВ-3, НВ-2. Автентифікація з підтвердженням, автентифікація джерела. Не реалізовано. В КЗЗ відсутні механізми захисту, які встановлюють джерело кожного об'єкта, що експортується або імпортується в КС.

НВ-1. Автентифікація вузла. Реалізовано. КЗЗ присутні механізми для реєстрації вузла або вузлів, які імпортують або експортують об'єкти в КС. (Механізм: система моніторингу Zabbix з мережею агентів, встановлених на серверах та керованих комутаторах).

НА-1. Базова автентифікація відправника. Реалізовано частково. В КЗЗ присутній механізм (реалізація: Сервіс електронного документообігу «Вчасно», ПЗ АЦСК для перевірки електронного цифрового підпису або КЕП, наприклад ПК «ІІТ Користувач ЦСК-1»).

НП-1. Базова автентифікація одержувача. Реалізовано. В КЗЗ наявний механізм, який здатний автентифікувати одержувача (реалізація: утиліти, ПЗ власної розробки та ПЗ АЦСК для перевірки електронного цифрового підпису або КЕП, наприклад ПК «ІІТ Користувач ЦСК-1»).

Після цього, потрібно надати рекомендації щодо рішення з'ясованих проблем, тобто з сторони програмно – апаратних можливостей буде налаштування різних організаційних аспектів, які допоможуть налаштувати циркуляцію інформації в ІТС. І вже потім буде створено правильні політики, які забезпечать порядок та правильну послідовність усіх інформаційних потоків на підприємстві, із-зі чого мінімізується негативний вплив на ІТС.

На підприємстві розроблено велика кількість документів (наказів та розпоряджень), які регламентують політику безпеки, щодо прав доступу до інформації, а також надання доступу до окремих приміщень та паперових документів. Крім того врегульовано політику безпеки щодо використання засобів шифрування та підписання електронних документів, антивірусного захисту. Визначені правила зберігання та знищення інформації.

Комплекс документації розроблений згідно вимог НД-ТЗІ та вимог Міністерства інфраструктури України, начальником Центру супроводу і підтримки ІТ разом з інженерами-програмістами підрозділу, відповідальними за впровадження політики безпеки на підприємстві. Всі накази, розпорядження та регламенти, узгоджені та підписані директором компанії, його заступниками.

З кожним документом ознайомлені все працівники ЦСПІТ з їх власним підписом, які реалізують ті чи інші заходи безпеки. Користувачі підприємства також ознайомлюються з документами, якщо політика безпеки стосується їх діяльності.

Відповідальність за реалізацію політики безпеки покладається на працівників ЦСПІТ або інших підрозділів, що окремо зазначається в кожному документі.

Додаткові заходи забезпечення політики безпеки, які потребують впровадження.

Враховуючі недоліки (відсутність реалізації), допущені при розробці та впровадженні комплексної системи захисту інформації на підприємстві, можна визначити додаткові організаційні заходи для їх усунення:

– розробити додаткові інструкції, якими регламентується порядок виконання робіт працівниками, пов’язаними з конфіденційністю, цілісністю та доступністю інформації.

– внести зміни до наказів про особисту матеріальну відповідальність, додавши до них норму, що всіх користувачі інформаційної системи несуть матеріальну відповідальність за цілісність робочої станції.

– згідно розробленої матриці розмежування підготувати та затвердити регламенти щодо правил обліку та зберігання, розмноження та знищення носіїв конфіденційної інформації, яка обробляється на ОІД.

– забезпечити контроль доступу користувачів до CD та DVD-дисководів, зовнішніх носіїв (флеш карти, USB-флеш пам’ять, зовнішні HDD та SSD накопичувачі), USB-портів комп’ютера засобами серверних операційних систем за допомогою групових політик.

– захистити локальні розділи жорсткого диску робочих станцій від випадкового або навмисного форматування через використання групових політик Active Directory.

– протоколювати (писати лог-журнали) всі дії користувачів з пристроями та файлами, які несуть конфіденційну інформацію та інформацію з обмеженим доступом ІзОД. Враховуючи велике апаратне навантаження для цих цілей пропонується придбання та використання окремого серверу.

– організувати регулярне збереження конфіденційної інформації та ІзОД на окремому зовнішньому носії з обмеженим або взагалі відсутнім мережевим доступом.

– замінити всі некеровані комутатори на керовані та заблокувати на них невживані порти вбудованими програмними засобами.

– встановити в підрозділах, де обробляється конфіденційна інформація та ІзОД, систему відеоспостереження.

– встановити систему охоронної сигналізації на всі приміщення, де циркулює інформація з обмеженим доступом.

– забезпечити опечатування кабінетів та приміщень, де циркулює інформація з обмеженим доступом.

Розробка політики безпеки

Враховуючи те, що в ТОВ "Експрес Україна" циркулює як конфіденціальна інформація так і інформація з обмеженим доступом, що стосується фінансових та матеріальних ресурсів компанії, найбільш доцільним буде забезпечити необхідний рівень захищеності при мінімальному залученні коштів. Одночасно необхідно не забувати, що великі об’єми циркулюючої в ІТС інформації потребують збереження її цілісності та доступності.

Покладаючись на такі умови та враховуючи вже реалізовані заходи, слід зупинитися на більш повноцінній та ефективній реалізації деяких базових функцій, які направлені на усунення таких ризиків інформаційної безпеки:

– несанкціонований перехват інформації на паперових або електронних носіях, внаслідок необмеженого та неконтрольованого доступу до приміщень

компанії (захист досягається за рахунок впровадження систем відеоспостереження, охоронної сигналізації та пристроїв опечатування дверей, що сигналізують про доступ до приміщення);

– несанкціоноване підключення внутрішнього або стороннього порушника до інформаційної системи підприємства через локальну мережу для розширення своїх повноважень або маскування, одержання та використання атрибутів доступу системи (захист досягається обмеженням доступу до мережевих портів та моніторингом дій користувачів в операційній системі та автоматизованих системах);

– пошкодження, шифрування або знищення масивів фінансової інформації, що зберігається на мережевих ресурсах, в файлових репозиторіях та базах даних, в результаті зловмисних або необережних дій (захист досягається шляхом використання офлайнових систем зберігання даних, архівування та бекапірованія).

Для впровадження комплексу протидій переліченим загрозам додатково до вже існуючих слід розробити наступні політики безпеки інформації:

– політика моніторингу та контролю доступу до приміщень та комп'ютеризованих робочих місць, націлена на зниження ризику від витоку інформації шляхом несанкціонованого заволодіння електронними та паперовими носіями, що містять агреговані дані про фінансову діяльність компанії, клієнтів та інформацію з грифом ДСК;

– політика моніторингу та контролю інформаційної мережі, створена для зниження ризику від витоку інформації шляхом підключення до мережевих ресурсів;

– політика резервного копіювання даних націлена збереження цілісності конфіденційної інформації та ІЗоД.

Політика моніторингу та контролю доступу до приміщень та комп'ютеризованих робочих місць

Реалізація цієї політики має гарантувати, що всі конфіденційні матеріали або документи з обмеженим доступом в паперовому або електронному вигляді будуть

недоступні до сторонніх осіб або персоналу під час припинення роботи з ними та відсутній контроль з боку власника інформації. Має бути забезпечений постійний візуальний та охоронний контроль за доступом в такі приміщення, включаючи протоколювання всіх подій до та після доступу в них.

Політика повинна забезпечити захист конфіденційної інформації про співробітників, фінансову діяльність, клієнтів та державні активи. Ця політика поширюється на всіх працівників компанії, які мають доступ в те чи інше приміщення в залежності від грифу доступу.

Реалізація політики:

– працівники повинні гарантувати, що вся конфіденційна інформація (на паперовому носії) або в електронній формі буде захищена на робочому місці в кінці робочого дня або коли вони будуть відсутні тривалий час;

– комп'ютер має бути заблокованим, коли робоче місце незайняте;

– комп'ютери повинні бути повністю вимкнені наприкінці робочого дня;

– будь-яку конфіденційну інформацію необхідно прибрати з робочого столу та закрити у спеціальному ящику, коли стіл незайнятий та наприкінці робочого дня;

– картотеки, що містять конфіденційну інформацію повинні зберігатись закритими, коли вони не використовуються;

– ключі що використовуються для доступу до конфіденційної інформації не повинні залишатися без нагляду персоналу;

– паролі не мають залишатися на нотатках, розміщених на комп'ютері або під ним, а також не мають бути записані у доступному місці для всіх;

– все що роздрукована на принтері та містить конфіденційну інформацію, не повене залишатись у лотках принтера;

– після утилізації конфіденційних документів вони мають бути подрібнені та поміщенні в спеціальні конфіденційні контейнери для сміття;

– ноутбуки та планшети мають бути заблокованими;

– зберігати пристрої зберігання даних (DVD, USB накопичувані) у замкненому ящику;

– після завершення робочого дня відповідальна особа повинна замкнути приміщення, активувати охоронну сигналізацію, опечатати кабінет та здати тубус з ключами на пост охорони під запис у спеціальному журналі.

Відповідальність

Працівник, який порушив цю політику, може зазнати дисциплінарного стягнення, отримати догану або навіть в окремих випадках бути звільненим.

Політика моніторингу та контролю інформаційної мережі.

Метою цієї політики є визначення стандартів для систем, які обстежують та обмежують користування Інтернету від будь-якого небажаного з'єднання в мережі організації. Ця політика розроблена для того, щоб співробітники користувались Інтернетом безпечно, а також гарантувати що усі інциденти будуть записуватись до спеціального серверу.

Ця політика поширюється на всіх працівників компанії, які мають доступ до інформаційної мережі компанії.

Реалізація політики:

– інженер-програміст повинен спочатку встановити у всіх кімнатах керовані комутатори, де раніше були некеровані;

– інженер-програміст має відключити усі незаймані порти на керованому комутаторі;

– інженер-програміст повинен приєднати усі комутатори до спеціального серверу, котрий записує лог-файли кожного користувача;

– має бути налаштоване розмежування мережі для різних працівників;

– встановлене розмежування потрібно контролювати і якщо немає доступу до якогось мережевого ресурсу, який не впроваджений до доступу працівника, цей ресурс має бути заблокований.

Відповідальність

Працівник, який порушив цю політику, може зазнати дисциплінарного стягнення, отримати догану або навіть в окремих випадках бути звільненим.

Політика резервного копіювання даних.

Метою даної політики є визначення строгого порядку резервного копіювання, який має вступати в силу при необхідності відновлення критичної інформації (конфіденційної) яку було повністю або частково втрачено. Така ситуація може бути викликана помилкою користувача АС, хакерською атакою, програмою-шифровальником, збоєм апаратного або програмного забезпечення, пожежею або будь яким іншим стихійним лихом. Дії відповідальних осіб мають бути строго регламентовані. Політика резервного копіювання стосується всієї IT-інфраструктури підприємства та її користувачів.

Реалізація політики:

– відповідальні за резервне копіювання мають бути визначені наказом. Функції відповідального мають бути закріплені також посадовою інструкцією;

– має бути затверджений графік резервного копіювання;

– ведеться журнал обліку носіїв та журнал обліку створення резервних копій;

– доступ в приміщення, де знаходиться система зберігання даних, має бути обмеженим;

– носії (картриджі) мають зберігатись в захищеному сховищі;

– відповідно графіку, спеціально назначена людина, повинна взяти ключі до серверної кімнати, де знаходиться система зберігання даних;

– після потрапляння у серверну кімнату відповідальний працівник повинен записати до журналу дату створення резервних копій;

– працівник має вставити картриджі та зробити резервні копії даних, дивиться щоб не було ніяких помилок;

– після закінчення операції по резервуванню даних, працівник має достати картриджі та покласти їх до сейфу, потім зачинити двері та віддати ключі від серверної кімнати назад.

Відповідальність

Працівник, який порушив цю політику, може зазнати дисциплінарного стягнення, отримати догану або навіть в окремих випадках бути звільненим.

2.12 Висновок

У другому розділі було зроблене детальне обстеження ІТС, з описом усіх інформаційних та фізичних середовищ, середовищ користувачів. Було проведено детальний аналіз та оцінка усіх ризиків щодо інформаційної безпеки з подальшим виявленням значущих загроз. Після аналізу усіх вразливостей, можливо побачити не ідеальну захищеність інформаційно-телекомунікаційної системи підприємства, недоліки якої можуть завдати великої шкоди інформації з подальшим наданням збитків підприємству.

Тому, згідно з проведеним аналізом, було розроблено та запропоновано політику безпеки для забезпечення найкращої захищеності та роботи всіх інформаційних систем на підприємстві.

3 ЕКОНОМІЧНИЙ РОЗДІЛ

Розробка політики безпеки комп'ютерної мережі потребує обґрунтування економічної її доцільності, виходячи з аналізу витрат на розробку та впровадження. Тому метою економічного розділу є здійснення відповідних розрахунків, які дозволять встановити економічний ефект від впровадження та налагодження систем політики безпеки комп'ютерної мережі.

3.1 Розрахунок (фіксованих) капітальних витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

До капітальних витрат належать витрати на розробку політики безпеки інформації, які визначаються виходячи з трудомісткості розробки політики безпеки інформації.

Визначення 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):

$$t = t_{тз} + t_{в} + t_{а} + t_{взз} + t_{озб} + t_{овр} + t_{д},$$ годин,

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;

$t_{взз}$ – 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.

Визначено, що відповідно до етапів розробки політики безпеки інформації, тривалість операцій склала наступні величини:

$t_{тз}$=16 годин, $t_{в}$=31 годин, $t_{тз}$=19 годин, $t_{вз}$=16 годин, $t_{озб}$=9 годин, $t_{овр}$=9 годин, $t_{д}$=10 годин. Отже,

$$t=16+31+19+16+9+9+10= 110 \text{ годин.}$$

Розрахунок витрат на створення політики безпеки інформації

Витрати на розробку політики безпеки інформації Крп складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки Ззп і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації Змч.

Розрахуємо витрати на створення ПБ. Розрахунок проводиться за формулою (3.1):

$$Крп = Ззп + Змч \text{ , грн.,} \qquad (3.1)$$

де $К_{рп}$ - 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 (3.2):

$$Ззп = t \cdot Зіб, грн, \qquad (3.2)$$

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 - 75 грн/год.

Відповідно до формули 3.2 , витрати на заробітну плату спеціаліста ІБ становлять:

$З_{зп}$ = 110 год · 75 грн/год,

$З_{зп}$ = 8250 грн.

У свою чергу, витрати машинного часу визначаються за формулою (3.3):

$$З_{мч}=t \cdot С_{мч} = 110 \cdot 9{,}33 = 1026 \text{ грн.}, \text{ по правому краю номер} \quad (3.3)$$

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 (3.4):

$$С_{мч} = P \cdot t_{нал} \cdot Се + \frac{Фзал \cdot На}{Fр} + \frac{Клпз \cdot Напз}{Fр} грн \quad (3.4)$$

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.

$$С_{мч} = 1{,}6 \cdot 3 \cdot 1{,}68 + \frac{7100 \cdot 0{,}3}{1920} + \frac{1670 \cdot 0{,}2}{1920} = 9{,}33 \text{ грн.}$$

Витрати на створення ПБ становлять:

$К_{рп}$= 9276 грн.

Відповідно до розроблених рекомендації щодо удосконалення існуючої системи інформаційної безпеки мережі ТОВ «Експрес Україна», а також рекомендацій та інструкції по безпосередній роботі з системою планується використання антивірусу Trend micro, який вже встановлений на комп'ютерах підприємства та потребує лише подовження ліцензії.

Апаратні засоби, які необхідно придбати відповідно до розроблених рекомендацій, зазначені у таблиці 3.1.

Таблиця 3.1 - Апаратні засоби, які необхідно придбати

Назва обладнання	Кількість, шт.	Ціна, грн.
Відіорегістратор Dahua Technology 1U PoE DH-NVR4216-16P-4KS2	1	2660
1МП купольна HDCVI відеокамера Dahua Technology DH-HAC-HDW1000RP-S3	10	4200
Кабель для відеокамер BNC+DC (100м)	2	600
2 ТБ HDD для відеорегістратора	1	2300
Сервер для журналювання подій безпеки DELL R320 (процесор Xeon six core e5-2430L 2 ГГЦ V2 2.40 ГГЦ/RAM 16 ГБ, RAID-контроллер PERC H710p)	1	10512
Жорсткий диск Western Digital Ultrastar DC HC310 HDD (SAS з'єднання) 6TB	1	10146

Продовження таблиці 3.1

Назва обладнання	Кількість, шт.	Ціна, грн.
Стрічкова система зберігання даних HP LTO-5 3000 1U RACKMOUNT	1	43600
Дата-картридж Hpe LTO-5 Ultrium 3TB	1	1500
Керовані комутатори Edge-core Ecs3510-28T	3	12075
Пульт керування Орион -16И.2	1	3470
Датчик відкриття дверей Satel B-2S	10	820
Датчик розбиття скла Satel INDIGO	10	4560
ІЧ Датчик руху DSC LC-100 PI	10	3140
Комплект опечатування кабінетів, тубус для них та шкафчик	10	3150

Всього буде затрачено на нове обладнання 102733 грн.

Витрати на встановлення обладнання та налагодження системи інформаційної безпеки складають 20% відсотків від первісної вартості програмного забезпечення, тобто 20546 грн.

Таким чином, за формулою (3.5), капітальні (фіксовані) витрати на створення політики інформаційної безпеки підприємства складають:

$$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} = 9276 + 102733 + 20546 = 132555 \text{ грн.} \quad (3.5)$$

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

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн;

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, тис. грн;

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

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу,

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

3.1.1 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають за формулою (3.6):

$$С = С_{в} + С_{к} + С_{ак}\text{ , грн.} \qquad (3.6)$$

$С = 0 + 132633,11 + 0 = 132633,11$ грн.

де $С_{в}$ - вартість відновлення й модернізації системи ($С_{в} = 0$);

$С_{к}$ - витрати на керування системою в цілому;

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак} = 0$ грн).

Витрати на керування системою інформаційної безпеки ($С_{к}$) складають за формулою (3.7):

$$С_{к} = С_{н} + С_{а} + С_{з} + С_{ел} + С_{о} + С_{тос}\text{, грн.} \qquad (3.7)$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються ($С_{н} = 0$ грн.).

Річні амортизаційні відрахування усього купленого обладнання із корисним строком використання 5 років, за прямолінійним методом нарахування амортизації складуть:

$С_{а} = 102733 / 5 = 20546,6$ грн.

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_{з}$), знаходиться за формулою (3.8):

$$С_{з} = З_{осн} + З_{дод}\text{, грн.} \qquad (3.8)$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 8000 грн. Додаткова заробітна плата – 10% від основної заробітної плати. Отже,

$С_з = 8000 \cdot 12 + 8000 \cdot 12 \cdot 0,1 = 105600$ грн.

Ставка ЄСВ для всіх категорій платників з 01.01.2019 р. складає 22%.

$С_{св} = 105600 \cdot 0,22 = 23232$ грн.

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою (3.9):

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.}, \quad (3.9)$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=1,6 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,68 грн/кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$С_{ел} = 1,6 \cdot 1920 \cdot 1,68 = 5160,96$ грн.

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат - 1% ($С_{тос} = 132555 \cdot 0,01 = 1325,55$ грн.).

Витрати на керування системою інформаційної безпеки ($С_к$) визначаються за формулою 3.7 відповідно:

$С_к = 0+20546,6 +105600+5160,96+0+1325,55 = 132633,11$ грн.

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають 132633,11 грн.

3.2 Оцінка можливого збитку від атаки на вузол або сегмент мережі

3.2.1 Оцінка величини збитку

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки для умовного підприємства.

Необхідні вихідні дані для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 2 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 1 година;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 3 годин;

$З_о$ – заробітна плата обслуговуючого персоналу (інженерів-програмістів), 9000 грн/міс;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 11000 грн/міс;

$Ч_о$ – чисельність обслуговуючого персоналу (інженерів-програмістів), 4 особи;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 26 осіб;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 12000 тис. грн. у рік;

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

I – число атакованих сегментів корпоративної мережі, 1;

N – середнє число атак на рік, 12.

Упущена вигода від простою атакованого сегмента корпоративної мережі знаходиться за формулою (3.10):

$$U = П_п + П_в + V, \qquad (3.10)$$

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

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

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

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:

$$П_П = \frac{11000 \cdot 12}{176} \cdot 2 = 1500 \text{ грн.},$$

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

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових і знаходиться за формулою (3.11):

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

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

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

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

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

$$П_{ви} = \frac{11000 \cdot 12}{176} \cdot 3 = 2250 \text{ грн.}$$

Витрати на відновлення сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{9000 \cdot 1}{176} \cdot 1 = 51{,}13 \text{ грн.}$$

$П_в = 2250 + 51{,}13 = 2301{,}13$ грн.

Втрати від зниження очікуваного обсягу прибутків за час простою атакованого вузла або сегмента корпоративної мережі визначаються за формулою

(3.12), виходячи із середньогодинного обсягу прибутку і сумарного часу простою сегмента корпоративної мережі:

$$V = \frac{O}{F_Г} \cdot (t_П + t_В + t_{ВИ}) \quad , \qquad (3.12)$$

$$V = \frac{12000000}{2080} \cdot (2 + 1 + 3) = 34615{,}38 \text{ грн.}$$

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

U = 1500+ 2301,13 +34615,38= 38416,51 грн.

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

$B = \sum_i \sum_n U = \sum_1 \sum_{12} 39166{,}51 = 460998{,}12$ грн.

3.2.2 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається за формулою (3.13) з урахуванням ризиків порушення інформаційної:

$$E = B \cdot R - C \text{ грн.}, \qquad (3.13)$$

де B – загальний збиток від атаки у разі перехоплення інформації, тис. грн;

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці (59%);

C – щорічні витрати на експлуатацію системи інформаційної безпеки.

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

E = 460998,12·0,59 –132633,11 = 139355,78 грн.

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки і знаходиться за формулою (3.14):

$$ROSI = \frac{E}{K}, \text{ частки одиниці,} \qquad (3,14)$$

де E – загальний ефект від впровадження системи інформаційної безпеки грн;

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

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{139355,78}{132555} = 1,05 \text{ частки одиниці.}$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції знаходиться за формулою (3.15):

$$ROSI > (N_{деп} - N_{інф})/100), \qquad (3.15)$$

де $N_{деп}$ – річна депозитна ставка, (18 %);

$N_{інф}$ – річний рівень інфляції, (9 %).

Розрахункове значення коефіцієнта повернення інвестицій:

1,05 > (18 – 9)/100 = 1,05 > 0,09.

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки і знаходиться за формулою (3.16):

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{1,05} = 0,95 \text{ років.} \qquad (3.16)$$

3.4 Висновок

Розробка систем політики безпеки ТОВ «Експрес Україна» є економічно доцільним, оскільки капітальні та експлуатаційні витрати будуть меншими за можливий відвернений збиток. Капітальні витрати складають 132555 грн., експлуатаційні – 132633,11 грн. Величина річного економічного ефекту складає 139355,78 грн. Коефіцієнт повернення інвестицій ROSI складає 1,05 грн/грн.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи було визначено:

У першому розділі було:

– описано стан інформаційної безпеки у світі та окремо в Україні;

– зазначено важливість створення політики безпеки з КСЗІ на підприємстві.

У другому розділі було:

– детально проведено аналіз об’єкта інформаційної діяльності. Була проаналізована нормативна-правова база на ОІД;

– зроблено класифікацію циркулюючої інформації на підприємстві з подальшою оцінкою усіх можливих загроз;

– відносно загроз побудовано модель загроз та порушника, за результатом яких було розроблено політику безпеки та її технічну реалізацію на об’єкті, яка виключає з ІТС підприємства усі можливі ризики.

У третьому розділі було:

– проведено розрахунок капітальних витрат на впровадження політики безпеки на підприємство;

– отримані дані після розрахунку, говорять про те, що впровадження встановленої політики безпеки та її технічна реалізація є доцільними для цього об’єкту.

ПЕРЕЛІК ПОСИЛАНЬ

1. Кіберзлочинність у світі . [Електронний ресурс] - Режим доступу: http://www.dut.edu.ua/ua/news-1-611-8410-fahivci-z-upravlinnya-informaciynoyu-ta-kibernetichnoyu-bezpekoyu-gotovi-do-vidbittya-kiberatak_kafedra-upravlinnya-informaciynoyu-ta-kibernetichnoyu-bezpekoyu

2. Статистика щодо кіберзлочинів в Україні. [Електронний ресурс] - Режим доступу: https://cyberpolice.gov.ua

3. НД ТЗІ 1.6-005-2013 «Про затвердження нормативного документа системи технічного захисту інформації» Київ: Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України, 2013

НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» . Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 2005.

4. ДСТУ 3396.1-96 «Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. » [Електронний ресурс] Режим доступу: https://tzi.com.ua/downloads/DSTU%203396.1-96.pdf

5. НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі»; Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 2000.

6. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999.

7. НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999.

8. НД ТЗІ 2.5-008-02 «Вимоги із захисту службової інформації від несанкціонованого доступу підчас оброблення в автоматизованих системах класу

2» Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 2002.

9. НД ТЗІ 2.5-010-03 «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу» Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 2003.

10. НД ТЗІ 3.7-001-99 «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі» Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 2003.

11. НД ТЗІ 3.6-001-2000 «Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу» Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 2000.

12. НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу» Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999.

13. Методичні рекомендації до виконання кваліфікаційних робіт бакалаврів спеціальності 125 кібербезпека/Упоряд.: О.В. Герасіна, Д.С. Тимофєєв, О.В. Кручінін, Ю.А. Мілінчук - Дніпро: НТУ "ДП", 2020.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	1	
4	А4	Вступ	1	
4	А4	Стан питання. Постановка задачі	5	
5	А4	Спеціальна частина	56	
6	А4	Економічний розділ	12	
7	А4	Висновки	1	
8	А4	Перелік посилань	2	
9	А4	Додаток А	1	
10	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	
14	А4	Додаток Д	1	

ДОДАТОК Б. Перелік матеріалів на електронному носії

1. Пояснювальна записка – Скрипнік Андрій 125-17-2.docx

2. Пояснювальна записка – Скрипнік Андрій 125-17-2.pdf

3. Презентація – Скрипнік Андрій 125-17-2.

ДОДАТОК В. Відгук керівника економічного розділу

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

Дата: _____ Підпис: _____

ДОДАТОК Г

Відгук керівника кваліфікаційної роботи

ВІДГУК

на кваліфікаційну роботу студента групи 125-17-2

Скрипніка Андрія Валерійовича

на тему: «Політика безпеки в інформаційно-телекомунікаційній систем і комунального підприємства ТОВ «Експрес Україна»

Пояснювальна записка складається зі вступу, трьох розділів і висновку, викладених на 73 сторінках.

Метою кваліфікаційної роботи є підвищення рівня захищеності інформації в ІТС ТОВ «Експрес Україна».

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: проведення обстеження ТОВ «Експрес Україна», проведення аналізу ризиків інформаційної безпеки з виявленням загроз; створення документів з політики безпеки.

Практичне значення результатів кваліфікаційної роботи полягає у підвищені рівня захисту інформації в ІТС організації, за рахунок розробки політик безпеки інформації.

Оформлення пояснювальної записки до кваліфікаційної роботи виконано з незначними відхиленнями від стандартів.

За час дипломування Скрипнік А.В. проявив себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації бакалавра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека»

.

Рівень запозичень у кваліфікаційній роботі не перевищує вимог «Положення про систему виявлення та запобігання плагіату».

Кваліфікаційна робота заслуговує оцінки «_____».

Керівник кваліфікаційної роботи **Горєв В.М.**

Керівник спец, розділу **Святошенко В.О.**