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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Малинки Богдана Леонідовича*

академічної групи *125-16-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплексна система захисту інформації інформаційно-телекомунікаційної системи підприємства ТОВ «ТехноСервіс»*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.ф.- м.н, проф Гусєв О.Ю.			
розділів:				
спеціальний	Ст. викл. Святошенко В.О.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Тимофєєв Д.С.			

Дніпро
2020

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту *Малинки Богдана леонідовича* академічної групи *125-16-1*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему *Комплексна система захисту інформації інформаційно-телекомунікаційної системи підприємства ТОВ «ТехноСервіс»*

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № __

Розділ	Зміст	Термін виконання
Розділ 1	Надасти загальний аналіз проблем інформаційної безпеки України, розглянуто стан інформаційної безпеки на підприємствах, які займаються розробкою програмного забезпечення в ігрової індустрії.	29.03.2020
Розділ 2	Розглянути необхідність розробки КСЗІ. Навести загальні відомості про об'єкт інформаційної діяльності, провести обстеження ОІД, категоріювання інформаційно-телекомунікаційної, підібрати профіль захищеності.	24.05.2020
Розділ 3	Розрахувати доцільність використання розробленої КСЗІ, та економічну ефективність впровадження її елементів в інформаційно-телекомунікаційну систему на об'єкті інформаційної діяльності.	14.06.2020

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі: 08.01.2020р.

Дата подання до екзаменаційної комісії: 15.06.2020р.

Прийнято до виконання _____ _____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 82 с., 2 рис., 21 табл., 7 додатки, 20 джерел.

Об`єкт дослідження: інормаційно-телекомунікаційна система ТОВ «ТехноСервіс».

Мета роботи: підвищення ефективності забезпечення безпеки інформації в ІТС ТОВ «ТехноСервіс».

Методи розробки: спостереження, порівняння, аналіз, опис.

В першому розділі кваліфікаційної роботи надано загальний аналіз проблем інформаційної безпеки України, розглянуто стан інформаційної безпеки на підприємствах, які займаються розробкою програмного забезпечення та машинного інтелекту.

В другому розділі кваліфікаційної роботи розглянуто необхідність розробки КСЗІ, стан інформаційної безпеки підприємства. Наведено загальні відомості про об'єкт інформаційної діяльності, проведено обстеження ОІД, категоріювання інформаційно-телекомунікаційної системи, підібрано профіль захищеності. Розраховано коефіцієнти ймовірності реалізації загроз, розроблено КСЗІ.

В третьому розділі кваліфікаційної роботи розраховано доцільність використання розробленої КСЗІ, та економічну ефективність впровадження її елементів в інформаційно-телекомунікаційну систему на об'єкті інформаційної діяльності а також розрахунок економічної ефективності впровадження системи контролю виконання політики інформаційної безпеки.

ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА, ОБ`ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, АНАЛІЗ ЗАГРОЗ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ

РЕФЕРАТ

Пояснительная записка: 82 с., 2 рис., 21 табл., 7 приложений, 20 источников.

Объект исследования: инормацийно-телекоммуникационная система ООО «ТехноСервіс». Все данные о предприятии были изменены в целях обеспечения анонимности предприятия.

Цель работы: разработка и впровадженння КСЗИ для ИТС ООО «ТехноСервіс».

Методы разработки: наблюдение, сравнение, анализ, описание.

В первом разделе квалификационной работы предоставлено общий анализ проблем информационной безопасности Украины, рассмотрено состояние информационной безопасности на предприятиях, занимающихся разработкой программного обеспечения и игровой индустрии.

Во втором разделе квалификационной работы рассмотрена необходимость разработки КСЗИ, состояние информационной безопасности в настоящее время. Приведены общие сведения об объекте информационной деятельности, проведено обследование ОИД, категорирование информационно-телекоммуникационной, подобрано профиль защищенности. Рассчитаны коэффициенты вероятности реализации угроз, разработаны КСЗИ.

В третьем разделе квалификационной работы рассчитаны целесообразность использования разработанной КСЗИ, и экономическую эффективность внедрения ее элементов в информационно-телекоммуникационную систему на объекте информационной деятельности, а также расчет экономической эффективности внедрения системы контроля исполнения политики информационной безопасности.

ИНФОРМАЦИОННО-ТЕЛЕКОМУНИКАЦИОННЫЕ СИСТЕМЫ, ОБЪЕКТ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ, АНАЛИЗ УГРОЗ, МОДЕЛЬ УГРОЗ, МОДЕЛЬ НАРУШИТЕЛЯ, КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

ABSTRACT

Explanatory note: 82 pages, 2 figures, 21 tables, 7 appendices, 20 sources.

Object of study: information and telecommunication system of TekhnoServis LLC. All data about the company have been changed in order to ensure the anonymity of the company.

Purpose: development and implementation of KSZI for ITS TekhnoServis LLC.

Development methods: observation, comparison, analysis, description.

The first section of the qualification work provides a general analysis of information security problems in Ukraine, the state of information security in enterprises engaged in software development and gaming industry.

The second section of the qualification work considers the need to develop KSZI, the state of information security at present. The general information on the object of information activity is given, the OID survey is carried out, the information and telecommunication categorization is carried out, the security profile is selected. Threat probability realization coefficients are calculated, KSZI is developed.

The third section of the qualification work calculates the feasibility of using the developed CCIS, and the economic efficiency of its elements in the information and telecommunications system at the object of information activities, as well as the calculation of economic efficiency of the information security policy control system.

INFORMATION AND TELECOMMUNICATION SYSTEM, OBJECT OF INFORMATION ACTIVITY, ANALYSIS OF THREATS, MODEL OF THREATS, MODEL OF THE VIOLATOR, COMPREHENSIVE INFORMATION PROTECTION SYSTEM

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

В роботі використовуються такі позначення і скорочення:

АС - автоматизована система;

ДСТУ - державний стандарт України;

ІзОД — інформація з обмеженим доступом;

ІТС – інформаційно-телекомунікаційна система;

КЗЗ — комплекс засобів захисту;

КС — комп'ютерна система;

КСЗІ — комплексна система захисту інформації;

НД — нормативний документ;

НД ТЗІ - нормативний документ системи технічного захисту інформації;

НСД — несанкціонований доступ;

ОІД – об’єкт інформаційної діяльності;

ОС — обчислювальна система;

ПЗ — програмне забезпечення.

ЗМІСТ

ВСТУП

Сучасний світ неможливо уявити без програмного забезпечення (ПЗ). Розробка ПЗ перетворилася на окрему галузь, що займає чільне місце у світовій економіці, в тому числі в Україні. У 2016 році світові витрати на ІТпослуги склали 1229 млрд дол. США, і ця галузь зростає щороку, в тому числі очікується зростання на 3,2% у 2017 році. При цьому із розвитком технологій, з новою технологічною революцією, цифровізацією світу значення розробки програмного продукту лише зростатиме.

Сьогодні Україна не залишається осторонь глобальних процесів. Наша держава одна з найкращих для розміщення замовлень у сфері аутсорсингу бізнес-процесів та ІТ, що підтверджує 24 місце у рейтингу привабливості. Слід зауважити, що такі досягнення завдячують багато в чому тому, що ринок є абсолютно новим. Він почав розвиватися вже за часів незалежності, і позбавлений багатьох вад, притаманних традиційним сферам економіки, які дісталися у спадок від Радянського Союзу: монополізації, експлуатації ресурсів, олігархізації і т.д. Ринок ПЗ – яскравий приклад нової економіки знань, який може стати локомотивом до переходу України для постіндустріальної економіки, яка вже давно є реальністю для розвинених країн.

Ринок розробки ПЗ сьогодні є здебільшого експортно-орієнтованим і займає третє місце за обсягами виручки, тож є одним із головних джерел надходження валютних коштів в Україну. Експортно-орієнтований сектор розробки ПЗ у 2016 році склав 3,2 млрд дол. США, що становить близько 26% експорту послуг за відповідний період і 7% сукупного експорту товарів і послуг. Таким чином ринок позитивно впливає на стабільність курсу національної валюти і цін в державі.

В умовах сучасного розвитку інформаційних технологій та середовища, нагальним питанням постає безпека інформаційних ресурсів. Те, що з одного боку спрощує та підвищує ефективність введення бізнесу, з іншого потребує сталих та регламентованих правил поводження з інформацією аби запобігти матеріальним збиткам. Слід зауважити, що в рамках нестабільної економічної ситуації в країні

керівництво організацій нерідко зневажає потребу у створенні та підтримці системи захисту інформації.

Однією із найважливіших вимог забезпечення сталого функціонування будь-якого підприємства є надійність роботи інформаційної системи та зовнішніх інформаційних ресурсів в мережі Internet.

Відповідний заданим вимогам рівень інформаційної безпеки (ІБ) може бути досягнутий виключно за умови комплексного підходу, що містить у собі програмні, апаратні та організаційні міри захисту. Доволі часто останніми нехтують, хоча вони є найбільш вагомими та в середньому повинні складати більше 50% від усіх заходів у цьому напрямку.

Стає очевидним, що створення КСЗІ являється фундаментальною частиною побудови режиму інформаційної безпеки для організації ефективної роботи структури будь-якого типу та масштабів. КСЗІ зводить до мінімуму наслідки не коректних або випадкових дій людини у системі, сприяє створенню культури інформаційної безпеки та дисциплінує співробітників компанії.

На рисунку 1.1 Відображено співвідношення основних типів кіберінцедентів в Україні.

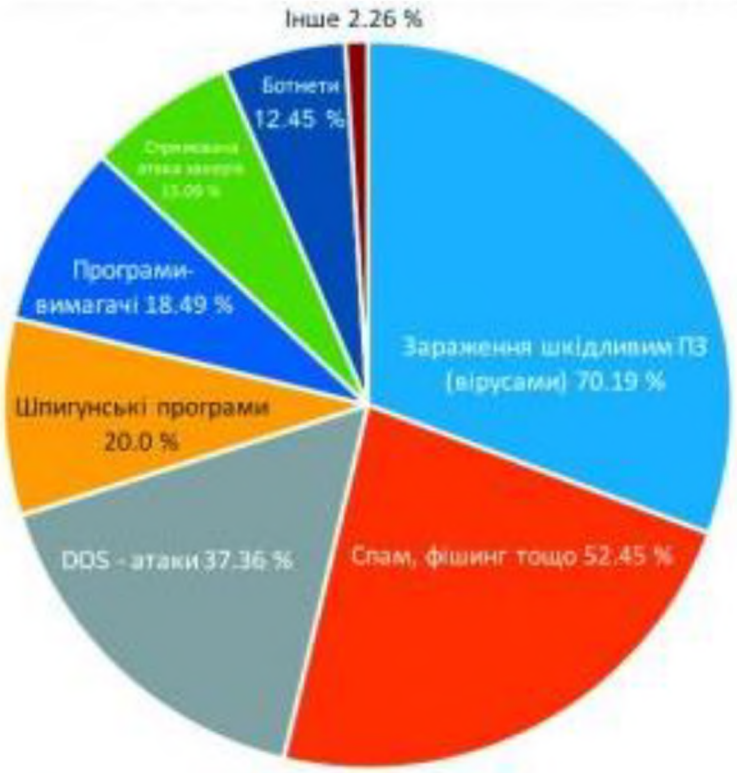

Рисунок 1.1 Співвідношення основних типів загроз в Україні

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

З процесом глобалізації та розвитку технологій, бізнесу та промисловості все більшої потреби в собі зазнають інформаційні технології (ІТ) та все що з ними пов'язано. За останні роки світ перейшов на збереження та обмін інформацією через комп'ютерні системи, мережу Інтернет, фізичні носії інформації та інше. Будь-яка сфера діяльності тепер насамперед спирається на використання ІТ, адже вони стали невід'ємною складовою життєдіяльності, що спонукало виникнення інформаційних відносин.

У сучасному світі інформацію слід ставити на один рівень із матеріальними та енергетичними ресурсами, оскільки вона є важливим показником якісних змін у житті суспільства. Постає питання безпеки інформації та її підтримки і забезпечення за допомогою сучасних методів. Дуже часто інформаційній безпеці приділяється недостатньо уваги, що потім несе за собою важкі наслідки. Економічні збитки, погіршення ділових відносин, погана репутація та недовіра працівників – усе це може відбутися з підприємством, що допустило витік інформації, яка потребувала захисту.

За перші шість місяців 2018 року працівники Департаменту кіберполіції супроводжували більше чотирьох тисяч кримінальних правопорушень у сфері протидії кіберзлочинності, з них - 2,3 тисячі – викрито протягом 2018 року. Про це йшлося під час наради керівництва Департаменту кіберполіції Національної поліції.

За словами начальника Департаменту кіберполіції Сергія Демедюка, серед основних напрямків діяльності підрозділу слід відмітити позитивну роботу з протидії злочинам у сфері кібербезпеки, платіжних систем, електронної комерції та боротьбу зі злочинами у сфері поширення протиправного контенту. Водночас, він відмітив стрімке збільшення кількості кримінальних правопорушень у сфері платіжних систем та кібербезпеки у літній період.

З огляду на рисунку 1.2 на зростання кіберзлочинності в Україні та розмірів її наслідків, указом Президента України було затверджено Стратегію кібербезпеки України , основною метою якої є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави .

Також було затверджено положення про Національний координаційний центр кібербезпеки, основними завданнями якого є: аналіз стану кіберзбезпеки, стану фінансового та організаційного забезпечення програм та заходів із реалізації державної політики у сфері забезпечення кібербезпеки України, участь у забезпеченні розроблення і впровадження суб'єктами забезпечення кібербезпеки механізмів обміну інформацією, необхідною для організації реагування на кібератаки і кіберінциденти, усунення їх чинників та негативних наслідків тощо.

Рисунок 1.2 Кількість кіберзлочинів 2019 року в Україні

Слід зазначити, що беручи до уваги вищезгадані прецеденти інформаційних атак, найчастішим способом одержання несанкціонованого доступу в систему є використання недосконалості побудови та дотримання правил поведінки користувачів у мережі Internet, правил користування електронною поштою.

У статті CERT-UA [20] зазначено, що використання безкоштовних поштових сервісів у службових цілях потребує обов'язкового узгодження з керівництвом організації, через можливе порушення корпоративної ПБІ. Використання таких сервісів для державних потреб не рекомендується. Хоча, за результатами опитування CERT-UA 134 державних установ у 2015 році з'ясовано, що тільки 16 з них користуються власним поштовим сервісом.

Основними проблемами стану захищеності інформації в інформаційно-телекомунікаційних системах малих підприємств є: небажання керівництва виділяти кошти на створення системи захисту інформації, відсутність організаційних правил поводження з інформацію, що має обмежений доступ, відмова у використанні ліцензійного основного та прикладного програмного забезпечення тощо.

Нагальним питанням постає повсюдне застосування і впровадження основ інформаційної безпеки незалежно від масштабів та форм власності підприємств.

1.2 Аналіз нормативно-правового забезпечення захисту інформації

Під час створення комплексної системи захисту інформації, як сукупності організаційних і інженерних заходів, програмно-апаратних засобів, слід керуватися низкою нормативно-правових документів та актів, серед них:

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

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

- НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі;

- НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу;

- НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу;

- НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2;

- НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі;

- 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;

- НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу;

Дія документу поширюється тільки на ІТС, в яких здійснюється обробка інформації автоматизованим способом. Його побудовано у вигляді керівництва, яке містить перелік робіт і посилання на діючі нормативні документи, у відповідності до яких ці роботи необхідно виконувати.

Нормативний документ призначений для суб'єктів інформаційних відносин, діяльність яких пов'язана з обробкою інформації, що підлягає захисту; розробників комплексних систем захисту інформації в ІТС; для постачальників компонентів ІТС, а також для фізичних та юридичних осіб, які здійснюють оцінку захищеності оброблюваної інформації на відповідність вимогам ТЗІ.

Встановлений цим НД ТЗІ порядок є обов'язковим для всіх суб'єктів системи ТЗІ в Україні незалежно від їхньої організаційно-правової форми та форми власності, в ІТС яких обробляється інформація, яка належить до державних інформаційних ресурсів, належить до державної чи іншої таємниці або окремих видів інформації, необхідність захисту якої визначено законодавством. Якщо в ІТС обробляються інші види інформації, то вимоги цього нормативного документа суб'єкти системи ТЗІ можуть використовувати як рекомендації.

1.3 Постановка задачі

У нормативних документах зазначена необхідність впровадження системи захисту інформації, на об`єктах інформаційної діяльності, де циркулює інформація

відкрита, що потребує захисту та інформація з обмеженим доступом. Власник підприємства визначає потребу в КСЗІ. Розробка КСЗІ починається з обстеження на ОІД. Під час обстеження ІТС розглядається як організаційно-технічна система, яка поєднує обчислювальну систему, фізичне середовище, середовище користувачів, оброблювану інформацію і технологію її обробки. Обгрунтуванням для створення КСЗІ є Акт категорювання об'єкту, закріплений в Додатку 1. Також обгрунтуванням для створення КСЗІ є Наказ на створення КСЗІ від директора компанії за сумісністю власник інформації.

Для створення КСЗІ необхідно:

- загальна характеристика ОІД;
- загальна структурна схема і склад обладнання, технічних і програмних засобів, їхні зв'язки, особливості конфігурації, архітектури й топології, програмні і програмно-апаратні засоби захисту інформації, взаємне розміщення засобів тощо;
- умови функціонування ОІД, особливостей розташування його на місцевості тощо;
- функціонального та кількісного складу користувачів, їхніх функціональних обов'язків та рівня кваліфікації;
- повноважень користувачів щодо допуску до відомостей, які обробляються в ІТС, доступу до ІТС та її окремих компонентів;
- повноважень користувачів щодо управління КСЗІ;
- визначаються завдання захисту інформації в ІТС, мета створення КСЗІ;
- здійснюється аналіз ризиків (вивчення моделі загроз і моделі порушника, можливих наслідків від реалізації потенційних загроз, величини можливих збитків та ін.) і визначається перелік суттєвих загроз;
- визначаються загальна структура та склад КСЗІ;

1.4 Висновки до першого розділу

Розглянуті актуальний стан злочинів в сфері інформаційної безпеки. Виявлено значне збільшення інцидентів порушення інформаційної безпеки на території України. Зазначена актуальність розвитку кібербезпеки.

В розділі приведено перелік нормативно-правових документів в сфері захисту інформації, зазначено основні положення. Серед документів, що є правовою основою забезпечення безпеки інформації розглянуті НД ТЗІ та їх галузі використання, Закони України, положення та накази.

Обґрунтовано потребу у створенні КСЗІ на підприємстві для запобігання НСД до важливих ресурсів системи. До етапів створення КСЗІ, що використані в роботі віднесені, відповідно до нормативної документації: обґрунтування необхідності створення, обстеження на ОІД, аналіз та оцінка інформаційних ризиків та розробка політики безпеки, що враховує загрози найвищого рівня

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальні відомості про типове підприємство.

ТОВ «ТехноСервіс» - глобальна компанія, що надає послуги з формування цифрової стратегії і розробки програмного забезпечення, з клієнтською базою. «ТехноСервіс» обслуговує своїх клієнтів в Північній Америці, Європі та в Азіатсько-Тихоокеанському регіоні. Штаб-квартира компанії розташована в місті Київ. «ТехноСервіс» надає послуги і створює технологічні рішення в таких індустріях як автомобілебудування, фінансові послуги, подорожі та готельний бізнес, охорона здоров'я, біотехнології, медіа та телекомунікації. У компанії працює близько 13 тисяч чоловік. Центральний офіс підрозділу машиного навчання розташований у місті Дніпро.

Данні про підприємство були частково змінені задля забезпечення анонімності підприємства.

Характеристика підприємства

Офіс компанії займає 3 поверхи з 4.

Адреса: вулиця Шевченка, 53, Дніпро́, Дніпропетровська область, 49000

Форма власності: приватна власність.

Режим роботи підприємства:

Час роботи: 09.00 – 18.00

Перерва: с 13.00 до 14.00

Робочі дні: понеділок – п’ятниця.

Пропускний режим

З усіх сторін свіну КЗ обмежена зовнішніми стінами будівлі.

На підприємстві вхід на територію здійснюється через КПП на головному вході на першому поверсі будівлі, де встановлено пункти охорони. Доступ на територію підприємства здійсньюєть через 2 ліфти, та внутрішній ресепшн компанії на 2 поверсі. Кожний співробітник та відвідувач проходить на об’єкт за допомогою електронної картки - пропуску. На прохідній встановлено електронні системи

контролю та турнікети, також в наявності 2 охоронця з металодетекторами. Охоронці дублюються на першому поверсі. Охорону здійснює власна служба охорони компанії цілодобово.

На ситуаційному плані на рисунку відображено положення об'єкту інформаційної діяльності відносно об'єктів місцевості.(Додаток 2/Рисунок1).

Таблиця 2.1 Прилеглі будівлі до ОІД

Номер	Назва будівлі	Опис	Адресса
1	Магазин Lifecell	Магазин Lifecell - 1 поврех 2-16 поверх - жила будівля	вулиця Виконкомівська, 7, Дніпро́, Дніпропетровська область, 49044
2	Креди Агриколь Банк Пао, Днепропетровская Дирекция	1 поверх - банк 2-4 поврех - жила будівля	вулиця Південна, 2, Дніпро́, Дніпропетровська область, 49044
3	Kings&Queens Coffee Point	1 поверхова будівля	вулиця Виконкомівська, 7, Дніпро́, Дніпропетровська область, 49000
4	Жила будівля	12 поверхів	вулиця Шевченка, 51, Дніпро́, Дніпропетровська область, 49000

Продовження таблиці 2.1 Прилеглі будівлі до ОІД

Номер	Назва будівлі	Опис	Адресса
5	Каскад Плаза	Багатоповерховий торгівельний центр та бізнес центр	бульвар Катеринославський, 1, Дніпро́, Дніпропетровська область, 49000
6	Торгівельний центр	Шпіль з годинником	бульвар Катеринославський, 2, Дніпро́, Дніпропетровська область, 49000
7	Адміністративне приміщення	4 поверхове	вулиця Шевченка, 30, Дніпро́, Дніпропетровська область, 49000
8	Торгівельний центр/ бізнес центр	1 поврех - торгівельний центр 2-4 поверх - бізнес центр	бульвар Катеринославський, 2, Дніпро́, Дніпропетровська область, 49000
9	Нежила будівля	12 поверхів	вулиця Шевченка, 32, Дніпро́, Дніпропетровська область, 49000

Продовження таблиці 2.1 Прилеглі будівлі до ОІД

Номер	Назва будівлі	Опис	Адресса
10	Жила будівля	5 поверхова жила булівля	вулиця Старокозацька, 6, Дніпро́, Дніпропетровська область, 49000
11	Жила будівля	5 поверхова жила булівля	вулиця Старокозацька, 6, Дніпро́, Дніпропетровська область, 49000
12	Reikartz Collection Дніпро	5 поверховий готель	вулиця Шевченка, 53а, Дніпро́, Дніпропетровська область, 49000
13	Module	Одноповерхова будівля, нічний клуб	вулиця Січових Стрільців, 5, Дніпро́, Дніпропетровська область, 49000
14	Теехнічна будівля	2 поверхи	вулиця Шевченка, 53, Дніпро́, Дніпропетровська область, 49044

Фізичні характеристики будівлі:

– зовнішні стіни – залізлбетонні пліти з верхнім шаром із червоної декоративної цегли;

– внутрішні стіни – гіпсокартон та фарба;

– дах будівлі викладений руберойдом. Вхід на дах здійснюється через спеціальне приміщенняна останньому етажі;

– підлога – залізобетонні плити перекриття, укриті плиткою;

– двері головного входу мають розміри 7000мм * 2300мм, виконані зі скла завтовшки 4мм, оздоблені 4 механізмами запирання, який використовують з 23.00 по 08.00 ;

– вікна приміщщення виконані з металопластику, 3070мм * 4500мм , вікна двухкамерні за без можливості відчиняти. Лише 5 вікон у будівлі мають можливість відчинятись;

– територія, навколо будівлі - відкрита.

– територію навколо будівлі впорядковано, вона має асфальтове покриття;

Фізичні характеристики приміщення :

– зовнішні стіни – залізлбетонні пліти з верхнім шаром із червоної декоративної цегли;

– внутрішні стіни – гіпсокартон та фарба;

– дах приміщення межується з підлогою 3-го поверху, додатково покритий плитами завтовшкі 12мм з мінерального волокна;

– підлога – залізобетонні плити перекриття, укриті плиткою;

– міжкімнатні двері мають розміри 1200 мм * 2000мм, виконані з ламінованого МДФ, кожна міжкімнатна дверь має один врізний замок;

– вікна приміщщення виконані з металопластику, 3070мм * 4500мм , вікна двухкамерні за без можливості відчиняти. У приміщенні наявне одне вікно з можливістю відкривання;

Двері не зачиняються, бо на об'єкті ведеться цілодобова охорона. Охорону здійснює внутрішня служба охорони компанії, яка ведеться 24 години на добу. До обов'язків охорони входить:

- Цілодобовий контроль пропускних пунктів;

- Контроль за системами спостереження;
- Реагування на інцеденти;

Таблиця 2.2 Системи комунікації, життєзабезпечення та зв'язку

Система комунікації	Вихід за межі КЗ	Характеристика
Система електро-постачання	+	Підключена до трансформаторної підстанції, яка має сторонніх споживачів і знаходиться за межами КЗ
Система опалення	+	Підключена до автономної мережі, за межами КЗ
Система каналізації	+	Підключена до міської мережі, яка знаходиться за межами КЗ
Система водопостачання	+	Підключена до автономної станції, яка знаходиться за межами КЗ
Телефонна лінія та Інтернет	+	Підключені до АТС «Фрегат"
Система вентиляції	+	Приточно-витяжна
Система сигналізації	-	Складається з датчиків руху Satel TOPAZ та датчиків диму АРТОН СПД-3.10 Б5.
Система кондиціонування	-	Спліт-система, що складається з двох блоків: зовнішнього та внутрішнього. Liberton AC 07C-P35. Габарити внутрішнього блоку 80x29x18,6 см, габарити зовнішнього блоку 60x48x25 см .

Таблиця 2.3 Перелік та розміщення ОТЗ/ДТЗС

Назва ОТЗ/ДТЗС	Розміщення	Мінімальна відстань	ОТЗ	ДТЗС
PC_1	Відділ розробки автоматизації / під робочим столом користувача	1,5	+	
PC_2	Відділ розробки автоматизації / під робочим столом користувача	1,5	+	
PC_3	Відділ розробки автоматизації / під робочим столом користувача	1,5	+	
PC_4	Відділ розробки автоматизації / під робочим столом користувача	3	+	
PC_5	Відділ розробки автоматизації / під робочим столом користувача	1,5	+	
PC_6	Відділ розробки автоматизації / під робочим столом користувача	1,5	+	
PC_7	Відділ розробки автоматизації / під робочим столом користувача	<1	+	
PC_8	Відділ розробки автоматизації / під робочим столом користувача	5	+	
PC_9	Відділ розробки автоматизації / під робочим столом користувача	1,7	+	
PCPR_1	Відділ розробки автоматизації / під робочим столом користувача	1,1	+	
PCPR_2	Відділ розробки автоматизації / під робочим столом користувача	1,2	+	
PCPR_3	Відділ розробки автоматизації / під робочим столом користувача	1,2	+	
PCPR_4	Відділ розробки автоматизації / під робочим столом користувача	1	+	
PCPR_5	Відділ розробки автоматизації / під робочим столом користувача	<1	+	
PCPR_6	Відділ розробки автоматизації / під робочим столом користувача	<1	+	

Продовження таблиці 2.3 Перелік та розміщення ОТЗ/ДТЗС

Назва ОТЗ/ДТЗС	Розміщення	Мінімальна відстань	ОТЗ	ДТЗС
PCPR_7	Відділ розробки автоматизації / під робочим столом користувача	<1	+	
PCPR_8	Відділ розробки автоматизації / під робочим столом користувача	<1	+	
PCPR_9	Відділ розробки автоматизації / під робочим столом користувача	1,3	+	
PCPR_10	Відділ розробки автоматизації / під робочим столом користувача	<1	+	
PCPR_11	Відділ розробки автоматизації / під робочим столом користувача	<1	+	
PCPR_12	Відділ розробки автоматизації / під робочим столом користувача	<1	+	
PCPDV_1	Відділ розробки автоматизації / під робочим столом користувача	3	+	
PCPDV_2	Відділ розробки автоматизації / під робочим столом користувача	4	+	
PCPDV_3	Відділ розробки автоматизації / під робочим столом користувача	4	+	
PCPDV_4	Відділ розробки автоматизації / під робочим столом користувача	5	+	
PCPDV_5	Відділ розробки автоматизації / під робочим столом користувача	6	+	
PCPDV_6	Відділ розробки автоматизації / під робочим столом користувача	4	+	
PCPDV_7	Відділ розробки автоматизації / під робочим столом користувача	4	+	
PCPDV_8	Відділ розробки автоматизації / під робочим столом користувача	5	+	
PCPDV_9	Відділ розробки автоматизації / під робочим столом користувача	6	+	

Продовження таблиці 2.3 Перелік та розміщення ОТЗ/ДТЗС

Назва ОТЗ/ДТЗС	Розміщення	Мінімальна відстань до КЗ /м	ОТЗ	ДТЗС
PCMDJS_1	Відділ розробки автоматизації / під робочим столом користувача	<1	+	
PCMDJS_2	Відділ розробки автоматизації / під робочим столом користувача	<1	+	
PCMDJS_3	Відділ розробки автоматизації / під робочим столом користувача	<1	+	
PCMDJS_4	Відділ розробки автоматизації / під робочим столом користувача	<1	+	
SW_1	Відділ розробки автоматизації / у металевому щитку на стіні	<1		+
SW_2	Відділ розробки автоматизації / у металевому щитку на стіні	<1		+
SW_3	Відділ розробки автоматизації / у металевому щитку на стіні	<1		+
SW_4	Відділ розробки автоматизації / у металевому щитку на стіні	<1		+
Кондиціонер 1	Відділ розробки автоматизації / біля стелі на стіні	<1		+
Кондиціонер 2	Відділ розробки автоматизації / біля стелі на стіні	<1		+
Камера відеоспостереження 1	Відділ розробки автоматизації / біля стелі на стіні у лівого боку кімнати	<1		+
Камера відеоспостереження 2	Відділ розробки автоматизації / біля стелі на стіні по центру кімнати	<1		+
Камера відеоспостереження 3	Відділ розробки автоматизації / біля стелі на стіні біля правого краю стіни	<1		+

Продовження таблиці 2.3 Перелік та розміщення ОТЗ/ДТЗС

Назва ОТЗ/ДТЗС	Розміщення	Мінімальна відстань до КЗ /м	ОТЗ	ДТЗС
Датчик руху 1	Відділ розробки автоматизації / біля стелі на стіні з лівого дальнього краю стіни	<1		+
Датчик руху 2	Відділ розробки автоматизації / біля стелі на стіні з правого дального краю стіни	<1		+
Датчик руху 3	Відділ розробки автоматизації / біля стелі на стіні з лівого ближнього краю	<1		+
Датчик руху 4	Відділ розробки автоматизації / біля стелі на стіні з правого ближнього краю	<1		+

Обстеження ОС

Під час роботи на у компнаії церкулює інформація з обмженим доступом, робота з якою чітко регламентован у політиці безпеки компанії.

В мережі компанії кожному комп'ютеру присвоєні імена, а саму мережу розділено на три робочі групи : директор, адміністратор, останні користувачі.

У межах ОІД, на якій проводилося обстеження не було адміністратора, але данна роль присутня у компанії. Кількість системних адміністраторів - 7 чоловік, кількість адміністраторів безпеки - 2 чоловік.

Кожна з цих груп має доступ лише до певних файлів, програм та інформації в цілому, у кожного користувача свої права доступу.

Обмін інформацією може відбуватись за допомогою локального серверу. У компанії також наявні принтери загального доступу, на схемі ОІД він не відображений, але в інших приміщеннях наявні прінтери, та співробітники її використовують.

Таблиця 2.4 Технічні засоби

Назва	Характеристика	Умовні позначення	Кількість	Серійний номер
Комутатор	D-Link DGS-1210-52MP Web Smart 48 x Gigabit Ethernet (10/100/1000 Мбит/с) 4 x SFP (mini-GBIC) Керований	SW_1 SW_2 SW_3 SW_4	4	HX424C15FB3/8
Робоча станція 1	ASUS D340MC i5-8400 (90PF01C1-M12070) Об'єм оперативної пам'яті 8 ГБ Чіпсет материнської плати Intel H310 потужність БП 350 Вт порти 1 x HDMI, 1 x VGA, Audio, 1 x DVI-D, 2 x USB 2.0, 2 x PS / 2, COM, 2 x USB 3.1, 1 x RJ45	PC_1 PC_2 PC_3 PC_4 PC_5 PC_6 PC_7 PC_8 PC_9	9	HEF34453801 25-HEF34453801 34
Робоча станція 2	Intel Xeon E-2288G (3.7 - 5.0 ГГц) / RAM 32 ГБ / HDD 1 ТБ + SSD 480 ГБ / nVidia Quadro P2000, 5 ГБ	PCPR_1 PCPR_2 PCPR_3 PCPR_4 PCPR_5 PCPR_6 PCPR_7 PCPR_8 PCPR_9 PCPR_10 PCPR_11 PCPR_12	12	HEF34453801 35-HEF34453801 47

Продовження таблиці 2.4 Технічні засоби

Назва	Характеристика	Умовні позначення	Кількість	Серійний номер
Робоча станція 3	Asus ZN242GDK-CA122T процесор Виробник процесора Intel Core i7-8750H 6 ядер 2,2 (4,1) ГГц 16 ГБ DDR4 1 ТБ + 512 ГБ 4 ГБ	PCPDV_1 PCPDV_2 PCPDV_3 PCPDV_4 PCPDV_5 PCPDV_6 PCPDV_7 PCPDV_8 PCPDV_9	9	HEF34453801 48-HEF34453801 57
Робоча станція 4	Apple iMac 21.5" Retina 4K (MRT32UA/A) 1TB 2019/4 ядра/AMD Radeon Pro 555/2 ГБ gDDR 5	PCMDJS_1 PCMDJS_2 PCMDJS_3 PCMDJS_4	4	HEF34453801 58-HEF34453801 62

2.2 Призначення серверу та особливості роботи

В ОІД, на якій проводилося обстеження немає серверу, він розташований в іншій серверній кімнаті на 5 поверсі, тому доступу до серверу мені надано не було, але всі ПК користувачів підключені до центральних серверів компанії. Сервер служить для розмежування прав доступу співробітників до файлових ресурсів. Також сервер слугує для локального зберігання загальних даних. Для підключення компьютерів до коммутатора використовують Високошвидкісний мережевий Патч корд UTP LAN кабель 40м для інтернету до 1000Мбіт / с. Призначений для використання в системах кабельних мереж Ethernet стандартів 10BASE-T (10 Мбіт / с), 100BASE-TX (Fast Ethernet, 100 Мбіт / с), і 1000BASE-T (Gigabit Ethernet, 1 Гбіт / с).

Підключення до мережевих пристроїв здійснюється через роз'єм RJ45 (8P8C).

2.3 Обстеження інформаційного середовища

Обстеження інформаційного середовища включає в себе інформацію, що планується до обробки за допомогою ІТС.

Власником інформації виступає директор. В автоматизованій системі відсутня таємна, службова інформація, а також інформація, що є власністю держави або відомості, які становлять державну таємницю.

За результатами проведеного обстеження в ІТС циркулюють наступні види інформації:

- відкрита інформація;
- конфіденційна інформація;
- персональні дані.

За режимом доступу інформація, яка обробляється за допомогою ІТС поділяється на:

- інформація з обмеженим доступом (ІзОД);
- відкрита, що потребує захисту;
- відкрита, не потребує захисту.

ІзОД буде представлена в ІТС у вигляді електронних документів створених за допомогою пакету прикладних програм Microsoft Office 2007, Adobe Reader або у роздрукованому паперовому вигляді. Паперові носії інформації зберігаються в сейфі.

Правила доступу до інформації встановлені власником. Доступ до ІзОД мають зареєстровані в системі користувачі, що належать до адміністративної ланки підприємства та безпосередньо працівники відділів, що розміщені в будівлі даного підприємства. Конфіденційна інформація має цінність, тому втрата або передача може завдати підприємству матеріальний збитків.

ІзОД, що циркулює в ІТС, буде зберігатися:

- на жорсткому магнітному диску;
- на пристроях зовнішньої пам’яті (USB флеш-накопичувач).

Документи, в яких містяться ІзОД, будуть друкуватися за допомогою

принтерів, які входять до складу ІТС. Копіювання на гнучкі носії та флеш накопичувачі здійснюється з дозволу адміністратора системи. Перелік відомостей, що становлять ІзОД, а також всі відомості за режимом доступу, за правовим режимом, а також за типом представлення в ІТС приведені та класифіковані у таблиці. Вимоги захисту встановлено власником згідно з вимогами нормативно-правових актів.

На досліджуваному ОІД циркулює інформація з обмеженим доступом - конфіденційна.

В мережі компанії кожному комп'ютеру присвоєні імена, а саму мережу розділено на 2 групи: адміністратор, користувач. Кожна з цих груп має доступ лише до певних файлів, програм та інформації в цілому, у кожного користувача свої права доступу.

Обмін інформацією може відбуватись за допомогою електронної пошти або через систему колективної розробки проектів GitHub або через внутрішньо розроблений сервіс ArtFramework. В таблиці 2.5 описані основні типи інформації, які церкулюють в ОІД, також описан правовий режим, режим доступу та критерії до забезпечення конфедеційності, цілісності, доступності.

Таблиця 2.5 Класифікація інформації

Вид інформації	Режим доступу	Правовий режим	К	Ц	Д
Програмний код	З обмеженим доступом	Конфедеційна	3	3	2
UI проекту	З обмеженим доступом	Конфедеційна	1	3	2
UX проекту	З обмеженим доступом	Конфедеційна	1	3	2
Тест дизайн	З обмеженим доступом	Конфедеційна	2	3	2
Програмний код автоматизації	З обмеженим доступом	Конфедеційна	2	3	2
Білд	З обмеженим доступом	Конфедеційна	2	3	2

Продовження таблиці 2.5 Класифікація інформації

Вид інформації	Режим доступу	Правовий режим	К	Ц	Д
Файл тестування автоматизації	З обмеженим доступом	Конфедеційна	3	2	3
Технічне завдання	З обмеженим доступом	Конфедеційна	2	3	2

Таблиця 2.6

Назва	Н1	Н2	Н3
Конфедеційність	Максимальне забезпечання конфедеційності інформації (К1)	Середній рівень забезпечення конфедеційності (К2)	Мінімальний рівень конфедеційності (К3)
Цілістнітсь	Максимальне забезпечання цілістності інформації (Ц1)	Середній рівень забезпечення цілістності (Ц2)	Мінімальний рівень цілістності (Ц3)
Доступність	Максимальне забезпечання Доступністі інформації (Д1)	Середній рівень забезпечення Доступністі (Д2)	Мінімальний рівень Доступністі (Д3)

Для кращого розуміння технологій обробки інформації на підприємстві надалі буде описан Аналіз технології обробітку інформації «Програмний код», в якій виділяються всі основні особливості обробки інформації на ТОВ «Техно Сервіс».

2.4 Аналіз технології обробітку інформації «Програмний код»

1- Спочатку використовують вже готові програмні рішеня, на основі яких буде вирішена задача. Підготовкою бази для проекту займаються головний розробник і головний програміст на локальних пк;

2 - Далі тестові прогрмні коди переробляють та формують задачу «Технічне завдання» для кожної команди віддіу. Головні розробники назначають відповідальних за певний етап роботи, також він відповідає за створення директорій на сервері для кожної команди.

3 - У компанії розробка ведеться колективно, тому кожний імпортує собі на ПК програмний код проекту, який дорабляється та в кінці дня екмпортується на центральний сервер для подальшої роботи з ним.

4- Після внесення змін у частини коду, збирається фінальна версія;

5- Всі результати змін та фінальна версія зберігається на сервері компанії та на локальних ПК головних розробників.

6- Далі готовий продукт, або чатсина готового продукту передається до відділу тестування ПО. У компанії за це відповідає інший офіс, яких знаходиться в іншій країні, тому програмне рішення передається по інтернету. Які після тестування продукту надсилають звіти з тестування, на основі яких дороблюється програмний код;

7- Запуск продукту. Прогрмані коди завантажують программу симулятор, який після завантаження починає тестувати працездатність.

8- При збоях працездатності програмного коду, його модифікують і знову повторюють процес з пункту 3.

Встановлене програмне забезпечання

На ПК користувачів відділу втсановлене наступне програмне забезпечення :

1)Microsoft Visual Studio 16.0 Preview 4.2- слугує для розробки інтерфейсу;

2)Віртуальний симулятор двігуна для тестування інтерфейсу, інформація не була надана про версію ПЗ;

3)Adobe Photoshop CC 2020 (21.0.3.91), слугує для роботи з дизайном інтерфейсу.

4)Microsoft Office 2019, слугує для роботи з документами та звітністю .

5)Інформація про антивірусне ПЗ не було надане, розробка компанії.

6)Інші програмні засоби кожний користувач конфігурує сам, але всі програмні засоби встановлюються лише після затвердженням служби безпеки.

Співробітники компанії конфігурують робочий простір самостійно. Встановлюють адміністратори за потреби користувачей, це обгрунтовано тим, що для робочого процесу потрібно використовувати безліч програмних засобів, які змінюються постійно. Середовище користувачів описано у таблиці 2.43, в якій описаний досвід працівника, його роль в компанії, рівень кваліфікації та освіта. Через те, що галузь для країни нова, тому знайти людину з освітою дуже важко.

Таблиця 2.8 Середовище користувачів

Користувач	Роль/посада	Рівень кваліфікації/освіта	Досвід (рік)
PC_1	Користувач/Розробник	Середня спеціальна освіта	9
PC_2	Користувач/Розробник	Відсутність спеціальної освіти	4
PC_3	Користувач/Розробник	Вища спеціальна освіта	5
PC_4	Користувач/Розробник	Вища спеціальна освіта	4
PC_5	Користувач/Розробник	Вища спеціальна освіта	5
PC_6	Користувач/Розробник	Відсутність спеціальної підготовки	6
PC_7	Користувач/Розробник	Відсутність спеціальної підготовки	6

Продовження таблиці 2.8 Середовище користувачів

Користувач	Роль/посада	Рівень кваліфікації/освіта	Досвід (рік)
PC_8	Користувач/Розробник	Вища спеціальна освіта	7
PC_9	Користувач/Розробник	Відсутність спеціальної підготовки	6
PCPR_1	Користувач/Програміст	Вища спеціальна освіта	4
PCPR_2	Користувач/Програміст	Вища спеціальна освіта	8
PCPR_3	Користувач/Програміст	Середня спеціальна освіта	6
PCPR_4	Користувач/Програміст	Відсутність спеціальної освіти	6
PCPR_5	Користувач/Програміст	Вища спеціальна освіта	7
PCPR_6	Користувач/Програміст	Вища спеціальна освіта	6
PCPR_7	Користувач/Програміст	Вища спеціальна освіта	4

Продовження таблиці 2.8 Середовище користувачів

Користувач	Роль/посада	Рівень кваліфікації/освіта	Досвід (рік)
PCPR_8	Користувач/Програміст	Відсутність спеціальної підготовки	8
PCPR_9	Користувач/Програміст	Відсутність спеціальної підготовки	6
PCPR_10	Користувач/Програміст	Вища спеціальна освіта	6
PCPR_11	Користувач/Програміст	Середня спеціальна освіта	7
PCPR_12	Користувач/Програміст	Відсутність спеціальної освіти	6
PCPDV_1	Користувач/Розробник автоматизованої частини	Вища спеціальна освіта	4
PCPDV_2	Користувач/Розробник автоматизованої частини	Вища спеціальна освіта	8
PCPDV_3	Користувач/Розробник автоматизованої частини	Вища спеціальна освіта	6
PCPDV_4	Користувач/Розробник автоматизованої частини	Відсутність спеціальної підготовки	6

Продовження таблиці 2.8 Середовище користувачів

Користувач	Роль/посада	Рівень кваліфікації/освіта	Досвід (рік)
PCPDV_5	Користувач/Розробник автоматизованої частини	Відсутність спеціальної підготовки	7
PCPDV_6	Користувач/Розробник автоматизованої частини	Вища спеціальна освіта	6
PCPDV_7	Користувач/Розробник автоматизованої частини	Середня спеціальна освіта	4
PCPDV_8	Користувач/Розробник автоматизованої частини	Відсутність спеціальної освіти	8
PCPDV_9	Користувач/Розробник автоматизованої частини	Вища спеціальна освіта	6
PCMDJS_1	Користувач/Головний розробник відділу	Вища спеціальна освіта	14
PCMDJS_2	Користувач/Головний розробник відділу	Вища спеціальна освіта	5
PCMDJS_3	Користувач/Головний розробник відділу	Вища спеціальна освіта	7
PCMDJS_4	Користувач/Головний розробник відділу	Вища спеціальна освіта	12

Продовження таблиці 2.8 Середовище користувачів

Користувач	Роль/посада	Рівень кваліфікації/освіта	Досвід (рік)
Admin_TD2 (не відноситься до ОІД, але регулює користувачей ОІД)	Адміністратор	Відсутність спеціальної освіти	5

Таблиця 2.9 Правила розмежування доступу

Користувач	Інформація	Ч	З	В	С
PCMDJS_1 PCMDJS_2 PCMDJS_3 PCMDJS_4	Програмний код	+	+	+	+
	UI проекту	+	+	+	+
	UX проекту	+	+	+	+
	Тест дизайн	+	+	+	+
	Програмний код автоматизації	+	+	+	+
	Білд	+	+	+	+
	Файл тестування автоматизації	+	+	+	+
	Технічне завдання	+	+	+	+

Продовження таблиці 2.9 Правила розмежування доступу

Користувач	Інформація	Ч	З	В	С
PCPDV_1 PCPDV_2 PCPDV_3 PCPDV_4 PCPDV_5 PCPDV_6 PCPDV_7 PCPDV_8 PCPDV_9	Програмний код	+	+	+	+
	UI проекту	+			
	UX проекту	+			
	Тест дизайн	+			
	Програмний код автоматизації	+	+	+	+
	Білд	+	+	+	+
	Файл тестування автоматизації	+			
PCPR_1 PCPR_2 PCPR_3 PCPR_4 PCPR_5 PCPR_6 PCPR_7 PCPR_8 PCPR_9 PCPR_10 PCPR_11 PCPR_12	Технічне завдання				
	Програмний код	+	+	+	+
	UI проекту	+			
	UX проекту	+			

Продовження таблиці 2.9 Правила розмежування доступу

Користувач	Інформація	Ч	З	В	С
	Тест дизайн	+	+	+	+
	Програмний код автоматизації	+	+	+	
	Білд	+	+	+	
	Файл тестування автоматизації	+	+	+	+
	Технічне завдання	+			
PC_1 PC_2 PC_3 PC_4 PC_5 PC_6 PC_7 PC_8 PC_9	Програмний код	+	+		
	UI проекту	+			
	UX проекту	+			
	Тест дизайн	+			
	Програмний код автоматизації	+	+		
	Білд	+	+		
	Файл тестування автоматизації	+	+	+	+
	Технічне завдання	+			

Ч - читання файлів ,З - запис файлів ,В - видалення файлів, С - створення файлів

2.5 Аналіз загроз та вразливостей

2.5.1 Модель порушника

Модель порушника відображає його практичні та теоретичні можливості, апріорні знання, час і місце дії тощо.

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.

Метою порушника можуть бути:

- отримання необхідної інформації у потрібному обсязі та асортименті;
- мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами (інтересами, планами);
- нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

Порушники спочатку поділяються на дві основні групи: зовнішні та внутрішні.

Зовнішніх порушників можна розділити на:

- добре озброєну та технічно оснащену групу, що діє зовні швидко і напролом;
- поодиноких порушників, що не мають допуску на об'єкт і намагаються діяти потайки й обережно, так як вони усвідомлюють, що сили реагування мають перед ним переваги.

Сторонні особи, що можуть бути порушниками:

- клієнти (представники організацій, громадяни);
- відвідувачі (запрошені з якого-небудь приводу);

- представники організацій, взаємодіючих з питань забезпечення систем життєдіяльності організації (енерго-, водо-, теплопостачання тощо);
- представники конкуруючих організацій (іноземних служб) або особи, що діють за їх завданням;
- особи, які випадково або навмисно порушили пропускний режим (без мети порушити безпеку);
- будь-які особи за межами контрольованої зони.

Потенціальних внутрішніх порушників можна розділити на:

- допоміжний персонал об'єкту, що допущений на об'єкт, але не допущений до життєво важливого центру ІТС;
- основний персонал, що допущений до життєво важливого центру (найбільш небезпечний тип порушників);
- співробітників служби безпеки, які часто формально не допущені до життєво важливого центру ІТС, але реально мають достатньо широкі можливості для збору необхідної інформації і скоєння акції.

Серед внутрішніх порушників можна виділити такі категорії персоналу: - користувачі (оператори) системи;

- персонал, що обслуговує технічні засоби (інженери, техніки);
- співробітники відділів розробки та супроводження програмного забезпечення (прикладні та системні програмісти);
- 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.

Крім професійного шпигунства, можна виділити три основних мотиви порушень: безвідповідальність, самоствердження та корисливий інтерес.

При порушеннях, викликаних безвідповідальністю, користувач цілеспрямовано або випадково виробляє руйнуючі дії, які не пов'язані проте зі злим умислом. У більшості випадків це наслідок некомпетентності або недбалості. Деякі

користувачі вважають одержання доступу до системних наборів даних значним успіхом, затіваючи свого роду гру заради самоствердження або у власних очах, або в очах колег.

Порушення безпеки ІТС може бути викликано корисливим інтересом користувача ІТС. У цьому випадку він буде цілеспрямовано намагатися подолати систему захисту для несанкціонованого доступу до інформації в ІТС.

Усіх порушників можна класифікувати за такими ознаками:

- за рівнем знань про ІТС;
- за рівнем можливостей;
- за часом дії;
- за місцем дії.

За рівнем знань про ІТС (в залежності від кваліфікації та професійної майстерності):

- володіє низьким рівнем знань, але вміє працювати з технічними засобами ІТС;
- володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІТС та їх обслуговування;
- володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації ІТС;
- знає структуру, функції й механізми дії засобів захисту інформації в ІТС, їх недоліки та можливості.

За рівнем можливостей (в залежності від методів і засобів, що використовуються):

- застосовує чисто агентурні методи отримання відомостей;
- застосовує пасивні засоби (технічні засоби перехоплення без модифікації компонентів системи);
- використовує тільки штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також

компактні носії інформації, які можуть бути тайком пронесені крізь пости охорони;

- застосовує методи та засоби активного впливу (модифікація та підключення додаткових технічних засобів, перехоплення з каналів передачі даних, впровадження спеціальних програмних закладок).

За часом дії (в залежності від активності або пасивності системи):

- у процесі функціонування (під час роботи компонентів системи);
- у період неактивності системи (у неробочий час, під час планових перерв у її роботі, перерв для обслуговування та ремонтів і т.д.);
- як у процесі функціонування, так і в період неактивності системи.

За місцем дії (в залежності від території доступу до засобів системи):

- без доступу на контрольовану територію організації;
- з контрольованої території без доступу до будівель та споруджень;
- усередині приміщень, але без доступу до технічних засобів;
- з робочих місць кінцевих користувачів (операторів);
- з доступом у зону даних (баз даних, архівів тощо);
- з доступом у зону управління засобами забезпечення безпеки. Враховуються також такі обмеження та припущення про характер дій

можливих порушників:

- робота з підбору та розстановки кадрів, а також заходи контролю за персоналом ускладнюють можливість створення коаліцій порушників, тобто злочинного угрупування (змови) і цілеспрямованих дій з подолання системи захисту двох і більше порушників;
- порушник, плануючи спробу НСД, приховує свої несанкціоновані дії від інших співробітників;
- НСД може бути наслідком помилок користувачів, адміністраторів, а також хиб прийнятої технології обробки інформації тощо.

Припускається, що в своєму рівні порушник - це фахівець вищої кваліфікації, який має повну інформацію про ІТС і засоби захисту. Така класифікація

порушників є корисною для використання в процесі оцінки ризиків, аналізу вразливості системи, ефективності існуючих і планових заходів захисту.

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

- ймовірність реалізації загрози;
- своєчасність виявлення;
- відомості про порушення.

Слід зауважити, що всі злочини, зокрема і комп'ютерні, здійснюються людиною. Користувачі ІТС, з одного боку, є її складовою частиною, а з іншого - основною причиною і рухаючою силою порушень і злочинів. Отже, питання безпеки захищених ІТС фактично є питанням людських відносин та людської поведінки.

Відповідно до однієї з методик розробки моделі порушників, модель можна відобразити системою таблиць.

Для побудови моделі використовуються усі можливі категорії, ознаки та характеристики порушників для більш точного їх аналізу, причому рівень загрози кожної з них вказується в дужках і оцінюється за 4-бальною шкалою.

Таблиця 2.10 Категорії порушників, визначених у моделі

Позначення	Визначення категорії	Рівень загроз
	Внутрішні по відношенню до ІТС	
ПВ1	• Технічний персонал, який обслуговує будови та приміщення (електрики, прибиральники тощо), в яких розташовані компоненти ІТС	1
ПВ2	• Персонал, який обслуговує технічні засоби ІТС (інженери, техніки)	2
ПВ3	• Користувачі (оператори) ІТС	2

Продовження таблиці 2.10 Категорії порушників, визначених у моделі

Позначення	• Визначення категорії	Рівень загроз
ПВ4	• Адміністратори ІТС, співробітники служби захисту інформації	3
ПВ5	Співробітники служби безпеки установи та керівники різних рівнів	4
	Зовнішні по відношенню до ІТС	
ПЗ1	Відвідувачі (запрошені з будь-якого приводу)	1
ПЗ2	Представники організацій, що взаємодіють з питань технічного забезпечення (енерго-, водо-, теплопостачання і таке інше)	2
ПЗ3	Хакери	3
ПЗ4	Агенти конкурентів або закордонних спецслужб «під прикриттям»	4

Таблиця 2.11 Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив порушення	Рівень загроз
М1	Безвідповідальність	1
М2	Самоствердження	2

Продовження таблиці 2.11 Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив порушення	Рівень загроз
М3	Корисливий інтерес	3
М4	Професійний обов'язок (ПЗ4)	4

Таблиця 2.12. Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС

Позначення	Основні кваліфікаційні ознаки порушника	Рівень загроз
К1	Володіє низьким рівнем знань, але вміє працювати з технічними засобами ІТС	1
К2	Володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІТС та їх обслуговування	2
К3	Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації ІТС	3
К4	Знає структуру, функції й механізми дії засобів захисту інформації в ІТС, їх недоліки та можливості	4

Таблиця 2.13 Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту

Позначення	Характеристика можливостей порушника	Рівень загроз
З1	Може лише підслуховувати розмови у приміщеннях та підглядати у документи на робочих місцях	1
З2	Використовує пасивні технічні засоби перехвату без модифікації інформації та компонентів ІТС	2
З3	Використовує лише штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні машинні носії інформації, які можуть бути приховано пронесено крізь охорону	3
З4	Використовує технічні засоби активного впливу з метою модифікації інформації та компонентів ІТС, дезорганізації систем обробки інформації	4

Таблиця 2.14 Специфікація моделі порушника за часом дії

Позначення	Характеристика можливостей порушника	Рівень загроз
Ч1	Під час повної бездіяльності ІТС з метою відновлення та ремонту	1
Ч2	Під час призупинки компонентів ІТС з метою технічного обслуговування та модернізації	2
Ч3	Під час функціонування ІТС (або компонентів системи)	3
Ч4	Як у процесі функціонування ІТС, так і під час призупинки компонентів системи	4

Таблиця 2.15 Специфікація моделі порушника за місцем дії

Позначення	Характеристика місця дії порушника	Рівень загроз
Д1	Усередині приміщень, але без доступу до технічних засобів ІТС	1
Д2	З робочих місць користувачів (операторів) ІТС	2
Д3	З доступом у зону зберігання баз даних, архівів тощо	3
Д4	З доступом у зону керування засобами забезпечення безпеки ІТС	4

На основі описаної методики будується 2 моделі порушника: модель внутрішнього порушника представлена в таблиці 2.16, модель зовнішнього порушника представлена в таблиці 2.17.

Таблиця 2.16 Модель порушника внутрішнього

Назва ПК у системі	Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сумма
PC_1	Користувач/Розробник	ПВЗ	МЗ	КЗ	ЗІ	ЧЗ	ЧЗ	16
PC_2	Користувач/Розробник	ПВЗ	МЗ	КЗ	ЗІ	ЧЗ	ЧЗ	16
PC_3	Користувач/Розробник	ПВЗ	МЗ	КЗ	ЗІ	ЧЗ	ЧЗ	16

Продовження таблиці 2.16 Модель порушника внутрішнього

Назва ПК у системі	Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сумма
PC_4	Користувач/Розробник	ПВЗ	МЗ	КЗ	ЗІ	ЧЗ	ЧЗ	16
PC_5	Користувач/Розробник	ПВЗ	МЗ	КЗ	ЗІ	ЧЗ	ЧЗ	16
PC_6	Користувач/Розробник	ПВЗ	МЗ	КЗ	ЗІ	ЧЗ	ЧЗ	16
PC_7	Користувач/Розробник	ПВЗ	МЗ	КЗ	ЗІ	ЧЗ	ЧЗ	16
PC_8	Користувач/Розробник	ПВЗ	МЗ	КЗ	ЗІ	ЧЗ	ЧЗ	16
PC_9	Користувач/Розробник	ПВЗ	МЗ	КЗ	ЗІ	ЧЗ	ЧЗ	16
PCPR_1	Користувач/Програміст	ПВЗ	МЗ	КЗ	ЗІ	ЧЗ	ЧЗ	16
PCPR_2	Користувач/Програміст	ПВЗ	МЗ	КЗ	ЗІ	ЧЗ	ЧЗ	16
PCPR_3	Користувач/Програміст	ПВЗ	МЗ	КЗ	ЗІ	ЧЗ	ЧЗ	16
PCPR_4	Користувач/Програміст	ПВЗ	МЗ	КЗ	ЗІ	ЧЗ	ЧЗ	16

Продовження таблиці 2.16 Модель порушника внутрішнього

Назва ПК у системі	Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сумма
PCPR_5	Користувач/Програміст	ПВЗ	МЗ	КЗ	ЗІ	ЧЗ	ЧЗ	16
PCPR_6	Користувач/Програміст	ПВЗ	МЗ	КЗ	ЗІ	ЧЗ	ЧЗ	16
PCPR_7	Користувач/Програміст	ПВЗ	МЗ	КЗ	ЗІ	ЧЗ	ЧЗ	16
PCPR_8	Користувач/Програміст	ПВЗ	МЗ	КЗ	ЗІ	ЧЗ	ЧЗ	16
PCPR_9	Користувач/Програміст	ПВЗ	МЗ	КЗ	ЗІ	ЧЗ	ЧЗ	16
PCPR_10	Користувач/Програміст	ПВЗ	МЗ	КЗ	ЗІ	ЧЗ	ЧЗ	16
PCPR_11	Користувач/Програміст	ПВЗ	МЗ	КЗ	ЗІ	ЧЗ	ЧЗ	16
PCPR_12	Користувач/Програміст	ПВЗ	МЗ	КЗ	ЗІ	ЧЗ	ЧЗ	16
PCPDV_1	Користувач/Розробник автоматизованої частини	ПВЗ	МЗ	КЗ	ЗІ	ЧЗ	ЧЗ	16

Продовження таблиці 2.16 Модель порушника внутрішнього

Назва ПК у системі	Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сумма
PCPDV_2	Користувач/Розробник автоматизованої частини	ПВЗ	МЗ	КЗ	ЗІ	ЧЗ	ЧЗ	16
PCPDV_3	Користувач/Розробник автоматизованої частини	ПВЗ	МЗ	КЗ	ЗІ	ЧЗ	ЧЗ	16
PCPDV_4	Користувач/Розробник автоматизованої частини	ПВЗ	МЗ	КЗ	ЗІ	ЧЗ	ЧЗ	16
PCPDV_5	Користувач/Розробник автоматизованої частини	ПВЗ	МЗ	КЗ	ЗІ	ЧЗ	ЧЗ	16
PCPDV_6	Користувач/Розробник автоматизованої частини	ПВЗ	МЗ	КЗ	ЗІ	ЧЗ	ЧЗ	16

Продовження таблиці 2.16 Модель порушника внутрішнього

Назва ПК у системі	Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума
PCPDV_7	Користувач/Розробник автоматизованої частини	ПВЗ	МЗ	КЗ	ЗІ	ЧЗ	ЧЗ	16
PCPDV_8	Користувач/Розробник автоматизованої частини	ПВЗ	МЗ	КЗ	ЗІ	ЧЗ	ЧЗ	16
PCPDV_9	Користувач/Розробник автоматизованої частини	ПВЗ	МЗ	КЗ	ЗІ	ЧЗ	ЧЗ	16
PCMDJS_1	Користувач/Головний розробник відділу	ПВЗ	МЗ	КЗ	ЗІ	Ч4	Ч4	18
PCMDJS_2	Користувач/Головний розробник відділу	ПВЗ	МЗ	КЗ	ЗІ	Ч4	Ч4	18

Продовження таблиці 2.16 Модель порушника внутрішнього

Назва ПК у системі	Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сумма
PCMDJS_3	Користувач/Головний розробник відділу	ПВ3	М3	К3	З1	Ч4	Ч4	18
PCMDJS_4	Користувач/Головний розробник відділу	ПВ3	М3	К3	З1	Ч4	Ч4	18
Admin_TD2	Адміністратор	ПВ4	М3	К4	З1	Ч4	Ч4	20

Таблиця 2.17 Модель порушника зовнішнього

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сумма
Технічний персонал	ПЗ2	М3	К1	З1	Ч1	Д1	9
Комунальний персонал бізнес центрц	ПЗ2	М3	К1	З1	Ч1	Д1	9

Продовження таблиці 2.17 Модель порушника зовнішнього

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума
Наймані ремонті послуги	ПЗ2	М3	К1	З1	Ч1	Д1	9
Хакери	ПЗ3	М3	К3	З4	Ч4	Д4	21
Клієнти компанії	ПЗ1	М3	К1	З1	Ч1	Д1	8
Агенти конкурентів	ПЗ4	М3	К2	З3	Ч4	Д3	19
Прибиральники бізнес центру	ПЗ2	М3	К1	З1	Ч1	Д1	9
Відвідувачі	ПЗ1	М3	К1	З1	Ч1	Д1	8

З таблиці 2.16 та 2.17 видно, що найбільшу загрозу, що має відношення до проблеми захисту інформації, становлять: агенти конкурентів, хакери,системний адміністратор та головний розробник відділу PCMDJS_1. Тому організація роботи цих особ повинна бути найбільш контрольованою, оскільки вони є основними потенційними порушниками безпеки інформації.

2.5.2 Модель загроз

За результатами впливу на інформацію та систему її обробки, загрози поділяються на чотири класи:

Порушення конфіденційності інформації (К) - отримання інформації користувачами або процесами всупереч встановленим правилам розмежування

доступу до інформації.

Порушення цілісності інформації (Ц) - повне або часткове знищення, викривлення, модифікація інформації, нав'язування хибної інформації тощо.

Порушення доступності інформації (Д) - часткова або повна втрата працездатності системи, блокування доступу до інформації в результаті некоректних дій адміністраторів, технічного обслуговуючого персоналу.

Загрози потенційно можуть завдати шкоди інформації, персоналу, клієнтам, обладнанню, процесам і програмно-технічним комплексам. Загрози можуть бути навмисними (Н), випадковими (В), природними (П). Повинні бути ідентифіковані як випадкові, так і навмисні джерела загроз. Загрози можуть бути ідентифіковані в загальному вигляді або за типами.

За походженням загрози поділяються на випадкові та навмисні. Випадкові загрози спричиняються помилками у програмному забезпеченні, збоями та відмовами апаратури та систем забезпечення, помилками персоналу тощо. Випадкові загрози, спричинені стихійними лихами (повінь, землетрус, пожежа тощо) розглядаються окремо. Навмисні загрози зумовлені цілеспрямованими діями порушників.

Для оцінки ймовірності реалізації загроз використовуються така шкала:

Ранжування ймовірності

Ймовірність	Назва
Менше 0,2	Низька
0,3-0,5	Середьня
0,6 - 0,8	Висока
Більше 0,8	Неприпустимо висока

Для оцінки завданної шкоди від загроз використовуються така шкала:

Ранжування за рівнем шкоди

Ймовірність	Назва
Менше 0,2	Низький
0,3-0,5	Середній

0,6 - 0,8	Високий
Більше 0,8	Неприпустимо високий

Оскільки неможливо одержати достатньо об'єктивні дані про ймовірність реалізації більшості з наведених загроз, ймовірність реалізації загроз визначено експертним методом, на основі аналізу статистичних даних.

В таблиці не розглядаються загрози, що використовують технічні канали витоку інформації (перехоплення побічних електромагнітних випромінювань і наведень, акусто-електричнихперетворень інформаційних сигналів, оптичних каналів витоку інформації).

У таблиці 2.6 описані основні загрози, які можуть виникати на підприємстві, сюди входять і внутрішні і звоншішні загрози, також входять як навмисні так і ненавмисні загрози.

Таблиця 2.18 Модель основних загроз

Загроза	Ймовірність	Рівень шкоди	К	Ц	Д
Уразливості веб-додатків	Висока	Високий	+	+	+
Розголошення інформації	Середня	Середній	+	-	-
Логічні атаки спрямовані на експлуатацію функцій додатка або логіки його функціонування	Висока	Високий	+	+	-
Використання КС компанії в своїх корисних цілях	Висока	Високий	-	-	-
Несанкціонований доступ до даних серверу	Висока	Високий	+	+	-
Зловживання службовим становищем	Висока	Середній	+	+	+

Продовження таблиці 2.18 Модель основних загроз

Загроза	Ймовірність	Рівень шкоди	К	Ц	Д
Створення клонів системи	Низька	Високий	-	-	+
Підробка тестів системи автоматизації	Низька	Дуже висока	-	+	-
Фізична крадіжка носіїв інформації	Середня	Високий	-	-	+
Віддалений доступ до КС компанії	Висока	Високий	+	+	+
Неліцензійне Програмне забезпечення	Висока	Середній	+	+	+
Несанкціоноване використання програм та ресурсів компанії	Висока	Середній	-	-	+
Загрози віддаленого запуску додатків	Висока	Високий	+	+	-
Збої електроживлення	Середня	Високий	-	-	+
DOS-атака / DDoS- атака	Середня	Середній	-	-	+
Ініціалізація забороненого програмного забезпечення	Висока	Середній	+	+	+

Продовження таблиці 2.18 Модель основних загроз

Загроза	Ймовірність	Рівень шкоди	К	Ц	Д
Підкуп працівників	Низька	Високий	-	-	+
Пожежа, повінь, землетрус, техногенні аварії	Низька	Дуже висока	+	+	+
Порушення пропускної швидкості	Середня	Середній	+	+	+
Фішинг	Середня	Середній	+	+	+
Порушення правил розмежування доступу	Висока	Високий	+	+	+
Несанкціонованого копіювання інформації на зовнішні носії інформації	Середня	Високий	+	-	-
Випадкове зараження програмних засобів комп'ютерними вірусами	Висока	Високий	+	+	+

Найбільш актуальними загрозами для ОІД вважаються:

- Порушення правил розмежування доступу;
- Ініціалізація забороненого програмного забезпечення;
- Загрози віддаленого запуску додатків;
- Несанкціоноване використання програм та ресурсів компанії;
- Неліцензійне Програмне забезпечення;

- Уразливості веб-додатків;
- Випадкове зараження програмних засобів комп'ютерними вірусами;
- Фішинг;

Якщо ідентифіковані загрози будуть використовувати відповідні вразливості і призведуть до інциденту інформаційної безпеки, негативними наслідками для підприємства може стати повна або часткова втрата інформації, пошкодження або заміна інформації, скомпрометованість інформації. Ці інциденти вплинуть на ресурси підприємства.

Враховуючи характеристики існуючої ІТС та вимог до властивостей інформації, відповідно до НД ТЗІ 2.5-005 -99, обрано стандартний функціональний профіль захищеності для системи:

КД-4. Абсолютна довірча конфіденційність. Не реалізована. Політика довірчої цілісності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС.

КД-3. Повна довірча конфіденційність. Не реалізована. Політика довірчої цілісності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС.

КД-2. Базова довірча конфіденційність. Реалізована. Персональні фото, документи.

КА-4. Абсолютна адміністративна конфіденційність. Не реалізована.Політика адміністративної конфіденційності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС.

КА-3. Повна адміністративна конфіденційність. Не реалізована.Політика адміністративної конфіденційності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС.

КА-2. Базова адміністративна конфіденційність. Реалізована. У системі реалізована можливість створення облікових записів. Адміністратор надає рівні доступу до обїектів користувачу. (файли системи)

КО-1. Повторне використання об'єктів.Не реалізована.Політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС.

КК-3. Перекриття прихованих каналів .Реалізовано. вірус який відкриває прихований канал, стеганографія.

КВ-4. Абсолютна конфіденційність при обміні. Не реалізована. Політика конфіденційності при обміні, що реалізується КЗЗ, повинна відноситись до всіх об'єктів і існуючих інтерфейсних процесів

КВ-3. Повна конфіденційність при обміні. Не реалізована. Політика конфіденційності при обміні, що реалізується КЗЗ, повинна відноситись до всіх об'єктів і існуючих інтерфейсних процесів

КВ-2. Базова конфіденційність при обміні. Реалізована. Обмін між Unity Hub серевером та менеджером пакетів у Unity3D . Електронна пошта передає з використанням протоколів захисту при обміні.

ЦД-4. Абсолютна довірча цілісність. Не реалізована. Політика довірчої цілісності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС

ЦД-3. Повна довірча цілісність. Не реалізована. Політика довірчої цілісності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС

ЦД-2. Базова довірча цілісність. Реалізована. У системі реалізована можливість надавати різні рвні доступу.

ЦА-4. Абсолютна адміністративна цілісність. Не реалізована.Політика адміністративної цілісності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС

ЦА-3. Повна адміністративна цілісність. Не реалізована.Політика адміністративної цілісності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС

ЦА-2. Базова адміністративна цілісність. У системі реалізована можливість створення облікових записів. Адміністратор надає рівні доступу до обїектів користувачу. Системні фали, паролі.

ЦО-1. Обмежений відкат. Реалізований. У системі наявна можливість відміни останніх дій у Unity3D, Adobe Photoshop , Adobe Illustrator, Visual Studio, Blender

3D, Substance Painter, Xcode.

ЦО-2. Повний відкат. Реалізований. Резервное копироывние.

ЦВ-3: Повна цілісність при обміні. Не реалізована.Політика цілісності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів КС і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовуваними механізмами, і спроможність користувачів і/або процесів керувати рівнем захищеності

ЦВ-2: Базова цілісність при обміні. Не реалізована.Електронна пошта.

ДС-3. Стійкість без погіршення характеристик обслуговування. Не реалізована. Інтерфейсом не надається можливості гарантувати стійксіть без погіршення обслуговування.

ДС-2. Стійкість з погіршенням характеристик обслуговування. Реалізована. Реалізована за допомогою своєчасного автоматичного зберігання всіх параметрів системи та референсів на дист або хмару.

ДЗ-3. Гаряча заміна будь-якого компонента . Не реалізована.Політика гарячої заміни, що реалізується КЗЗ, повинна забезпечувати можливість заміни будь-якого компонента без переривання обслуговування

ДЗ-2. Обмежена гаряча заміна. Не реалізована.Політика гарячої заміни, що реалізується КЗЗ, повинна визначати множину компонентів КС, які можуть бути замінені без переривання обслуговування

ДЗ-1. Модернізація. Реалізована. Додаткові резерви КС надають можливість модернезувати КС із забезпеченням безеперебійної роботи(Оновлення ПО).

ДВ-3. Вибіркове відновлення. Реалізована. Інтерфейся КС дозволяють виконати вибіркове відновлення(окремих дисків, областей диску).

ДВ-2. Автоматизоване відновлення. Реалізована. Інтерфейся КС дозволяють виконати автоматизоване відновлення(параметри після відновлення = параметри до збою) .

ДВ-1. Ручне відновлення. Реалізована. Інтерфейся КС дозволяють виконати ручне відновлення(параметри відновлення задаються вручну).

НР-5. Аналіз в реальному часі. Реалізована. Інтерфейси моніторингу стану систему дозволяють отримувати сигнали про небезпеку при ненормальній роботи КС. У системі реалізований журнал подій - вхід у систему, також системи оповіщення при критичній помилці .

НИ-3. Множинна ідентифікація і автентифікація. Реалізована. У КС інтегрована система аутентифікації TouchID яка сканую відбиток пальцю користувача. Також реалізовано запаролені облікових записів КС.

НК-2. Двонаправлений достовірний канал. Реалізована. Зв'язок з використанням даного каналу ініціюватися користувачем або КЗЗ. Введення данних з клавіатури. Може реалізувати тільки людина.

НО-1. Виділення адміністратора. Не реалізована. В КС передбачені окремі облікові записи. Один з правами адміністратора та декілька з правами користувачів, але користувачі не заходять у систему як адміністратори.

НЦ-3. КЗЗ з функціями диспетчера доступу. Не реалізована.Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів

НЦ-2. КЗЗ з гарантованою цілісністю. Не реалізована.Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів

НЦ-1. КЗЗ з контролем цілісності. Не реалізована.Політика цілісності КЗЗ повинна визначати склад КЗЗ і механізми контролю цілісності компонентів, що входять до складу КЗЗ. Перевірка системи на цілістнітсь, антивірусне ПО.

НТ-3. Самотестування в реальному часі. Реалізована. У системі реалізована можливість самотестування у реальному часі. При неправильному спрацюваані системи, приймаються певні міри. (Якщо ігровий двігун Unity дає збій, система це розуміє і швидко зберігає параметри проетку).

НВ-3.Ідентифікація і автентифікація при обміні. Не реалізована . Політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ

НВ-2: Автентифікація джерела даних. Реалізована. Якщо намагатись встановити КЗЗ, система перевіряє джерела, з якого буде воно встановлене. Шіфрування та ЕЦП.Kerberos.

НА-2: Автентифікація відправника з підтвердженням. Не раелізована.

НА-1: Базова автентифікація відправника. Реалізована. У бінарніку файлу заносяться данні про створений файл, на якому ПК та ким це було зроблено.

2.7 Розробка КСЗІ

Заходи, що представлені в КСЗІ, направлені на зниження ризиків реалізації загрози через основні вразливості ІТС, які описані у таблиці 2.6. Модель основних загроз, спираючись на існуючий аналіз ризиків. Першочергово необхідно ввести заходи для зниження ризиків, що мають критичний рівень ризику. До цієї категорії відноситься випадкове зараження програмних засобів комп'ютерними вірусами через неякісне антивірусне ПЗ, некомпетентність персоналу, ініціалізація не регламентованого програмного забезпечення, несанкціоноване копіювання.

Для забезпечення безпеки будуть використовуватись програмні адміністративні та інженерно-технічні заходи для забезпечення безпеки інформації. Всі програмні адміністративні та інженерно-технічні заходи довзолені Положення про технічний захист інформації в Україні, затвердженого Указом Президента України від 27 вересня 1999 р. № 1229.

На результат вибору програмного засобу для певної задачі було поставлено ряд критерії, яким повинен відповідати додаток:

- Вартість програмного засобу не повинен перевищувати середню вартість в сегменті;
- Наявність тестового періоду програмного засобу для впровадження в ІТС;

- Своєчасне оновлення програмного засобу розробниками;

- Срок дії програмного засобу повинен бути не менше ніж 6 місяців з моменту розробки КСЗІ;

- Форма ліцензії - підписка (обрано для того, щоб при завершені ліцензії можна було змінити програмний засіб);

- Зручність та простота програмного засобу для користувача;

- Стабільність;

- Відсутність потребу у навчанні співробітників компанії;

В таблиці 2.19 описані програмні та технічні засоби захисту, які входять до КСЗІ.

Таблиця 2.19 Обрані програмні засоби антивірусного захисту

Назва засобу	Призначення засобу	Область захисту захисту	Срок дії програмного засобу
Symantec Endpoint Protection 14.07-1098.22	Комплекс засобів захисту програмного забезпечення антивірусного захисту інформації	Призначене для захисту робочих станцій користувачів від дій шкідливого програмного забезпечення та реагуванні на виявлення даних програм та інформації, а також мережевих атак.	Дійсний з 06.03.2018 до 06.03.2021
Програмний продукт антивірусного захисту інформації ESET Endpoint Protection	Комплекс засобів захисту програмного забезпечення антивірусного захисту інформації	Призначене для захисту робочих станцій користувачів від дій шкідливого програмного забезпечення та реагуванні на виявлення даних програм та інформації, а також мережевих атак.	Дійсний з 15.05.2017 до 15.05.2020
Програмний продукт антивірусного захисту «Panzor Cloud Antivirus»	Комплекс засобів захисту програмного забезпечення антивірусного захисту інформації	Призначене для захисту робочих станцій користувачів від дій шкідливого програмного забезпечення та реагуванні на виявлення даних програм та інформації, а також мережевих атак.	Дійсний з 25.09.2017 до 25.09.2020

Продовження таблиці 2.19 Обрані програмні засоби антивірусного захисту

Назва засобу	Призначення засобу	Область захисту захисту	Срок дії програмного засобу
Комплекс засобів захиступрограмного забезпечення антивірусного захисту інформації "Zillya! Антивірус для Бізнесу"	Комплекс засобів захисту програмного забезпечення антивірусного захисту інформації	Призначений для антивірусного захисту інформації в різних операційних системах. Відповідає вимогамнормативних документів системи технічного захисту інформації в Україні в обсязі функцій, зазначених у документі "Програмне забезпечення антивірусного захисту інформації "Zillya! Антивірус для Бізнесу".	Дійсний з 01.06.2017 до 01.06.2020

В таблиці 2.20 описані програмні засоби захисту файлів, які входять до КСЗІ. На вибір влинуло мала кількість програмних засобів, які дозволені держспецзв'язком, тому програмний засіб захисту обігу файлів обрали другий, а саме Safetica Full DLP версії 9.03.11, виробництва компанії Safetica Technologies. Це обумовлено тим, що программа версії 9.03.11 має протоколи захисту з алгоритмом аналізу блоків зображення та срок дії програмного засобу значно вищий ніж у першому випадку.

Таблиця 2.20 Обрані програмні засоби захисту обігу файлів

Назва засобу	Призначення засобу	Область захисту захисту	Срок дії програмного засобу
Safetica Full DLP» версії 8.108	Програмний продукт захисту інформації	Призначене для захисту обігу файлів в ІТС.	Дійсний з 28.09.2018 до 28.09.2021
Програмний продукт захисту інформації Safetica Full DLP версії 9.03.11, виробництва компанії Safetica Technologies (Чехія)	Програмний продукт захисту інформації	Призначене для захисту обігу файлів в ІТС.	Дійсний з 24.01.2020 до 24.01.2023

При розробці політики безпеки для підприємства, спираючись на наявність конфіденційної інформації, яка обробляється в ІТС, фінансових та матеріальних ресурсів, які є у розпорядженні власника ІТС, обрано принцип, при якому впровадження інформаційного захисту буде доцільним - досягнення необхідного рівня захищеності інформації за мінімальних затрат і допустимого рівня обмежень на технологію її обробки в ІТС.

Заходи, що представлені в політиці інформаційної безпеки, направлені на зниження ризиків реалізації загрози через вразливості ІТС, спираючись на існуючий аналіз ризиків. Першочергово необхідно ввести заходи для зниження ризиків по парі загроза/вразливість, що мають критичний рівень ризику. До цієї категорії відноситься випадкове зараження програмних засобів комп'ютерними вірусами через неякісне антивірусне ПЗ.

До припустимого рівня ризику відносяться: несанкціоноване копіювання інформації; ненавмисні дії користувачів, що призводять до відмови функціонування мережі чи окремих її елементів, пошкодження обладнання;

порушення цілісності інформації, що зберігається внаслідок апаратного або програмного збою.

Для зниження рівня ризику зараження програмних засобів комп'ютерними вірусами, розробляється політика антивірусного захисту, що включає організаційні та технічні методи та політика моніторингу та фільтрації використання мережі Інтернет користувачами системи, що також має вплив на цей ризик. Використані адміністративні засоби наведені у таблиці 2.7.

Таблиця 2.21 Використанні адміністративні засоби

Назва засобу	Опис
Політика розмежування прав доступу	Політика розмежування прав доступу Політика розмежування прав доступу регламентує правила доступу користувачів і процесів до пасивних об'єктів. Відповідно до НД ТЗІ 1.4-001-2000, мають виконуватися наступні дії: - кожне робоче місце повинно мати свого користувача, який несе відповідальність за його працездатність та за дотримання всіх вимог і процедур, пов'язаних з обробкою інформації та її захистом. Користувач повинен бути забезпечений відповідними інструкціями і навчений всім вимогам і процедурам; - для попередження неавторизованого доступу до даних, ПЗ, інших ресурсів, керування механізмами захисту здійснюється адміністратором системи; - за всі зміни ПЗ, створення резервних і архівних копій несе відповідальність адміністратор. Такі роботи виконуються за його дозволом; - кожний користувач має свій унікальний ідентифікатор і пароль. Право видачі цих атрибутів надається адміністратору. Атрибути для адміністраторів надає адміністратор безпеки ІТС. Видача атрибутів дозволяється тільки після документальної реєстрації особи як користувача; - користувачі проходять процедуру автентифікації для отримання доступу до ресурсів ІТС; - атрибути користувачів змінюються двічі на рік , а невикористовуванні і скомпрометовані – видаляються.

Продовження таблиці 2.21 Використанні адміністративні засоби

Назва засобу	Опис
Політика антивірусного захисту	Політика включає в себе інструкції для користувачів із застосування антивірусного ПЗ Рекомендації для уникнення проблем з зараженням вірусами: - на початку роботи з системою, переконатися, що антивірусне ПЗ увімкнено; - завжди скануйте носії інформації та підозрілі файли або файли з невідомого джерела на наявність вірусів; - зберігайте резервні копії важливих даних в безпечному місці; - ніколи не завантажувати файли з невідомих чи підозрілих джерел; - не відкривайте невідомі вам файли, що прикріплені до електронної пошти від невідомого, підозрілого або ненадійного джерела. Видаляйте ці вкладення відразу, «подвійним видаленням», шляхом спорожнення кошика.
Курси підвищення кваліфікації для адміністраторів ІТС	Адміністративні засоби, а саме курси підвищення кваліфікації адміністраторів ІТС, до складу яких повинно входити: - Підвищення рівня обізнаності про кібербезпеку; - Підвищення рівня обізнаності про забезпечення безпеки інформації на підприємстві; - Підвищення рівня адміністрування ІТС(розмежування доступу, антиврусна політика, контроль дозволених програмних засобів);

Продовження таблиці 2.21 Використанні адміністративні засоби

Назва засобу	Опис
Курси підвищення кваліфікації для користувачей ІТС	Адміністративні засоби, а саме курси підвищення кваліфікації користувачей ІТС, до складу яких повинно входити: - Підвищення рівня обізнаності про кібербезпеку; - Підвищення навичок забезпечення безпеки інформації для бізнес процесів; - Надбання навичок для роботи

Інженерно-технічних засобів захисту на підприемстві не потрібно, так як цим займається внутріщня служба безпеки офісної будівлі, яка вже забезпечує підприємство послугами. До складу засобів які надає служба безпеки входять:

- Система відеоспостереження;
- Системи датичіків руху, диму та відериття;
- Комплекси металодетекторів на пропускних пунктах;

2.8 Висновки до другого розділу

У рамках другого розділу роботи було виконано обстеження на ОІД, розглянуто: обчислювальну систему, інформаційне середовище, фізичне середовище, середовище користувачів. Проведено аналіз та оцінку ризиків інформаційної безпеки і виділено значущі загрози. За результатами обстеження на ОІД та аналізу інформаційних ризиків, можна виділити недосконалості інформаційно-телекомунікаційної системи підприємства. Недоліки можуть стати причинами появи вразливостей інформації та завдати збитків підприємству.

Згідно з проведеним аналізом, запропоновані до впровадження комплексної системи захисту інформації для забезпечення ефективної роботи всіх складових системи.

Також були описані основні програмні, адмінстративні та інженерно-технічні рішення КСЗІ, які впливають на основні загрози ІТС.

3 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою розрахунків є економічне обґрунтування доцільності впровадження комплексної системи захисту інформації. Для цього визначено економічну ефективність використання основних результатів, що отримані в ході виконання роботи.

Економічна доцільність визначається розрахунками:

- капітальних витрат, що потребує КСЗІ;
- експлуатаційних витрат;
- річного економічного ефекту від впровадження КСЗІ.

3.1 Розрахунок капітальних витрат

3.1.1 Визначення трудомісткості розробки КСЗІ

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

$$t = tmз + tв + ta + tвз + tозб + tовр + tд, \text{ годин,}$$

де ttз - тривалість складання ТЗ на розробку ПБІ = 23 годин;

$t_в$ - тривалість розробки концепції безпеки інформації у організації = 17 годин;

$t_а$ - тривалість процесу аналізу ризиків = 14 годин;

$t_{вз}$ - тривалість визначення виімог заходів, методів та засобів захисту = 19 годин;

$t_{озб}$ - тривалість виробу основних рішень з забезепечення БІ = 11 годин;

$t_{овр}$ - тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організацій = 13 годин;

$t_д$ - тривалість документального оформлення ПБ = 16 годин.

Отже, t = 23 + 17 + 14 + 19 + 11 + 13 + 16 = 113 годин

3.1.2 Розрахунок витрат на створення елементів КСЗІ

Витрати на розробку КСЗІ $К_{рп}$ складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки $З_{зп}$ і вартості витрат машинного часу, що необхідний для розробки КСЗІ $З_{мч}$.

$$К_{рп} = З_{зп} + З_{мч} .$$

$$К_{рп} = З_{зп} + З_{мч} = 20114 + 653,7 = 20767,7 \text{ грн}$$

$$З_{зп} = t * З_{іб} = 113 * 178 = 20114 \text{ грн}$$

де t – загальна тривалість розробки КСЗІ, годин;

Зіб – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину = 178 грн/год.

Вартість машинного часу для розробки КСЗІ на ПК визначається за формулою:

$$З_{мч} = t * С_{мч} = 113 * 5,78 = 653,7 \text{ грн}$$

де t – трудомісткість підготовки документації на ПК, годин;

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

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = P \cdot t_{нал} \cdot Се + \frac{Фзал \cdot На}{Fр} + \frac{Клпз \cdot Напз}{Fр}, \text{ грн;}$$

$С_{мч}$=0,9 * 3 * 1,68 + ((7290* 0,3)/1920) + ((2300 * 0,19)/1920) = 4,536 + 1,13 + 0,119 = 5,78 грн

Вартість ПК = 24300 грн, срок корисної служби = 42 місяці.

Накопичена амортизація = (24300* 42)/5 * 12 = 17010 грн

Залишкова вартість = 24300- 17010= 7290 грн

Для розробки використовують такі програмні засоби:

- Microsoft 365, вартість ліцензії = 1 540 грн, але не враховуємо через те, що програмний продукт вже наявний ;
- Adobe Acrobat Reader DC , вартість ліцензії = 760 грн на місяць;

Symantec Endpoint Protection	1980 грн ліцензія
Safetica Full DLP	1399 грн ліцензія
Кількість ПК	35
Всього	(1980 + 1399)*35 = 118 265 грн

-
-
-

Відповідно до розроблених рекомендації щодо застосування розробки в підприємства ТОВ «ТехноСервіс» планується використання програмних засобів, які вже встановлені на підприємстві, також для розробки потрібно інженерно-технічні засоби.

3.1.3 Капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки.

Капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} = 147379грн$$

$$К = 20114 + 118\ 265 + 0 + 0 + 3600 + 5400 = 147379\ грн$$

де $К_{рп}$ – вартість розробки КСЗІ та залучення для цього зовнішніх консультантів = 20114 грн

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ) = 118 265 грн.

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення = 0

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів = 0 грн

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу = 3600 грн

$К_н$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки = 5400 грн

3.2 Розрахунок експлуатаційних витрат

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

За методикою Gartner Group до поточних (експлуатаційних) варто відносити наступні витрати:

- вартість Upgrade-відновлення й модернізації системи (Св);
- витрати на керування системою в цілому (Ск);
- витрати, викликані активністю користувачів системи інформаційної безпеки (Сак - "активність користувача").

Річні експлуатаційні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_в + С_к + С_{ак}, \text{ грн}$$

$$С = 0 + 157493,69 + 0 = 157493,69 \text{ грн}$$

де $С_в$ - вартість відновлення й модернізації системи $С_в = 0$ грн;

$С_к$ - витрати на керування системою в цілому = 157493,69 грн;

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

Витрати на керування системою інформаційної безпеки ($С_к$) складають:

$$С_к = С_н + С_а + С_з + С_{ел} + С_о + С_{тос}, \text{ грн.}$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються = $С_н = 0$ грн.

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн}$$

де Зосн, Здод - основна і додаткова заробітна плата відповідно, грн на рі

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 28480 грн. Додаткова заробітна плата – 10% від основної заробітної плати. Виконання роботи щодо налаштувань інфраструктури безпечних підключень мобільних користувачів до інтрамережі підприємства потребує залучення спеціаліста інформаційної безпеки на 0,25 ставки. Отже,

$$С_з = (28480 * 12 + 28480 * 12 * 0,1) * 0,25 = (341760 + 34176) * *0,25 = 93984 \text{ грн}$$

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

$$С_{єв} = 93984 *0,22 = 20676,48 \text{ грн}$$

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

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.},$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=0,9 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:

$$С_{ел} = 0,9 * 1920 * 1,68 = 2903,04 \text{ грн}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат - 1%

$$С_{тос} = 147379* 0,01 = 1473,79 \text{ грн}$$

$С_а$ – річний фонд амортизаційних відрахувань, так як використовуються лише програмні засоби, то річний фонд амортизаційних відрахувань дорівнює;

$$С_а = 118\ 265 \text{ х } 0,5 = 59132,5 \text{ грн.}$$

Витрати на керування системою інформаційної безпеки визначаються:

$$С_к = 0 + 59132,5 + 93984 + 2903,04 + 0 + 1473,79 = 157493,69 \text{ грн}$$

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають 157493,69 грн.

3.3 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, 1 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 3 години;

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

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 10400 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 19800 грн./міс.;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 1 особи;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 35 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 10000 тис. грн. у рік;

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

I – число атакованих сегментів корпоративної мережі, 5;

N – середнє число атак на рік, 2.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V,$$

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:

$$П_п = ((19800 * 12) / 176) * 1 = 1350 \text{ грн}$$

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:

$$П_в = П_{ви} + П_{пв} + П_{зч},$$

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 $t_{ви}$:

$$П_{ви} = ((19800 * 12) / 176) * 3 = 8100 \text{ грн.}$$

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

$$П_{пв} = ((12800 * 1) / 176) * 2 = 145{,}45 \text{ грн}$$

Витрати на заміни встаткування або запасних частин можуть скласти 0 грн.

Тоді витрати на відновлення працездатності вузла або сегмента корпоративної мережі складуть:

$$П_в = 8100 + 145,45 + 0 = 8245,45 \text{ грн}$$

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

$$V = \frac{O}{Fг} \cdot (t_П + t_В + t_{ВИ})$$

$$V = (10000000 / 2080) * (1 + 3 + 2) = 28846,15 \text{ грн}$$

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.

$$U = 1350 + 8245,45 + 28846,15 = 38441,6 \text{ грн}$$

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

$$B = 5 * 2 * 38441,6 = 384416,038 \text{ грн}$$

3.4 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B \cdot R - C$$

грн.,

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

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці = 58%;

С – щорічні витрати на експлуатацію системи інформаційної безпеки.

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

$$E = 384416,038 * 0,58 - 157493,69 = 65467,612 \text{ грн}$$

3.5 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:

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

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 = 65467,612 / 147379= 0,44 частки одиниці,

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$ROSI > (N_{деп} – N_{інф})/100),$$

де $N_{деп}$ – річна депозитна ставка, (23%);

$N_{інф}$ – річний рівень інфляції, (14%).

Розрахункове значення коефіцієнта повернення інвестицій:

0,44 > (23 – 14)/100 = 0,4 > 0,09.

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

T = 1/0,44 = 2,27 років.

3.6 Висновки до 3 розділу:

Згідно з отриманими даними під час розрахунку економічної частини - капітальні затрати становлять 147379 грн, експлуатаційні - 135205,58 грн. Згідно з підрахунками, створені елементи КСЗІ є доцільними з економічної точки зору.

Загальний збиток від атаки на вузол або сегмент корпоративної мережі організації склав 384416,038 грн. Загальний ефект від впровадження системи

інформаційної безпеки склав 65467,612 грн. Згідно с коефіцієнтом ROSI який становить 0,44 - створені елементи КСЗІ є цілком доцільними. Термін окупності елементів КСЗІ становить 2,27 років .

Додаток 1

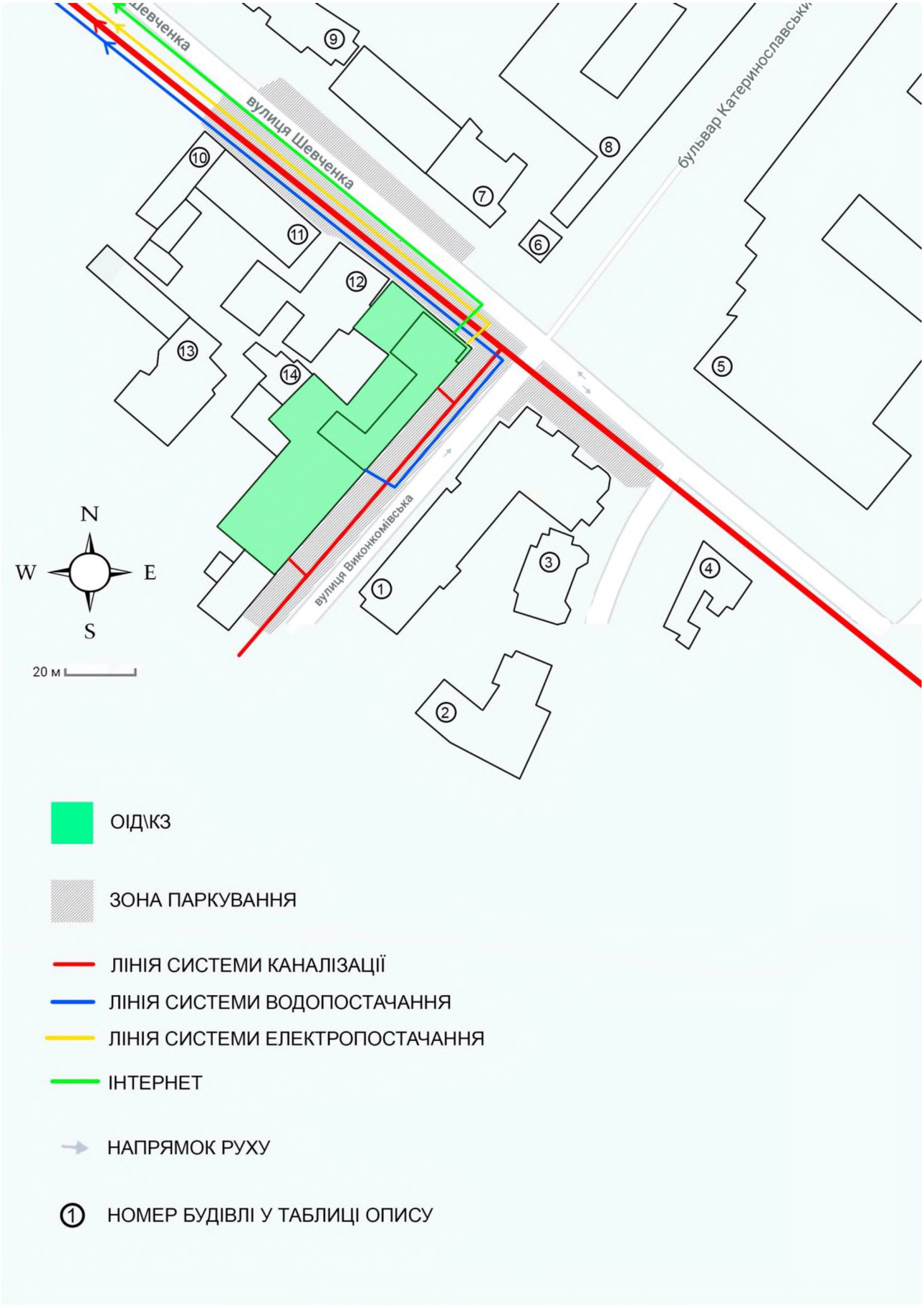

Рисунок1. Ситуаційний план

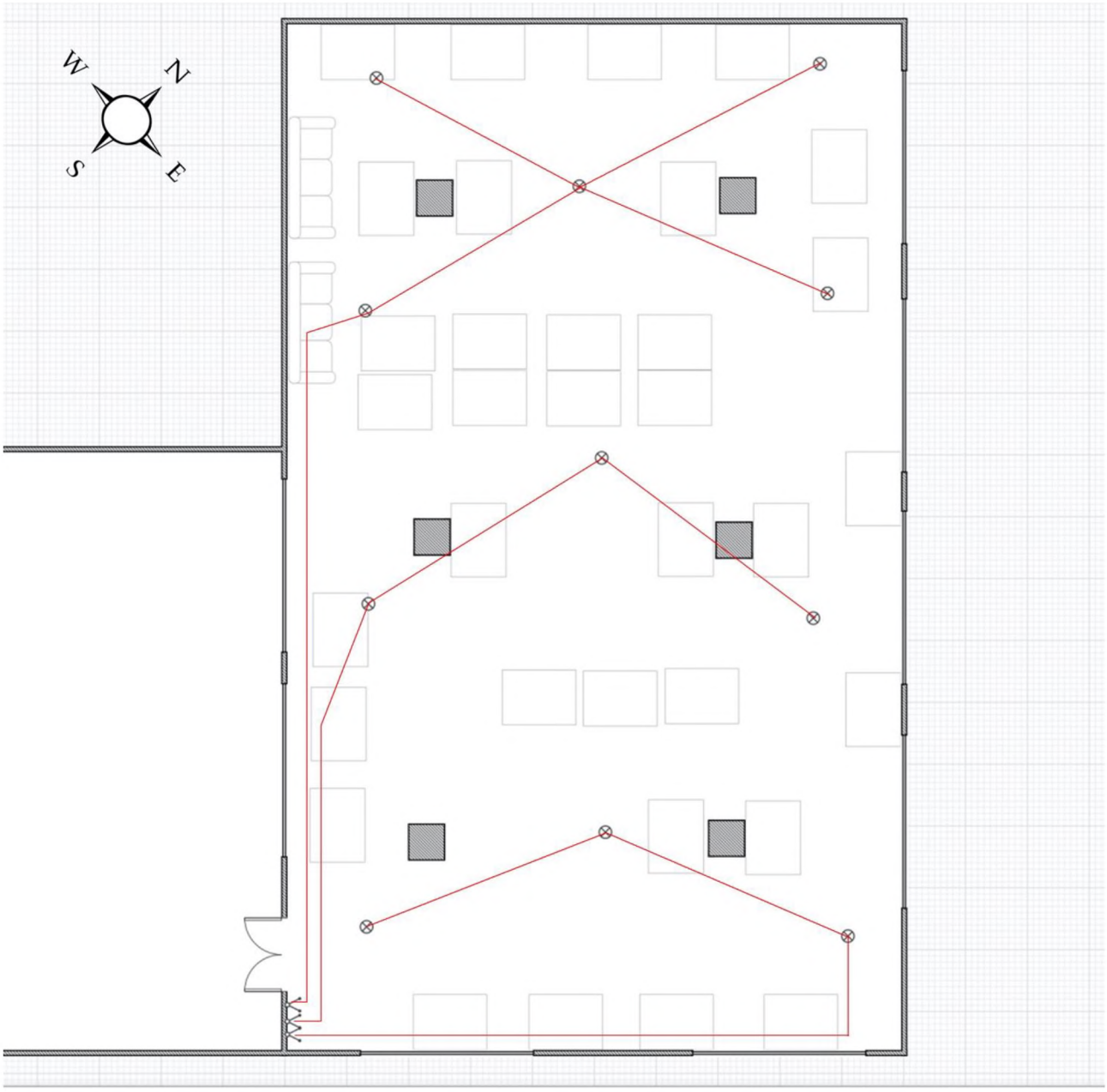

Рисунок2. Схема системи електропостачання

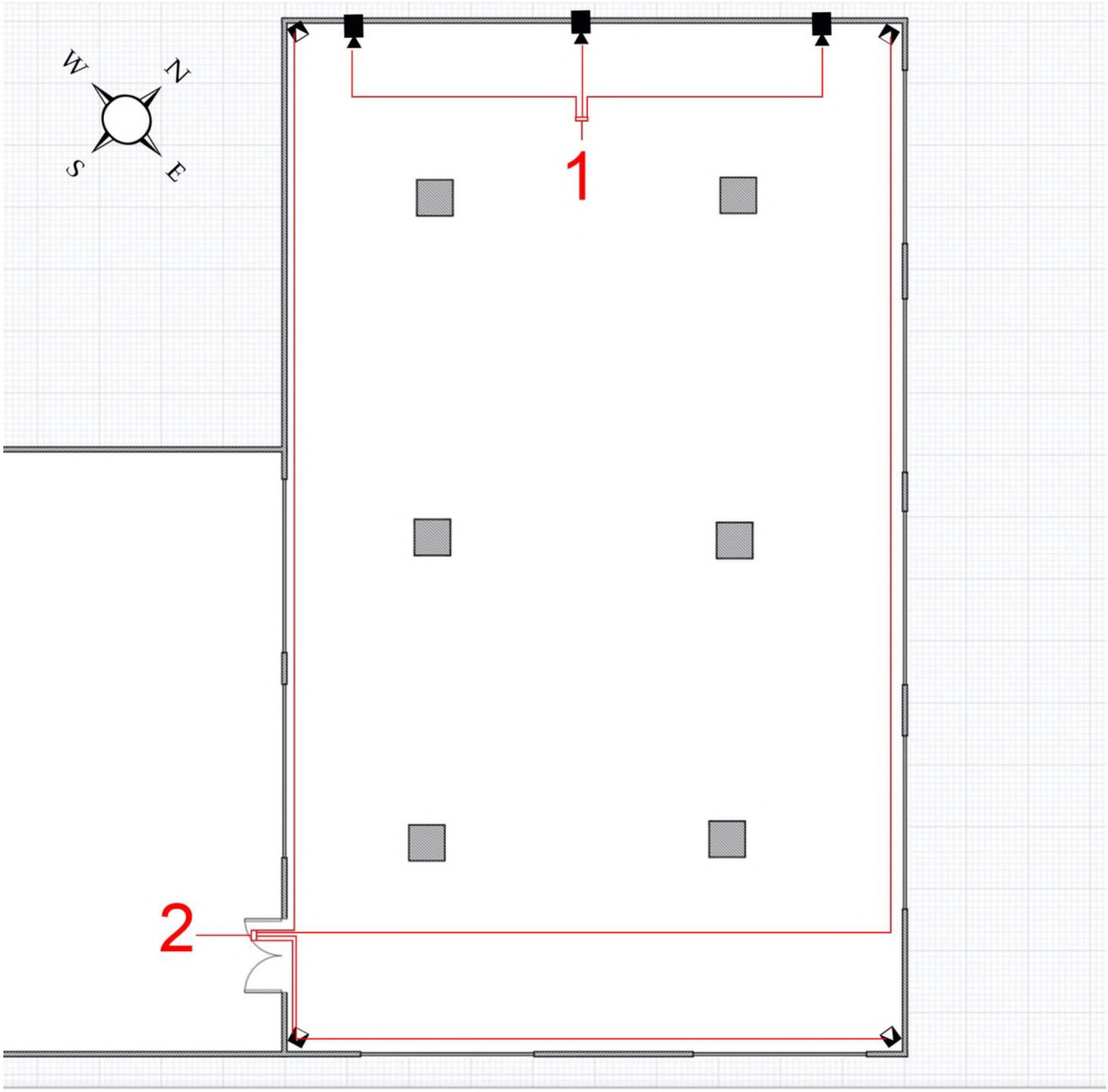

Рисунок4. Схема системи датчиків

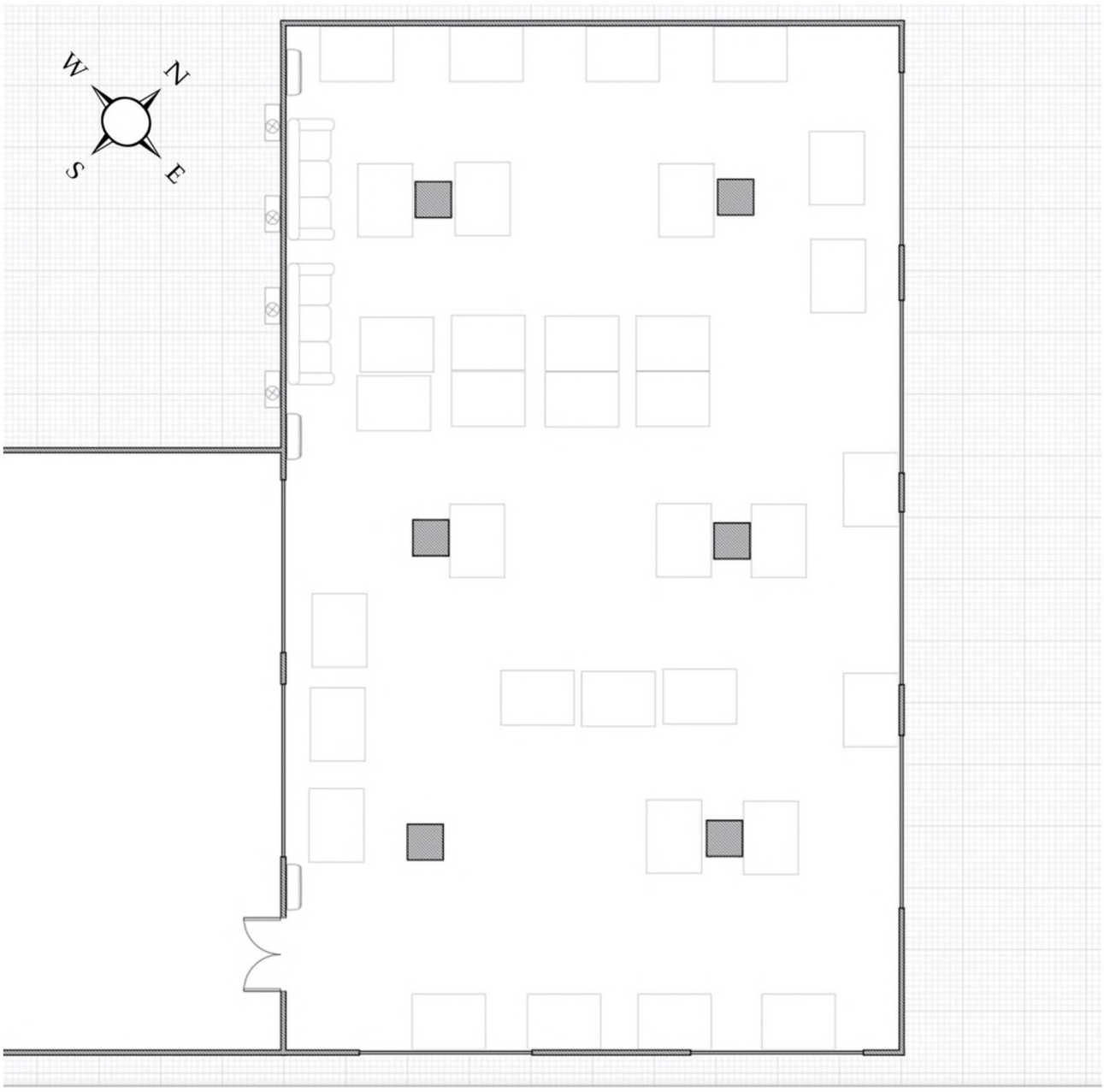

Рисунок5. Схема системи кондиціонування та опалення

Рисунок 6. Схема основних та допоміжних технічних засобів

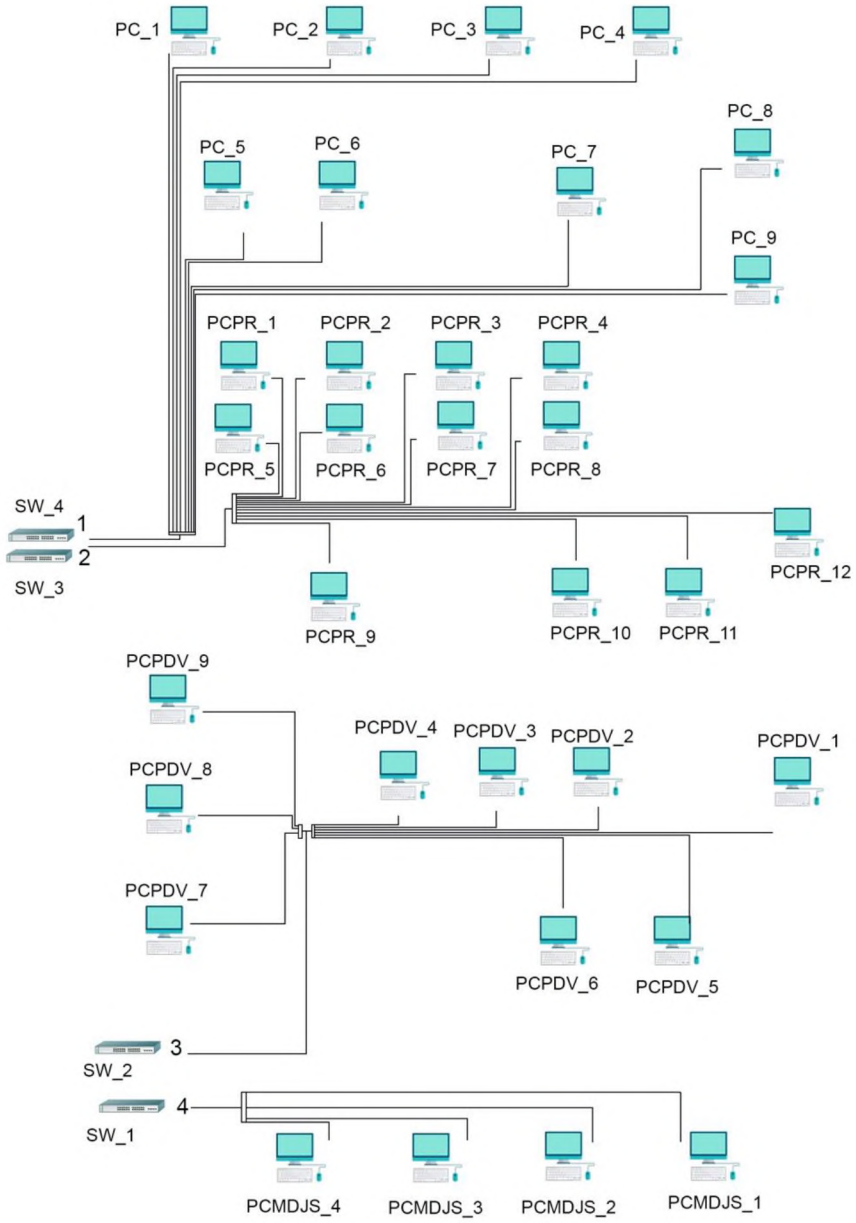

Рисунок 7. Структурна схема

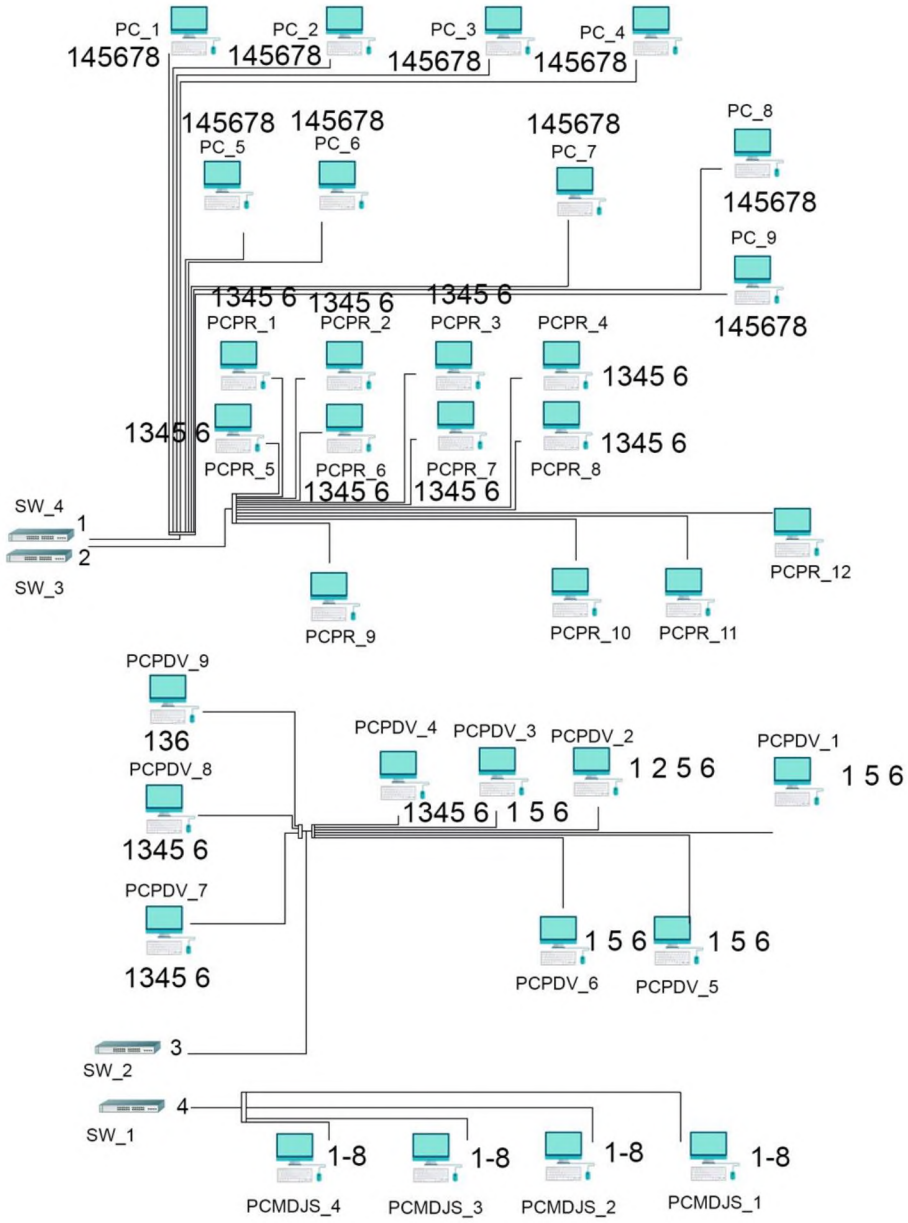

Рисунок 8. Схема інформаційних потоків

Додаток 2. Акт категорювання

Гриф обмеження доступу

Прим. № ___

ЗАТВЕРДЖУЮ

Керівник установи-власника
(розпорядника, користувача) об'єкта

_директор Журавльов. А. С.

(посада, підпис, ініціали, прізвище)

01. 03. 2020

М.П.

АКТ

категоріювання _ТОВ «ТехноСервіс»

(найменування об'єкта категоріювання)

1. Підстава для категоріювання _____

(рішення про створення КСЗІ, закінчення терміну дії акта категоріювання,

_____

зміна ознаки, за якою була встановлена категорія об'єкта, тощо;

_____

посилання/реквізити на розпорядчий документ про призначення комісії з категоріювання)

2. Вид категоріювання _____первинне _____

(первинне, чергове, позачергове)

_____

(у разі чергового або позачергового категоріювання вказується категорія, що була встановлена до цього категоріювання; посилання/реквізити на документ, яким було встановлено цю категорію)

3. На ОІД здійснюється обробка інформації технічними засобами _____

(обробка інформації технічними засобами та/або озвучування інформації)

4. Ступінь обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на об'єкті

_____ конфіденційна інформація _____

(передбачена законом таємниця (крім державної); службова інформація; конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України "Про доступ до публічної інформації"; інша конфіденційна інформація, вимога щодо захисту якої встановлена законом)

5. Встановлена категорія___4 категорія, до четвертою категорії відносяться об'єкти, в яких циркулює службова та конфіденційна інформація, вимога щодо захисту якої встановлена законом_____

Голова комісії _____ К. А. Березовий

(підпис) (ініціали, прізвище)

Члени комісії: _____ В. О. Онищенко_

(підпис) (ініціали, прізвище)

____.____. 20___

Додаток 3. Наказ на створення КСЗІ

Н А К А З

м. Київ

1.03.2020 №101

Про створення комплексної системи
захисту інформації в автоматизованій
системі класу «4» ІТС ТОВ
«ТехноСервіс»

На виконання вимог статті 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» (зі змінами) та п.16 «Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», затверджених Постановою Кабінету Міністрів України від 26.03.2006 року №373 (зі змінами).

НАКАЗУЮ:

1. Створити комплексну систему захисту інформації в автоматизованій системі класу «4» для обробки інформації з обмеженим доступом.

2. Відповідальному за службу захисту інформації в автоматизованих системах Йощенко С.В., забезпечити супроводження робіт зі створення комплексної системи захисту інформації.

3. Контроль за виконанням наказу покласти на заступника директора інженерного відділу – Андрієнко Л. Г.

Директор А.С. Журавлев

Додаток 4. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	1	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	1 Розділ	3	
6	А4	2 Розділ	40	
7	А4	3 Розділ	10	
8	А4	Висновки	1	
9	А4	Список посилань	3	
10	А4	Додаток 1	4	
11	А4	Додаток 2	1	
12	А4	Додаток 3	1	
13	А4	Додаток 4	1	
14	А4	Додаток 5	1	
15	А4	Додаток 6	1	
16	А4	Додаток 7	1	

Додаток 5. Перелік документів на оптичному носії

1. Пояснювальна_записка.docx
2. Пояснювальна_записка.pdf
3. Презентація.pptx

Додаток 6. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____
(підпис) (ініціали, прізвище)

Додаток 7. ВІДГУК

Керівник

СПИСОК ПОСИЛАНЬ

1) Ринок розробки програмного забезпечення [Електронний ресурс] Режим доступу: https://regulation.gov.ua/dialogue/it-i-telekom/14-rinok-rozrobki-programnogo-zabezpecenna
2) Закон України «Про інформацію» від 02.10.1992 No2657-XII // Відомості Верховної Ради України. - 1992. - No 48. [Електронний ресурс]. Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2657-12 Класифікація "інформації в законодавстві України".
3) Закон України "Про захист персональних даних" від 01.06.2010 No 2297-VI // Відомості Верховної Ради України. - 2010. - No 5[Електронний ресурс]. Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2297-17.
4) НД ТЗІ 1.1-002-99: Загальні положення з захисту інформації в комп'ютерних системах від НСД (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. № 22); [Електронний ресурс]. Режим доступу до ресурсу: http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46074&cat_id=38835
5) НД ТЗІ 1.4-001-2000: Типове положення про службу захисту інформації в автоматизованій системі (введено в дію Наказом ДСТСЗІ СБУ від 04.12.2000 р. № 53); [Електронний ресурс]. Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=102122&showHidden=0
6) НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. № 22).; [Електронний ресурс]. Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article;jsessionid=15FDA2B2745B1390AC937214804F2E76?showHidden=1&art_id=102089&cat_id=89734&ctime=1344502332348
7) НД ТЗІ 3.7-001-99: Методичні вказівки щодо розробки технічного завдання

на створення комплексної системи захисту інформації в автоматизованій системі (введено в дію Наказом ДСТСЗІ СБУ від 28.04.199 р. № 22) [2-4,6-8,9]. [Електронний ресурс]. Режим доступу до ресурсу: http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46074&cat_id=38835

8) ДСТУ ISO/IEC 27002:2015 [Електронний ресурс] // ДСТУ. - 2015. - Режим доступу до ресурсу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66911.

9) Етапи створення КСЗІ [Електронний ресурс] - Режим доступу до ресурсу: http://www.vaas.gov.ua/news/zaxist-informacijnix-sistem-vazhlive- zavdannya-sogodennya/.

10) Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 05.07.1994 No80-VI // Відомості Верховної Ради України. - 1994. - No 80. [Електронний ресурс]. - Режим доступу: http://zakon4.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

11) Закон України "Про захист інформації в автоматизованих системах" від 05.07.1994 No80-VI // Відомості Верховної Ради України. - 1994 р., N 31. [Електронний ресурс]. - Режим доступу https://zakon.rada.gov.ua/laws/show/2594-15

12) Асоціаційя підприємств промислової автоматизації України (АППАУ). [Електронний ресурс]. - Режим доступу: https://appau.org.ua/en/

13) Індустрія 4.0 (І 4.0) в Україні. [Електронний ресурс]. - Режим доступу: https://www.proxis.ua

14) Методичні вказівки до виконання економічної чатини дипломного проекту зі спеціальності 125 Кібербезпека/Упорядн. Д. П. Пілова. – Дніпро: Національний технічний університет «Дніпровська політехніка», 2019.

15) Поняття нормативно-правове забезпечення. [Електронний ресурс]. - Режим доступу: https://lpnu.ua

16) Методичні рекомендації до виконання дипломних робіт (проектів) бакалаврів та магістрів спеціальностей 125 Кібербезпека, 172

Телекомунікації та радіотехніка / О.Ю. Гусєв, О.В. Герасіна, О.М. Алексеев, О.В. Кручинін – Дніпро: НГУ, 2018. – 52 с.

17) Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.2–004–99. – Київ: ДСТСЗІ СБ України, 1999. – 55 с.

18) НД ТЗІ 2.5-004 - Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. - [Чинний від 28.04.1999] - К. : ДСТСЗІ СБУ, 1999. - No22 - (Нормативний документ системи технічного захисту інформації).

19) НД ТЗІ 2.5-005 - Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. - [Чинний від 28.04.2000] - К. : ДСТСЗІ СБУ, 2000. - No22- (Нормативний документ системи технічного захисту інформації).

20) Етапи створення КСЗІ [Електронний ресурс] - Режим доступу до ресурсу: http://www.vaas.gov.ua/news/zaxist-informacijnix-sistem-vazhlive- zavdannya-sogodennya/.