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 *Заворіна Івана Дмитровича*

академічної групи *125-16-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Політика безпеки інформації інформаційно-телекомунікаційної системи Машинобудівного коледжу Дніпровського національного університету*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доц. Флоров С.В			
розділів:				
спеціальний	к.т.н., доц. Флоров С.В			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Лізунова Т.Л.			

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 ***Заворіну Івану Дмитровичу*** **академічної групи** ***125-16-2***
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Політика безпеки інформації інформаційно-телекомунікаційної системи Машинобудівного коледжу Дніпровського національного університету***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 26.05.20 № 275-с

Розділ	Зміст	Термін виконання
Розділ 1	Обстеження *інформаційно-телекомунікаційної системи Машинобудівного коледжу Дніпровського національного університету*	29.03.2020
Розділ 2	*Розробка політики безпеки інформації*	24.05.2020
Розділ 3	*Техніко-економічне обґрунтування доцільності впровадження запропонованих у проекті рішень*	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: 93 ст., містить 2 рис., 23 табл.,8 додатків, 9 джерел. Об'єкт розробки: політика безпеки інформації інформаційно-телекомунікаційної системи Машинобудівного коледжу Дніпровського національного університету.

Мета проекту: підвищення рівня захищеності інформації в ІТС Машинобудівного коледжу Дніпровського національного університету.

У першому розділі описано об'єкт обстеження: рід діяльності, відомості про фізичне середовище об'єкту, його інформаційна система, обладнання, програмне забезпечення, інформаційні потоки. Також виконана: класифікація інформації, що обробляється в ІТС, визначено перелік джерел загроз, перелік вразливостей та перелік актуальних для ІТС загроз.

У другому розділі описано існуючий профіль захищеності та виконано вибір нового профілю захищеності коледжу, також були розроблені рекомендації, щодо покращення інформаційної безпеки ОІД.

В третьому розділі були розраховані витрати на впровадження та річну підтримку політики безпеки. Також, було доведено економічну доцільність введення в експлуатацію заходів і засобів, розроблених в другому розділі.

Результати дослідження можуть бути застосовані для реалізації політики інформаційної безпеки Машинобудівного коледжу Дніпровського національного університету.

ПОЛІТИКА БЕЗПЕКИ, ІНФОРМАЦІЙНА БЕЗПЕКА, ВРАЗЛИВОСТІ, НАВЧАЛЬНИЙ ЗАКЛАД, КІБЕРБЕЗПЕКА.

РЕФЕРАТ

Пояснительная записка: 93 с., содержит 2 рис., 23 табл., 8 приложений, 9 источников.

Объект разработки: политика безопасности информации информационно-телекоммуникационной системы Машиностроительного колледжа Днепровского национального университета имени.

Цель проекта: повышение уровня защищенности информации в ИТС Машиностроительного колледжа Днепровского национального университета.

В первом разделе описано объект обследования: род деятельности, сведения о физической среде объекта, его информационная система, оборудование, програм- мное обеспечение, информационные потоки. Также выполнена: классификация ин-формации, которая обрабатывается в ИТС, определен перечень источников угроз, перечень уязвимостей и перечень актуальных для ИТС угроз.

Во втором разделе описано существующий профиль защищенности и выполнен выбор нового профиля защищенности колледжа, также были разработаны рекомендации по улучшению информационной безопасности ОИД. В третьем разделе были рассчитаны затраты на внедрение и годовую поддержку политики безопасности. Также было доказано экономическую целесообразность введения в эксплуатацию мероприятий и средств, разработанных во второй главе.

Результаты исследования могут быть использованы для реализации политики информационной безопасности Машиностроительного колледжа Днепровского национального университета.

ПОЛИТИКА БЕЗОПАСНОСТИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, УЯЗВИМОСТИ, УЧЕБНОЕ ЗАВЕДЕНИЕ, КИБЕРБЕЗОПАСНОСТЬ.

ABSTRACT

Explanatory note: 93 p., 2 fig., 23 tables.,8 appendices, 9 sources

Object of development: Information security policy of the information and telecommunication system of the Engineering College of Dnipro National University named.

Project goal: increasing the level of information security in the ITS of the Engineering College of Dnipro National University.

The first section describes the object: tipe of activity, physical environment of the object, information system, equipment, software, information flows. Also performed: a classification of information that is processed in ITS, list of the threats sources, a list of vulnerabilities, and a list of threats relevant for ITS.

The second section describes the existing security profile and sets up the selection of a new security profile for college. Also have been developed recommendations for ensuring information security of the object of information activity.

In the third section, the costs of implementation and annual support of the security policy have been calculated. It was also proved the economic feasibility of commissioning the measures and tools developed in the second chapter.

The research results can be used to implement a security system, which was organized by the Engineering College of Dnipro National University.

SECURITY POLICY, INFORMATION SECURITY, VULNERABILITIES, EDUCATIONAL INSTITUTION, CYBER SECURITY.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС - автоматизована система;

ЗУ – закон України;

ІБ – інформаційна безпека;

ІТС – інформаційно-телекомунікаційна система;

КЗ – контрольована зона;

КЗЗ - комплекс засобів захисту від несанкціонованого доступу;

КС - комп’ютерна система;

КСЗІ – комплексна система захисту інформації;

НД ТЗІ – нормативний документ в галузі технічного захисту інформації.

НСД - несанкціонований доступ;

ОЗП – оперативний запам’ятовуючий пристрій;

ОІД – об'єкт інформаційної діяльності;

ОС – операційна система;

ПБ – політика безпеки;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

ПКМУ – постанова Кабінету Міністрів України

СУБД – система управління базами даних;

ЗМІСТ

с.

ВСТУП

На сьогодні інформатизація торкнулася всіх сфер нашого життя. Майже жодна людина не може уявити своє існування без комп’ютеру, смартфону чи інтернету. Тож не дивовижно, що сфера освіти також не обходиться без інформаційних технологій.

У розвитку комп'ютерної техніки і програмного забезпечення дуже важливу роль зіграли наукові установи та вищі навчальні заклади. Зокрема, в ВУЗах розробляються, випробовуються і впроваджуються передові проекти в сфері ІТ. З ростом кіберзлочинності захист конфіденційної інформації та наукових розробок в навчальних установах стає особливо актуальною.

У сучасних умовах можна стверджувати: інформація стала стратегічним національним ресурсом - одним з основних багатств будь-якої країни. Більшість інформаційних систем, які належать державним установам мають інформацію, яка потрапивши до зловмисника може призвести до значних економічних втрат та іншим негативним наслідкам. Саме цьому необхідна забезпечити інформаційну безпеку для навчальних закладів. Для вирішення проблеми інформаційної безпеки стає задача розробки політики безпеки.

Таким чином, метою цієї роботи є розробка політики безпеки інформації інформаційно-телекомунікаційної системи Машинобудівного коледжу Дніпровського національного університету.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Загальні відомості про Машинобудівний коледж Дніпровського національного університету.

Об’єктом інформаційної діяльності є державний заклад фахової передвищої освіти Машинобудівний коледж Дніпровського національного університету. Адреса: 49081, Україна, м. Дніпро, вул. Бердянська, 5.

Основними напрямами діяльності коледжу є підготовка кваліфікованих фахівців для галузей машинобудування та економіки згідно з державним замовленням і договірними зобов’язаннями. Існує з 1958 р.

До структури коледжу ввійшли машинобудівне, економічне та підготовче відділення. Навчально-виховний процес здійснюють 42 педагогічних працівників, які об’єднані в 3 предметних та 5 циклових комісіях. Для забезпечення освітньої діяльності створені такі служби коледжу: практичного психолога, фізичного виховання, охорони праці, бухгалтерія, відділ кадрів, юридичний відділ, господарський відділ. Станом на 01.01.2020р. контингент студентів коледжу складає 410 осіб за денною формою навчання. Навчально-лабораторна база коледжу розміщується у трьох навчальних корпусах.

Заклад працює з понеділка по суботу з 8:00 до 17:00.

1.2 Обґрунтування необхідності створення КСЗІ

Згідно ПКМУ №373 від 29 березня 2006 р. «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», захисту в системі підлягає конфіденційна інформація, службова інформація, таємна інформація.

Згідно Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», для створення комплексної системи захисту інформації з обмеженим доступом, вимога щодо захисту якої встановлена

законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюються в порядку, встановленому законодавством.

Відповідальність за забезпечення захисту інформації в системі покладається на власника системи, тобто директора. Власник системи, в якій обробляються інформація з обмеженим доступом утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним. Служба захисту інформації являється основою КСЗІ.

Так як інформаційні ресурси коледжу складаються з відкритої, службової та інформації з обмеженим доступом, захист якої передбачається законодавчо, необхідно створити КСЗІ.

1.3 Обстеження ОІД

1.3.1 Відомості про фізичне середовище ОІД

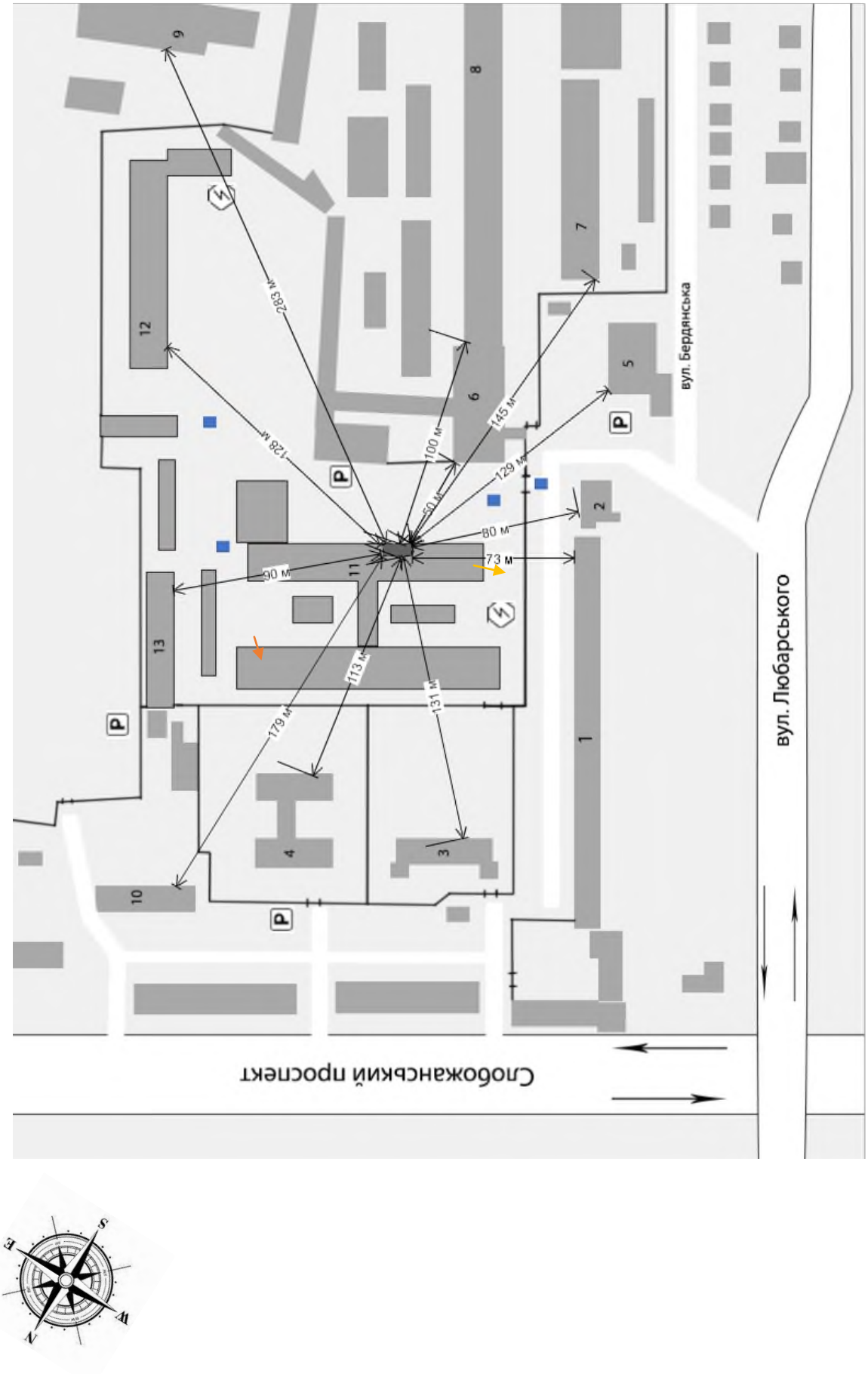
З північного заходу від ОІД на відстані 200 м. знаходиться Слобожанський проспект з інтенсивним транспортним потоком. З південного заходу знаходиться вул. Любарського. Південно західною стороною паркан ОІД межує з двором житлового будинку №1. З південно східної сторони під будівлею ОІД розташований паркінг. Ще один паркінг знаходиться за парканом ОІД під адміністративною будівлею №5. З південно східної сторони також до території ОІД примикають складські приміщення будівлі №6 і №9. У таблиці 1.1 наведено, які об’єкти оточують будівлю з ОІД

Таблиця 1.1 - Характеристика будівель, оточуючих будівлю з ОІД

№ п/п	Тип будівлі	Кількість поверхів	Опис	Відстань від ОІД
1	Житловий будинок	9	Вул. Бердянська, 1	73м.
2	Магазин	1	Вул. Бердянська, 1а	80 м.
3	Дошкільний навчальний заклад	2	Слобожанський проспект, 2/4	131 м.
4	Дошкільний навчальний заклад	2	Слобожанський проспект, 4а	113 м.
5	Житловий будинок	9	Вул. Бердянська, 7	129 м.
6	Автомайстерня	1	Вул. Тьоміна, 1а	50 м.
7	Адміністративна будівля	4	Вул. Бердянська, 5а	145 м.
8	Адміністративна будівля	5	Вул. Артільна, 9	100 м.
9	Адміністративна будівля	3	Вул. Артільна, 9Б	283 м.
10	Житловий будинок	9	Слобожанський проспект, 6а	179 м.
11	Навчальний заклад	3	1 корпус коледжу. ОІД КЗ знаходиться на 2 поверсі. Вул. Бердянська, 5	
12	Навчальний заклад	4	2 корпус коледжу	128 м.
13	Навчальний заклад	1	3 корпус коледжу	90 м.

На рисунку 1.1 показано ситуаційний план, де зображені всі об’єкти, що описуються в таблиці 1.1.

Рисунок 1.1. Ситуаційний план Масштаб 1:500



Таблиця 1.2 - Умовні позначення ситуаційного плану:

Позначення	**Зміст**
	ОІД
-----	Межа КЗ
	Система опалення
	Каналізаційний люк
	Напрямок руху вулицею
	Місце парковки
	Трансформаторна станція
	Електропостачання

1.3.2 Загальні відомості про будівлю, в якій знаходиться ОІД

ОІД розташований на 2 поверсі 1го корпусу коледжу. ОІД являє собою кабінет директора, заступника директора і приймальню.

Комунікації, а саме електромережа, водопостачання та опалення, проходять через ОІД та виходять за межі будівлі через підвал. Каналізаційний люк знаходиться з заходу від будівлі корпусу, система опалення також виходить з заходу на вулицю, а система електропостачання продовжується за межами будівлі зі східної сторони.

Стіни будівлі, в якій знаходиться ОІД зроблені з цегли з зовнішньою шпаклівкою. Територія навколо заасфальтована. Територія огорожена залізо-бетонним парканом. Товщина зовнішніх стін – 400 мм, внутрішніх стін – 300 мм. Вікна – дерев’яні і металопластикові, подвійні, 2500 х 2000 мм. Вхідні двері металеві – 3000 х 2000 мм. З північно-західної сторони є пожежний вихід (металеві двері) – 3000 х 2000 мм. З північно-східної сторони є пожежна драбина, що веде на дах. Висота стель поверхів 3 м. Підлога - ламінат і лінолеум. Перший поверх займає бібліотека, читальна і комп’ютерна зала, кафетерій, спортивна зала, туалет. На другому поверсі знаходяться навчальні

кабінети, бухгалтерія, відділ кадрів, серверна, ОІД. Третій поверх займають навчальні аудиторії.

Комп'ютери у навчальних кабінетах і комп'ютерній залі мають вихід у мережу Інтернет через Ethernet підключення провайдера «Датагруп».

У додатках Б і В зображено генеральний план ОІД і схему комунікацій на ОІД.

Таблиця 1.3 - Характеристика фізичного середовища ОІД

Критерій	**Опис**
1	**2**
Наявність охорони та перепускний режим	На вході у будівлю сидить сторож, який має відмічати сторонніх відвідувачів. Територія КЗ огорожена парканом. Територія ОІД не має огорож і знаходиться в приміщенні на другому поверсі. Сигналізація відсутня.
Режим доступу до компонентів фізичного середовища ІТС	Доступ до компонентів ІТС має директор, секретар, заступник директора.
Вплив зовнішніх чинників, захищенність від технічної розвідки	Захисту від технічної розвідки немає. Об'єкт досить вразливий до зовнішніх чинників, таких як антропомофні, фізичні і природні.
Наявність елементів комунікацій, систем життєзабезпечення й зв'язку, що виходить за межі КЗ	Через об'єкт проходить система опалення, електропостачання, мережа інтернет. Усі комунікації виходять за межі КЗ. Система опалення складається з металевих труб і радіаторів. Система електропостачання підключена до щиту на першому поверсі. Бухгалтерія має окрему мережу.

Продовження таблиці 1.3

1	2
Системи заземлення та характеристики	Головні заземлювачі за допомогою сталевої полоси поєднуються з заземлюючим контуром. Заземлюючий контур виробляється зі стальної полоси товщиною не менш 100 мм^2.
Умови зберігання магнітних, оптико-магнітних, паперових та інших носіїв інформації	Паперові носії інформації зберігаються у сейфі та у шафах. Флеш-накопичувачі зберігається у сейфі та у ящику столу.
Наявність проектної та експлуатаційної документації на компоненти фізичного середовища	Присутня.

1.3.3 Основні та допоміжні технічні засоби

Зображені на рисунку 1.2 основні та допоміжні технічні засоби, більш детально описані із вказанням відстані до меж контрольованої зони у таблиці 1.5

Таблиця 1.5 – Опис основних технічних засобів та допоміжних технічних засобів

Тип	**Модель**	**Місце знаходження**	**Відстань до межі ОІД**	**Кількість**
1	**2**	**3**	**4**	**5**
Маніпулятор типу «Миша»	Logitech B100 USB Black	Приймальня	1,5 м	26
		Кабінет заступника директора	0,5 м	
		Кабінет директора	1 м	
		Відділ кадрів	3 м	
		Бухгалтерія	30 м	
		Кабінет системного адміністратора	40 м	
		Серверна	6 м	
		Навчальні кабінети	6 м	

Продовження таблиці 1.5

1	2	3	4	5
Клавіатура	Logitech K120 USB	Приймальня	1,5 м	26
		Кабінет заступника директора	0,5 м	
		Кабінет директора	1 м	
		Відділ кадрів	3 м	
		Бухгалтерія	30 м	
		Кабінет системного адміністратора	40 м	
		Серверна	6 м	
		Навчальні кабінети	6 м	
Монітор	Acer 193w	Приймальня	1,5 м	26
		Кабінет заступника директора	0,5 м	
		Кабінет директора	1 м	
		Відділ кадрів	3 м	
		Бухгалтерія	30 м	
		Кабінет системного адміністратора	40 м	
		Серверна	6 м	
		Навчальні кабінети	6 м	

Продовження таблиці 1.5

1	2	3	4	5
Робочий комп'ютер	Acer Veriton S2660G	Приймальня	1,5 м	26
		Кабінет заступника директора	0,5 м	
		Кабінет директора	1 м	
		Відділ кадрів	3 м	
		Бухгалтерія	30 м	
		Кабінет системного адміністратора	40 м	
		Серверна	6 м	
		Навчальні кабінети	6 м	
Принтер	HP LaserJet 1000	Приймальня	1 м	7
		Відділ кадрів	3 м	
		Бухгалтерія	30 м	
		Навчальний кабінет	35 м	
Сервер	Dell PowerEdge T40	Серверна	5 м	1
Комутатор	TP-LINK TL-SG116	Серверна	5 м	1
Роутер	D-Link DAP- 231	Приймальня	1,5 м	3
		Серверна	5 м	
		Бухгалтерія	30 м	

Продовження таблиці 1.5

1	2	3	4	5
Сейф	Днепр 600	Кабінет директора	0,5 м	6
		Кабінет заступника директора	0,5 м	
		Відділ кадрів	3 м	
		Бухгалтерія	30 м	

1.3.4 Обчислювальна система ОІД

У інформаційно-технічній системі коледжу також використовуються робочі комп'ютери на інших поверхах корпусу в навчальних аудиторіях і читальній залі аналогічні вказаним комп'ютерам. Тому далі буде розглядатися частина системи, яка розташована на другому поверсі. Використовується 26 робочих комп'ютерів, 7 принтерів, 3 wi-fi роутери, 1 комутатор, 1 сервер. За комп'ютерами працюють відповідні співробітники (викладачі, директор, заступник директору, співробітники відділу кадрів і бухгалтерії) а також за необхідністю студенти у навчальних кабінетах. Всі користувачі мають доступ до мережі Інтернет. Всі робочі комп'ютери об'єднані в локальну мережу. Комп'ютери в бухгалтерії об'єднані в окрему мережу. Два роутери дублюють сигнал від першого для збільшення площі покриття мережі. Топологія мережі – «Зірка».

Операційна система, встановлена на комп'ютерах: Windows 10 Pro (ліцензія).

Операційна система, встановлена на сервері: Windows Server 2016.

У додатку Ґ наверено схему мережевої топології ІТС

Таблиця 1.6 – Основні технічні засоби та їх характеристика

Пристрій	**Компонент**	**Характеристика**	**Інвентарний номер**
1	**2**	**3**	**4**
Робочий комп’ютер Acer Veriton S2660G (DT.VQXME.005)	Процесор	Модель центрального процесора: Intel Core i3-8100 Кількість ядер: 4 ядра Частота центрального процесора: 3,6 ГГц	001050 – 001076
	ОЗП	Обсяг ОЗП: 8 ГБ Кількість слотів ОЗП: 1 Тип оперативної пам'яті: DDR3 Частота оперативної пам'яті: 1333 МГц	
	Жорсткий диск	Обсяг накопичувача: 1 ТБ Тип накопичувача: HDD	
	Відеокарта	Модель графічного процесора: Intel UHD Graphics 630 Тип відеокарти: інтегрований	
	Інтерфейси	4 x USB 2.0 1 x LAN (RJ-45) 1 x DisplayPort 1 x VGA 1 x HDMI	

Продовження таблиці 1.6

1	2	3	4
Сервер Dell PowerEdge T40	Процесор	Тип процесора: Чотирьохядерний Intel Xeon E-2224G (3.5 - 4.7 ГГц) Кількість гнізд під процесори: 1 Чіпсет: Intel C246	001080
	ОЗП	Об'єм оперативної пам'яті: 8 ГБ Тип оперативної пам'яті: UDIMM ECC DDR4-2666 МГц Максимальний обсяг ОЗП: до 64 ГБ, 4 слоти	
	Жорсткий диск	1 ТБ, SATA	
	Інтерфейси	Інтерфейс HDD: SATA Передня панель: 2 x USB 3.0 2 x USB 2.0 Задня панель: 4 x USB 3.0 1 x PS / 2 для підключення клавіатури і миші 2 x DisplayPort 1 x LAN (RJ-45) 1 x COM (послідовний порт) 1 x аудіовхід 1 x аудіовихід Слоти розширення: 1 x PCIe x16 3.0 2 x PCIe x4 3.0	

1	2	3	4
Монітор Acer 193w	Екран	Діагональ екрану 19 " Дозвіл екрану 1440x900 Тип матриці TN Покриття екрану: антиблікове	001090 – 001116
Комутатор TP-LINK TL-SG116	Комутатор	16 портів Gigabit Ethernet	001200 - 001202
Роутер D-Link DAP- 231	Загальні характеристики	Частота роботи Wi-Fi: 2.4 ГГц Швидкість LAN портів: 100 Мбіт/с Швидкість Wi-Fi: 300 Мбіт/с WAN-порт: Ethernet Шифрування: WPA-PSK / WPA-PSK2	001205-001207
	Інтерфейси	1x10/100 Мбіт/с Ethernet WAN	
	Бездротові можливості	802.11b 802.11g 802.11n	
	Антени	Конструкція антен: знімні Кількість антен: 2 зовнішні антени	
	Підтримка протоколів	DHCP PPPoE L2TP PPTP	
Принтер HP LaserJet 1000	Принтер	Лазерний друк (ч/б) Максимальна роздільна здатність друку: 600x600 dpi Інтерфейси: USB	001210-001216

На комп’ютерах співробітників встановлене наступне програмне забезпечення

Таблиця 1.7 – Опис встановленого ПЗ

Тип ПЗ	**Назва**	**Версія**	**Ліцензія**
Системне	Windows 10 Pro	10.0.18363.836	Корпоративна
Системне	Avast Free Antivirus	20.3.2405	Free
Системне	CCleaner	3.0	Free
Системне	Wireshark	2.6.17	Free
Системне	WinRar	5.90	Free
Системне	Realtek Ethernet Controller Driver	5.826.605.2014	Free
Прикладне	Пакет Office 365 Business преміум (Word, Excel, PowerPoint, Outlook, SharePoint, OneDrive, OneNote, Microsoft Teams, Publisher, Access)	11425.20202	Корпоративна
Прикладне	Skype	8.43	Free
Прикладне	Foxit Reader	7.3.6.321	Free
Прикладне	Google Chrome	81.0.4044.129	Free
Спеціалізоване	Компас-3D	18.1	Навчальний комплект
Спеціалізоване	Mathcad	6.0	Навчальний комплект

1.3.5 Перелік персоналу, що має відношення до ОІД, та їх обов’язки:

1. Директор, Черніков Сергій Іванович:

- керування уставом організації освіти, навчальною, науковою, адміністративно-господарської і фінансово-економічною діяльністю;
- затвердження робочих навчальних планів і програми, графіків навчальних процесів, правил внутрішнього розпорядку;
- затверджує структуру управління, штатний розклад, посадові інструкції працівників організації освіти;
- формування контингенту учнів, забезпечення їх соціального захисту;
- координування роботи з роботодавцями та соціальними партнерами;
- розпорядження наявним майном і коштами, забезпечення обліку, збереження й поповнення навчально-матеріальної бази, дотримання правил санітарно-гігієнічного режиму;
- організація переоснащення та реорганізація матеріально-технічної бази;
- керування роботи педагогічної ради;
- забезпечення впровадження і залучення інноваційних технологій освіти;
- здійснює підбір і розстановку кадрів, забезпечує необхідний рівень педагогічного та виховного процесу;
- надавання уповноваженому органу щорічного звіту про результати навчальної, наукової та фінансової діяльності.

2. Заступник директора, Прокуда Галина Володимирівна :

- керування плануванням і розподілом педагогічного навантаження викладачів на навчальний рік;
- організація необхідної роботи з придбання, розробки, переробки навчально-методичної документації, форм і змісту всієї навчально-організаційної документації;
- організовує і здійснює роботи з проведення ліцензування, атестації та акредитації коледжу;
- забезпечення своєчасного складання встановленої звітної документації;

- здійснення контролю за роботою підлеглих, підписує табель обліку їх робочого часу;
- організація розвитку позабюджетної діяльності та зростання позабюджетного доходу;
- заміщення директора в разі його відсутності.

3. Секретар, Кузьміна Алла Борисівна:

- підготовка проектів наказів і розпоряджень по руху контингенту учнів;
- оформлення особистих справ, студентських квитків, книжок успішності;
- участь в організації проміжної і державних підсумкової атестації;
- ведення діловодства, в тому числі і в електронній формі;
- участь в роботі приймальної комісії;
- оформлення заявок на обліково-звітну документацію.

4. Системний адміністратор, Стрежекур Юрій Миколайович:

- слідкування за станом локальної мережі, підтримання її в належному стані;
- встановлення і оновлення ПЗ;
- перевірка журналів подій;
- відповідальність за інформаційну безпеку в коледжі;
- проведення необхідних заходів та відповідна модернізація системи;
– відповідальність за резервне копіювання;
- встановлення оновлень і налаштування операційних систем;
- керування сервером;

5. Прибиральниці, Гречана Людмила Олександрівна, Івакіна Людмила Іванівна:

- підтримка чистоти в приміщенні у встановлений час.

1.3.6 Інформаційне середовище ОІД

У цьому розділі описана інформація, що циркулює в ІТС. Інформація представлена в електронному та друкованому вигляді. Перелік інформації вказаний у таблиці 1.8.

Таблиця 1.8 – Інформація, що циркулює на об’єкті

№ п/п	Інформація	Опис	Режим доступу	Правовий режим
1	**2**	**3**	**4**	**5**
1	Інформація для забезпечення навчального і наукового процесів.	Робочі плани спеціальностей, робочі програми дисциплін, учбові графіки.	Відкрита	-
2	Договори, угоди	Договори щодо надання послуг як підприємством, так і іншими підприємствами (наприклад, обслуговування системи, послуги охорони)	Обмежений доступ	Комерційна таємниця
3	Накази і розпорядження директора	Накази з основної діяльності, накази з особового складу	Відкрита	-
4	Журнали реєстрації документації	Журнали наказів, вхідної, вихідної документації, обліку звернень громадян.	Обмежений доступ	Для службового користування

1	2	3	4	5
5	Постанови з вищестоящих організацій	Вхідна документація	Відкрита	-
6	Інформація про студентів і працівників	Персональні, паспортні дані	Обмежений доступ	Конфіденційна інформація
7	Звіти системного адміністратора	Інформація про корпоративну мережу, програмне забезпечення, технічне обслуговування	Обмежений доступ	Для службового користування
8	Бухгалтерські звіти	Інформація щодо витрат, нарахування заробітних плат	Обмежений доступ	Комерційна таємниця

Описана у таблиці 1.8 інформація має такі властивості:

– конфіденційність;

– цілісність;

– доступність.

Таблиця 1.9 – Класифікація інформації, за властивостями

Інформація	**Рівень конфіденційності**	**Рівень цілісності**	**Рівень доступністі**
Інформація для забезпечення навчального і наукового процесів.	К1	Ц3	Д4
Договори, угоди	К3	Ц4	Д4
Накази і розпорядження директора	К1	Ц3	Д3
Журнали реєстрації документації	К2	Ц2	Д2
Постанови з вищестоящих організацій	К1	Ц5	Д3
Інформація про студентів і працівників	К4	Ц4	Д4
Звіти системного адміністратора	К4	Ц3	Д3
Бухгалтерські звіти	К4	Ц4	Д4

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

Рівні конфіденційності:

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

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

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

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

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

Рівні цілісності:

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

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

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

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

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

Рівні доступності:

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

доступності інформації;

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

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

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

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

1.3.7 Технологія обробки інформації в ІТС

В цьому розділі описується перелік і порядок дій, що виконуються з інформацією в ІТС.

Завідуючі кафедр складають навчальні плани спеціальностей, програми дисциплін, учбові графіки, передають заступнику директора на перевірку і узгодження планів у друкованому вигляді і копією на електронну пошту. Після перевірки інформація для забезпечення навчального і наукового процесів затверджується директором, завантажуються на сервер і доводяться до відома педагогічного складу та студентів.

Накази і розпорядження директора з особового складу, діяльності коледжу готує директор чи його секретар, затверджує директор. Секретар робить копії наказів і розсилає по електронній пошті персоналу, заносить в паперовий журнал і завантажує копію на сервер. Далі системний адміністратор додає наказ на сайт коледжу.

Постанови з вищестоящих організацій, наприклад з Міністерства освіти і науки України з’являються на сайті Міністерства освіти і науки України. З сайту співробітники коледжу завантажують накази і ознайомлюються з ними з робочих комп’ютерів. Також секретар заносить наказ у журнал вхідної документації.

Договори, угоди складаються в електронному вигляді, можуть бути

відскановані, та обов’язково друкуються. Надалі зберігаються в сейфі. Доступ має лише директор і бухгалтерія.

При наданні документів до зарахування в коледж у випадку студентів чи при влаштуванні на роботу у випадку співробітників студент чи співробітник заповнює заяву зі своїми персональними даними. Далі інспектор відділу кадрів формує особові справи, де зберігаються документи з персональними даними. Особові справи зберігаються на паперовому носії в сейфі у відділі кадрів. Особові справи можуть видаватися співробітникам коледжу, відповідальним за їх обробку згідно з наказом директора.

Звіти системного адміністратора складаються системним адміністратором на основі даних про корпоративну мережу, програмне забезпечення, технічне обслуговування і завантажуються на сервер, де, в свою чергу, з ними може ознайомитись директор.

Бухгалтерські звіти складаються в електронному вигляді бухгалтером, передається на підпис директору через окрему мережу, підписується цифровий підпис і передається в казначейство і налогову інспекцію головним бухгалтером. Звіти зберігаються на флеш накопувачі у сейфі в кабінеті директора.

Інформація з обмеженим доступом не озвучуються.

На рисунку 1.2 зображено схему інформаційних потоків в ІТС

Рисунок 1.2 – Інформаційні потоки в ІТС

Проаналізувавши інформаційні потоки можна скласти таблицю доступу, де буде зазначено можливості користувачів АС відносно об’єктів.

Таблиця 1.10 – Матриця доступу до інформації

Користувачі	**Інформація**	**Рівень можливостей в ІТС**	**Доступ до ІТС та компонентів**
1	**2**	**3**	**4**
Директор	1 – Ч, З, К, М, Д, В; 2 – С, Ч, З, Д; 3 – С, Ч, З, М, К, Д, В; 4 – Ч; 5 – Ч, З, К, Д; 6 – Ч, З, К, Д; 7 – Ч, З, К, Д; 8 – Ч, З, К, Д;	Користувач здатний взаємодіяти з апаратною та програмною частиною ІТС	Адміністративний доступ
Заступник директора	1 – С, Ч, З, К, М, Д, В; 3 – Ч, З, К, Д; 4 – Ч; 5 – Ч, З, К, Д; 6 – Ч, З, К, Д;	Користувач здатний взаємодіяти з апаратною та програмною частиною ІТС	Адміністративний доступ
Завідуючі кафедр	1 – С, Ч, З, К, М, Д; 3 – Ч, З, К, Д; 5 - Ч, З, К, Д;	Користувач здатний взаємодіяти з апаратною та програмною	Доступ користувача

	6 - Ч, З, К, Д;	частиною ІТС	

Продовження таблиці 1.10

1	2	3	4
Секретар	1 – Ч, З, К, Д; 3 - С, Ч, З, К, Д; 4 – С, Ч, З, К, М, Д, В; 5 - Ч, З, К, Д; 6 - Ч, З, К, Д;	Користувач здатний взаємодіяти з апаратною та програмною частиною ІТС	Доступ користувача
Системний адміністратор	1 – Ч, З, К, Д, В; 3 – Ч, З, К, М, Д; 4 – Ч, З, К, Д; 5 – Ч, З, К, Д; 7 – С, Ч, З, К, М, Д, В;	Користувач здатний взаємодіяти з апаратною та програмною частиною ІТС на професійному рівні.	Адміністративний доступ
Бухгалтер	1 – Ч, З, К, Д; 2 – Ч, З; 3 - Ч, З, К, Д; 4 – Ч; 5 - Ч, З, К, Д; 6 - Ч, З, К, Д; 8 – С, Ч, З, К, М,	Користувач здатний взаємодіяти з апаратною та програмною частиною ІТС	Доступ користувача

	Д;		
Інспектор відділу кадрів	1 - Ч, З, К, Д; 3 - Ч, З, К, Д; 5 – Ч, З, К, Д; 6 – С, Ч, З, К, М, Д, В;	Користувач здатний взаємодіяти з апаратною та програмною частиною ІТС	Доступ користувача

Продовження таблиці 1.10

1	**2**	**3**	**4**
Викладачі	1 - Ч, З, К, Д; 3 - Ч, З, К, Д; 5 - Ч, З, К, Д;	Користувач здатний взаємодіяти з апаратною та програмною частиною ІТС	Доступ користувача
Студенти	1 - Ч, З, К, Д; 3 - Ч, З, К, Д; 5 - Ч, З, К, Д;	Користувач здатний взаємодіяти з програмною частиною ІТС	Доступ користувача

Умовні скорочення в таблиці 1.10:

– С – створення;

– Ч – читання;

– З – зберігання;

– К – копіювання;

– М – модифікація;

– Д – друк;

– В – видалення/знищення.

1.4 Аналіз загроз інформації, що циркулює на ОІД

1.4.1 Аналіз джерел загроз

Джерела загроз безпеки інформації можна розділити на антропогенні, техногенні і стихійні. Для інформації, що обробляється в ІТС можуть бути характерними такі види джерел загроз:

1. Антропогенні. Внутрішні по відношенню до ІТС;

1.1 Директор;

1.2 Заступник директора;

1.3 Секретар;

1.4 Системний адміністратор;

1.5 Завідуючі кафедр;

1.6 Викладачі;

1.7 Бухгалтер;

1.8 Інспектор відділу кадрів;

2. Антропогенні. Зовнішні по відношенню до ІТС;

2.1 Технічний персонал, що обслуговує будівлю (Прибиральниця, електрики, сантехники і т.д)

2.2 Сторож;

2.3 Студенти;

2.4 Відвідувачі (запрошені представники організацій, сторонні особи, які увійшли в КЗ непоміченими);

2.5 Звільнені співробітники;

2.6 Члени преступних організацій;

2.7 Особи, що навмисне проникнули в мережу коледжу із зовнішніх

мереж (хакери);

3. Техногенні;

3.1 Сервер та ПЗ, встановлене на ньому;

3.2 Комп’ютери та ПЗ, встановлене на них;

3.3 Wi-Fi роутери;

3.4 Мережі комунікацій (опалення, електропостачання);

4. Стихійні;

4.1 Пожежа;

4.2 Бойові дії;

Всі джерела загроз мають різну ступінь небезпеки (Коп), яку можна кількісно оцінити, провівши їх ранжування. Кожен показник оцінюється експертно-аналітичним методом за п'ятибальною системою, де 1 відповідає мінімальному ступеню впливу оцінюваного показника на небезпеку використання джерела, а 5 - максимальному. В якості критеріїв порівняння (показників) обрано:

Можливість виникнення джерела (К1) - визначає ступінь доступності до об'єкта (для антропогенних джерел), віддаленість від об'єкта, що захищається (для техногенних джерел) або особливості обстановки (для стихійних джерел).

Готовність джерела (К2) - визначає ступінь кваліфікації і бажання здійснення реалізувати загрозу (для антропогенних джерел), або наявність необхідних умов (для техногенних і стихійних джерел).

Фатальність (К3) - визначає ступінь неможливості усунення наслідків реалізації загрози.

Таблиця 1.11 – Ступені можливості виникнення джерела загрози

№ п/п	**К1**
1	**2**
1	Немає доступу до об’єкта (для антропогенних);

	джерело дуже віддалене від об’єктів захисту і не може впливати на нього (для техногенних); на ОІД відсутні будь-які передумови виникнення джерела загрози (для стихійних);
2	Має дуже обмежену можливість доступу до об’єкта (для антропогенних); джерело дуже віддалене від об’єктів захисту, але все ще може впливати на нього (для техногенних); на ОІД є деякі передумови виникнення джерела загрози, але імовірність їх прояву дуже мала (для стихійних);

Продовження таблиці 1.11

1	**2**
3	Джерело має обмежений доступ до технічних і програмних засобів обробки інформації (для антропогенних); джерело знаходиться поблизу будівлі, де знаходиться ОІД, або в тій самій будівлі (для техногенних); довгий час не було жодного прояву джерела загрози, втім, є передумови для його появи (для стихійних);
4	Джерело має доступ до технічних і програмних засобів обробки інформації, що захищається, але це не є його функціональним обов’язком (для антропогенних); Джерело знаходиться в тому ж приміщенні (для техногенних); ОІД не знаходиться у зоні дії катаклізмів, втім, імовірність прояву джерела загрози висока (для стихійних);
5	Джерело має повний доступ до технічних і програмних засобів обробки інформації, що захищається, а також максимальні повноваження доступу (для антропогенних);

	сам об’єкт містить джерело загрози (для техногенних); ОІД знаходиться у зоні дії катаклізмів (для стихійних);

Таблиця 1.12 – Ступені готовності джерела загрози

№ п/п	**К2**
1	Інформація не представляє інтересу для джерела. Не має ніяких відповідних можливостей (для антропогенних); На ОІД немає жодних можливостей для виникнення джерела загрози (для техногенних і стихійних);
2	Реалізація загрози не вигідна для джерела. Має недостатній рівень знань для реалізації загрози (для антропогенних); Загроза слабо реалізовується - тобто існують об'єктивні причини на самому об'єкті або в його оточенні, що перешкоджають реалізації загрози (для техногенних і стихійних);
3	Джерелу вигідна реалізація загрози. Має можливість створення і запуску користувачем власних програм з новими функціями по обробці інформації. Може навчитися методам, що реалізують загрозу (для антропогенних); Прояв джерела загрози можливий, але швидше за все він не зможе проявити себе (для техногенних і стихійних);

4	Джерелу дуже вигідна реалізація загрози. Має можливість управління функціонуванням мережею, тобто впливом на базове програмне забезпечення, її склад і конфігурацію (рівень системного адміністратора) (для антропогенних); Прояв джерела загрози можливий (для техногенних і стихійних);
5	Мета виконавця. Має всі можливості для проектування і ремонту технічних засобів, в тому числі включення до складу мережі власних технічних засобів з новими функціями по обробці інформації (для антропогенних); Умови сприяють прояву джерела загрози (для техногенних і стихійних);

Таблиця 1.13 – Фатальність наслідків

№ п/п	**КЗ**
1	Результати прояву загрози не можуть вплинути на діяльність об'єкта захисту.
2	Результати прояву загрози можуть призвести до часткового руйнування об'єкта захисту, які майже не потребують витрат на його відновлення.
3	Результати прояву загрози можуть призвести до часткового руйнування об'єкта захисту, які не потребують значних витрат на його відновлення.
4	Результати прояву загрози можуть призвести до руйнування об'єкта захисту, і до значних на відновлення наслідків, порівнянних з витратами на створення нового об'єкту і суттєвого обмеження часу доступу до ресурсів, що захищаються.
5	Результати прояву загрози можуть призвести до повного руйнування об'єкта захисту, і як наслідок до непоправних втрат і

	виключення можливості доступу до інформаційних ресурсів, що захищалися.

Ступінь небезпеки (Коп)і знаходиться по формулі:

$$(\text{Коп})\text{і} = \frac{(\text{К1}*\text{К2}*\text{К3})}{125}; \quad (1.1)$$

Таблиця 1.13 – Ранжування загроз

Джерело загрози	**К1**	**К2**	**К3**	**К оп**
Директор	5	2	4	0,32
Заступник директора	4	2	4	0,256
Секретар	4	2	3	0,192
Системний адміністратор	5	4	4	0,64
Завідуючі кафедр	4	3	3	0,288
Викладачі	4	3	3	0,288
Бухгалтер	4	2	3	0,192
Інспектор відділу кадрів	4	2	3	0,192
Технічний персонал	3	1	2	0,048
Сторож	3	1	2	0,048
Студенти	3	3	3	0,216
Відвідувачі	2	3	3	0,144
Звільнені співробітники	1	4	3	0,096
Члени преступних організацій	1	5	4	0,16

Хакери	3	5	4	0,48
Сервер та ПЗ, встановлене на ньому	5	3	4	0,48
Комп’ютери та ПЗ, встановлене на них	5	3	4	0,48
Wi-Fi роутери	5	4	4	0,64
Мережі комунікацій	5	2	3	0,24
Пожежа	3	3	5	0,36
Бойові дії	3	3	5	0,36

Проаналізувавши дані з таблиці 1.13, можна знехтувати такими джерелами загроз (Коп < 0.19):

- Бухгалтер;
- Інспектор відділу кадрів;
- Звільнені співробітники;
- Технічний персонал;
- Сторож;
- Члени преступних організацій;
- Відвідувачі;

1.4.2 Аналіз вразливостей

Виходячи з аналізу можливих загроз на ОІД можна зазначити такі вразливості:

1 Об’єктивні:

1.1 Технічні канали витоку інформації;

1.2 Можливість несанкціонованого підключення до бездротової мережі;

1.3 Несвоєчасне оновлення ПЗ;

1.4 Відсутність коректного розмежування прав доступу до об’єктів;

1.5 Можливість зараження системи комп’ютерними вірусами;

1.6 Відсутність механізмів протидії несанкціонованому підключенню знімних носіїв до комп’ютерів;

2 Суб’єктивні:

2.1 Помилки користувачів (впровадження і використання програм, що не є необхідними для виконання службових обов’язків; запуск програм, здатних викликати критичні зміни в системі);

2.2 Недбале зберігання та облік документів, носіїв інформації, баз даних;

2.3 Помилки системного адміністратора (неправильне конфігурування та адміністрування системи захисту, операційної системи; неправомірне відключення засобів захисту);

2.4 Відсутність відеонагляду;

2.5 Відсутність служби охорони;

2.6 Відсутність сигналізації

2.7 Недосконалість протипожежної системи (присутні лише вогнегасники і пожежні рукави на поверхах);

2.8 Відсутність регламентованого порядку встановлення та планової зміни паролів, критеріїв до їх створення і контролю їх зберігання;

3 Випадкові:

3.1 Збій обладнання;

3.2 Відмова обладнання;

3.3 Втрата чи псування носіїв інформації;

Усі вразливості мають різну ступінь небезпеки, яку можна кількісно оцінити за допомогою ранжування.

Фатальність (К1) - визначає ступінь впливу вразливості в наслідку реалізації загрози.

Доступність (К2) - визначає зручність (можливість) використання

вразливості джерелом загроз.

Кількість (К3) - визначає кількість елементів об'єкта, яким характерна вразливість.

Таблиця 1.14 – Фатальність

№ п/п	К1
1	**2**
1	Використання вразливості не призведе до серйозних наслідків.
2	Вразливість може призвести до реалізації загрози, але ймовірність цього досить мала.
3	Використання вразливості може призвести до реалізації загрози.

Продовження таблиці 1.14

1	**2**
4	Використання вразливості швидше за все призведе до реалізації загрози.
5	Використання вразливості точно призведе до реалізації загрози.

Таблиця 1.15 – Доступність

№ п/п	К2
1	Вразливість неможливо або надзвичайно важко використати.
2	Використання вразливості потребує великої кількості часу та ресурсів.
3	Для використання вразливості необхідні певні умови.
4	Вразливість може використати будь-яка людина, яка володіє

	необхідними знаннями, вміннями чи привілеями.
5	Вразливість може використати практично будь-хто.

Таблиця 1.16 – Кількість

№ п/п	К3
1	0-1 елемент
2	2-9 елементів
3	10-14 елементів
4	15-25 елементів
5	25+ елементів

Ступінь небезпеки (Коп)f знаходиться по формулі:

$$(\text{Коп})\text{f} = \frac{(\text{К1}*\text{К2}*\text{К3})}{125}; \quad (1.2)$$

Таблиця 1.17 – Ранжування вразливостей

Вразливість	К1	К2	К3	К оп
1	**2**	**3**	**4**	**5**
Технічні канали витоку інформації	3	2	3	0,144
Можливість несанкціонованого підключення до бездротової мережі	3	4	2	0,192
Несвоєчасне оновлення ПЗ	3	4	5	0,48
Відсутність коректного	4	5	5	0,8

розмежування прав доступу до об’єктів				
Можливість зараження системи комп’ютерними вірусами	3	4	5	0,48
Відсутність механізмів протидії несанкціонованому підключенню знімних носіїв до комп’ютерів	4	4	5	0,64
Помилки користувачів	3	5	5	0,6
Недбале зберігання та облік документів, носіїв інформації, баз даних	4	4	4	0,512
Помилки системного адміністратора	4	4	5	0,64

Продовження таблиці 1.17

1	**2**	**3**	**4**	**5**
Відсутність відеонагляду	3	5	2	0,24
Відсутність служби охорони	3	3	1	0,072
Відсутність сигналізації	3	4	2	0,192
Недосконаліть протипожежної системи	3	3	3	0,216
Вразливість	К1	К2	К3	К оп
Відсутність регламентованого порядку встановлення та планової зміни паролів, критеріїв до їх створення і контролю їх зберігання	3	4	5	0,48
Збій обладнання	3	3	5	0,36
Відмова обладнання	2	3	5	0,24

Втрата чи псування носіїв інформації	2	3	4	0,192

Проаналізувавши дані з таблиці 1.17, можна знехтувати такими вразливостями (Коп < 0.19):

Технічні канали витоку інформації;

Відсутність служби охорони;

1.4.3 Аналіз загроз

Таким чином, виходячи із аналізу джерел загроз і вразливостей в таблиці 1.13 і таблиці 1.17 можна скласти наступний перелік актуальних джерел загроз і вразливостей:

- Д1 – Директор;
- Д2 - Заступник директора;
- Д3 - Секретар;
- Д4 - Системний адміністратор;
- Д5 - Завідуючі кафедр;
- Д6 – Викладачі;
- Д7 - Студенти;
- Д8 - Хакери;
- Д9 - Сервер та ПЗ, встановлене на ньому;
- Д10 - Комп’ютери та ПЗ, встановлене на них;
- Д11 - Wi-Fi роутери;
- Д12 - Мережі комунікацій;
- Д13 - Пожежа;
- Д14 - Бойові дії;
- В1 - Можливість несанкціонованого підключення до бездротової мережі;
- В2 - Несвоєчасне оновлення ПЗ;

- В3 - Відсутність коректного розмежування прав доступу до об’єктів;

- В4 - Можливість зараження системи комп’ютерними вірусами;

- В5 - Відсутність механізмів протидії несанкціонованому підключенню знімних носіїв до комп’ютерів;

- В6 - Помилки користувачів;

- В7 - Недбале зберігання та облік документів, носіїв інформації, баз даних;

- В8 - Помилки системного адміністратора;

- В9 - Відсутність відеонагляду;

- В10 - Відсутність сигналізації;

- В11 - Недосконаліть протипожежної системи;

- В12 - Відсутність регламентованого порядку встановлення та планової зміни паролів, критеріїв до їх створення і контролю їх зберігання;

- В13 - Збій обладнання;

- В14 - Відмова обладнання;

- В15 - Втрата чи псування носіїв інформації;

Далі можна скласти матрицю взаємозв’язку актуальних джерел загроз і вразливостей, в якій розраховується коефіцієнт небезпеки реалізації загроз (атак) як добуток коефіцієнтів небезпеки відповідних вразливостей і джерел загроз, які були знайдені в таблицях 1.13 і 1.17.

	Джерела загроз										
Вразливості	Д1	Д2	Д3	Д4	Д5	Д6	Д7	Д8	Д9	Д10	Д1
В1	-	-	-	-	-	-	0,04	0,092	-	-	-
z	-	-	-	0,3	-	-	-	0,23	0,23	0,23	0,3
В3	-	-	-	-	-	-	0,17	0,38	-	-	-
В4	-	-	-	0,3	-	-	-	0,23	0,23	0,23	0,3
В5	-	-	0,12	-	0,18	0,18	0,13	-	-	-	-
В6	-	-	-	-	-	-	-	0,28	-	-	-
В7	0,16	0,13	0,1	-	0,14	0,14	0,11	-	-	-	-
В8	-	-	-	-	-	-	0,13	0,3	-	-	-
В9	-	-	-	-	-	-	-	-	0,11	0,11	-
В10	-	-	-	-	-	-	0,04	-	-	-	-
В11	-	-	-	-	-	-	-	-	-	-	-

Таблиця 1.18 – Матриця взаємозв’язку джерел загроз і вразливостей

Продовження таблиці 1.18

Вразливості	Д1	Д2	Д3	Д
В12	-	-	-	-
В13	-	-	-	-
В14	-	-	-	-
В15	0,06	0,04	0,03	-

Таким чином, використовуючи пороговий коефіцієнт 0,1 можна не розглядати наступні загрози через малу вірогідність їх здійснення на ОІД:

- Можливість несанкціонованого підключення до мережі студентами та хакерами (В1Д7, В2Д8);

- Проникнення на ОІД студентів в не робочий час через відсутність сигналізації (В10Д7).

- Знищення інформації та матеріальних цінностей пожежею через недосканалість протипожежної системи (В11Д1, В10Д1).

- Втрата носіїв інформації співробітниками або внаслідок пожежі чи бойових дій (В15Д1, В15Д2, В15Д3, В15Д5, В15Д6, В15Д13, В15Д14).

Далі в таблиці 1.19 класифіковано загрози за їх впливом на властивості інформації (конфіденційність, цілісність, доступність).

Таблиця 1.19 – Класифікація загроз за впливом на властивості інформації

Загрози	**Властивості інформації**		
	Конфіденційність	**Цілісність**	**Доступність**
1	**2**	**3**	**4**
Доступ зловмисникам до вразливостей в програмному коді ПЗ через несвоєчасне оновлення ПЗ системним адміністратором	+	+	+
Випадкове зараження системи комп’ютерними вірусами працівниками чи студентами	+	+	+
Несанкціоноване копіювання інформації на знімні носії	+	-	-

Продовження таблиці 1.19

1	2	3	4
Помилки користувачів, що призводять до втрати інформації чи надання доступу зловмисникам	+	+	+
Поцуплення чи ознайомлення з інформацією з обмеженим доступом внаслідок недбалого зберігання документів	+	-	+
Отримання доступу до мережі хакерами в наслідку помилки системного адміністратора при налаштуванні	+	+	+
Злам слабких паролів чи їх крадіжка з метою проникнення у систему.	+	+	-
Збої у функціонуванні системи, що призводять до втрати чи пошкодження інформації, що в ній циркулює.	-	+	+
Відмова технічних засобів, яка призводить до зупинки у проце сі функціонування системи	-	-	+

1.5 Висновок і постановка задачі

У першому розділі описаний об'єкт:

– вид його діяльності;

– загальна інформація про будівлю, у якій розташований ОІД;

– відомості про устаткування;

– відомості про інформаційну систему і інформаційні потоки;

– відомості про персонал та доступ персоналу до об’єктів АС.

Було виконано аналіз вразливостей і джерел загроз. На основі аналізу було створено матрицю актуальних загроз і виявлено елементи ІТС, які потребують найбільшого захисту. Отримані результати будуть використані в наступному розділі для розробки рекомендацій для покращення політики безпеки ІТС Машинобудівного коледжу Дніпровського національного університету.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Оцінки існуючого стану захищеності

Згідно з НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу»:

Критерії є методологічною базою для визначення вимог з захисту інформації в комп'ютерних системах від несанкціонованого доступу; створення захищених комп'ютерних систем і засобів захисту від несанкціонованого доступу; оцінки захищеності інформації в комп'ютерних системах і їх придатності для обробки критичної інформації (інформації, що вимагає захисту). Критерії надають:

1. Порівняльну шкалу для оцінки надійності механізмів захисту інформації від несанкціонованого доступу, реалізованих в комп'ютерних системах.

2. Базу (орієнтири) для розробки комп'ютерних систем, в яких мають бути реалізовані функції захисту інформації.

Згідно з НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу»:

Стандартний функціональний профіль захищеності являє собою перелік мінімально необхідних рівнів послуг, які повинен реалізовувати КЗЗ обчислювальної системи АС, щоб задовольняти певні вимоги щодо захищеності інформації, яка обробляється в даній АС.

Виходячи з того, що ІТС коледжу баготокомп'ютерний баготокористувачевий комплекс, об’єднаний в локальні мережі і має доступ в мережу Інтернет, а в системі циркулює як відкрита, так і інформація з обмеженим доступом, то це АС 3 класу.

Отже, відповідно класу автоматизованої системи потрібно провести

аналіз існуючого функціонального профілю захищеності і розробити функціональний профіль захищеності, який буде відповідати вимогам для захисту інформації від загроз, що були описані у першому розділі.

Існуючий профіль захищеності:

3.КЦД.1 (умовно реалізовано) {КД – 1, КВ – 1, ЦД – 1, ЦА – 1, ЦО – 1, ЦВ – 1, ДС – 1, ДВ – 1, НР – 2, НИ – 1, НО – 1, НЦ – 1, НТ – 2, НВ – 1, НА – 1}

Рекомендований профіль захищеності:

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

У таблиці 2.1 наведено, як можуть реалізовуватись наступні послуги безпеки.

Таблиця 2.1 – Критерії захищеності інформації

Критерії	**Механізм реалізації (3.КЦД.1)**	**Механізм реалізації (3.КЦД.2)**
1	**2**	**3**
КД - 2	-	Створення групових політик для розмежування прав доступу через Active Directory
КА – 2	-	Створення групових політик для розмежування прав доступу через Active Directory
КО – 1	-	Вбудовані засоби Windows
КВ – 1	SSL – протокол при передачі	SSL – протокол при передачі
ЦД – 1	У системі є розділення на користувачів, у яких є ряд	Створення групових політик для розмежування прав

	повноважень пов’язаних з можливістю модифікації об’єкту.	доступу через Active Directory

Продовження таблиці 2.1

1	2	3
ЦА – 2	-	Створення групових політик для розмежування прав доступу через Active Directory
ЦО – 1	Windows автоматично створює попередні версії файлів і папок, змінених з моменту створення останньої точки відновлення.	Засоби Active Directory (засоби для створення резервних копій інформації на сервері та засоби для відновлення групових політик та інших параметрів)
ЦВ – 2	-	Контроль цілісності об`єктів здійснюється за допомогою UAC (User Account Control).
ДР – 1	-	Active Directory (Можливість розподілу користувачів дозволяє обмежити користування ресурсів конкретним користувачам)

ДВ – 1	В системі Windows є можливість відновлення відом ого захищенного стану після відмови або переривання обслуговування системи у разі збою.	Засоби Active Directory (засоби для створення резервних копій інформації на сервері та засоби для відновлення групових політик та інших параметрів)

Продовження таблиці 2.1

1	**2**	**3**
НР – 2	В системі є журнал подій, що реєструються. Адміністратор має повноваження до його перегляду і аналізу.	В системі є журнал подій, що реєструються. Адміністратор має повноваження до його перегляду і аналізу.
НИ – 2	Для входу у систему користувач повинен вводити логін та пароль	Для входу у систему користувач повинен вводити логін та пароль
НК – 1	Достовірний канал використовується виключно користувачем для ідентифікації та автентифікації	Достовірний канал використовується виключно користувачем для ідентифікації та автентифікації
НО – 2	-	Розподілення облікових записі в системного адміністратора і адміністратора безпеки.
НЦ – 2	-	В разі виявлення порушення

		цілісності будь-якого із своїх компонентів КЗЗ повідомляє адміністратора. Дані про це зберігаються в журналі подій.
НТ – 2	Існує можливість тестування елементів системи за запитом користувача з відповідними повноваженнями.	Існує можливість тестування елементів системи за запитом користувача з відповідними повноваженнями.

Продовження таблиці 2.1

1	**2**	**3**
НВ – 1	Протокол аутентифікації Kerberos надає механізм за замовчуванням для сервісів аутентифікації і даних авторизації, необхідних користувачеві для доступу до ресурсу і виконання завдання на цьому ресурсі.	Протокол аутентифікації Kerberos надає механізм за замовчуванням для сервісів аутентифікації і даних авторизації, необхідних користувачеві для доступу до ресурсу і виконання завдання на цьому ресурсі.

Базова довірча конфіденційність (КД – 2).

Ця послуга дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. В системі, яка реалізує послугу довірча конфіденційність на рівні КД-2, атрибути доступу об'єктів і користувачів повинні містити інформацію, що використовується КЗЗ для розмежування доступу до об'єктів з боку конкретного користувача. Додатково повинна існувати можливість

встановлювати, які користувачі можуть активізувати конкретний процес, що дозволяє одержати можливість обмеженого керування потоками інформації.

Базова адміністративна конфіденційність (КА-2).

Послуга адміністративна конфіденційність дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від захищених об'єктів до користувачів. В системі, яка реалізує послугу адміністративна конфіденційність на рівні КА-2, атрибути доступу об'єктів і користувачів повинні містити інформацію, що використовується КЗЗ для розмежування доступу до об'єктів з боку конкретного користувача. Додатково повинна існувати можливість встановлювати, які користувачі можуть активізувати конкретний процес, що дозволяє одержати можливість обмеженого керування потоками інформації.

Повторне використання об'єктів (КО-1).

Політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС. Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані. Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною.

Мінімальна довірча цілісність (ЦД-1).

На даному рівні користувач, домену якого належить об'єкт, може накладати обмеження на доступ до об'єктів з боку інших користувачів. Керування правами має грубу вибірковість.

Базова адміністративна цілісність (ЦА-2).

Ця послуга дозволяє адміністратору чи спеціально авторизованому користувачу керувати потоками інформації від користувачів і процесів до захищених об'єктів. Згідно з політикою адміністративної цілісності (в повній аналогії з адміністративною конфіденційністю) об'єкту привласнюються

атрибути доступу, що визначають домен, якому повинні належати ті користувачі чи процеси, які намагаються модифікувати об’єкт. На даному рівні адміністратор може накладати обмеження на доступ до об'єктів з боку користувачів.

Обмежений відкат (ЦО-1).

Політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкотити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу.

Квоти (ДР-1).

Всі захищені об'єкти КС (наприклад, дисковий простір, тривалість сеансу, час використання центрального процесора і т. ін.) повинні ідентифікуватись і контролюватись диспетчером доступу шляхом накладення обмежень на максимальний обсяг даного ресурсу, що може бути виділений користувачу.

Ручне відновлення (ДВ-1).

Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов КС і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція КС. Після відмови КС або переривання обслуговування КЗЗ повинен перевести КС до стану, із якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження. Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути КС до нормального функціонування.

Захищений журнал (НР-2).

Політика реєстрації, що реалізується КЗЗ, повинна визначати перелікподій, що реєструються. КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки. Журнал

реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події. КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування. Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації.

Одиночна ідентифікація і автентифікація (НИ-2).

Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ. Перш ніж дозволити будьякому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен автентифікувати цього користувача з використанням захищеного механізму. КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування.

Однонаправлений достовірний канал (НК – 1).

Дана послуга дозволяє гарантувати, що користувач взаємодіє безпосередньо з КЗЗ і ніякий інший користувач або процес не може втручатись у взаємодію (підслухати або модифікувати інформацію, що передається). Рівні даної послуги ранжируються в залежності від того, чи має КЗЗ можливість ініціювати захищений обмін, чи це є прерогативою користувача.

Розподіл обов'язків адміністраторів (НО-2).

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

КЗЗ з гарантованою цілісністю (НЦ-2).

Ця послуга визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами. Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів.

Самотестування при старті (НТ-2).

Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ. КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження, при ініціалізації КЗЗ.

2.2 Проектні рішення – рекомендації, щодо модернізації політики безпеки

2.2.1 Теоретична складова

Згідно НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу»:

Під політикою безпеки інформації слід розуміти набір законів, правил, обмежень, рекомендацій і т. ін., які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз. Термін "політика безпеки" може бути застосовано щодо організації, АС, ОС, послуги, що реалізується системою (набору функцій), і т. ін. Чим дрібніше об'єкт, відносно якого застосовується даний термін, тим конкретнішими і формальніше стають правила. Далі для скорочення замість словосполучення "політика безпеки інформації" може використовуватись словосполучення "політика безпеки", а замість словосполучення "політика безпеки інформації, що реалізується послугою" — "політика послуги" і т. ін.

Політика безпеки інформації в АС є частиною загальної політики безпеки організації і може успадковувати, зокрема, положення державної політики у галузі захисту інформації. Для кожної АС політика безпеки інформації може бути індивідуальною і може залежати від технології обробки інформації, що реалізується, особливостей ОС, фізичного середовища і від багатьох інших чинників. Тим більше, одна й та ж сама АС може реалізовувати декілька різноманітних технологій обробки інформації. Тоді і політика безпеки інформації в такій АС буде складеною і її частини, що відповідають різним технологіям, можуть істотно відрізнятись.

Політика безпеки повинна визначати ресурси АС, що потребують захисту, зокрема установлювати категорії інформації, оброблюваної в АС. Мають бути сформульовані основні загрози для ОС, персоналу, інформації різних категорій і вимоги до захисту від цих загроз. Як складові частини загальної політики безпеки інформації в АС мають існувати політики забезпечення конфіденційності, цілісності і доступності оброблюваної інформації. Відповідальність персоналу завиконання положень політики безпеки має бути персоніфікована.

Політика безпеки інформації, що реалізуються різними КС будуть відрізнятися не тільки тим, що реалізовані в них функції захисту можуть забезпечувати захист від різних типів загроз, але і в зв'язку з тим, що ресурси КС можуть істотно відрізнятись. Так, якщо операційна система оперує файлами, то СУБД має справу із записами, розподіленими в різних файлах.

Частина політики безпеки, яка регламентує правила доступу користувачів і процесів до ресурсів КС, складає правила розмежування доступу.

2.2.2 Організаційні заходи щодо забезпечення реалізації політики безпеки інформації

Інформація, яка циркулює у коледжі, зберігається не лише в

електронному форматі, а тому ця політика охоплює безпеку інформації, що зберігається на всіх носіях інформації.

Дотримання цієї політики є обов'язковим для всього персоналу, який працює в коледжі. Працівник, який не дотримується Політики, може бути підданий дисциплінарному стягненню відповідно до дисциплінарної політики коледжу. Керівництво коледжу забов’язане забезпечити обізнаність своїх працівників про існування цієї політики та її зміст.

Необхідно провести заходи щодо підвищення кваліфікації персоналу в сфері користування інформаційними системами. Весь персонал системи управління повинен проходити відповідну підготовку з питань інформаційної безпеки.

Необхідно провести заходи щодо підвищення кваліфікації персоналу в роботі з документами та інформацією з обмеженим доступом.

Контроль доступу повинен підтримуватися на належному рівні для всіх систем коледжу, забезпечуючи користувачам відповідні права доступу до систем.

Доступ до всіх інформаційних ресурсів повинен здійснюватися через безпечний процес входу. Весь доступ до інформаційних ресурсів повинен реєструватися та контролюватися системним адміністратором для виявлення можливого неправомірного використання систем чи інформації.

Доступ до системних команд має бути обмежений для тих осіб, які мають право виконувати функції адміністрування або управління системою.

Впровадження нового або оновлення програмного забезпечення повинно бути ретельно сплановано та керовано системним адміністратором.

2.2.3 Політика управління програмним забезпеченням

Мета та сфера застосування політики:

Ця політика розповсюджується на всіх користувачів інформаційної системи коледжу та встановлює політику щодо управління програмним

забезпеченням відповідно до законодавства.

Метою цієї політики є встановлення відповідних правил щодо обслуговування та оновлення програмного забезпечення в коледжі.

Відповідальність:

Відповідальність за виконання цієї політики несе системний адміністратор.

Рекомендації:

Щоб запобігти порушенню авторських прав та захистити всі інформаційні системи системний адміністратор має проводити регулярні аудити та ретельно контролювати оновлення програмного забезпечення.

Програмне забезпечення не повинно встановлюватися на будь-який ПК у коледжі сторонніми працівниками чи студентами, крім системного адміністратора.

Перед встановленням програмного забезпечення і оновленнями системний адміністратор має провести тестування ПЗ у захищеному середовищі.

Оновлення безпеки операційних систем повинні бути встановлені в розумні терміни з моменту їх випуску, але лише після тестування. У виняткових обставинах може знадобитися негайно застосувати будь-які визнані критичні виправлення для захисту від будь-яких вразливостей.

Оновлення програмного забезпечення рекомендується проводити у вихідні дні або після робочого часу студентів, щоб не переривати навчальний процес. В критичних обставинах можна проводити оновлення в будь який час.

Після проведення оновлення чи встановлення ПЗ системний адміністратор має надати звіт проведених робіт директору. Звіт системного адміністратора буде включати:

- Назву ПЗ;
- Версію оновлення;
- Дату оновлення;

Після оновлення ПЗ користувачі системи, яких стосується оновлення

мають бути сповіщені про це.

2.2.4 Політика розмежування доступу

Мета та сфера застосування політики:

Ця політика розповсюджується на всіх користувачів інформаційної системи коледжу та встановлює політику щодо розмежування доступу до інформації відповідно до законодавства.

Метою цієї політики є створення порядку розмежування доступу користувачів і забезпечення умов, в яких тільки уповноважені члени персоналу можуть збирати та переглядати відповідну інформацію.

Відповідальність:

Відповідальність за виконання цієї політики несе системний адміністратор.

Рекомендації:

Для аутентифікації користувачів на робочих станціях персоналу, комп'ютерів у навчальних аудиторіях має бути застосоване рольове управління доступом. Необхідно надати атрибути доступу користувачам, розподілити їх по групах за допомогою засобів розмежування доступу Active Directory.

Атрибути доступу користувачів вказані у таблиці 2.2

Таблиця 2.2 – атрибути доступу:

Користувач	**Інформація**	**ПЗ**
1	**2**	**3**

Системний адміністратор	1 - Ч 3 – Ч, З, К 5 – Ч, З, К 7 – С, Ч, З, К, М, Д, В	9 - Вк, Вст, О, В 10 - Вк, Вст, О, В 11 - Вк, Вст, О, В 12 - Вк, Вст, О, В 13 - Вк, Вст, О, В 14 - Вк, Вст, О, В 15 - Вк, Вст, О, В 16 - Вк, Вст, О, В 17 - Вк, Вст, О, В 18 - Вк, Вст, О, В
Директор	1 – Ч, З, К, М, Д, В 2 – С, Ч, З, К, М, Д, В 3 - С, Ч, З, К, М, Д, В 4 – Ч 5 – Ч, З, К, Д 6 – Ч, З, К, Д 7 – Ч, З, К, Д 8 – Ч, З, Д	9 - Вк 10 - Вк 12 – Вк 13 – Вк 14 – Вк 15 – Вк 16 - Вк

Продовження таблиці 2.2

1	**2**	**3**

Заступник директора	1 – С, Ч, З, К, М, Д, В 3 – Ч 4 – Ч 5 – Ч, З, К, Д 6 – Ч, З, К, Д	9 - Вк 10 - Вк 12 - Вк 13 - Вк 14 - Вк 15 - Вк 16 - Вк
Секретар	1 – Ч, К, Д 3 - С, Ч, З, К, М, Д 4 - С, Ч, З, К, М, Д, В 5 – Ч, З, К, Д 6 – Ч, З, К, Д	9 - Вк 10 - Вк 12 - Вк 13 - Вк 14 - Вк 15 - Вк 16 - Вк
Завідуючі кафедр	1 – С, Ч, З, К, М, Д, В 3 – Ч 5 – Ч, З, К, Д 6 - Ч, З, К, Д	9 - Вк 10 - Вк 12 - Вк 13 - Вк 14 - Вк 15 - Вк 16 - Вк

Продовження таблиці 2.2

1	**2**	**3**

Викладачі	1 – С, Ч, З, К, М, Д, В 3 – Ч 5 – Ч, З, К, Д 6 – Ч	9 - Вк 10 - Вк 12 - Вк 13 - Вк 15 - Вк 16 – Вк 17 – Вк 18 – Вк
Бухгалтер	2 – Ч, К 3 – Ч 5 – Ч 6 - Ч, З, К, Д; 8 – С, Ч, З, К, М, Д;	9 - Вк 10 - Вк 12 - Вк 13 - Вк 14 - Вк 15 - Вк 16 – Вк
Інспектор відділу кадрів	1 - Ч, З, К, Д; 3 - Ч, З, К, Д; 5 – Ч, З, К, Д; 6 – С, Ч, З, К, М, Д, В;	9 - Вк 10 - Вк 12 - Вк 13 - Вк 14 - Вк 15 - Вк 16 – Вк

Продовження таблиці 2.2

1	2	3
Студенти	1 - Ч, З, К, Д; 3 - Ч, З, К; 5 - Ч, З, К;	9 - Вк 10 - Вк 12 - Вк 13 - Вк 15 - Вк 16 – Вк 17 – Вк 18 – Вк

Перелік інформації та ПЗ:

1) Інформація для забезпечення навчального і наукового процесів (*інформація);*

2) Договори, угоди (*інформація);*

3) Накази і розпорядження директора (*інформація);*

4) Журнали реєстрації документації (*інформація);*

5) Постанови з вищестоящих організацій (*інформація);*

6) Інформація про студентів і працівників (*інформація);*

7) Звіти системного адміністратора (*інформація);*

8) Бухгалтерські звіти (*інформація);*

9) Avast Free Antivirus (*програмне забезпечення);*

10) CCleaner (*програмне забезпечення);*

11) Wireshark (*програмне забезпечення);*

12) WinRar (*програмне забезпечення);*

13) Пакет Office 365 Business преміум (Word, Excel, PowerPoint, Outlook, SharePoint, OneDrive, OneNote, Microsoft Teams, Publisher, Access) (*програмне забезпечення);*

14) Skype (*програмне забезпечення);*

15) Foxit Reader (*програмне забезпечення);*

16) Google Chrome (*програмне забезпечення);*

17) Компас-3D (*програмне забезпечення);*

18) Mathcad (*програмне забезпечення);*

Для інформації:

– С – створення;

– Ч – читання;

– З – зберігання;

– К – копіювання;

– М – модифікація;

– Д – друк;

– В – видалення/знищення.

Для ПЗ:

– Вст – встановлення;

– Вк – використання ;

– О – оновлення;

– В – видалення/знищення.

Будь-які спроби отримати неналежний доступ до інформації мають виявлятися та зберігатися в журналі аудиту системного адміністратора.

Політика безпеки переглядається раз на рік директором. У разі виникнення форс-мажорних ситуацій політика безпеки може бути переглянута раніше..

2.2.5 Політика використання знімних носіїв інформації та зовнішніх інтерфейсів

Мета та сфера застосування політики:

Ця політика розповсюджується на всіх користувачів інформаційної системи коледжу та встановлює політику щодо використання зовнішніх носіїв інформації.

Метою політики є зазначення порядку і правил використання знімних носіїв інформації та зовнішніх інтерфейсів.

Відповідальність:

Виконання цієї політики має контролювати системний адміністратор. Співробітники, що ознайомились з політикою безпеки несуть повну відповідальність за її виконання.

Рекомендації:

До зовнішніх інтерфейсів на робочих комп'ютерах співробітників відносяться USB-порти.

Всі USB-накопичувачі співробітників, які використовуються для зберігання інформації з обмеженим доступом мають бути зареєстровані системним адміністратором.

Інформація про коледж, яка вважається, не може зберігатися на будь-якому несанкціонованому та незашифрованому пристрої зберігання даних чи носіях (наприклад, USB, персональний ноутбук). Лише системний адміністратор може дозволити використання пристрою для цієї мети.

В разі, коли зникає необхідність зберігання інформації з обмеженим доступом на носіях, необхідно її видаляти з носія без можливості відновлення інформації.

USB-порти мають бути обмежені для підключення незареєстрованиї носіїїв системним адміністратором за допомогою засобів Active Directory.

2.2.6 Політика захисту мережі

Мета та сфера застосування політики:

Ця політика поширюється на всіх користувачів інформаційних систем коледжу та встановлює політику коледжу щодо управління мережею.

Метою цієї політики є відповідний технічний та процедурний контроль для зменшення впливу потенційних мережевих ризиків.

Відповідальність:

Відповідальною особою за виконання політики є системний адміністратор.

Рекомендації:

Мережею коледжу має керувати уповноважений та кваліфікований працівник, а саме системний адміністратор. Системний адміністратор повинен знати про проблеми інформаційної безпеки, що можливі у мережі.

Мережа має буде розроблена та налаштована для забезпечення високої продуктивності та надійності для задоволення потреб коледжу, забезпечуючи високий ступінь контролю доступу та діапазон обмежень привілеїв.

Мережа буде розділена на окремі домени з маршрутизацією та контролем доступу, що працюють між доменами. Для захисту мережі бухгалтерії повинні використовуватися належно налаштовані брандмауери. Рекомендується виділити окремий сегмент мережі з відкритим доступом для використання студентами в навчальних цілях.

Необхідно вимкнути широкомовлення SSID для відключення видимості корпоративної точки доступу до Wi-Fi. Співробітники, яким необхідно буде бездротове підключення до мережі мають звернутися до системного адміністратора, який введе на пристроях співробітників правильний SSID і пароль.

Забороняється ділитися конфіденційними даними через відкриту студентську мережу.

Системний адміністратор має змінювати паролі від налаштувань роутерів і Wi-Fi кожні 3 місяці. Пароль має задовольняти рекомендації політики вибору і зміни паролів. Захист бездротового режиму має бути на основі WPA2.

В налаштуваннях роутерів фунція QSS має бути відключена.

Рекомендується вимкнути протокол DHCP та включити фільтрацію

довірених MAC-адресів, для унеможливлення виділення IP-адреси при спробі несанкціонованого підключення.

За виконання даної політики системний адміністратор має звітувати директору.

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

2.2.7 Політика вибору і зміни паролів

Мета та сфера застосування політики:

Ця політика поширюється на всіх користувачів інформаційних систем коледжу та встановлює правила використання паролів для автентифікації.

Метою цієї політики є встановлення порядку вибору та зміни паролів користувачами.

Відповідальність:

Відповідальною особою за виконання політики є системний адміністратор. Співробітники, що ознайомились з політикою безпеки несуть повну відповідальність за збереження паролів.

Рекомендації:

Усі паролі системного рівня (Адміністратор тощо) необхідно міняти щомісяця.

Усі паролі на рівні користувача (наприклад, електронна пошта, веб, настільний комп’ютер тощо) потрібно змінювати щонайменше кожні півроку.

Усі паролі на рівні користувача та на рівні системи повинні відповідати описаним нижче стандартам.

Усі користувачі повинні знати, як вибрати надійні паролі. Сильні паролі мають такі характеристики:

1) Мають містити щонайменше три з п'яти наступних класів символів:

- Символи нижнього регістру;

- Символи верхнього регістру;

- Числа;

- Знаки пунктуації;

- Спеціальні символи (Наприклад: @, #, $, %, ^, &);

2) Містить від 8 до 15 буквено-цифрових символів.

3) Пароль не може бути словом, яке можна знайти у словнику.

4) Пароль не має бути словом поширеного використання, таким як:

- Комп'ютерні терміни та назви, команди, сайти, компанії, обладнання, програмне забезпечення. Паролі ніколи не повинні бути "Password1" або будь-якими подібними варіаціями;

- Імена родичів, домашніх тварин, друзів, колег тощо;

- День народження та інша особиста інформація, наприклад, адреси та номери телефонів;

- Шаблони слів чи чисел, такі як aaabbb, qwerty, zyxwvuts, 123321 тощо;

- Будь-який з перерахованих вище пунктів, написаний задом- наперед;

Захисні заходи:

1) Не можна повідомляти паролі нікому, включаючи системного адміністратора. Всі паролі слід розглядати як конфіденційну інформацію.

2) Паролі ніколи не слід записувати на папері і зберігати у доступному для всіх місці або зберігати в електронному вигляді без шифрування.

3) Не можна розголошувати пароль в електронній пошті, чаті чи іншому електронному спілкуванні.

Виконання політики контролює системний адміністратор підприємства за допомогою вбудованих засобів аутентифікації в ОС. За 3 дні до планової зміни паролів співробітники мають бути повідомлені про це під час увімкнення робочих комп’ютерів. В день планової зміни паролів співробітники мають змінити свої паролі для входу в облікові записи.

2.2.8 Політика фізичної охорони коледжу

Метою цієї політики є встановлення комплексу заходів щодо забезпечення безпеки функціонування коледжу, організації пропускного режиму, збереження майна, життя та здоров'я співробітників і студентів.

Відповідальність:

Відповідальність за виконання політики несе служба несе директор.

Рекомендації:

Для організації ефективної охорони коледжу необхідно:

- Створити службу безпеки або укласти договір з охоронною організацією;

- Розмістити пост фізичної охорони на вході у будівлю, який має бути обладнаний «тривожною кнопкою» для термінового зв'язку з поліцією;

- Співробітником служби безпеки проводити обходи території у неробочий час;

- Встановити системи контролю та управління доступом, інтегрувавши в неї студентські квитки. Встановити турнікети, металодетектори на вході;

- Встановити системи відеоспостереження на вході, у коридорах;

- Оснастити навчальний заклад системою охоронно-пожежної сигналізації;

- Проводити регулярні заняття з учнями з техніки безпеки і реагування при виникненні позаштатних ситуацій;

- Охоронці повинні регулярно проводити профілактичні заходи з охорони закладу, тренування надзвичайних ситуацій, заняття з ОБЖ, тощо.

Виконання політики контролюється охоронцем за допомогою аналізу журналу відвідувачів, нагляду за територією за допомогою системи відеоспостереження. При зміні в політиці безпеки всі співробітники сповіщуються про це. Після ознайомлення з політикою співробітники підписуються у журналі з техніки безпеки.

2.3 Висновок спеціального розділу

В спеціальній частині було проаналізовано існуючий функціональний профіль захищеності, обрано рекомендований профіль, що відповідає вимогам, необхідним для підвищення стану захищеності.

Були розроблені рекомендації з покращення існуючої політики безпеки для вирішення актуальних загроз інформаційної безпеки, які були описані у першому розділі, а саме:

- Організаційні заходи щодо забезпечення реалізації політики безпеки інформації;
- Політика управління програмним забезпеченням;
- Політика розмежування доступу;
- Політика використання знімних носіїв інформації та зовнішніх інтерфейсів;
- Політика захисту мережі;
- Політика вибору і зміни паролів;
- Політика фізичної охорони коледжу.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

3.1 Мета техніко-економічного обґрунтування дипломного проекту

Метою виконання економічного розділу є визначення економічної ефективності використання запропонованих у технічній частині засобів та заходів для покращення інформаційної безпеки Машинобудівного коледжу Дніпровського національного університету .

Для визначення економічної доцільності необхідно визначити капітальні та річні експлуатаційні витрати на засоби і заходи для покращення інформаційної безпеки, визначити річний економічний ефект від впровадження засобів і заходів, розрахувати коефіцієнт повернення інвестицій та термін окупності капітальних інвестицій. На основі цих показників можна визначити, чи будуть прибутковими запропоновані рішення.

3.2 Визначення витрат на розробку політики безпеки інформації

3.2.1 Розрахунок капітальних (фіксованих) витрат

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

За методикою Gartner Group до фіксованих (капітальних) варто відносити наступні витрати:

– вартість розробки проекту інформаційної безпеки;

– витрати на залучення зовнішніх консультантів;

– вартість первісних закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ);

– вартість створення основного й додаткового програмного забезпечення;

– витрати на первісні закупівлі апаратного забезпечення;

– витрати на інтеграцію системи інформативної безпеки у вже існуючу корпоративну систему (встановлення обладнання, програмного забезпечення та налагодження системи інформаційної безпеки);

– витрати на навчання технічних фахівців і обслуговуючого персоналу.

Згідно з розробленою у попередньому розділі політикою безпеки і заходам, що в ній описані, актуальними капітальними витратами можна вважати наступні:

– вартість розробки проекту інформаційної безпеки;

– вартість первісних закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ);

– витрати на інтеграцію системи інформативної безпеки у вже існуючу корпоративну систему (встановлення обладнання, програмного забезпечення та налагодження системи інформаційної безпеки);

– витрати на навчання технічних фахівців і обслуговуючого персоналу.

Розрахунок витрат на розробку проекту політики інформаційної безпеки включає в себе визначення трудомісткості розробки ПБ і розрахунок витрат на розробку ПБ.

Трудомісткість розраховується за формулою 3.1:

$$t = t_{об} + t_а + t_{вз} + t_{озб} + t_д, \text{ год} \quad (3.1)$$

де $t_{об}$ – тривалість проведення обстеження підприємства;

$t_а$ – тривалість процесу аналізу ризиків;

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

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

$t_д$ – тривалість документального оформлення політики безпеки.

Час, витрачений на розробку політики інформаційної безпеки наведено у таблиці 3.1.

Таблиця 3.1 – Часові показники трудомісткості розробки ПБ

Показник	**Кількість годин**
1	**2**
$t_{об}$	56

Продовження таблиці 3.1

1	**2**
$t_а$	12
$t_{вз}$	12
$t_{озб}$	15
$t_д$	14

За формулою 3.1 трудомісткість розробки ПБ становить:

t = 56 год + 12 год + 12 год + 15 год + 14 год,

t = 109 год.

Витрати на розробку ПБ являються сумою витрат на заробітну плату спеціаліста і вартості витрат машинного часу, необхідного для розробки ПБ. Розраховуються за формулою 3.2:

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

де $К_{рп}$ - витрати на розробку політики безпеки інформації;

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

$З_{мч}$ – вартість витрат машинного часу, необхідного для розробки ПБ;

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

де *t* - трудомісткість розробки ПБ, годин;

$З_{іб}$ – середньогодинна заробітна плата спеціаліста з інформаційної безпеки, грн/год;

За формулою 3.3:

$$З_{зп} = 109 \cdot 50$$

$$З_{зп} = 5450 \text{ грн.}$$

Вартість машинного часу для розробки ПБ визначається за формулою 3.4:

$$З_{мч} = t \cdot С_{мч} \quad (3.4)$$

де $С_{мч}$ - вартість 1 години машинного часу ПК, грн./год.

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = P \cdot С_е + \frac{Ф_{зал} \cdot Н_а}{Fр} + \frac{К_{лпз} \cdot Н_{апз}}{Fр} \quad (3.5)$$

де Р – встановлена потужність ПК, кВт;

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

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

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

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

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

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

де Р = 0,18 кВт;

$С_е$ = 1,68 грн/кВт·година;

$Ф_{зал}$ = 7000, грн.;

$Н_а$ = 1/3 на рік;

$Н_{апз}$ = 100% на рік;

$К_{лпз}$ = 2200, грн.;

$F_р$ = 1920

$$С_{мч} = 0{,}18 \cdot 1{,}68 + \frac{7000 \cdot 1/3}{1920} + \frac{2200 \cdot 1}{1920}$$

$$С_{мч} = 2{,}66 \text{ грн}$$

За формулою 3.4:

$$З_{мч} = 109 \cdot 2{,}66$$

$$З_{мч} = 290 \text{ грн}$$

За формулою 3.2:

$$К_{рп} = 5450 + 290$$

$$К_{рп} = 5740 \text{ грн}$$

Таким чином, капітальні витрати визначаються згідно прийнятих вище рішень політики безпеки за формулою 3.6:

$$К = К_{рп} + К_{зпз} + К_{навч} + К_{н} \quad (3.6)$$

де $К_{зпз}$ – вартість закупівель ліцензійного програмного забезпечення;

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

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

Так як ліцензійне програмне забезпечення вже було встановлене, то у розрахунку враховується лише закупівля Active Directory, а саме $К_{зпз}$ = 4160 грн.

Під $К_{навч}$ мається на увазі одноразовий кваліфікаційний захід для співробітників, з питань ознайомлення з новою редакцією політики безпеки. Даний захід проводиться спеціалістом ІБ, тому додатково йому виплачується сума у розмірі 500 грн, окрім виплати за розробку нової редакції ПБ. $К_{навч}$ = 500 грн.

Під $К_{н}$ маються на увазі витрати на встановлення обладнання для фізичної охорони коледжу, а саме встановлення охоронно-пожежної сигналізації коштує 5000 грн, вартість встановлення системи відеоспостереження з п’яти відеокамер становить 5000 грн, вартість турнікету на вхід 8000 грн. Таким чином, $К_{н}$ = 18000 грн.

За формулою 3.6:

$$К = 5740 + 4160 + 500 + 18000$$

$$К = 28400 \text{ грн}$$

3.2.2 Розрахунок експлуатаційних (поточних) витрат

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

Для коледжу актуальними будуть наступні витрати:

– заробітна плата обслуговуючого персоналу;

– кваліфікаційні заходи та перевірка знань персоналу стосовно правил, регламентованих політикою безпеки;

– технічне й організаційне адміністрування й сервіс.

Оскільки методи захисту, передбачені політикою безпеки, мають більш організаційний характер, поточними витратами можна вважати заробітну платню системного адміністратора і двох співробітників служби безпеки, витрати на електроенергію, що буде витрачено за рік роботи системи охорони та витрати пов’язані з діяльністю користувачів, тож поточні витрати розраховуються за формулою 3.7:

$$С = С_{зп} + С_{ел} + С_{дк} + С_{а} \quad (3.7)$$

де, С – сума поточних витрат, грн;

$С_{ел}$ – витрати на електроенергію, що буде витрачено за рік роботи системи охорони, грн;

$С_{зп}$ – сума заробітної платні персоналу, грн;

$С_{дк}$ – сума витрат, пов’язаних з діяльністю користувачів, грн;

$С_{а}$ – річний фонд амортизаційних відрахувань, грн;

Витрати на заробітну платню персоналу складаються з суми заробітної платні системного адміністратора і двох співробітників служби безпеки, котрі будуть працювати через добу.

$$С_{зп} = С_{зпад} + 0,22 \cdot (2 \cdot С_{зпох}) \quad (3.8)$$

де $С_{зпад}$ - заробітна платня системного адміністратора, грн на рік;

$С_{зпох}$ - заробітна платня охоронця, грн на рік;

Заробітна платня охоронця одного охоронця на рік становить 96000 грн

У свою чергу, витрати на заробітну платню системного адміністратора розраховуються за формулою 3.9:

$$С_{зпад} = (З_{осн} + З_{дод}) + 0,22 \cdot (З_{осн} + З_{дод}) \quad (3.9)$$

де $З_{осн}$ – основна заробітна плата системного адміністратора на рік;

$З_{дод}$ – додаткова заробітна плата системного адміністратора за проведення кваліфікаційних заходів та перевірку знань та навичок персоналу стосовно правил, регламентованих політикою безпеки;

Додаткова заробітна платня складає 500 грн за проведення одного кваліфікаційного заходу. Такі заходи планується проводити раз на 3 місяці, тож фактично за місяць системний адміністратор отримуватиме 167 грн додаткової заробітної платні. Основна заробітна платня системного адміністратора на рік становить 132000 грн.

Отже, за формулою 3.9 витрати на заробітну платню системного адміністратора становлять:

$$С_{зпад} = (132000 + 2004) + 0,22 \cdot (132000 + 2004)$$

$$С_{зпад} = 163485 \text{ грн}$$

Таким чином, за формулою 3.8 витрати на заробітну платню персоналу на рік становлять:

$$С_{зп} = 163485 + (2 * 96000) + 0,22 \cdot (2 * 96000)$$

$$С_{зп} = 397725 \text{ грн}$$

Вартість електроенергії, що споживається апаратурою системи безпеки протягом року визначається за формулою 3.10:

$$С_{ел} = Р \cdot F_р \cdot Ц_е \quad (3.10)$$

де Р – потужність апаратури, 0,024 кВт;

$F_р$ – річний фонд робочого часу системи безпеки, становить 8760 год;

$Ц_е$ – тариф на електроенергію, 1,68 грн/кВт·годин;

За формулою 3.10 слідує:

$$С_{ел} = 0,024 \cdot 8760 \cdot 1,68$$

$$С_{ел} = 353 \text{ грн.}$$

Витрати, пов’язані з діяльністю користувачів являють собою витрати, що спричинені професійною діяльністю. Такими витратами вважається знос обладнання через частий перезапис інформації на жорстких дисках серверу у процесі роботи, що приводить сервер у неробочий стан. Такі витрати включають у себе вартість полагодження серверу, профілактична заміна компонентів. За рік, вартість таких витрат сягатиме 1000 грн. Отже, $С_{дк}$ = 1000 грн.

Термін амортизації капітальних витрат складає 24 місяці. Річний фонд амортизаційних відрахувань визначається за формулою 3.11:

$$С_а = \frac{К}{24} \cdot 12 \qquad (3.11)$$

$$С_а = \frac{28400}{24} \cdot 12$$

$$С_а = 14200$$

Таким чином, за формулою 3.7 розраховуємо експлуатаційні витрати:

$$С = 397725 + 353 + 1000 + 14200$$

$$С = 413278 \text{ грн}$$

3.3 Оцінка величини збитку у разі реалізації загроз

Метою оцінки є відображення втрат прибутку в разі реалізації загрози інформаційної безпеки.

До загроз інформаційній системі коледжу з можливими економічними втратами можна віднести:

1) Доступ зловмисникам до вразливостей в програмному коді ПЗ через несвоєчасне оновлення ПЗ системним адміністратором, що призведе до простою системи, втрати доступності, конфіденційності інформації і подальшим економічним збиткам.

2) Несанкціоноване читання, модифікація або видалення інформації студентами або хакерами через некоректне розмежування прав доступу до об'єктів приводить до втрати конфіденційності, цілісності і доступності інформації, що в свою чергу призводить до подальших грошових втрат.

3) Випадкове зараження системи комп'ютерними вірусами працівниками чи студентами, що призводить до втрати доступності і конфіденційності інформації і веде до простою системи.

4) Несанкціоноване копіювання інформації на знімні носії приводить до втрати конфіденційності, цілісності і доступності інформації, що в свою чергу призводить до подальших грошових втрат.

5) Помилки користувачів, що призводять до втрати інформації чи надання доступу зловмисникам призведе до простою системи, втрати доступності, конфіденційності інформації і подальшим економічним збиткам.

6) Отримання доступу до мережі хакерами в наслідку помилки системного адміністратора при налаштуванні призведе до простою системи, втрати доступності, конфіденційності інформації і подальшим економічним збиткам.

7) Таємне проникнення та поцуплення технічних засобів через відсутність відеонагляду може призвести до простою системи, втрати ціоісності, доступності, конфіденційності інформації і прямим матеріальним втратам.

8) Злам слабких паролів чи їх крадіжка з метою проникнення у систему, що призведе до втрати доступності, цілісності, конфіденційності інформації і подальшим економічним збиткам.

9) Збої у функціонуванні системи, що призводять до втрати чи пошкодження інформації, що в ній циркулює призведе до простою у

функціонуванні системи і втраті доступності і цілісності.

10) Відмова технічних засобів, яка призводить до зупинки у процесі функціонування системи простою у функціонуванні системи і втраті доступності.

Для розрахунку збитків від реалізації цих загроз використовуємо формулу 3.11:

$$U = П_п + П_в \quad (3.12)$$

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

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

Втрати від зниження продуктивності співробітників атакованого сегменту мережі розраховуються за формулою 3.12. Вартість відновлення працездатності сегменту мережі розраховуються за формулою 3.13.

$$П_п = \frac{\Sigma З_с}{F} \cdot t_п \quad (3.13)$$

$$П_в = П_{ви} + П_{пв} + П_{зч} \quad (3.14)$$

де F – місячний фонд робочого часу;

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

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

$П_{ви}$ – 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

Пви і Ппв розраховуються за формулами 3.15 і 3.16 відповідно:

$$П_{ви} = \frac{ЗЗ_с}{F} \cdot t_{ви} \quad (3.15)$$

$$П_{пв} = \frac{С_{запад}}{F} \cdot t_в \quad (3.16)$$

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

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

$С_{запад}$ – заробітна плата системного адміністратора, грн на місяць;

Відповідно до списку загроз інформаційній системі коледжу можна розрахувати можливі збитки в разі їх реалізації. За формулами 3.11 – 3.14 розрахуємо витрати:

$$П_п = \frac{160000}{150} \cdot 5$$

$П_п$ = 5333 грн

$$П_{ви} = \frac{160000}{150} \cdot 16$$

$П_{ви}$ = 17067 грн

$$П_{пв} = \frac{13623}{150} \cdot 8$$

$П_{пв}$ = 726 грн

$П_в$ = 17067 + 726 + 0

$П_в$ = 17793 грн

$$U = 5333 + 17793$$

$$U = 23126 \text{ грн}$$

Тобто через одноразову реалізацію загрози 1 збитки для коледжу становитимуть 23126 грн.

Аналогічним методом проводяться розрахунки збитків від інших вразливостей і результати розрахунків наведені у таблиці 3.2:

Таблиця 3.2 – Розрахунок річних обсягів збитків від реалізації загроз

Загроза	**Збиток від одиничної реалізації загрози, грн**	**Передбачувана кількість реалізацій загрози на рік, шт.**	**Вірогідність реалізації загрози**	**Річні збитки від реалізації загрози**
1	**2**	**3**	**4**	**5**
Доступ зловмисникам до вразливостей через несвоєчасне оновлення ПЗ	23126	1	0,8	18500
Несанкціоноване читання, модифікація або видалення інформації	100431	1	1	100431
Зараження системи комп’ютерними	60328	1	0,8	48262,4

вірусами				
Несанкціоноване копіювання інформації на знімні носії	100431	1	0,8	80344,8

Продовження таблиці 3.2

1	**2**	**3**	**4**	**5**
Помилки користувачів, що призводять до втрати інформації	40995	1	1	40995
Несанкціонований доступ до мережі	70021	1	0,8	56016,8
Таємне проникнення та поцуплення технічних засобів	58439	1	1	58439
Злам слабких паролів чи їх крадіжка з метою проникнення у систему	56021	1	0,8	44816,8
Збої у функціонуванні системи	72713	1	0,6	43627,8
Відмова	53774	1	0,6	32264,4

технічних засобів				
Загалом				523698

3.3.1 Загальний ефект від впровадження системи інформаційної безпеки. Загальний ефект від впровадження системи інформаційної безпеки визначається за формулою 3.15:

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

де В – загальний збиток від атаки на вузол або сегмент корпоративної мережі, грн;

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

За формулою 3.17 визначимо:

$$E = 523698 – 413278$$

$$E = 110420 \text{ грн.}$$

3.4 Загальна оцінка економічної ефективності системи захисту інформації

Загальна оцінка економічної ефективності системи захисту інформації здійснюється на основі таких показників, як:

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

– термін окупності капітальних інвестицій То.

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

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

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

Отже, за формулою 3.16:

$$ROSI = 110420 / 28400$$

$$ROSI = 3,89$$

Проект вважається економічно доцільним, якщо розрахунковий коефіцієнт ефективності перевищує річний рівень прибутковості альтернативного варіанта, розраховується за формулою 3.17:

$$ROSI > (Nдеп – Nінф) / 100 \quad (3.19)$$

де Nдеп = 9 – річна депозитна ставка, %;

Nінф = 5 – річний рівень інфляції, %.

Оскільки 3,89 > 0,04, то проект можна вважати економічно доцільним.

Термін окупності капітальних інвестицій То показує, за скільки років капітальні інвестиції окупаються за рахунок загального ефекту від впровадження системи інформаційної безпеки і розраховується за формулою 3.18:

$$To = K / E = 1 / ROSI \quad (3.20)$$

$$To = 0,26 \text{ року}$$

3.5 Висновок економічного розділу

В розділі були проведені розрахунки капітальних і річних експлуатаційних витрат. Було визначено збережені збитки від можливих реалізацій загроз.

Було з’ясовано, що запропонована політика безпеки та введення заходів і засобів, згідно цієї політики є економічно вигідними для Машинобудівного коледжу. Термін окупності капітальних інвестицій є досить малим (0,26 року), а коефіцієнт ефективності перевищує річний рівень прибутковості альтернативного варіанта (3,89 > 0,04). Отже, впровадження обраних рішень є доцільним.

ВИСНОВОК

Під час виконання дипломного проекту було виконано обстеження об’єкту інформаційної діяльності Машинобудівного коледжу Дніпровського національного університету.

Було описано фізичне та інформаційне середовище об’єкту. Було проведено аналіз інформаційних потоків і класифікацію інформації, що циркулює на об’єкті згідно положень ЗУ «Про інформацію».

Після цього було проведено аналіз загроз та їх джерел та визначено перелік актуальних загроз для ІТС шляхом експертної оцінки.

Було оцінено існуючий профіль захищеності, а також розроблено новий функціональний профіль захищеності (згідно з НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі»), що відповідає вимогам, необхідним для запобігання інцидентів інформаційної безпеки.

На основі визначених актуальних загроз були створені рекомендації по вдосконаленню захищеності ІТС Машинобудівного коледжу Дніпровського національного університету.

У економічній частині було розраховано капітальні і експлуатаційні витрати на підтримку заходів і засобів, що були запроваджені для зниження ризиків

актуальних загроз. Було з’ясовано, що запропоновані політика безпеки та

введення заходів і засобів, згідно цієї політики є економічно вигідними для Машинобудівного коледжу.

ПЕРЕЛІК ПОСИЛАНЬ

1) ПКМУ №373 [Електронний ресурс]. – 2006. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/373-2006-п.

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

3) НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу" [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: https://tzi.ua/assets/files/НД-ТЗІ-2.5-004-99.pdf.

4) НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу" [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=101870&cat_id=89734&ctime=1344501089407.

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

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

7) Закон України "Про захист персональних даних" [Електронний ресурс] // 2297-VI. – 30.01.2018. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2297-17.

8) ДСТУ 3396.2-97 "Захист інформації. Технічний захист інформації. Терміни та визначення." [Електронний ресурс]. – 1998. – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38934&cat_id=3883.

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

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	Розділ 1. Стан питання. Постановка задачі	43	
6	А4	Розділ 2. Спеціальна частина	23	
7	А4	Розділ 3. Економічна частина	15	
8	А4	Висновок	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А. Відомість матеріалів кваліфікаційної роботи	1	
11	А3	Додаток Б. Генеральний план ОІД	1	
12	А3	Додаток В. Генеральний план ОІД (схема комунікацій)	1	
13	А4	Додаток Г. Умовні позначення генерального плану	2	
14	А4	Додаток Ґ. Мережева топологія ІТС	1	
15	А4	Додаток Д. Перелік документів на оптичному носії	1	
16	А4	Додаток Е. Відгук керівника економічного розділу	1	
17	А4	Додаток Є. Відгук керівника дипломної роботи	1	

ДОДАТОК Б

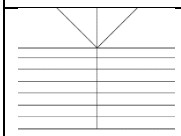
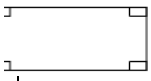
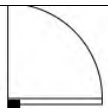
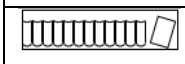
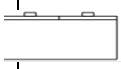
Рисунок 1 – Генеральний план ОІД

ДОДАТОК В

Рисунок 2 – Генеральний план ОІД (схема комунікацій)

ДОДАТОК Г

Таблиця 1 - Умовні позначення генерального плану

Позначення	Зміст
	Межа ОІД
	Сходи
	Стельовий освітлювач
	Стіл
	Стілець
	Офісне крісло
	Двері
	Рослина
	Комп’ютер
	Книжна шафа
	Шафа
	Сейф
	Принтер
	Роутер

	Сервер
	Диван

Продовження таблиці 1

	Унітаз
	Раковина
	Комутатор
	Розетка
	Електрична проводка
	Вихід проводки до трансформатора
	Вимикач світла
	Радіатор опалення
	Труба опалення з виходом до інших поверхів

ДОДАТОК Ґ

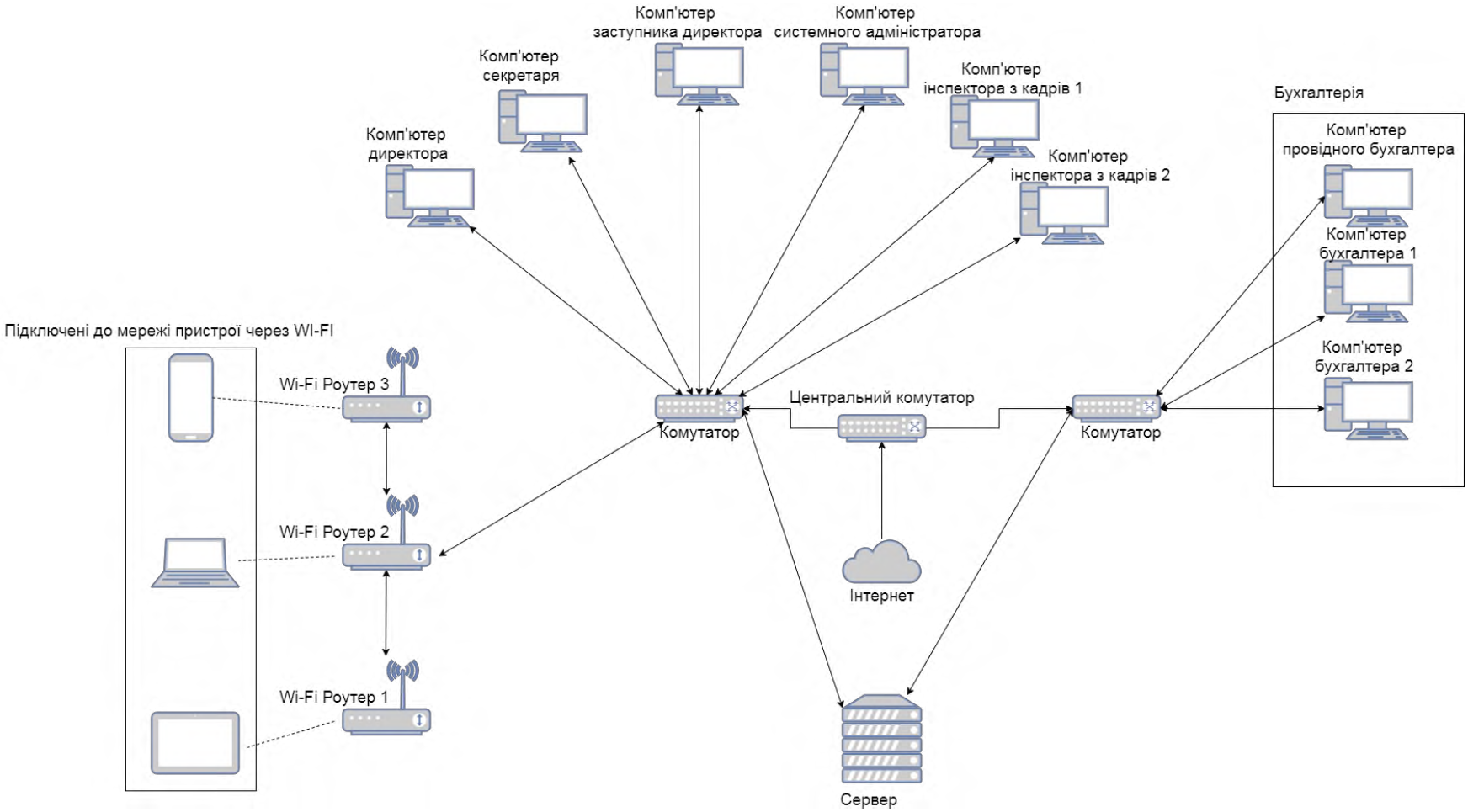


Рисунок 1 – мережева топологія ІТС

ДОДАТОК Д. Перелік документів на оптичному носії

- Заворін І.Д_125-16-2.docx
- Заворін І.Д_125-16-2.pptx

ДОДАТОК Е. Відгук керівника економічного розділу

Керівник економічного розділу

к.е.н., доц. Пілова Д.П Підпис: _____

ДОДАТОК Є. Відгук керівника кваліфікаційної роботи

«Розробка політики безпеки інформації інформаційно-телекомунікаційної системи Машинобудівного коледжу Дніпровського національного університету».

студента групи 125-16-2 Заворіна Івана Дмитровича

Кваліфікаційна робота за спеціальністю «Кібербезпека» Заворіна І.Д.. представлена пояснювальною запискою на 93 ст., містить 2 рис., 23 табл.,8 додатків, 9 джерел.

Мета кваліфікаційної роботи – розробка політики безпеки об'єкту інформаційної діяльності. Тема і зміст кваліфікаційної роботи повністю відповідає технічному завданню на дипломну роботу.

У ході виконання кваліфікаційної роботи були вирішені наступні питання: аналіз існуючих загроз, обґрунтування необхідності створення комплексної системи захисту інформації для Машинобудівного коледжу Дніпровського національного університету, приведена модель загроз та порушника для підприємства, прийняті проектні рішення щодо захисту інформації.

У економічному розділі були розраховані витрати на впровадження політики безпеки і визначено економічну доцільність розробки політики безпеки.

До недоліків проекту слід віднести окремі незначні неточності у формулюванні.

В цілому кваліфікаційну роботу виконано у відповідності до вимог, які пред'являються до кваліфікаційної роботи бакалавра і заслуговує оцінки "відмінно", а Заворін Іван Дмитрович – присвоєння йому кваліфікації "фахівець з організації інформаційної безпеки" освітньокваліфікаційного рівня "бакалавр".

Керівник кваліфікаційної роботи к.т.н., доц. Флоров С.В.

Дата: Підпис: