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 *Котовенка Дениса Євгеновича*

академічної групи *125-19ск-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка підсистеми захисту інформації в інформаційно-комунікаційній системі приватного підприємства «Юнайтед колорс»*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.т.н., проф. Корнієнко В.І.			
розділів:				
спеціальний	ст. викл. Мєшков В.І.			
економічний	к.е.н., доц. Романюк Н.М.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2022

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту *Котовенку Денису Євгеновичу* **академічної групи** *125-19ск-1*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Розробка підсистеми захисту інформації в інформаційно-комунікаційній системі приватного підприємства «Юнайтед колорс»***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 18.05.2022 № 268-с

Розділ	Зміст	Термін виконання
Розділ 1	Обстеження ІТС, створення моделі загроз та моделі порушника. Визначення об'єктів захисту	29.03.2022
Розділ 2	Розробка проектних рішень для створення комплексної системи захисту інформації в ІТС	24.05.2022
Розділ 3	Розрахунок експлуатаційних витрат, визначення збитків від витоку ІзОД, розрахунок витрат на забезпечення інформаційної безпеки	14.06.2022

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

Дата видачі: 08.01.2022р.

Дата подання до екзаменаційної комісії: 15.06.2022р.

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

РЕФЕРАТ

Пояснювальна записка: __ с., __ рис., _ табл., __ додатка, __ джерел.

Об’єкт розробки: комплексна система захисту інформації для ІТС приватного підприємства «Юнайтед колорс».

Мета роботи: забезпечення необхідного рівня захисту інформації, яка обробляється в ІТС приватного підприємства «Юнайтед колорс».

У спеціальній частині дана характеристика усіх компонентів ІТС приватного підприємства «Юнайтед колорс»; висунуті основні вимоги щодо захисту інформації в автоматизованій системі. Обґрунтовано вибір засобів захисту інформації.

В економічному розділі розраховані капітальні інвестиції на придбання складових комплексної системи захисту інформації та обґрунтована доцільність використання засобів захисту інформації в ІТС приватного підприємства «Юнайтед колорс».

Практичне значення проекту полягає в рекомендації організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечать необхідний рівень захисту інформації в ІТС «Юнайтед колорс».

Розроблений комплекс засобів захисту призначений для використання в ІТС «Юнайтед колорс», з метою захисту відкритої інформації та інформації з обмеженим доступом.

МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ПРОФІЛЬ ЗАХИЩЕННОСТІ, КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, КОМПЛЕКС ЗАСОБІВ ЗАХИСТУ.

ABSTRACT

Explanatory note: ___ pp., ___ pic., ___ table, ___ app, ___ sources.

Object of development: comprehensive information security system for ITS of the private enterprise "United Colors".

Purpose: to ensure the required level of protection of information processed in the ITS of the private enterprise "United Colors".

In the special part the characteristic of all components of ITS of the private enterprise "United colors" is given; the basic requirements for information protection in the automated system are put forward. The choice of means of information protection is substantiated.

The economic section calculates capital investments for the acquisition of components of a comprehensive information security system and substantiates the feasibility of using information security tools in the ITS of the private enterprise "United Colors".

The practical significance of the project is to recommend organizational and engineering measures, software and hardware that will provide the necessary level of information protection in the ITS "United Colors".

The developed set of protection means is intended for use in ITS "United Colors", for the purpose of protection of open information and information with limited access.

THREAT MODEL, INFRINGER MODEL, SECURITY PROFILE, COMPREHENSIVE INFORMATION PROTECTION SYSTEM, COMPLEX OF PROTECTION MEANS.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

АТС – автоматична телефонна станція;

ВС – суб'єктивні загрози;

ЗІ – захист інформації;

КЗ – контрольована зона;

КЗЗ – комплекс засобів захисту;

КР – керованість;

КС – комп'ютерна система;

КСЗІ – комплексна система захисту інформації;

НД – нормативний документ;

НС – навмисні загрози;

НСД - несанкціонований доступ;

ОІД – об'єкт інформаційної діяльності;

ОС – обчислювальна система;

П.І.Б – прізвище, ім'я, по батькові.

ПЗ – програмне забезпечення;

РС – робоча станція;

ТЗІ – технічний захист інформації;

ТП – трансформатора підстанція;

GSM – Groupe Special Mobile;

HDD – Hard Disk Drive (жорсткий диск);

SATA – Serial ATA;

USB – Universal Serial Bus (універсальна послідовна шина).

ЗМІСТ

с.

ВСТУП

З урахуванням сьогоднішніх вимог щодо захисту інформації, є велика необхідність створення комплексної системи захисту інформації. Раніше це було потрібно лише для великих підприємств та установ, де обробляється інформація, що належить державі. Але сьогодні це потрібно для багатьох підприємств, на яких хочуть зберегти конфіденційність, цілісність та доступність важливої інформації.

Безпека інформації отриманої у ході діяльності підприємства є дуже важлива, тому що порушення конфіденційності інформації може призвести до втрати клієнтів та нанесення збитків підприємству.

Захист інформації в інформаційно-телекомунікаційній системі полягає в створенні організаційних і інженерних заходів та використанні програмно-апаратних засобів, що зможуть зменшити ймовірність реалізації загроз і розмір завданих збитків, пов'язаних з діями конкурентів чи комп'ютерних злочинців.

Відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством.

Створення КЗЗ здійснюється в усіх ІТС, де обробляється інформація, яка належить до державних інформаційних ресурсів, належить до державної чи іншої таємниці або до окремих видів інформації, необхідність захисту якої визначено законодавством, а також в ІТС, де така необхідність визначена власником інформації відповідно до пункту 5.8 НД ТЗІ 3.7-003 -2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі».

Постановою Кабінету Міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» захисту в системі підлягає інформація, яка становить державну або іншу передбачену законом таємницю.

Відповідно до статті 24 Закону Украйни «Про захист персональних даних» в органах державної влади, органах місцевого самоврядування, а також у володільцях чи розпорядниках персональних даних, що здійснюють обробку персональних даних, яка підлягає повідомленню відповідно до цього Закону, створюється (визначається) структурний підрозділ або відповідальна особа, що організовує роботу, пов'язану із захистом персональних даних при їх обробці.

Кінцевим завданням роботи є зменшення ймовірності реалізації загроз й розміру завданих збитків від існуючих загроз та відповідності обробки інформації в ІТС до чинного законодавства України із захисту інформації шляхом створення КСЗІ.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Обстеження інформаційно-телекомунікаційної системи «Юнайтед колорс»

Під інформаційно-телекомунікаційною системою слід розуміти організаційно-технічну систему, що реалізує інформаційну технологію і об'єднує ОС, фізичне середовище, персонал і інформацію, яка обробляється [1].

ІТС «Юнайтед колорс» призначена для автоматизації обробки інформації, яка створюється в ході роботи підприємства.

Автоматизована система підприємства належить до класу 3 згідно з встановленою НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу" класифікацією: автоматизовані системи, створені на базі розподіленого багатомашинного багатокористувачевого комплексу [2].

1.1.1 Обґрунтування необхідності створення КСЗІ

Відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством.

Створення КЗЗ здійснюється в усіх ІТС, де обробляється інформація, яка належить до державних інформаційних ресурсів, належить до державної чи іншої таємниці або до окремих видів інформації, необхідність захисту якої визначено законодавством, а також в ІТС, де така необхідність визначена власником інформації відповідно до пункту 5.8 НД ТЗІ 3.7-003 -2005 «Порядок

проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі».

Постановою Кабінету Міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» захисту в системі підлягає інформація, яка становить державну або іншу передбачену законом таємницю.

Фінансово-економічні переваги у разі створення КСЗІ в ІТС «Юнайтед колорс».

1.1.2 Обстеження обчислювальної системі ІТС «Юнайтед колорс»

Обчислювальна система – сукупність програмних-апаратних засобів, призначених для обробки інформації [1].

На даному об’єкті інформаційної діяльності [3] «Юнайтед колорс» обчислювальна система використовується для обробки фото та відео, ведення бухгалтерського обліку та іншої документації, пов’язаної з діяльністю підприємства.

Для забезпечення високопродуктивної роботи використовуються графічні робочі станції, які призначені для роботи з графікою і відео редакторами. На підприємстві розміщено 2 графічні станції характеристики яких наведені у таблиці 1.1.

Таблиця 1.1 – Характеристика графічних робочих станції

№ з/п	Характеристика	Найменування
1	2	3
1	Чипсет материнської плати	Intel H510 (PRIME H510M-K)
2	Процесор	Intel Core i5-10400F (2.9-4.3 ГГц)
3	Пам’ять	DDR4 16 ГБ Hynix
4	Відеопам’ять	nVidia GeForce GTX 1650, 4 ГБ

Продовження таблиці 1.1

1	2	3
5	Твердотільний накопичувач (SSD)	SSD 1 ТБ
6	Оптичний привід	DVD+/-RW
7	Блок живлення	500 Вт
8	Порти	1 x PS/2 2 x USB 3.2 Gen 1 Type-A 4 x USB 2.0 1 x LAN (RJ-45) 3 x аудіороз'єми 1 x DVI-D 1 x HDMI 2.0 1 x DisplayPort

Для відображення інформації з графічних станцій використовуються монітори Samsung S24R350.

Інші 2 комп’ютера не використовуються для роботи з графікою, тому вони обладнані іншими комплектуючими. Характеристика двох інших комп’ютерів наведена у таблиці 1.2.

Таблиця 1.2 – Характеристика робочих станції

№ з/п	Характеристика	Найменування
1	2	3
1	Чипсет материнської плати	Intel H410
2	Процесор	Intel Core i5-10400 (2.9 - 4.3 ГГц)
3	Пам’ять	DDR4 8 ГБ Hynix
4	Відеопам’ять	Intel UHD 630 Graphics

Продовження таблиця 1.2

№ з/п	Характеристика	Найменування
1	2	3
5	Твердотільний накопичувач (SSD)	SSD 256 ГБ
6	Оптичний привід	DVD+/-RW
7	Блок живлення	300 Вт
8	Порти	1 x PS/2 порт для клавіатури 1 x PS/2 порт для миші 4 x USB 2.0 Type-A 1 x HDMI 1.4 (для інтегрованої відеокарти) 1 x VGA (для інтегрованої відеокарти) 1 x DisplayPort 1 x LAN (RJ-45) 3 x аудіороз'єми

Для відображення інформації з робочих станцій використовуються монітори Samsung S24R350.

1.1.2.1 Фізичне та логічне об’єднання робочих станцій

Локальна мережа ІТС «Юнайтед колорс» побудована на фізичній топології «зірка» і логічної топології «шина». У мережі кожна робоча станція приєднана до маршрутизатора за допомогою витої пари CAT5e з коннекторами RJ-45. Логічне підключення показано на рисунку 1.1.

Усі робочі станції знаходяться у робочій групі. Це дозволяє спільно використовувати файли, папки і принтери.

На підприємстві є підключення до мережі Інтернету через провайдера «Київстар». На кожній робочій станції є доступ до мережі Інтернет.

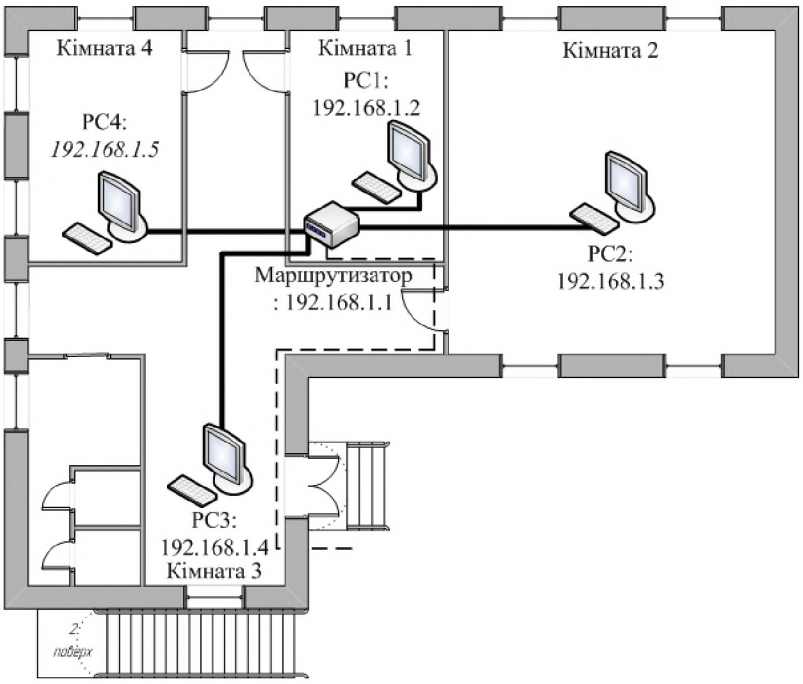


Рисунок 1.1 – Логічне підключення робочих станцій

План об’єднання робочих станцій у мережу наведено у додатку.

У якості маршрутизатору використовується Asus RT-N18U. Маршрутизатор дозволяє передавати інформацію у мережі на швидкості 1000 Мбіт/с. Характеристики маршрутизатора наведені у таблиці 1.3.

Таблиця 1.3 – Характеристика маршрутизатора Asus RT-N18U [4]

№ з/п	Характеристика	Найменування
1	WAN-порт	USB 4G, Ethernet
2	Підтримка протоколів	PPPoE, IPsec, L2TP, PPTP
3	Порти	4 x LAN (RJ45) 10/100/1000 Мбіт/с 1 x WAN (RJ45) 10/100/1000 Мбіт/с 1 x USB 3.0
4	Стандарти зв'язку	802.11b: 1, 2, 5.5, 11 Мбіт/с 802.11g: 6,9,12,18,24,36,48,54 Мбіт/с 802.11n: до 450 Мбіт/с 802.11n Turbo: до 600 Мбіт/с
5	Частота роботи Wi-Fi	2,4 ГГц
6	Максимальна споживана потужність	19 Вт

Доступ до безпровідної мережі (Wi-Fi) обмежено паролем.

1.1.2.2 Обладнання для фото та відео зйомки

Для фото і відео зйомки на ОІД «Юнайтед колорс» використовуються 3 фотоапарати та 2 відеокамери. Головною характеристикою для усього обладнання являється місце для збереження інформації (фото, відео) на карті пам’яті. Найменування обладнання та карт пам’яті наведені у таблиці 1.4.

Таблиця 1.4 – Обладнання для фото та відео зйомки

№ з/п	Найменування	Підтримка карт пам'яті	Карта пам’яті
1	Sony NEX-FS100	SD, SDHC, SDXC, MS Duo	TRANSCEND 256GB SDXC CLASS 10 UHS-I
2	Canon XA25	SD, SDHC, SDXC	TRANSCEND 256GB SDXC CLASS 10 UHS-I
3	Canon EOS 5D Mark III	CompactFlash, SD, SDHC, SDXC	TRANSCEND 256GB SDXC CLASS 10 UHS-I
4	Nikon D800E	CompactFlash, SD, SDHC, SDXC	TRANSCEND 256GB SDXC CLASS 10 UHS-I
5	Panasonic Lumix DMC-GH4	SD, SDHC, SDXC	TRANSCEND 256GB SDXC CLASS 10 UHS-I

У таблиці 1.4 наведені основні карти пам’яті, які використовуються під час роботи. Запасні карти пам’яті знаходяться у керівника підприємства.

1.1.2.3 Периферійне обладнання

Для друку фотографій використовуються три фотопринтери Epson L1800, які підключені до комп’ютерів через інтерфейс USB 2.0. Розміщення фотопринтерів показано на додатку А. Головні характеристика наведені у таблиці 1.5.

Таблиця 1.5 – Характеристика фотопринтера Epson L1800 [5]

№ з/п	Характеристика	Найменування
1	Технологія друку	Струменева
2	Кольоровість друку	Кольорова
3	Тип чорнила	Водорозчинні
4	Максимальний формат	A3
5	Підтримка ОС	– OS X – Windows
6	Споживана потужність	16 Вт
7	Ширина, глибина, висота, мм	705 x 322 x 215
8	Вага, кг	12,5

Також для зберігання інформації використовуються 4 зовнішніх жорстких диска Seagate Backup Plus 3 ТБ USB 3.0, які зберігаються у керівника підприємства. Характеристика зовнішніх дисків наведена у таблиці 1.6.

Таблиця 1.6 – Характеристика зовнішнього жорсткого диска Seagate Backup Plus 3 ТБ USB [6]

№ з/п	Характеристика	Найменування
1	Форм-фактор	3.5
2	Обсяг пам'яті	3 ТБ
3	Інтерфейс	USB 3.0

Для роботи з графікою використовується графічний планшет Wacom Intuos Pro Medium, який працює через USB інтерфейс.

Секретні ключі для програмного забезпечення «M.E.Doc IS» зберігаються на USB флеш-накопичувачі, який знаходиться у керівника.

1.1.2.4 Інша офісна техніка

Телефонний апарат Panasonic KX-TG6611UAB, який підключено до телефонної лінії та використовуються для діяльності підприємства. Трубка на даному апараті бездротова

1.1.2.5 Програмне забезпечення обчислювальної системи

Програмне забезпечення графічної станції.

Операційна система графічної станції:

– Windows 10 Professional 64-bit.

Функціональне програмне забезпечення графічної станції:

– Adobe Photoshop Lightroom – це комплексне програмне забезпечення для обробки фотографій [7];
– Adobe Photoshop – це графічний редактор для редагування растрових зображень;
– Sony Vegas Pro – професійна програма для редагування і монтажу відео, а також запису і монтажу аудіо-доріжок;
– Microsoft Word 365 – програмне забезпечення для створення, перегляду і редагування текстових документів;
– Microsoft Excel 365 – програмне забезпечення для роботи з електронними таблицями;
– Skype – програмне забезпечення для текстового, голосового та відео зв'язку через мережу інтернет;
– VLC media player - медіаплеєр для відтворення мультимедійних файлів;
– Google Chrome – веб-переглядач для відображення інформації із комп'ютерної мережі (браузер).

Програмні засоби захисту інформації:

– ESET NOD32 Antivirus – програмне забезпечення для захисту від вірусних загроз та атак хакерів.

Програмне забезпечення робочої станції.

Операційна система робочої станції:

– Windows 10 Professional 64-bit.

Функціональне програмне забезпечення робочої станції:

– Microsoft Word 365 – програмне забезпечення для створення, перегляду і редагування текстових документів;
– Microsoft Excel 365 – програмне забезпечення для роботи з електронними таблицями;
– Skype – програмне забезпечення для текстового, голосового та відео зв'язку через мережу інтернет;
– VLC media player – медіаплеєр для відтворення мультимедійних файлів;
– Google Chrome – веб-переглядач для відображення інформації із комп'ютерної мережі (браузер).

Бухгалтерське програмне забезпечення:

– 1С: Підприємство 8.3– програмне забезпечення для бухгалтерського та податкового обліку;
– «M.E.Doc» – забезпечення для обміну документами в електронному вигляді з контролюючими органами (реєстрація податкових накладних в ЄРПН) і контрагентами (обмін рахунками, актами і податковими накладними).

Програмні засоби захисту інформації:

– ESET NOD32 Antivirus – програмне забезпечення для захисту від вірусних загроз та атак хакерів.

DVD-диски з ПЗ знаходяться у керівника.

1.1.3 Обстеження фізичного середовища ІТС «Юнайтед колорс»

1.1.3.1 Місцезнаходження ІТС «Юнайтед колорс»

Об'єкт інформаційної діяльності «Юнайтед колорс» розташований на першому поверсі двоповерхового будинку.

ОІД «Юнайтед колорс» знаходиться за адресою вул. Старокозацька, буд. 33а. Навколо будівлі впорядкована територія, яка частково покрита асфальтом,

та є пішохідна зона і місце для паркування. ОІД розташовано на першому поверсі двоповерхового будинку. Контрольована зона визначена наказом керівника підприємства №1 від 10.10.2014, і обмежена стінами першого поверху будівлі.

Визначаються сусідні об'єкти та споруди, які розташовані поруч із ОІД «Юнайтед колорс». Сусідні об'єкти та споруди, кількість поверхів, напрям та відстань до цих об'єктів наведено у таблиці 1.7.

Таблиця 1.7 – Сусідні об'єкти та споруди

№ з/п	Найменування об'єкту	Адреса	Кількість поверхів	Напрям від об'єкту	Відстань до об'єкту, мм
1	Житловий будинок	Вул. Старокозацька, буд. 29а	2	Північ	11000
2	Трансформаторна підстанція	–	1	Північний схід	3000
3	Склад-магазин	Вул. Старокозацька, буд. 33б	1	Схід	6000
4	Місце для паркування	–	–	Південь	8000
5	Житловий будинок	Вул. Старокозацька, буд. 35	5	Південь Захід	11000 16000
6	Житловий будинок	Вул. Старокозацька, буд. 33	4	Захід	11300
7	Місце для паркування	–	–	Захід	8000
8	Проїжджа частина	Вул. Старокозацька	–	Захід	27500
9	Житловий будинок	Вул. Старокозацька, буд. 31	5	Північний захід	4300

Цей перелік використовується для запобігання розвідки ррізними засобами.

1.1.3.2 Архітектурно-будівельні особливості приміщень

Для організації організаційних, інженерних і технічних заходів захисту інформації встановлюються архітектурно-будівельні особливості приміщень:

– товщина стін: зовнішні – 500 мм; внутрішні – 100 мм;

– висота перекриття – 3000 мм;

– склад зовнішніх стін – цеглина;

– склад внутрішніх стін – оштукатурений гіпсокартон;

– стеля - залізобетонна монолітна заливна товщиною 150 мм;

– покриття підлоги – ламінована підлога 12 мм;

– вікна (11 шт. Розміром 1300 х 1400 мм) – металопластикові з двокамерним склопакетом. товщина скла 3 мм. Всередині приміщення на всіх вікнах знаходяться жалюзі та зовні використовуються металеві захисні ролети;

– внутрішні двері (4 шт.) Типові дерев'яні одностулкові, розміром 900х2000 мм. товщиною 40 мм;

– зовнішні двері (1 шт. - двостулкові розміром 1300х2050 мм.) – металеві, завтовшки 110 мм. Товщина металу - 3 мм.

1.1.3.3 Системи життєзабезпечення

На підприємстві є системи електроживлення, опалення, каналізації, водопостачання, вентиляції, занулення та сигналізації. Деякі системи виходять за межі контрольованої зони. Перелік систем, що виходять за межі КЗ наведено у таблиці 1.8.

Таблиця 1.8 – Системи, що виходять за межі КЗ

№ з/п	Назва системи життєзабезпечення
1	Електроживлення
2	Опалення
3	Каналізації
4	Водопостачання
5	Телефонного зв’язку

6	Інтернету

Опис систем життєзабезпечення та способи їх підключення наведено у таблиці 1.9.

Таблиця1.9 – Характеристика систем життєзабезпечення

№ з/п	Вид комунікації	Спосіб підключення
1	Система електроживлення	Підключено до трансформаторної підстанції № 10, котра знаходиться в північно-східному напрямку від ОІД і розташована на віддаленості 3м. Підключено за допомогою силових кабелів через електричний стовп к розподільному щиту. Є в наявності автоматичні вимикачі диференціального струму та стабілізатор напруги. Обслуговує сторонніх споживачів. Виходить за межі КЗ
2	Система опалення	Підключена до міської мережі опалення, котра знаходиться на заході від ОІД, і виходить за межі КЗ (самопливна система опалення)
3	Система каналізації	Підключена до міської мережі каналізації, котра знаходиться в південно-східному напрямку від ОІД на відстані 3,2 м, і виходить за межі КЗ
4	Система водопостачання	Підключена до міського водоканалу, котра знаходиться на заході від ОІД, і виходить за межі КЗ
5	Система занулення	Захисне заземлення (нейтральна точка ТП має з'єднання с землею). Виходить за межі КЗ
6	Система телефонного зв'язку	Підключена до АТС «VEGA». На офіс виділено 2 номери (номер для приймальні; номер для охоронної системи). Виходить за межі КЗ
7	Інтернет	Підключено до провайдера «Київстар»
8	Система вентиляції	Припливно-витяжна вентиляція
9	Система сигналізації	Підприємство підключено до пульту приватного охоронного підприємства «ОКО–2», який

		підключений до телефонної лінії та GSM-модулю

Згідно з розробленою таблицею характеристик систем життєзабезпечення, можливо виявити більшу кількість загроз, що здійснюватися технічними каналами або несанкційованим доступом.

Також для захисту інформації важливо знати місцезнаходження та відстань робочих станцій до границі контрольованої зони.

Схематичне місцезнаходження з відповідним найменуванням основних технічних засобів та номери кімнат показано на рисунку 1.2.

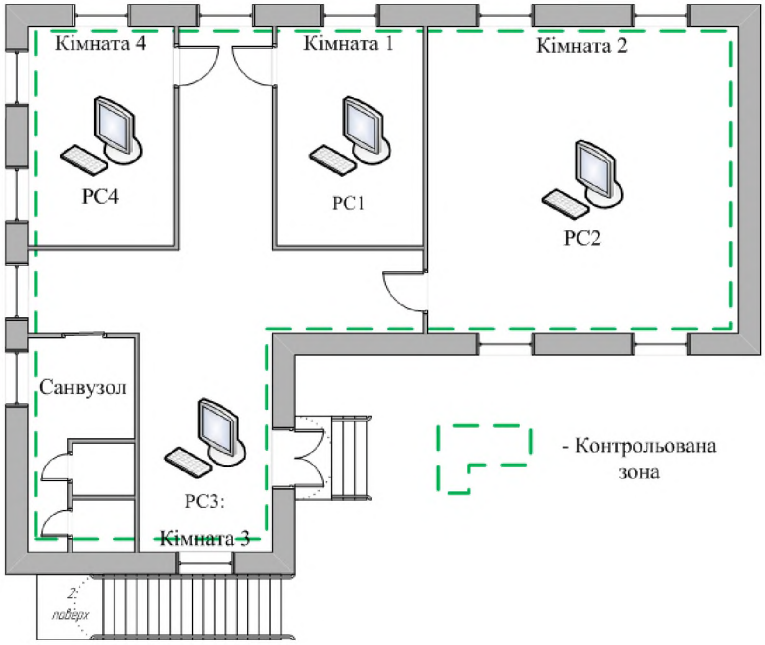


Рисунок 1.2 – Схематичне місцезнаходження основних технічних засобів

Мінімальна відстань до границі КЗ та допоміжних технічних засобів для основних технічних засобів наведено у таблиці 1.10.

Таблиця 1.10 – Мінімальна відстань до границі КЗ

№ з/п	Найменування основних технічних засобів	Місцезнаходження	Мінімальна відстань до границі КЗ	Мінімальна відстань до допоміжних технічних засобів
1	PC1	Кімната 1	3500 мм	1500 мм
2	PC2	Кімната 2	1000 мм	500 мм
3	PC3	Кімната 3	1500 мм	500 мм

4	PC4	Кімната 4	1800 мм	1500 мм

Мінімальна відстань до границь КЗ та допоміжних засобів призначається для захисту інформації від витоку каналами побічних електромагнітних випромінювань і наведень.

1.1.3.3 Внутрішній трудовий розпорядок

Розпорядок роботи: Підприємство працює з понеділка по п’ятницю. Вихідні дні: субота та неділя. Графік роботи з 9.00 до 18.00. Перерва з 13.00 до 14.00.

Прибирання приміщення проводиться кожного дня з 8.30 до 9.00.

Пропускний режим: доступ на ОІД здійснюється через головні двері. Двері закриті на звичайний замок, який відкривається за допомогою ключа. Для зняття приміщення з основної охорони вводиться код. В кінці робочого дня приміщення ставиться на охорону.

Пропуск клієнтів, технічного персоналу та інших людей на підприємство узгоджується з керівником чи бухгалтером. Знаходження цих людей можливо лише за умови наявності працівників «Юнайтед колорс» на території підприємства.

Режим контрольованої зони забезпечується в робочий час інженерними конструкціями будівлі. В неробочий час забезпечуються інженерними конструкціями будівлі та охоронною сигналізацію.

Кожен компонент АС забороняється виносити за межі ОІД без письмової згоди керівника.

1.1.4 Обстеження середи користувачі ІТС «Юнайтед колорс»

1.1.4.1 Штат працівників

Керівник – 1 особа. Координує роботу всіх ділянок; займається фото-відео зйомкою та монтажем. Використовує графічну робочу станцію (PC4) та усе програмне забезпечення, яке встановлено на ній. Знаходиться у кімнаті 4.

Системний адміністратор – 1 особа. Займається адмініструванням системи. Використовує робочу станцію (PC1) та усе програмне забезпечення, яке встановлено на ній. Знаходиться у кімнаті 1.

Бухгалтер – 1 особа. Веде бухгалтерську та іншу фінансову документацію, економічні розрахунки. Займається обліком клієнтів. Використовує робочу станцію (PC3) та усе програмне забезпечення, яке встановлено на ній. Знаходиться у кімнаті 3.

Фотограф – 1 особа. Займається фото-відео зйомкою. Знаходиться у кімнаті 2.

Дизайнер – 1 особа. Займається фото-відео обробкою та монтажем. Використовує графічну робочу станцію (PC2) та усе програмне забезпечення, яке встановлено на ній. Знаходиться у кімнаті 2.

Прибиральниця – 1 особа. Надає клінінгові послуги на підприємстві. Інвентар для прибирання приміщень знаходиться в санвузлі.

Всього 6 осіб.

План розміщення знаходження працівників показано на рисунку 1.3.

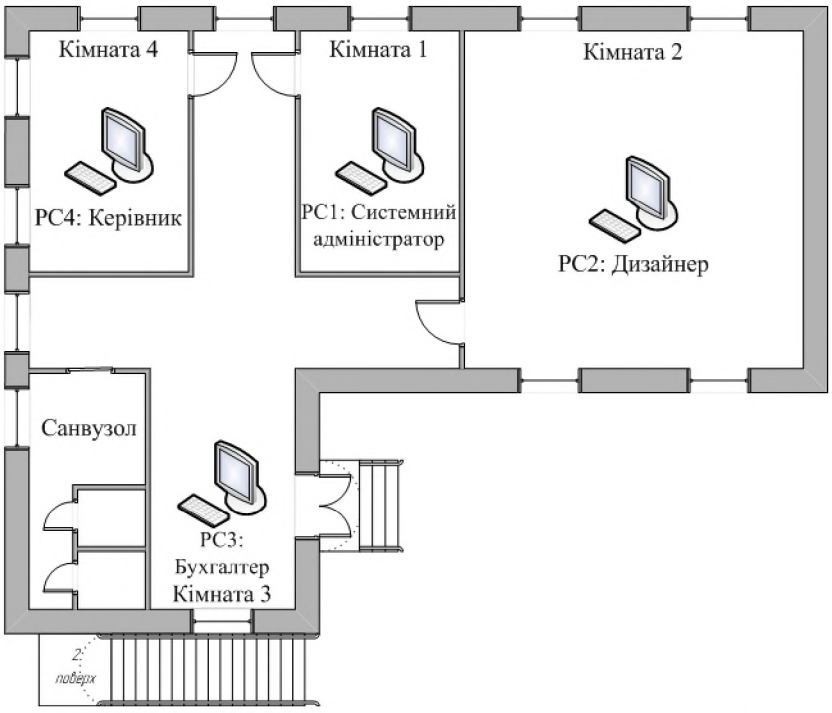


Рисунок 1.3 – Робочі станції та кімнати працівників

Інший технічний персонал викликається у разі потреби зі згоди керівника чи бухгалтера.

1.1.4.2 Користувачі ІТС «Юнайтед колорс»

Облікові записи створює системний адміністратор. Кожен працівник має локальний обліковий запис на своїй робочій станції з правами адміністратора. Перелік користувачів у відповідності з робочою станцією наведено у таблиці 1. 11.

Таблиця 1.11 – Перелік користувачів ІТС «Юнайтед колорс»

№ з/п	Працівник	Обліковий запис	Робоча станція
1	Системний адміністратор	SysAdmin	PC1 (робоча станція)
2	Дизайнер	Designer	PC2 (графічна станція)
3	Бухгалтер	Accountant	PC3 (робоча станція)
4	Керівник	Head	PC4 (графічна станція)

Ім’я користувача та пароль від облікових записів користувачі обирають самі. Кожен пароль зберігається на робочій станції керівника в документі Word, який стоїть під паролем (відомий лише керівнику).

Для деякого програмного забезпечення використовуються додаткові облікові записи для авторизації. Перелік ПЗ наведено у таблиці 1.12.

Таблиця 1.12 – Облікові записи для ПЗ

№ з/п	Робоча станція	Програмне забезпечення	Користувач	Обліковий запис
1	PC3	1С: Підприємство 8.3(PC3)	Head, Accountant	Head, Accountant
2	PC3	«M.E.Doc IS» (PC3)	Head, Accountant	Head, Accountant
3	PC3, PC4	Приват24 для бізнесу (через браузер)	–	–

Користувачі системи мають облікові записи для ПЗ з тими же іменами, але використовуються інші паролі для авторизації.

Затверджувати КСЗІ буде керівник. Усі повноваження керування КСЗІ будуть надані керівнику та системному адміністратору.

Служба захисту інформації на підприємстві відсутня. У ролі адміністратора безпеки назначається керівник.

Клієнти мають доступ до відкритої інформації та можуть знаходитися на території підприємства.

1.1.5 Обстеження інформації ІТС «Юнайтед колорс»

Відповідно до категорії об’єкта (IV), визначеної в акті категоріювання, було встановлено, що інформація на об’єкті відноситься до відкритої інформації та інформації з обмеженим доступом, що не становить державної таємниці, і тому віднесена до конфіденційної інформації.

Конфіденційна інформація – інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов відповідно до Закону України № 2939-VI від 13 січня 2011 року «Про доступ до публічної інформації».

Також на підприємстві обробляються персональні дані працівників та клієнтів. Вони також віднесені до конфіденційної інформації відповідно до Статті 5 Закону України № 2297-VI від 1 червня 2010 року «Про захист персональних даних».

Перелік та кваліфікація інформації, що обробляється в ІТС «Юнайтед колорс» наведено у таблиці 1.13.

Таблиця 1.13 – Перелік типів інформації

№ з/п	Тип інформації	Тип носія	Режим доступу	Вид інформації	Має доступ
1	Персональні дані	Електронний, паперовий	ІзОД	Конфіденційна	Керівник Бухгалтер
2	Ціни на послуги	Електронний, паперовий	Відкритий	Відкрита	Усі

Продовження таблиці 1.13

№ з/п	Тип інформації	Тип носія	Режим доступу	Вид інформації	Має доступ
3	Квитанції	Електронний, паперовий	Відкритий	Відкрита	Усі
4	Фото/відео	Електронний, паперовий	ІзОД	Конфіденційна	Керівник Дизайнер Фотограф Клієнт
5	Бухгалтерський і податковий облік	Електронний, паперовий	ІзОД	Конфіденційна	Керівник Бухгалтер
6	Секретні ключі «M.E.Doc IS»	Електронний	ІзОД	Конфіденційна	Керівник Бухгалтер

Деякі типи інформації складаються з певного переліку матеріальних носіїв та інформації. Більш докладний опис складу деяких типів інформації наведено у таблиці 1.14.

Таблиця 1.14 – Склад типів інформації

№ з/п	Тип інформації	Склад
1	Персональні дані працівників	а) паспорт; б) трудова книжка; в) ідентифікаційний номер фізичної особи; г) документ про освіту.
2	Персональні дані клієнтів	а) П.І.Б; б) електронна пошта; в) телефон.
3	Квитанції	а) адреса підприємства; б) телефон підприємства; в) № замовлення; г) П.І.Б, електронна пошта, телефон; ґ) найменування послуг; д) вартість послуг та факт оплати; е) підпис замовника; ж) підпис та прізвище представника підприємства.
4	Бухгалтерський і податковий облік	а) єдиний податок; б) єдиний соціальний внесок; в) податок на додану вартість; г) податок на заробітну плату.

Також до кожного типу інформації висунуті певні вимоги щодо захисту окремих властивостей інформації та системи (конфіденційності (К), цілісності (Ц), доступності (Д) та спостережності(С)) які наведено у таблиці 1.15.

Таблиця 1.15 – Вимоги щодо захисту інформації та системи

№ з/п	Тип інформації	Вимоги щодо захисту інформації			Вимоги до захисту системи	
		К	Ц	Д	С	Д
1	Інформація 1	+	–	–	+	–
2	Інформація 2	–	+	+	+	+
3	Інформація 3	–	+	+	+	+
4	Інформація 4	+	+	–	–	–
5	Інформація 5	+	+	+	+	+
6	Інформація 6	+	–	–	+	–

Згідно з таблицею 1.15 будуть висунуті вимоги щодо захисту інформації та системи.

До кожного окремого процесу ресурсів ІТС «Юнайтед колорс» мають доступ певні користувачі з встановленими правами. Перелік цих ресурсів наведено у таблиці 1.16.

Таблиця 1.16 – Ресурси ІТС «Юнайтед колорс»

№ з/п	Ресурс	Користувач	Процес	Права
1	PC1	SysAdmin	а) Microsoft Word 365 б) Microsoft Excel 365 в) Skype г) VLC media player ґ) Google Chrome д) ESET NOD32 Antivirus	У
2	PC2	Designer	а) Adobe Photoshop Lightroom б) Adobe Photoshop в) Sony Vegas Pro г) Microsoft Word 365 ґ) Microsoft Excel 365 д) Skype	У

Продовження таблиці 1.16

№ з/п	Ресурс	Користувач	Процес	Права
3	PC3	Accountant	а) Microsoft Word 365 б) Microsoft Excel 365 в) Skype г) VLC media player ґ) Google Chrome д) ESET NOD32 Antivirus е) 1С: Бухгалтерія 8.3 є) «M.E.Doc IS»	У
4	PC4	Head	а) Adobe Photoshop Lightroom б) Adobe Photoshop в) Sony Vegas Pro г) Microsoft Word 365 ґ) Microsoft Excel 365 е) Skype є) VLC media player ж) Google Chrome з) ESET NOD32 Antivirus 8	У
5	Інтернет	Усі користувачі	–	У
6	Маршрутизатор Asus RT-N18U	SysAdmin	–	У
7	Обладнання для фото та відео зйомки	Designer, Head, Фотограф	–	У
8	Принтери	Усі користувачі	–	У
9	Зовнішні жорсткі диски	SysAdmin, Head	–	У
10	Графічний планшет Wacom Intuos Pro Medium (підключен до PC2)	Designer, Head	–	У
11	Флеш-накопичувач з секретними ключами «M.E.Doc IS»	Accountant, Head	–	У

Продовження таблиці 1.16

№ з/п	Ресурс	Користувач	Процес	Права
12	DVD-диски з ПЗ	SysAdmin, Head	–	У
13	1С: Підприємство 8.3(РС3)	Accountant, Head	–	У
14	«M.E.Doc IS» (РС3)	Accountant, Head	–	У
15	Ціни на послуги (РС3)	Accountant, Head, Designer, SysAdmin	–	У

Примітка. У таблиці 1.16 використовуються такі позначення: С – створення; Ч – читання; Р – редагування; В – видалення; У – усі права.

У таблиці 1.16 у графі «Користувач» наведені користувачі, у яких є доступ до відповідного ресурсу. Іншім користувачам доступ до ресурсу обмежений.

Ресурси «1С: Бухгалтерія 8.3» та «M.E.Doc» складаються з переліку файлів, баз даних, конфігурацій, які розташовуються на РС3.

1.1.6 Обстеження технології оброблення інформації ІТС «Юнайтед колорс»

ІТС «Юнайтед колорс» використовується для збору, зберігання, оброблення, передавання та використання даних, які отримуються у ході діяльності підприємства. Діяльність підприємства спрямована на фото та відео обробку, та додатково потребує ведення бухгалтерського та податкового обліку.

1.1.6.2 Процес обробки заказу клієнта

Клієнт робить заказ на отримання послуг через стільниковий або мобільний телефон, чи домовляється на території підприємства «Юнайтед колорс» з керівником або бухгалтером. Залишає П.І.Б та стільниковий телефон,

в деяких випадках залишає електрону пошту. Ця інформація заноситься в квитанцію в ПЗ «1С: Бухгалтерія 8.3» на РС3 бухгалтером або керівником. Ця квитанція роздруковується у двох екземплярах та додатково заповнюється керівником чи бухгалтером (ціни на послуги зберігаються на РС3). Один екземпляр залишається у бухгалтера, інший передається клієнту у руки (квитанції зберігаються необмежений час).

В встановлений день проводиться фото чи відео зйомка на території підприємства «Юнайтед колорс» на обладнання для фото та відео зйомки керівником чи фотографом. Інформація на носіях інформації обладнання для фото та відео зйомки залишається на невідомий час чи до моменту коли на носії закінчується пам'ять для зберігання.

Уся інформація, яка була отримана під час зйомки, передається на графічну станцію РС2 чи РС4 в окрему папку, яка створюється окремо для кожного клієнта. Обробляється керівником чи дизайнером у функціональному програмному забезпеченні графічної станції.

Готовий матеріал зберігається на накопичувачі графічної станції та на зовнішньому жорсткому диску.

Після демонстрації готового матеріалу клієнту на графічній станції, матеріал, якщо потрібно, обробляється знову. Та після оплати клієнтом готівкою чи безготівковим розрахунком на рахунок підприємства, бухгалтер чи керівник перевіряє факт здійснення платежу та вносить відповідні дані до квитанції. Після чого, готовий матеріал копіюється дизайнером чи керівником на знімний чи оптичний носій клієнта з РС2 чи РС4. Якщо потрібно, то фотографії друкуються на одному з трьох фотопринтерів.

1.1.6.3 Бухгалтерський та податковий облік

Для бухгалтерського та податкового обліку використовується РС3. Бухгалтер та керівник використовує бухгалтерське програмне забезпечення «1С: Бухгалтерія 8.3» та «M.E.Doc IS». Для роботи ПЗ «M.E.Doc IS» використовуються мережа інтернет та секретні ключі, які зберігаються на USB

флеш-накопичувачі, який знаходиться у керівника, та видається бухгалтеру в разі потреби для роботи в ПЗ.

При прийомі на роботу у працівника збираються персональні дані, які зазначені у таблиці 1.14. Інформація зберігається у ПЗ «1С: Бухгалтерія 8.3» та «M.E.Doc IS» на РС3. В паперовому вигляді зберігається у бухгалтера в кімнаті 3.

Заробітна плата розраховується в програмному забезпечені «M.E.Doc IS» та нараховується через онлайн-сервіс «Приват24 для бізнесу» [8] через мережу інтернет (браузер Chrome) на РС3.

1.1.6.4 Схема інформаційних потоків ІТС «Юнайтед колорс»

Для графічного представлення технології оброблення інформації в ІТС «Юнайтед колорс» розробляється схема інформаційних потоків.

Схема інформаційних потоків відображає взаємодію між основними компонентами системи. Кожний ресурс цієї системи має свої процеси, доступ до яких відкривається певному набору користувачів. Наприклад, РС 3 відкриває доступ до двох процесів: 1С: Підприємство 8.2 та «M.E.Doc IS». Ці процеси мають певний перелік ресурсів (квитанції, персональні дані, бухгалтерський і податковий облік), доступ до яких відкрито бухгалтеру та користувачу. Також на РС 3 зберігаються ціни на послуги з відкритим доступом для всіх користувачів ІТС: клієнти, фотограф, дизайнер, бухгалтер, керівник, системний адміністратор. Доступ на змінення є тільки у бухгалтера та керівника.

Дана схема інформаційних потоків спрощує розуміння взаємодії між основними компонентами (процеси, користувачі та ресурси) ІТС «Юнайтед колорс» для кожного окремого компонента ІТС.

Інформаційна взаємодія між основними компонентами ІТС «Юнайтед колорс» представлена у структурній схемі інформаційних потоків на рисунку 1.4.

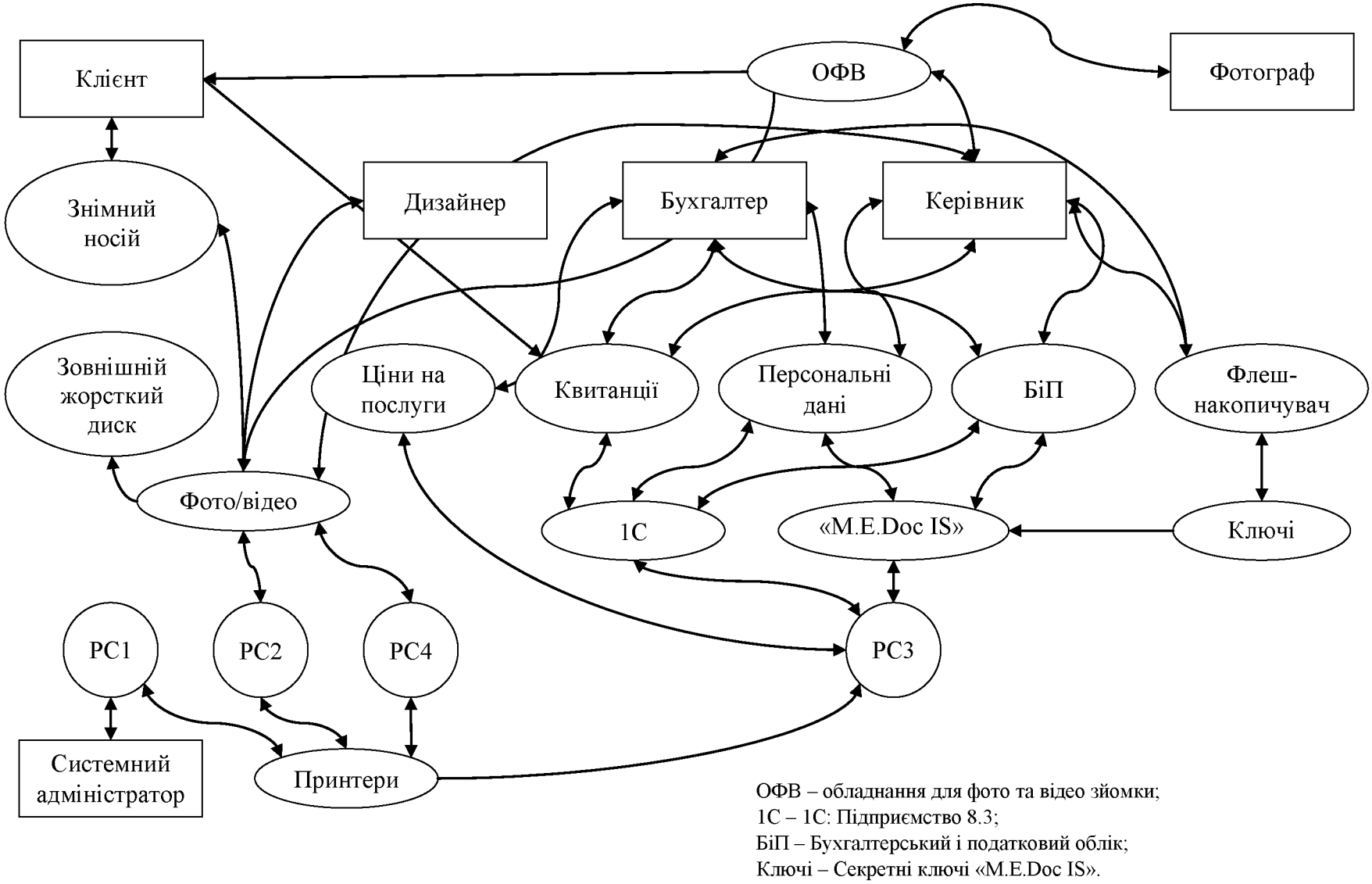


Рисунок 1.4 – Структурна схема інформаційних потоків

1.1.7 Перелік об’єктів захисту ІТС «Юнайтед колорс»

За результатами обстеження середовищ функціонування ІТС для розробки політики безпеки інформації для ІТС «Юнайтед колорс» треба однозначно визначити об’єкти захисту на які вона буде поширюватися. Перелік об’єктів захисту наведено у таблиці 1.17.

Таблиця 1.17 – Перелік об’єктів захисту

№ з/п	Об’єкт захисту	Тип носія	Ресурс
1	Персональні дані	Електронний	PC3
2	Фото/відео	Електронний	PC2, PC4, Зовнішні жорсткі диски
3	Бухгалтерський і податковий облік	Електронний	PC3
4	Ціни на послуги	Електронний	PC3
5	Секретні ключі «M.E.Doc IS»	Електронний	Флеш-накопичувач з секретними ключами «M.E.Doc IS»
6	1С: Бухгалтерія 8.3	Електронний	PC3
7	«M.E.Doc IS»	Електронний	PC3
8	PC2	–	–
9	PC3	–	–
10	PC4	–	–
11	Зовнішні жорсткі диски	–	–
12	Флеш-накопичувач з секретними ключами «M.E.Doc IS»	–	–
13	Системи життєзабезпечення ІТС	–	–
14	Персонал	–	–

На основі переліку об’єктів захисту будуть визначені потенційні внутрішні та зовнішні загрози для ІТС «Юнайтед колорс».

1.2 Постановка задачі

За результатами обстеження середовищ функціонування ІТС «Юнайтед колорс», потрібно виконати наступні задачі:

1) розробити модель загроз та модель порушника;
2) сформувати завдання із захисту інформації;
3) розробити концепцію політики безпеки;
4) розробити часткове технічне завдання на створення КСЗІ;
5) викласти вимоги до функціональних послуг безпеки;
6) вибрати засоби захисту інформації для реалізації профілю захищеності.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

Найменування і сфера застосування

Найменування: розробка комплексної системи захисту інформації для інформаційно-телекомунікаційної системи приватного підприємства «Юнайтед колорс».

Призначення розробки

Призначення даного роботи є розробка підсистеми захисту інформації від несанкціонованого доступу в інформаційно-телекомунікаційній системі підприємства, яка дозволить забезпечити необхідний рівень безпеки інформації.

Завдання із захисту інформації

На підставі матеріалів обстеження та моделі загроз визначаються основні завдання щодо захисту інформації, які повинні поширюватися на усі об'єкти захисту. В ІТС «Юнайтед колорс» визначені наступні основні завдання щодо захисту інформації:

– забезпечити визначені властивостей інформації (конфіденційності, цілісності, доступності) під час створення та експлуатації ІТС «Юнайтед колорс»;

– своєчасно виявляти та знешкоджувати загрози для об'єктів захисту ІТС «Юнайтед колорс», причин та умов, які спричиняють (можуть привести до) порушення її функціонування та розвитку;

– ефективно знешкоджувати (попереджувати) загрози для об'єктів захисту ІТС «Юнайтед колорс» шляхом впровадження правових, морально-етичних, фізичних, організаційних, технічних та інших заходів забезпечення безпеки;

– керувати засобами захисту інформації, контролювати роботу персоналу з боку адміністратора безпеки, оперативно повідомляти про спроби НСД до об'єктів захисту ІТС «Юнайтед колорс»;

– реєструвати, збирати, зберігати дані про всі події в системі, які мають відношення до безпеки інформації;

– створити умови для максимально можливого відшкодування та локалізації збитків, що завдаються неправомірними (несанкціонованими) діями фізичних та юридичних осіб, впливом зовнішнього середовища та іншими чинниками, зменшення негативного впливу наслідків порушення безпеки на функціонування ІТС [9].

2.1 Розробка моделі загроз та моделі порушника

2.1.1 Розробка моделі загроз для ІТС «Юнайтед колорс»

Для формування вимог до КСЗІ розробляється модель загроз для інформації. Під моделлю загроз розуміють абстрактний формалізований або неформалізований опис методів і засобів здійснення загроз [1]. В свою чергу, під загрозою маються на увазі будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків АС[1].

Загрози можуть мати об'єктивну або суб'єктивну природу. Суб’єктивні поділяються на навмисні та випадкові відповідно до НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі».

Тому розглядаються 3 види загроз:

1) навмисні суб’єктивні (навмисні дії потенційних порушників);
2) випадкові суб’єктивні (помилки персоналу (користувачів));
3) об’єктивні (зміна умов фізичного середовища; збої і відмови у роботі обладнання та технічних засобів ІТС; наслідки помилок під час проектування та розробки компонентів ІТС).

А також існує 3 можливі способи, якими можуть здійснюватися загрози в ІТС:

1) технічними каналами;
2) каналами спеціального впливу;

3) несанкціонованим доступом.

Більша частин загроз в ІТС «Юнайтед колорс» здійснюється несанкціонованим доступом.

Для кожної загрози визначаються певні вразливості. Під вразливістю слід розуміти нездатність системи протистояти реалізації певної загрози або сукупності загроз [9]. Перелік усіх виявлених вразливостей в ІТС «Юнайтед колорс» наведено у таблиці 2.1.

Таблиця 2.1 – Виявлені вразливості в ІТС «Юнайтед колорс»

№ з/п	Вразливість
1	Відсутність резервного копіювання інформації
2	Відсутність резервних апаратних засобів
3	Відсутність резервного підключення до мережі інтернет
4	Відсутність постійного контролю за технічним персоналом
5	Відсутність постійного контролю за клієнтами
6	Відсутність захисту обладнання від змін
7	Відсутність безперебійного джерела живлення
8	Неякісне обслуговування технічного персоналу
9	Відсутність умов та правил використання обчислювальної системи
10	Можливість підключення носіїв інформації клієнтів
11	Відсутність правил перевірки носіїв інформації
12	Неефективність ПЗ захисту інформації
13	Відсутність регулярного поновлення ПЗ
14	Відсутність регулярного поновлення операційної системи
15	Відсутність регулярної перевірки системи ПЗ захисту інформації
16	Використання РС у якості адміністратора
17	Відсутність постійного виходу із системи під час відлучення від РС
18	Відсутність обмеження прав до ПЗ
19	Недосконалість ПЗ
20	Недосконале налаштування ПЗ
21	Відсутність обмеження доступу до мережі інтернет
22	Відсутність реєстрації дій і подій у системі
23	Відсутність навчання у сфері ЗІ
24	Відсутність інвентаризації
25	Відсутність резервних носіїв інформації

26	Відсутність правил використання та зберігання носіїв інформації
27	Відсутність процедури знищення носіїв інформації
28	Відсутність процедури видалення інформації
29	Відсутність міжмережевого екрану

Продовження таблиці 2.1

№ з/п	Вразливість
30	Відсутність процедури зміни паролів для доступу до системи та ПЗ
31	Недосконалість системи автентифікації
32	Відсутність умов та правил використання обчислювальної системи
33	Недбалість персоналу
34	Відсутність періодичної перевірки системи пожежної та охоронної сигналізації
35	Відсутність періодичної перевірки та обслуговування обладнання та технічних засобів АС
36	Відсутність тренувань у разі виникнення надзвичайних ситуацій

Визначений перелік взраливостей не є вичерпним. Тому, у разі виявлення інших вразливостей, перелік доповнюється.

Для визначення найбільш ймовірних загроз та побудування моделі загроз приймається 5 рівнів небезпеки загроз, які поділяються наступним чином:

I – рівень, при якому ймовірність реалізації загрози мінімальний та нанесені збитки відсутні (властивості інформації та ОС не порушені);

II – рівень, при якому ймовірність реалізації загрози нижче середнього та нанесені збитки нижче середніх (можливо відновити інформацію та є доступ до ОС);

III – рівень, при якому ймовірність реалізації загрози середній та нанесені збитки середні (можливо відновити інформацію, але немає доступу до ОС);

IX – рівень, при якому ймовірність реалізації загрози вище середнього та нанесені збитки вище середнього (неможливо відновити інформацію, але є доступ до ОС);

X – рівень, при якому ймовірність реалізації загрози максимальний та нанесені збитки максимальні (неможливо відновити інформацію і відсутній доступ до ОС) ;

Перелік виявлених навмисних суб'єктивних загроз в ІТС «Юнайтед колорс» наведено у таблиці 2.2. Де для кожної загрози існують певні джерела виникнення загрози та відповідні вразливості (таблиця 2.1) з одним чи декількома рівнями небезпеки. Рівень небезпеки загрози, в деяких випадках, визначається як вплив на ІТС «Градн-колорс» взагалі.

Таблиця 2.2 – Навмисні суб'єктивні загрози в ІТС «Юнайтед колорс»

№ з/п	Загроза	Джерело	Вразливість	Рівень небезпеки загрози
1	Порушення фізичної цілісності ІТС	а) комп'ютерні злочинці; б) конкуренти; в) клієнти; д) персонал; г) технічний персонал.	1	X
			2	IX
			3	II
			4	III
			5	III
			6	III
2	Порушення режимів функціонування систем життєзабезпечення ІТС	а) комп'ютерні злочинці; б) конкуренти; в) клієнти; д) персонал; г) технічний персонал.	2	III
			3	II
			4	II
			5	II
			7	IX
			8	III
3	Порушення режимів функціонування ІТС	а) комп'ютерні злочинці; б) конкуренти; в) клієнти; д) персонал; г) технічний персонал.	2	III
			3	II
			4	II
			5	II
			7	III
			8	II
4	Впровадження і використання комп'ютерних вірусів, закладних пристроїв та інших засобів розвідки	а) комп'ютерні злочинці; б) конкуренти; в) клієнти; д) персонал; г) технічний персонал.	4	IX
			5	IX
			9	II
			10	IX
			11	IX
			12	II
			13	II
			14	II
			15	X
			16	IX
			17	III

			18	I
			19	I
			20	I
			21	I
			22	IX

Продовження таблиці 2.2

№ з/п	Загроза	Джерело	Вразливість	Рівень небезпеки загрози
5	Використання з корисливою метою персоналу ІТС	а) комп'ютерні злочинці; б) конкуренти; в) клієнти; д) технічний персонал.	9	I
			10	IX
			16	IX
			18	I
			21	I
			22	X
			23	I
6	Крадіжки носіїв інформації, виробничих відходів	а) комп'ютерні злочинці; б) конкуренти; в) клієнти; д) персонал; г)технічний персонал.	1	IX
			4	IX
			5	IX
			24	II
			25	III
			26	IX
			27	II
7	Несанкціоноване копіювання носіїв інформації	а) комп'ютерні злочинці; б) конкуренти; в) клієнти; д) персонал; г)технічний персонал.	4	II
			5	II
			10	II
			16	X
			17	I
			21	I
			22	X
			26	II
			27	I
8	Читання залишкової інформації з оперативної пам'яті РС, зовнішніх накопичувачів	а) комп'ютерні злочинці; б) конкуренти; в) клієнти; д) персонал; г)технічний персонал.	4	II
			5	II
			6	I
			12	II
			13	II
			14	II
			15	II
			16	X
			17	II
			18	I

			20	I
			22	X
			28	IX

Продовження таблиці 2.2

№ з/п	Загроза	Джерело	Вразливість	Рівень небезпеки загрози
9	Одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача	а) комп'ютерні злочинці; б) конкуренти; в) клієнти; д) персонал; г)технічний персонал.	4	IX
			5	IX
			12	I
			13	I
			14	I
			15	II
			16	II
			18	X
			21	I
			22	IX
			29	II
			30	IX
			31	II
10	Впровадження і використання стороннього ПЗ	а) комп'ютерні злочинці; б) конкуренти; в) клієнти; д) персонал; г)технічний персонал.	4	I
			5	I
			10	IX
			11	IX
			12	III
			13	II
			14	II
			15	II
			16	IX
			17	II
			18	IX
			21	I
			22	IX
			23	I
			32	I

Примітка. Вразливості наведені у таблиці 2.1.

Перелік виявлених випадкових суб'єктивних загроз в ІТС «Юнайтед колорс» наведено у таблиці 2.3. Де для кожної загрози існують певні джерела

виникнення загрози та відповідні вразливості (таблиця 2.1) з одним чи декількома рівнями небезпеки.

Таблиця 2.3 – Випадкові суб'єктивні загрози в ІТС «Юнайтед колорс»

№ з/п	Загроза	Джерело	Вразливість	Рівень небезпеки загрози
1	Руйнування апаратних ресурсів	а) клієнти; б) персонал; в) технічний персонал.	2	II
			4	X
			5	X
			7	X
			8	III
			23	III
			32	III
			33	II
2	Руйнування програмних ресурсів	а) персонал; б) технічний персонал.	1	IX
			13	II
			14	II
			16	IX
			18	IX
			22	IX
			23	II
			33	II
3	Руйнування інформаційних ресурсів	а) персонал; б) технічний персонал.	1	IX
			13	I
			14	I
			16	IX
			18	I
			22	X
			23	II
			33	II
4	Ненавмисне пошкодження носіїв інформації	а) клієнти; б) персонал; в) технічний персонал.	1	IX
			5	III
			25	IX
			26	III

			33	I
5	Неправомірна зміна режимів роботи ІТС	а) персонал; б) технічний персонал.	16	X
			18	IX
			22	III
			23, 32, 33	II

Продовження таблиці 2.3

№ з/п	Загроза	Джерело	Вразливість	Рівень небезпеки загрози
6	Ініціювання тестуючих або технологічних процесів	а) персонал; б) технічний персонал.	16	X
			18	IX
			22	I
			23	I
			32	I
			33	II
7	Неумисне зараження ПЗ комп'ютерними вірусами	а) персонал; б) технічний персонал.	10	III
			12	I
			13	II
			14	II
			15	X
			16	IX
			18	IX
			19	I
			20	I
			22	I
			23	IX
			26	III
			32	III
			33	II
8	Помилки під час введення інформації в систему (Помилки під час виведення даних із системи)	а) клієнти; б) персонал; в) технічний персонал.	1	IX
			5	II
			6	II
			13	I

			14	I
			16	I
			18	IX
			22	II
			33	I

Продовження таблиці 2.3

№ з/п	Загроза	Джерело	Вразливість	Рівень небезпеки загрози
9	Дії, що можуть призвести до розголошення конфіденційної інформації	а) клієнти; б) персонал; в) технічний персонал.	4	IX
			5	IX
			10	IX
			16	IX
			19	I
			20	I
			21	I
			22	IX
			23	III
			26	IX
			33	X
10	Некомпетентне застосування засобів захисту	а) персонал;	4	I
			5	I
			13	IX
			14	IX
			15	IX
			16	I
			18	I
			22	III
			23	IX
			32	IX
			33	X

Примітка. Вразливості наведені у таблиці 2.1.

Перелік виявлених об’єктивних загроз в ІТС «Юнайтед колорс» наведено у таблиці 2.4. Де для кожної загрози (порушення цілісності чи втрата інформації) існують певні джерела виникнення загрози та відповідні

вразливості (таблиця 2.1) з одним чи декількома рівнями небезпеки. В якості джерел виникнення загроз виступають різноманітні атмосферні явища, збої у подачі електроенергії, пожежа, війна та інші фактора.

Таблиця 2.4 – Об'єктивні загрози в ІТС «Юнайтед колорс»

№ з/п	Загроза	Джерело	Вразливість	Рівень небезпеки загрози
1	Порушення фізичної цілісності та режимів функціонування ІТС	а) атмосферні явища; б) війна; в) забруднення обладнання; г) збої і відмови у роботі обладнання та технічних засобів АС; ґ) збої і відмови у роботі ПЗ; д) збої подачі електроенергії; е) збої у підключенні до мережі інтернет; є) землетрус; ж) обвал дерев; з) пожежа; и) ремонт систем життєзабезпечення; і) терористичний акт;	1	X
			2	III
			3	II
			7	IX
			33	I
			34	X
			35	III
			36	I
2	Втрата інформації	а) атмосферні явища; б) війна; в) забруднення обладнання; г) збої і відмови у роботі обладнання та технічних засобів АС; ґ) збої і відмови у роботі ПЗ; д) збої подачі електроенергії; е) збої у підключенні до мережі інтернет;	1	IX
			2	III
			3	II
			7	IX
			33	I
			34	IX
			35	III
			36	I

		є) землетрус; ж) обвал дерев; з) пожежа; и) ремонт систем життєзабезпечення; і) терористичний акт;		

Примітка. Вразливості наведені у таблиці 2.1.

На підставі виявлених об’єктивних (О), навмисних(НС) та випадкових (ВС) суб’єктивних можливих загроз в ІТС «Юнайтед колорс» по рівню небезпеки загроз (ІХ та Х) визначається перелік можливих загроз для визначених об’єктів захисту (таблиця 1.17).

Визначаються на які властивості інформації (конфіденційність, цілісність та доступність) та системи (спостережність і керованість) впливають певні загрози. Під цими властивостями розглядаються наступні поняття:

1) конфіденційність (К) – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом [1];
2) цілісність (Ц) – властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом [1];
3) доступність (Д) – властивість ресурсу системи (КС, послуги, об’єкта КС, інформації), яка полягає в тому, що користувач і/або процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний [1];
4) спостережність (С) – властивість КС, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об’єктів [1];
5) керованість (КР) – керованість та доступність комп'ютерної системи [10].

Також визначається джерело загрози та найбільш можливі способи здійснення загроз відповідно до переліку складаних виявлених загроз об'єктивної та суб'єктивної природи.

В якості джерел суб'єктивних загроз виступають наступні категорії осіб:

а) комп'ютерні злочинці;

б) конкуренти;

в) клієнти;

г) персонал;

д) технічний персонал.

В якості джерел об'єктивних загроз виступають наступі події та обставини:

а) атмосферні явища;

б) війна;

в) забруднення обладнання;

г) збої і відмови у роботі обладнання та технічних засобів АС;

ґ) збої і відмови у роботі ПЗ;

д) збої подачі електроенергії;

е) збої у підключенні до мережі інтернет;

є) землетрус;

ж) обвал дерев;

з) пожежа;

и) ремонт систем життєзабезпечення;

і) терористичний акт.

Перелік виявлених загроз в ІТС «Юнайтед колорс» не є вичерпаним, та може змінюватися на протязі усієї діяльності підприємства «Юнайтед колорс» у зв'язку з можливими змінами в ІТС «Юнайтед колорс» чи іншими обставинами. Модель загроз дозволяє частково сформувати завдання на створення КСЗІ для ІТС «Юнайтед колорс».

На підставі цих критеріїв створюється модель загроз із зазначенням об'єктів захисту (таблиця 1.17) та джерелом виникнення деяких видів загроз,

загроз з відповідними вразливостями, та властивостями інформації та системи, на котрі впливають ці вразливості в ІТС «Юнайтед колорс», яка наведена у таблиці 2.5.

Таблиця 2.5 – Модель загроз ІТС «Юнайтед колорс»

№ з/п	Об’єкт захисту	Вид загрози	Загроза	Джерело	Вразливість	Властивість інформації			Властивість системи	
						К	Ц	Д	С	КР
1	8 – 13	НС	1	а – д	1	–	+	+	+	+
					2	–	–	+	–	+
2	13	НС	2	а – д	7	–	–	+	–	+
3	1 – 12	НС	4	а – д	4	+	+	–	–	–
					5	+	+	–	–	–
					10	+	–	+	–	–
					11	+	–	+	–	–
					15	+	–	+	–	–
					16	+	–	+	–	+
					22	–	–	–	+	–
4	1 – 12, 14	НС	5	а, б, в, д	10	+	–	–	–	–
					16	+	–	–	+	–
					22	–	–	–	+	–
5	8 – 12	НС	6	а – д	1	+	–	+	+	+
					4, 5	+	–	+	+	+
					26	+	–	+	+	–
6	8 – 12	НС	7	а – д	16	+	–	–	+	–
					22	–	–	–	+	–
7	1 – 12	НС	8	а – д	16	+	–	–	–	–
					22	–	–	–	+	–
					28	+	–	–	–	–

Продовження таблиці 2.5

№ з/п	Об’єкт захисту	Вид загрози	Загроза	Джерело	Вразливість	Властивість інформації			Властивість системи	
						К	Ц	Д	С	КР
8	1 – 10	НС	9	а – д	4	+	–	–	–	–
					5	+	–	–	–	–
					18	+	–	–	–	–
					22	–	–	–	+	–
					30	+	–	–	+	–
9	1 – 10	НС	10	а – д	10	+	–	–	–	–
					11	+	–	–	–	–
					16	+	+	–	+	–
					18	–	+	+	+	–
					22	–	–	–	+	–
10	8 – 12	ВС	1	в – д	4	–	+	+	–	+
					5	–	+	+	–	+
					7	–	+	+	–	+
11	6, 7	ВС	2	г, д	1	–	+	+	–	+
					16	–	+	+	–	+
					18	–	–	+	–	+
					22	–	–	–	+	–
12	1 – 5	ВС	3	г, д	1	–	+	+	+	+
					16	–	+	+	+	+
					22	–	–	–	+	–
13	11, 12	ВС	4	в – д	1	–	+	+	–	–
					25	–	–	+	–	–
14	6 – 10	ВС	5	г, д	16	–	–	+	+	+
					18	–	–	+	+	+

Продовження таблиці 2.5

№ з/п	Об'єкт захисту	Вид загрози	Загроза	Джерело	Вразливість	Властивість інформації			Властивість системи	
						К	Ц	Д	С	КР
15	6 – 10	ВС	6	г, д	16	–	+	+	+	+
					18	–	+	+	+	–
16	6 – 10	ВС	7	г, д	15	–	+	+	–	+
					16	–	+	+	–	+
					18	–	+	+	–	–
					23	–	+	+	–	+
17	1 – 4	ВС	8	г, д	1	–	+	–	–	–
					18	–	+	–	–	–
18	1 – 4	ВС	9	в – д	4, 5	–	–	–	+	–
					10	+	–	–	–	–
					16	+	–	–	+	–
					22	+	–	–	+	–
					26	+	–	–	+	–
					33	+	–	–	–	–
19	1 – 14	О	1, 2	а – і	1, 7, 34	–	+	+	–	+

Примітка. '+' – впливає; '–' - не впливає.

2.1.2 Розробка моделі порушника для ІТС «Юнайтед колорс»

Для ІТС «ГРАДН-КОЛОРС» необхідно визначити перелік можливих порушників. Модель порушника – абстрактний формалізований або неформалізований опис порушника відповідно до НД ТЗІ 1.1-003-1999 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу», в якій потрібно визначати:

1) можливу мету порушника та її градацію за ступенями небезпечності для ІТС;

2) категорії осіб, з числа яких може бути порушник;

3) припущення про кваліфікацію порушника;

4) припущення про характер його дій.

Модель порушника розробляється згідно з рекомендаціями наведеними у НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі».

В якості порушників в ІТС «Юнайтед колорс» можуть виступати наступні категорії осіб:

1) клієнти;
2) комп'ютерні злочинці;
3) конкуренти;
4) персонал;
5) технічний персонал.

Рівні можливостей порушників визначають права, які надані в ІТС «Юнайтед колорс»:

1) перший рівень (І) визначає найнижчий рівень можливостей ведення діалогу з ІТС – можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;
2) другий рівень (ІІ) визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;

3) третій рівень (III) визначається можливістю управління функціонуванням ІТС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;
4) четвертий рівень (IX) визначається повним обсягом можливостей осіб, що здійснюють проектування, реалізацію, впровадження, супроводження програмно-апаратного забезпечення ІТС, аж до включення до складу ІТС власних засобів з новими функціями обробки інформації.

Також порушники в ІТС «Юнайтед колорс» можуть використовувати різні методи і способи для реалізації загроз:

1) використовують виключно агентурні методи одержання відомостей;
2) використовують пасивні технічні засоби перехоплення інформаційних сигналів;
3) використовують виключно штатні засоби ІТС або недоліки проектування КСЗІ для реалізації спроб НСД;
4) використовують способи і засоби активного впливу на ІТС, що змінюють конфігурацію системи (підключення додаткових або модифікація штатних технічних засобів, підключення до каналів передачі даних, впровадження і використання спеціального ПЗ тощо).

Метою порушника можуть бути:

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

Відповідно до приведених вище критеріїв розробляється опис порушників в ІТС «Юнайтед колорс». Модель порушника наведена у таблиці 2.6, але вона може змінюватися на протязі діяльності підприємства, у разі виявлення нових критеріїв та інших обставин.

Таблиця 2.6 – Модель порушника ІТС «Юнайтед колорс»

№ з/п	Категорія осіб	Рівень можливостей	Методи і способи	Мета порушника
1	Клієнти	I	1, 3	1
2	Комп'ютерні злочинці	IX	1, 2, 3, 4	1, 2, 3
3	Конкуренти	II	1, 2, 3	3
4	Персонал	III	3	2
5	Технічний персонал	II	1, 3	3

Модель порушника визначає джерела виникнення загроз та найбільш небезпечні категорії осіб для ІТС «Юнайтед колорс»: комп'ютерні злочинці та конкуренти.

2.2 Розробка концепції політики безпеки інформації ІТС «Юнайтед колорс»

Під політикою слід розуміти сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок обробки інформації [1].

Положення концепції політики безпеки.

Правовими засадами для захисту інформації в автоматизованій системі є чинне законодавство України та нормативні документи із технічного захисту інформації.

Політика безпеки інформації поширюється на усі об'єкти захисту і повинна використовуватися для всіх процесів, та є обов'язковою для усіх користувачів автоматизованої системи «Юнайтед колорс».

Основними принципами політики інформаційної безпеки є підтримання належного захисту інформації із забезпеченням цілісності, конфіденційності та доступності. Це в першу чергу стосується інформації з обмеженим доступом.

Захист інформації в автоматизованій системі реалізовувати у відповідності до вимог технічного завдання та завдань захисту інформації.

Політикою безпеки повинні будуть визначені вимоги до комплексу засобів захисту.

При використанні АС користувачі повинні мати знання у сфері захисту інформації.

Політика переглядається в міру необхідності, але не менше одного разу на рік. Причинами внесення змін в політики є зміни в автоматизованій системі «Юнайтед колорс».

2.3 Розробка часткового технічного завдання на створення КСЗІ В ІТС «Юнайтед колорс»

Також складається часткове технічне завдання на розроблення системи захисту інформації, яке включає вимоги до системи захисту інформації. Вимоги щодо захисту інформації в ІТС «Юнайтед колорс» визначаються відповідно до визначених вимог під час обстеження інформації та моделі загроз, де більша кількість загроз направлена на конфіденційність та цілісність інформації. Тому основними вимогами до системи захисту інформації являються вимоги, які повинні знизити ймовірність реалізації загроз і величину завданих збитків. Для визначення цих вимог (послуг безпеки) складається перелік основних вразливостей системи відповідно до моделі загроз, який наведено у таблиці 2.7.

Таблиця 2.7 – Основні вразливості системи

№ з/п	Вразливість
1	Відсутність резервного копіювання інформації
2	Відсутність резервних апаратних засобів
3	Відсутність безперебійного джерела живлення
5	Використання РС у якості адміністратора
6	Відсутність реєстрації дій і подій у системі
7	Відсутність процедури видалення інформації
8	Відсутність обмеження прав до ПЗ
9	Відсутність процедури зміни паролів для доступу до системи та ПЗ
10	Відсутність навчання у сфері ЗІ

11	Відсутність правил використання та зберігання носіїв інформації
12	Відсутність періодичної перевірки системи пожежної та охоронної сигналізації
13	Відсутність регулярної перевірки системи ПЗ захисту інформації
14	Відсутність перевірки носіїв інформації після підключення до системи

В ІТС «Юнайтед колорс» відповідно до визначених вимог, розробленої моделі загроз та основних вразливостей системи повинні реалізуватися послуги безпеки з підвищеними вимогами до забезпечення конфіденційності і цілісності оброблюваної інформації. Послуги безпеки повинні протистояти вразливостям системи, тому було обрані наступні:

{ КД-2, КА-2, КО-1, ЦД-1, ЦА-2, ЦО-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2 }.

Послуги безпеки, які визначені в даному профілі захищенності, являються обов’язковими для реалізації.

2.4 Вимоги до функціональних послуг безпеки

Викладення вимог до функціональних послуг, які визначено профілем захищености для ІТС «Юнайтед колорс», повинні реалізовуватися відповідно до вимог визначених у НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу».

КД-2. Базова довірча конфіденційність.

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. Керування правами доступу на даному рівні має невисоку вибірковість. Користувач, домену якого належить об'єкт (процес) може вказати, які групи користувачів і, можливо, які конкретні користувачі мають право одержувати інформацію від об'єкта (ініціювати процес). Для такої системи можна

побудувати часткову матрицю доступу користувачів до захищених об'єктів і процесів.

КА-2. Базова адміністративна конфіденційність.

Послуга адміністративна конфіденційність дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від захищених об'єктів до користувачів.

Політика адміністративної конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.

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

Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження

КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта.

КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного процесу через керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес.

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної конфіденційності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту

КО-1. Повторне використання об'єктів.

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

ЦД-1. Мінімальна довірча цілісність.

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 (на рівні розподілу потоків інформації між групами користувачів). Для такої системи можна побудувати часткову матрицю доступу користувачів до захищених об'єктів.

Політика довірчої цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.

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

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

КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту

ЦА-2. Базова адміністративна цілісність.

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. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування аналогічно рівням послуги довірча цілісність з тією відмінністю, що тільки адміністратор або авторизований адміністратором користувач має право включати і вилучати користувачів, процеси і об'єкти до/з конкретних доменів або піддоменів.

ЦО-1. Обмежений відкат.

Відкат є багатосторонньою послугою, що дозволяє відновлюватися після помилок користувача, збоїв програмного забезпечення або апаратури і підтримувати цілісність баз даних, додатків, побудованих на транзакціях і т. ін. Дана послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкатити) захищений об’єкт до попереднього стану. Рівні даної послуги ранжируються на підставі множини операцій, для яких забезпечується відкат.

Мається на увазі, що відкат — завжди доступна автоматизована послуга. Використання відкладеного резервування, що вимагає втручання користувача для завантаження резервного носія, не є реалізацією відкату. Якщо система реалізує дану послугу, то її використання має фіксуватись в журналі. Відміна операції не повинна приводити до видалення з журналу запису про операцію, яка пізніше була відмінена.

НР-2. Захищений журнал.

Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, 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.

НИ-2. Одиночна ідентифікація і автентифікація.

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 будь-якому 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

НК-1. Однонаправлений достовірний канал.

Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ.

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

НО-2. Розподіл обов'язків адміністраторів.

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.

НЦ-2. КЗЗ з гарантованою цілісністю.

Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів.

КЗЗ повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування.

Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

НТ-2. Самотестування при старті.

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.

Для реалізації цих послуг безпеки потрібно обрати засоби захисту інформації.

2.5 Вибір засобів захисту для реалізації профілю захищеності

Для вибору засобів захисту інформації використовується «Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом», в якому визначені функціональні послуги безпеки засобів, реквізити документа, що засвідчує відповідність вимогам НД з ТЗІ та інша інформація.

Для реалізації профілю захищеності треба проаналізувати можливості ПЗ, яке вже використовується в ІТС «Юнайтед колорс». ПЗ антивірусного захисту

ESET NOD32 Antivirus 8, яке вже використовується в ІТС «Юнайтед колорс», що відповідно до статті 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» для створення КСЗІ повинні використовуватися засоби захисту інформації, які мають сертифікат відповідності або експертний висновок.

Перелік функціональних послуг безпеки для засобів захисту інформації наведено у таблиці 2.8.

Таблиця 2.8 – Функціональні послуги безпеки ПЗ

№ з/п	Найменування засобу	Функціональні послуги безпеки	Реквізити документа, що засвідчує відповідність вимогам НД з ТЗІ
1	Операційна система Microsoft Windows 10 Professional	КД-2, КВ-1, КО-1, ЦД-1, ЦА-1, ЦВ-1, ЦО-1, ДР-1, ДЗ-2, ДВ-2, НР-1, НР-2, НИ-1, НИ-2, НК-1, НО-3, НЦ-2, НТ-2, НВ-1	Експертний висновок № 1027 Дійсний до 26.09.2022
2	Програмний комплекс “M.E.Doc”	КА-2, КВ-1, ЦА-1, ЦО-1, ЦВ-1, ДЗ-1, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-2 Рівень гарантій Г-3	Експертний висновок № 1244 Дійсний до 28.05.2024
3	ESET NOD32 Antivirus (ENDpoint security)	КА-2, ЦА-1, ЦА-2, ДС-1, ДЗ-1, ДР-1, ДВ-1, НР-1, НР-2, НИ-1, НИ-2, НК-1, НО-1, НО-2, НЦ-1	Експертний висновок № 1258 Дійсний до 11.06.2024

Функціональні послуги безпеки профілю захищеності повністю реалізуються ПЗ. Перелік послуг безпеки та чим слідує реалізувати ці вимоги до функціональної послуг безпеки наведено у таблиці 2.9.

Таблиця 2.9 – Реалізація вимог послуг безпеки в ІТС «Юнайтед колорс»

№ з/п	Послуга безпеки	Чим реалізовується
1	КД-2	Забороняється запис атрибутів, зміну дозволів і зміну

		власників дисків папок, підпапок та файлів для усіх користувачів в додаткових параметрах безпеки дисків Microsoft Windows 10 Professional
2	КА-2	Розмежування прав в Microsoft Windows 10 Professional, 1С: Підприємство 8.3 та «M.E.Doc IS»
3	КО-1	Авторизація в Microsoft Windows 10 Professional та «1С: Підприємство 8.3»
4	ЦД-1	Забороняється запис атрибутів, зміну дозволів і зміну власників дисків папок, підпапок та файлів для усіх користувачів в додаткових параметрах безпеки дисків Microsoft Windows 10 Professional
5	ЦА-2	Забороняється запис атрибутів, зміну дозволів і зміну власників дисків папок, підпапок та файлів для усіх користувачів в додаткових параметрах безпеки дисків Microsoft Windows 10 Professional
		Розмежування прав в Microsoft Windows 10 Professional надається тільки адміністратору безпеки
		Заборона змін налаштувань ПЗ ЗІ ESET NOD32 Antivirus (ENDpoint security)
6	ЦО-1	Налаштування функцій відновлення системи і дискові простори в Microsoft Windows 10 Professional для резервування інформації. Можливість автоматичного відновлення ситеми у разі збоїв
		Налаштування автоматичного архівування в «1С:Підприємство 8.3»
		Налаштування резервного копіювання в «M.E.Doc IS»
7	НР-2	Використання журналу подій Microsoft Windows 10 Professional для об’єктів захисту та для безпеки системи
		Налаштування журналу реєстрації в «1С: Підприємство 8.3»
		Налаштування журналу реєстрації подій в «M.E.Doc IS»
		Налаштування журналу реєстрації подій в ESET NOD32 Antivirus (ENDpoint security)
8	НИ-2	Використання окремої ідентифікації і автентифікації в Microsoft Windows 10 Professional, «1С:Підприємство 8.3» та «M.E.Doc IS», ESET NOD32 Antivirus (ENDpoint security)
9	НК-1	Функціональні послуги Microsoft Windows 10 Professional, «1С:Підприємство 8.3», «M.E.Doc IS» та ESET NOD32 Antivirus (ENDpoint security), які використовуються для

		початкової ідентифікації і автентифікації

Продовження таблиці 2.9

№ з/п	Послуга безпеки	Чим реалізовується
10	НО-2	Дві адміністративні ролі в Microsoft Windows 10 Professional: адміністратор безпеки (керівник) та системний
11	НЦ-2	Функціональні послуги Microsoft Windows 10 Professional (група користувачів «СИТЕМА»)
12	НТ-2	Функції самотестування при старті Microsoft Windows 10 Professional, «1С:Підприємство 8.3» та «M.E.Doc IS»

Окрім реалізації послуг безпеки профілю захищеності для захисту інформації в ІТС «Юнайтед колорс» рекомендується ввести організаційні і апаратні заходи для реалізації окремих послуг безпеки і захисту інформації щодо наступних взраливостей:

– відсутність навчання у сфері ЗІ: створити програму навчання з захисту інформації;

– відсутність правил використання та зберігання носіїв інформації: зберігати усі носії інформації з ІзОД у керівника в кабінеті;

– відсутність перевірки носіїв інформації після підключення до системи: відключити автозапуск усіх носіїв інформації в Microsoft Windows 10 Professional та перевіряти кожен носій інформації антивірусним ПЗ ESET NOD32 Antivirus (ENDpoint security);

– відсутність періодичної перевірки системи пожежної та охоронної сигналізації: проводити перевірку систем зі згоди охоронного підприємства;

– відсутність регулярної перевірки системи ПЗ захисту інформації: налаштувати щотижневе сканування антивірусним ПЗ ESET NOD32 Antivirus (ENDpoint security);

– відсутність безперебійного джерела живлення: для розрахунку вихідної потужності джерела безперебійного живлення треба визначити максимальну споживану потужність обладнання. Планується використовувати джерела живлення для кожної кімнати окремо. Тому визначається максимальна

споживана потужність обладнання відповідно до документації обладнання, яка наведена у таблиці 2.10.

Таблиця 2.10 – Максимальна споживна потужність обладнання

№ з/п	Місцезнаходження обладнання	Найменування обладнання	Максимальна споживана потужність
1	Кімната 1	PC 1	500 Вт
		Samsung S24R350	25 Вт
		Asus RT-N18U	19 Вт
		Epson L1800	16 Вт
		Всього	560 Вт
2	Кімната 2	PC 2	850 Вт
		Samsung S24R350	85 Вт
		Epson L1800	16 Вт
		Всього	951 Вт
3	Кімната 3	PC 3	500 Вт
		Samsung S24R350	25 Вт
		Epson L1800	16 Вт
		Panasonic KX-TG6611UAB	2,3 Вт
		Всього	543,3 Вт
4	Кімната 4	PC 4	850 Вт
		Samsung S24R350	85 Вт
		Всього	935 Вт

При виборі ІБЖ рекомендується щоб вихідна потужність ІБЖ перевищувала максимальну споживану потужність на 20–30% [12]. Тому розраховується значення вихідної потужності для кожної кімнати по формулі: Вихідна потужність = Максимальна споживана потужність + 20% (2.1) та вибирається ІБЖ. Вибір ІБЖ наведено у таблиці 2.11.

Таблиця 2.11 – Вибір ІБЖ для ІТС «Юнайтед колорс»

№ з/п	Місцезнаходження обладнання	Вихідна потужність	ІБЖ	Вихідна потужність ІБЖ
1	Кімната 1	672 Вт	APC Back-UPS 1100BA	1100 ВА / 660 Вт

2	Кімната 2	1141,2 Вт	FSP EP-2000 (EP2000)	2000 ВА / 1200 Вт
3	Кімната 3	651,96 Вт	APC Back-UPS 1100BA	1100 ВА / 660 Вт
4	Кімната 4	1122 Вт	FSP EP-2000 (EP2000)	2000 ВА / 1200 Вт

Дані ІБЖ дозволять зберегти необхідну інформації після відключення електроживлення в ІТС «Юнайтед колорс»;

– відсутність резервного копіювання інформації: для реалізації резервного копіювання інформації (послуги безпеки ЦО-1) потрібно обрати обладнання, котре буде повторювати ємність носіїв інформації встановлених в РС. Пропонується встановити на кожен РС додатково 250 ГБ SSD.

2.6 Висновок

В спеціальній частині були визначені основні вимоги із захисту інформації в ІТС «Юнайтед колорс» та розроблено часткове технічне завдання на створення КСЗІ.

Були висунуті вимоги до функціональних послуг безпеки профілю захищеності та вибрані засоби захисту інформації для реалізації цих послуг безпеки за допомогою організаційних, програмних та апаратних заходів.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Метою даного розділу є обґрунтування економічної доцільності розробки підсистеми захисту інформації в інформаційно-комунікаційній системі приватного підприємства «Юнайтед колорс». Для досягнення цієї необхідно здійснити наступні розрахунки: капітальні витрати на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов'язані з виготовленням апаратури, приладів, програмного забезпечення; річні експлуатаційні витрати на утримання і обслуговування об'єкта проектування; річний економічний ефект від впровадження запропонованих заходів; показники економічної ефективності впровадження системи захисту на підприємстві.

3.1 Розрахунок (фіксованих) капітальних витрат

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

Витрати на впровадження системи захисту інформації на підприємстві визначаються, виходячи з трудомісткості кожної операції, та належать до капітальних витрат.

Визначення трудомісткості розробки підсистеми захисту інформації в інформаційно-комунікаційній системі підприємства

Трудомісткість розробки системи захисту інформації на підприємстві визначається тривалістю кожної робочої операції, до яких належать наступні:

– тривалість складання технічного завдання на розробку підсистеми захисту інформації в інформаційно-комунікаційній системі підприємства, $t_{тз}$=10 годин;

– тривалість аналізу нормативних документів у сфері інформаційної безпеки, $t_{нд}$=8 години;

– тривалість аналізу загроз інформаційній безпеці, $t_{зі}$=16 години;

– тривалість обрання функціонального профілю захищеності і класу АС, $t_{пз}$=14 години;

– тривалість розробки підсистеми захисту інформації в інформаційно-комунікаційній системі підприємства, $t_{знд}$=42 години;

– тривалість підготування технічної документації для впровадження запропонованих рішень, $t_{д}$=9 години.

– .

Отже,

$$t = t_{тз} + t_{нд} + t_{зі} + t_{пз} + t_{знд} + t_{д} = 10+8+16+14+42+9 = 99 \text{ годин.}$$

Розрахунок витрат на розробку підсистеми захисту інформації в інформаційно-комунікаційній системі підприємства

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

$$К_{рп} = З_{зп} + З_{мч} .$$

$$К_{рп} = З_{зп} + З_{мч} = 18711 + 438{,}57 = 19149{,}57 \text{ грн.}$$

$$З_{зп} = t\, З_{пр} = 99*189 = 18711 \text{ грн.}$$

де t – загальна тривалість розробки політики безпеки, годин;

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

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

$$З_{мч} = t*С_{мч} = 99*4{,}43 = 438{,}57 \text{ грн.}$$

де $t_д$ – трудомісткість підготовки документації на ПК, годин;

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

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = 0,9 \cdot 2 \cdot 1,68 + \frac{4211 \cdot 0,4}{1920} + \frac{5116 \cdot 0,4}{1920} = 4,43 \text{ грн.}$$

Розробка підсистеми захисту інформації в інформаційно-комунікаційній системі приватного підприємства «Юнайтед колорс» реалізована за допомогою використання наявного програмного та апаратного забезпечення, у зв'язку з чим додаткові витрати не виникають.

Витрати на навчання технічних фахівців і обслуговуючого персоналу ($К_{навч}$) складатимуть 2000 грн.

Витрати на встановлення обладнання та налагодження системи ($К_н$) інформаційної безпеки складатимуть 2000 грн.

Таким чином, капітальні (фіксовані) витрати на розробку засобів підвищення рівня інформаційної безпеки складуть:

$$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_н =$$
$$= 19149,57+2000+2000 = 23149,57 \text{ грн.}$$

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

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

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

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

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

$К_н$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки.

3.1.1 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

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

де $С_в$ - вартість відновлення й модернізації системи;

$С_к$ - витрати на керування системою в цілому;

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

Оскільки розробку підсистеми захисту інформації в інформаційно-комунікаційній системі приватного підприємства «Юнайтед колорс» реалізовано за допомогою використання наявного програмного та апаратного забезпечення, у зв'язку з чим додаткові витрати щодо оновлення не виникають.

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

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

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються сукупною величиною витрат на організаційні заходи, які складуть 7000 грн.

Оскільки розробку підсистеми захисту інформації в інформаційно-комунікаційній системі приватного підприємства «Юнайтед колорс» реалізовано за допомогою використання наявного програмного та апаратного

забезпечення, додаткові витрати за амортизаційними відрахуваннями не виникають.

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

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

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

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 18800 грн. Додаткова заробітна плата – 8% від основної заробітної плати. Виконання роботи щодо впровадження системи захисту інформації на підприємстві потребує залучення спеціаліста інформаційної безпеки на 0,25 ставки. Отже,

$$С_з = (18800*12 + 18800*12*0,08)*0,25 = 60912 \text{ грн.}$$

Ставка ЄСВ для всіх категорій платників з 01.01.2021 р. складає 22%.

$$С_{єв} = 60912*0,22 = 13400,64 \text{ грн.}$$

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

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

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=0,85 кВт);

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

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

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

$$С_{ел} = 0,85*2*1920*1,68 = 5483,52 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат – 2% ($С_{тос}$ = 23149,57*0,02=462,99 грн).

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

$$С_к = 7000+60912+13400,64+5483,52+462,99 = 87259,15 \text{ грн.}$$

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = 87259,15 \text{ грн.}$$

3.2 Оцінка можливого збитку

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

Оцінка можливого збитку від атаки на вузол або сегмент мережі

Необхідні *вихідні дані* для розрахунку:

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

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

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 2 години;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 21000 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 18800 грн./міс.;

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

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 6 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 330 тис. грн. на рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин, 600 грн;

I – число атакованих сегментів корпоративної мережі, 1;

N – середнє число атак на рік, 42.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V,$$

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

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

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

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

$$П_{п} = \frac{\sum З_{с}}{F} t_{п} = \frac{18800*6}{176} * 2 = 1281,82 \text{ грн},$$

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

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

$$П_{в} = П_{ви} + П_{пв} + П_{зч},$$

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

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

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

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

$$П_{ви} = \frac{\sum З_{с}}{F} t_{ви} = \frac{18800*6}{176} * 2 = 1281,82 \text{ грн.}$$

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

$$П_{пв} = \frac{\sum З_{о}}{F} t_{в} = \frac{21000*1}{176} * 1 = 119,32 \text{ грн.}$$

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

$$П_{в} = 1281,82+119,32+600 = 2001,14 \text{ грн.}$$

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

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

$$V = \frac{320000}{2080} \cdot (2 + 1 + 2) = 769{,}23 \text{ грн.}$$

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

$$U = 1281{,}82+2001{,}14+769{,}23= 4052{,}19 \text{ грн.}$$

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

$$B = \sum_i \sum_n U = \sum_1 \sum_{42} 4052{,}19 = 170191{,}98 \text{ грн.}$$

3.2.1 Загальний ефект від впровадження системи інформаційної безпеки

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

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

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

R – вірогідність успішної реалізації загрози (70%);

С – щорічні витрати на експлуатацію системи інформаційної безпеки.

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

$$E = 170191,98*0,7 – 87259,15 = 31875,39 \text{ грн.}$$

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Для встановлення економічної ефективності визначають такі показники як: коефіцієнт повернення інвестицій (ROSI) та термін окупності капітальних інвестицій (T_o).

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

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

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

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

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{31875,39}{23149,57} = 1,38 \text{ частки одиниці,}$$

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

$$ROSI > (N_{деп} – N_{інф})/100),$$

де $N_{деп}$ – річна депозитна ставка, (8%);

$N_{інф}$ – річний рівень інфляції, (6%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$1{,}38 > (8 - 6)/100 = 1{,}38 > 0{,}02.$$

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

$$T_o = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{1{,}38} = 0{,}73 \text{ років.}$$

3.4 Висновок

Таким чином, виходячи з наведених розрахунків, розробка підсистеми захисту інформації в інформаційно-комунікаційній системі приватного підприємства «Юнайтед колорс» може вважатися економічно доцільною. Про це свідчить значення коефіцієнт повернення інвестицій (ROSI=1,38), яке є вищим за дохідність альтернативного вкладення коштів (1,38>0,02). При середньорічній величині кількості атак у 42 атаки економічний ефект складатиме 31875,39 грн. за капітальних витрат величиною 23149,57 грн., що дозволяє отримати 1,38 грн. на одну гривню вкладених коштів. Експлуатаційні витрати складають 87259,15 грн.

ВИСНОВКИ

В кваліфікаційній роботі було проведено обстеження інформаційно-телекомунікаційної системи «Юнайтед колорс», визначені об’єкти захисту, складено перелік користувачів системи та визначені їх права.

Проведений аналіз загроз визначив понад 36 вразливостей в системі підприємства. Для реалізації Комплексу заході захисту запропоновані критерії захищеності КД-2, КА-2, КО-1, ЦД-1, ЦА-2, ЦО-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2 які були перевірені на реалізацію в системі. Визначено необхідність реалізації додаткових Організаційних, Програмних та Апаратних засобів для реалізації захисту інформаційно-телекомунікаційної системи «Юнайтед колорс».

ПЕРЕЛІК ПОСИЛАНЬ

1 НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу»;

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

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

4 Сетевое оборудование – RT-N18U – ASUS (Електрон. ресурс) / Спосіб доступу: URL: http://www.asus.com/ru/Networking/RTN18U/. – Загол. з екрана;

5 Epson L1800 – Каталог – Epson Россия (Електрон. ресурс) / Спосіб доступу: URL: http://www.epson.ru/catalog/printers/epson-l1800/;

6 Backup Plus Desktop Drive | Seagate (Електрон. ресурс) / Спосіб доступу: URL:http://www.seagate.com/gb/en/external-hard-drives/desktop-hard-drives/backup-plus-desk/. – Загол. з екрана;

7 Фоторедактор | Скачати Adobe Photoshop Lightroom 5 – Adobe (Електрон. ресурс) / Спосіб доступу: URL: http://adobe.com/ua/products/photoshop-lightroom.html. – Загол. з екрана;

8 Інтернет-банк Приват24 для юридичних осіб - Банк для тих, хто любить Україну (Електрон. ресурс) / Спосіб доступу: URL: https://privatbank.ua/. – Загол. з екрана;

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

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

11 НД ТЗІ 3.7-003 -2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі»;

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	1 Розділ	26	
6	А4	2 Розділ	31	
7	А4	3 Розділ	11	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	
14	А4	Додаток Д	5	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК

на кваліфікаційну роботу бакалавра на тему:
Розробка підсистеми захисту інформації в інформаційно-комунікаційній системі приватного підприємства «Юнайтед колорс»
ст. гр. 125-19ск-1 Котовенка Дениса Євгеновича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на __ сторінках та містить __ рисунків, __ таблиць, __ джерел та __ додатка.

Об'єкт розробки: комплексна система захисту інформації для ІТС приватного підприємства «Юнайтед колорс».

Мета роботи: забезпечення необхідного рівня захисту інформації, яка обробляється в ІТС приватного підприємства «Юнайтед колорс».

У спеціальній частині дана характеристика усіх компонентів ІТС приватного підприємства «Юнайтед колорс»; висунуті основні вимоги щодо захисту інформації в автоматизованій системі. Обґрунтовано вибір засобів захисту інформації.

Розроблений комплекс засобів захисту призначений для використання в ІТС «Юнайтед колорс», з метою захисту відкритої інформації та інформації з обмеженим доступом.

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

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

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

Керівник

ДОДАТОК Д. Ситуаційний план ОІД «Юнайтед колорс»

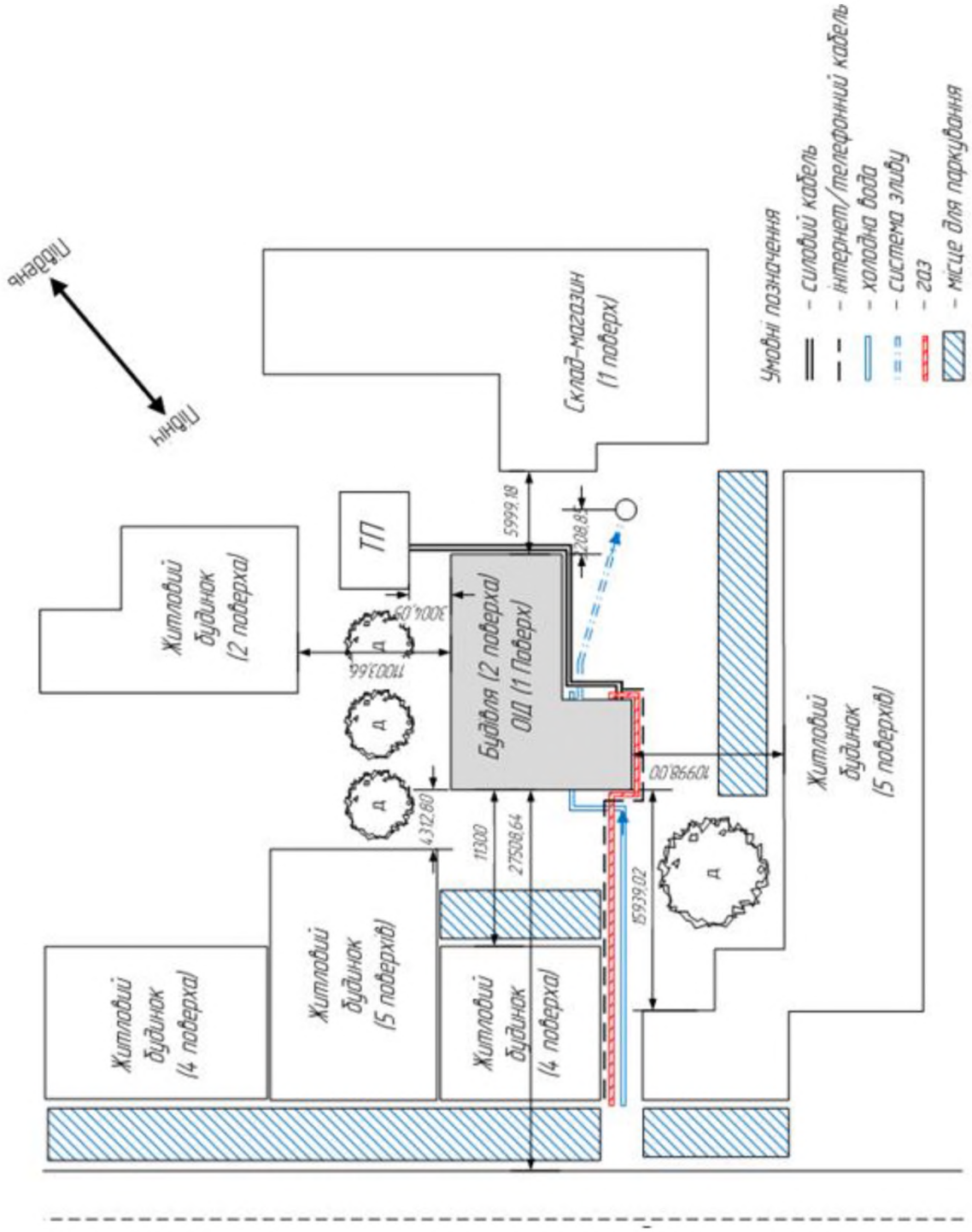


Рисунок 1 – Ситуаційний план ОІД «Юнайтед колорс»

Генеральний план ІОД «Юнайтед колорс»

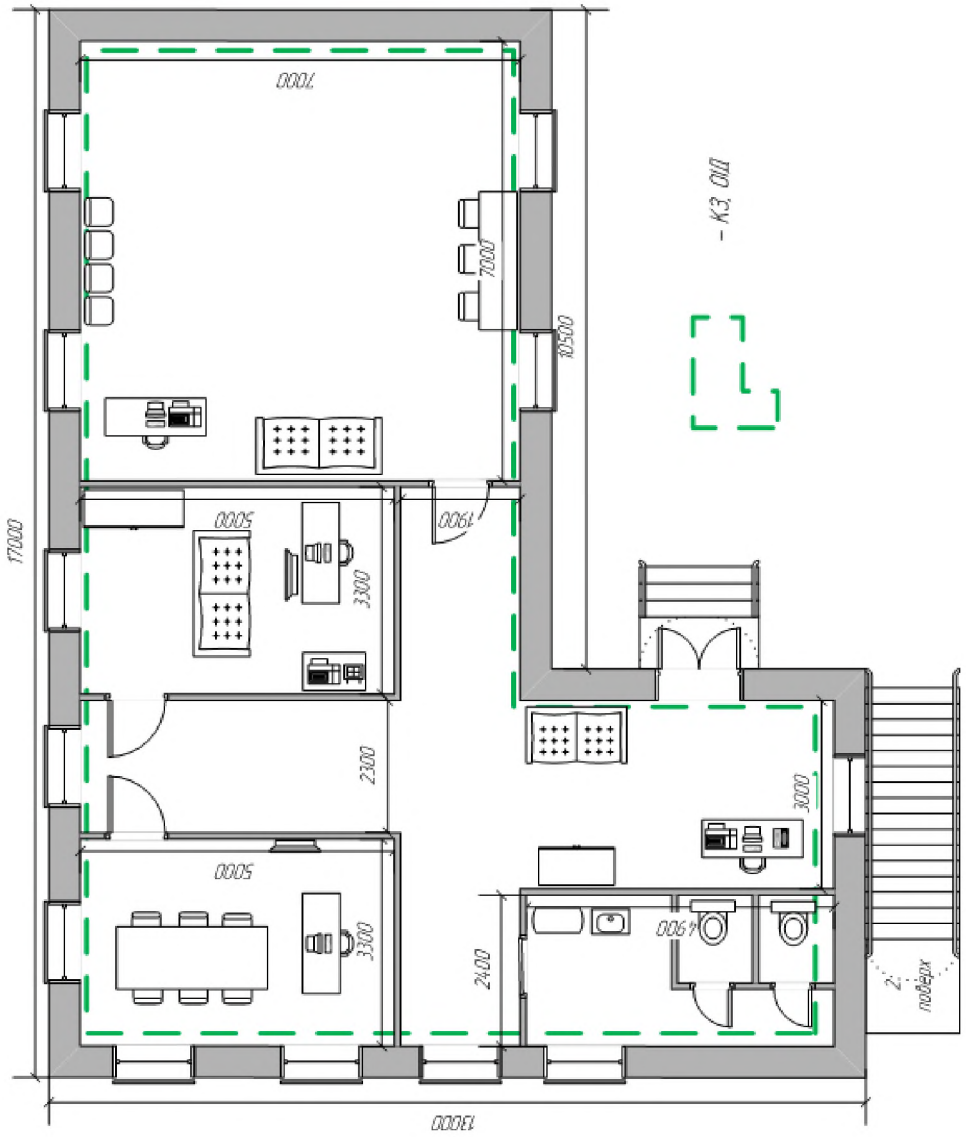


Рисунок 2 – Генеральний план ОІД «Юнайтед колорс»

ДОДАТОК Г. Інші плани ОІД «Юнайтед колорс»

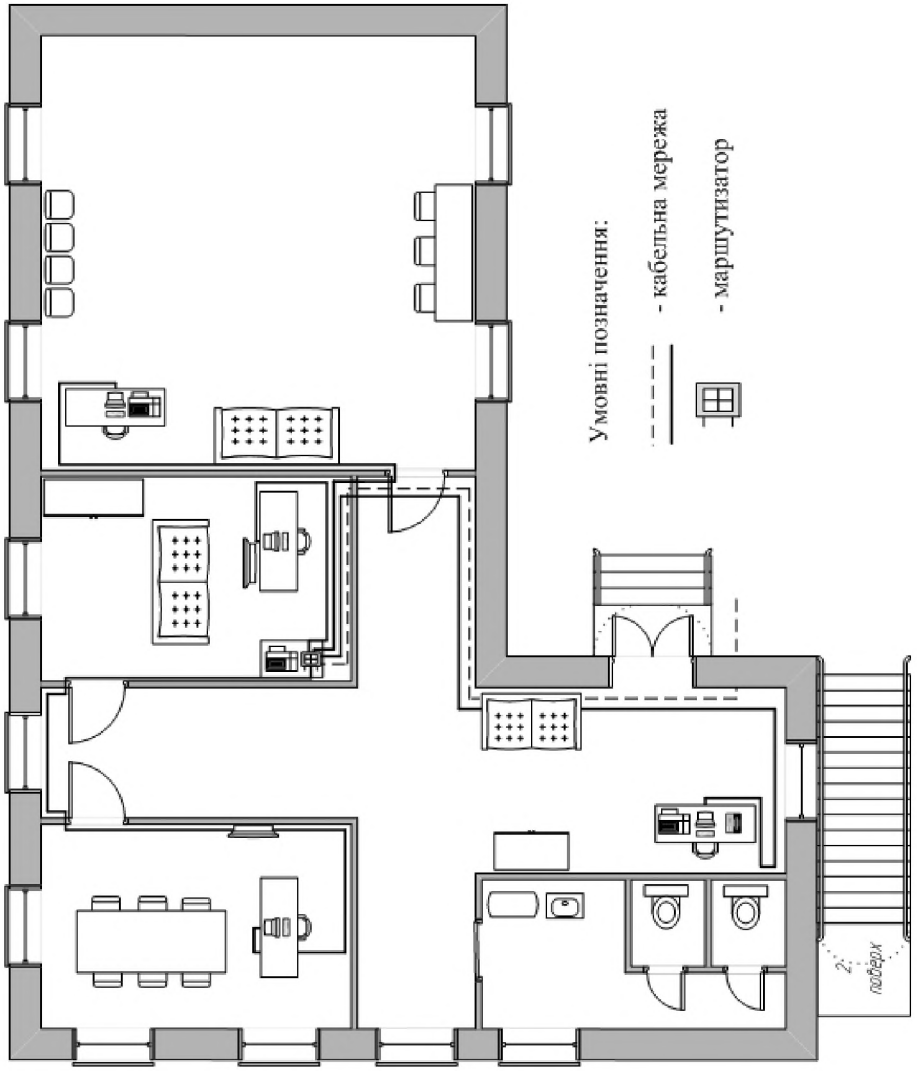


Рисунок 3 – План об'єднання робочих станцій

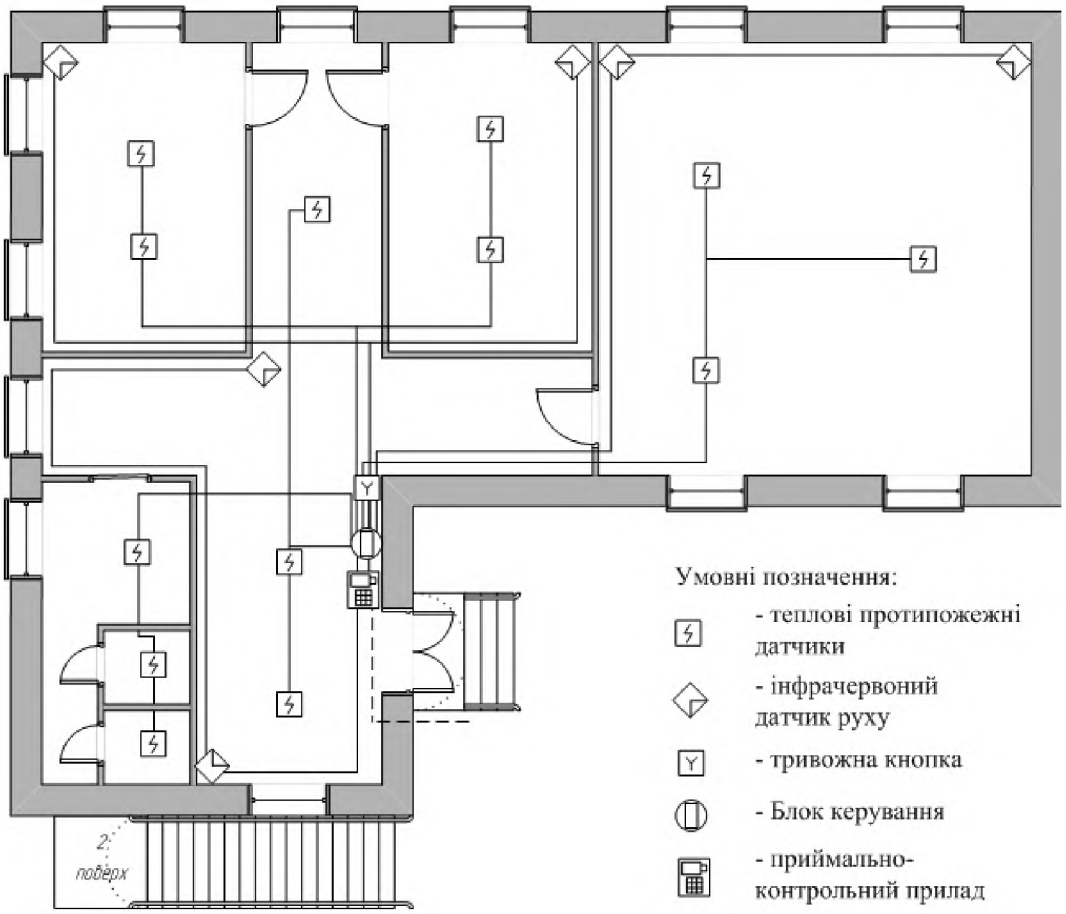


Рисунок 4 – План пожежної та охоронної сигналізації

Умовні позначення:

 - комбіновані протипожежні датчики

 - інфрачервоний датчик руху

 - тривожна кнопка

 - Блок керування

 - приймально-контрольний прилад

 - Лінії зв'язку

 - рабоче місце

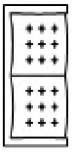
 - маршрутизатор

 - телевізор

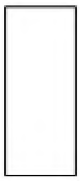
 - принтер

 - телефон

 - газовий котел для опалення

 - диван

 - шафа

 - стіл

 - стут

 - металеві ролети

 - умивальник