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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента	***Хричова Олександра Вадимовича***
академічної групи	***125-18-2***
спеціальності	***125 Кібербезпека***
спеціалізації[1]	
за освітньо-професійною програмою	***Кібербезпека***
на тему	***Комплексна система захисту інформації***
інформаційно-телекомунікаційної системи ТОВ «Reni»	

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	д.т.н., проф. Корнієнко В.І.			
розділів:				
спеціальний	ст. викл. Кручінін О.В			
економічний	к.е.н., доцент Пілова Д.П.	90	Відмінно	

Рецензент				

Нормоконтролер	ст. викл. Тимофєєв Д. С.			

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 ***Хричову О. В.*** **академічної групи** **125-18-2**
(прізвище та ініціали) (шифр)

спеціальності ***125 Кібербезпека***

За освітньо-професійною програмою ***Кібербезпека***

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

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

Розділ	Зміст	Термін виконання
Розділ 1	*Загальні відомості про підприємство «Reni». Обстеження інформаційно телекомунікаційної системи. Аналіз загроз інформації, що циркулює в ІТС підприємства.*	10.05.2022
Розділ 2	*Аналіз існуючого стану послуг безпеки в ІТС, розробка проектних рішень.*	25.05.2022
Розділ 3	*Економічне обґрунтування доцільності витрат пов'язаних з впровадженням запропонованих рішень.*	10.06.2022

Завдання видано_____ Корнієнко В.І.
(підпис керівника) (прізвище, ініціали)
Дата видачі завдання: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Хричов О.В
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 100 с., 7 рис., 15 табл., 5 додатка, 14 джерел.

Об’єкт дослідження: інформаційно - телекомунікаційна система ТОВ «Reni».

Предмет розробки: комплексна система захисту інформації інформаційно - телекомунікаційної системи підприємства ТОВ «Reni».

Метою даної роботи є: розробка проектних рішень для забезпечення захисту інформації, яка обробляється в ІТС ТОВ «Reni», на заданому рівні.

У першому розділі кваліфікаційної роботи наведено загальні відомості про підприємство та визначена необхідність створення КСЗІ. Виконано обстеження середовища функціонування ІТС. А саме: фізичного середовища, обчислювальної системи, інформаційного середовища та середовище користувачів. Розроблено модель порушника та модель загроз.

У спеціальній частині було визначено профіль захищеності та описані реалізовані послуги захищеності в ІТС, а також прийняті організаційно-технічних проектні рішення.

У розділі економічної частини, були зроблені розрахунки фінансових витрат на запровадження обраних проектних рішень, а також щорічну підтримку. На підставі представлених розрахунків було доведено економічну доцільність впровадження обраних рішень.

ІНФОРМАЦІЙНО – ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА, КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ПРОФІЛЬ ЗАХИЩЕНОСТІ, ЕКОНОМІЧНА ДОЦІЛЬНІСТЬ.

ABSTRACT

Explanatory note: 100 p., 7 pic., 15 tab, 5 applications, 14 sources.

Object of research: information and telecommunication system of LLC «Reni».

Subject of development: complex information protection system of information and telecommunication system of LLC «Reni».

The purpose of this work is: development of design solutions to ensure the protection of information processed in the ITS LLC "Reni", at a given level.

In the first section of the qualification work the general information about the enterprise is given and the necessity of creation of CIPS is defined. A survey of the ITS operating environment was performed. Namely: physical environment, computer system, information environment and user environment. A model of the violator and a model of threats have been developed.

In the special part the security profile was defined and the implemented security services in ITC were described, as well as the organizational and technical design decisions were made.

In the section of the economic part, calculations of financial costs for the implementation of selected project solutions, as well as annual support were made. Based on the presented calculations, the economic feasibility of implementing the selected solutions was proved.

INFORMATION - TELECOMMUNICATION SYSTEM, COMPREHENSIVE INFORMATION PROTECTION SYSTEM, THREATS MODEL, VIOLATION MODEL, PROTECTION PROFILE, PROTECTION PROTECTION.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

RAID — (англ. Redundant Array of IndependentDisks — надлишковий масив незалежних (самостійних) дисків)

АРМ — автоматизоване робоче місце;

АС — автоматизована система;

БД — база даних

БФП — багато-функціональний пристрій;

ДСТУ — державний стандарт України;

ЗУ — закон України;

ІзОД — інформація з обмеженим доступом;

ІТС — інформаційно-телекомунікаційна система;

КЗЗ — комплекс засобів захисту;

КСЗІ — комплексна система захисту інформації;

НД ТЗІ — нормативний документ в галузі технічного захисту інформації;

НСД — несанкціонований доступ;

ОІД — об'єкт інформаційної діяльності;

ОС — операційна система.

ПК — персональний комп'ютер;

ПБ — політика безпеки;

ПЗ — програмне забезпечення;

РС — робоча станція;

ТОВ — товариство з обмеженою відповідальністю;

ФС — файловий сервер;

ЗМІСТ

ВСТУП

На сьогоднішній день проблема підтримки необхідного показника безпеки інформації на підприємстві є однією з головних завдань. Так як сфера інформаційних технологій швидко формується, багато організацій використовують ІТС, з цим виникає все більше зловмисників і загроз у сфері інформаційної безпеки.

Безперервне поліпшення комплексної організації безпеки інформації необхідно як самому підприємству так і його клієнтам. Оскільки викрадення, знищення або модифікація інформації може завдати істотної репутаційної та фінансової шкоди організації та її замовникам.

У даній кваліфікаційній роботі розглядається товариство з обмеженою відповідальністю «Reni». Компанія займається розробкою програмного забезпечення. Цей напрям в ІТ-сфері є дуже перспективним і на сьогоднішній день багато фірм реалізується в ньому. Процес створення ПЗ є достатньо складним з точки зору його реалізації. При цьому на різних етапах створення ПЗ циркулює інформація яка становить комерційну таємницю. Звісно для її захисту необхідно приймати певні мірі що до її убезпечення.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1. Загальні відомості про підприємство

Товариство з обмеженою відповідальністю (ТОВ) «Reni» - компанія яка має невеликий штат людей, але активно шукає нових працівників. Фірма займається розробкою програмного забезпечення (ПЗ) для різних сфер бізнесу. «Reni» надають такі послуги:

- розробку програмного забезпечення;
- консалтинг, аудит і менеджмент в сфері розробки програмного забезпечення;
- розробка в середовищі Java;
- розробка в середовищі Ruby on Rails;
- розробка в середовищі PHP;
- тестування програмного забезпечення;
- розробка в середовищі Wordpress.

Компанія веде свою діяльність на протязі 2 років . Директор «Рені» колишній розробник програмного забезпечення в великій компанії. Розробники і системний адміністратор також вихідці з то їж компанії, що і директор. Всі вони ентузіасти своєї справи та ставлять високі вимоги до свого продукту. Тому всі проекти компанії проходять тестування майже на всіх стадіях розробки.

1.2 Підстави створення КСЗІ

Підставою для визначення необхідності створення КСЗІ є норми та вимоги чинного законодавства, які встановлюють обов'язковість обмеження доступу до певних видів інформації, та забезпечення її конфіденційності, цілісності і доступності, або прийняте власником інформації рішення щодо цього, якщо нормативно-правові акти надають йому право діяти на власний розсуд. [6] Вихідні дані для обґрунтування необхідності створення КСЗІ у загальному випадку одержуються за результатами:

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

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

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

Обґрунтування необхідності створення КСЗІ на підприємстві:

На підприємстві циркулює інформація —персональні дані користувачів. Згідно з Законом України «Про захист персональних даних», кожна людина має право на невтручання в особисте життя, у зв'язку з обробкою персональних даних. Вимоги цього закону е підставою для створення КСЗІ на підприємстві.

Крім того, компанія має ще інформацію з обмеженим доступом, яка, відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» та згідно з [4], повинна оброблятися в системі із застосуванням комплексної системи захисту інформації або СУІБ.

Також існує економічна доцільність створення КСЗІ — комерційна таємниця, оскільки інформація, що циркулює на підприємстві, та продукт, що створюється на підприємстві може втратити свою позицію на ринку, якщо вихідний код та база даних будуть перехоплені конкурентами.

На підставі проведеного аналізу приймається рішення про необхідність створення КСЗІ.

1.3 Процес створення КСЗІ.

Процес створення КСЗІ складається з декількох етапів.

1. Процес обстеження ІТС. Складається з опису підприємства, середовища функціонування ІТС. Виявлення в ІТС елементів, що можуть так чи інакше вплинути на безпеку інформації в цілому.

2. Процес аналізу загроз та побудови моделі порушника. Відповідно до НД ТЗІ 1.1-003-99 "Термінологія вгалузі захисту інформації в комп'ютерних системах від несанкціонованого доступу" [5] загроза —будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків АС.

Загрози для інформації, що обробляється в АС, на сам перед залежать від характеристик ОС, фізичного середовища, персоналу, технологій обробки та інших чинників і можуть мати суб'єктивну об'єктивну або об'єктивну природу. Мають бути визначені основні види загроз для безпеки інформації, які можуть бути реалізовані стосовно АС і повинні враховуватись в побудові моделі загроз.

1.4 Обстеження ІТС

1.4.1 Обстеження фізичного середовища ІТС

ОІД знаходиться в приміщенні товариства з обмеженою відповідальністю (ТОВ) «Reni» за адресою: Україна, м. Дніпро, вул. Старокозацька, 51. Ситуаційний план наведено на рис. 1. Будівля, в якій знаходиться ОІД, що обстежується, має вісім поверхів і збудована з цегли та бетонних конструкцій, яка утеплена окремим спеціальним покриттям та зовні ще покрита декоративними алюмінієвими пластинами. Дах будівлі виконаний пласким з бетонних конструкцій з покриттям . В будівлі є підземний паркінг. Ситуаційний план наведено на рис. 1.1.

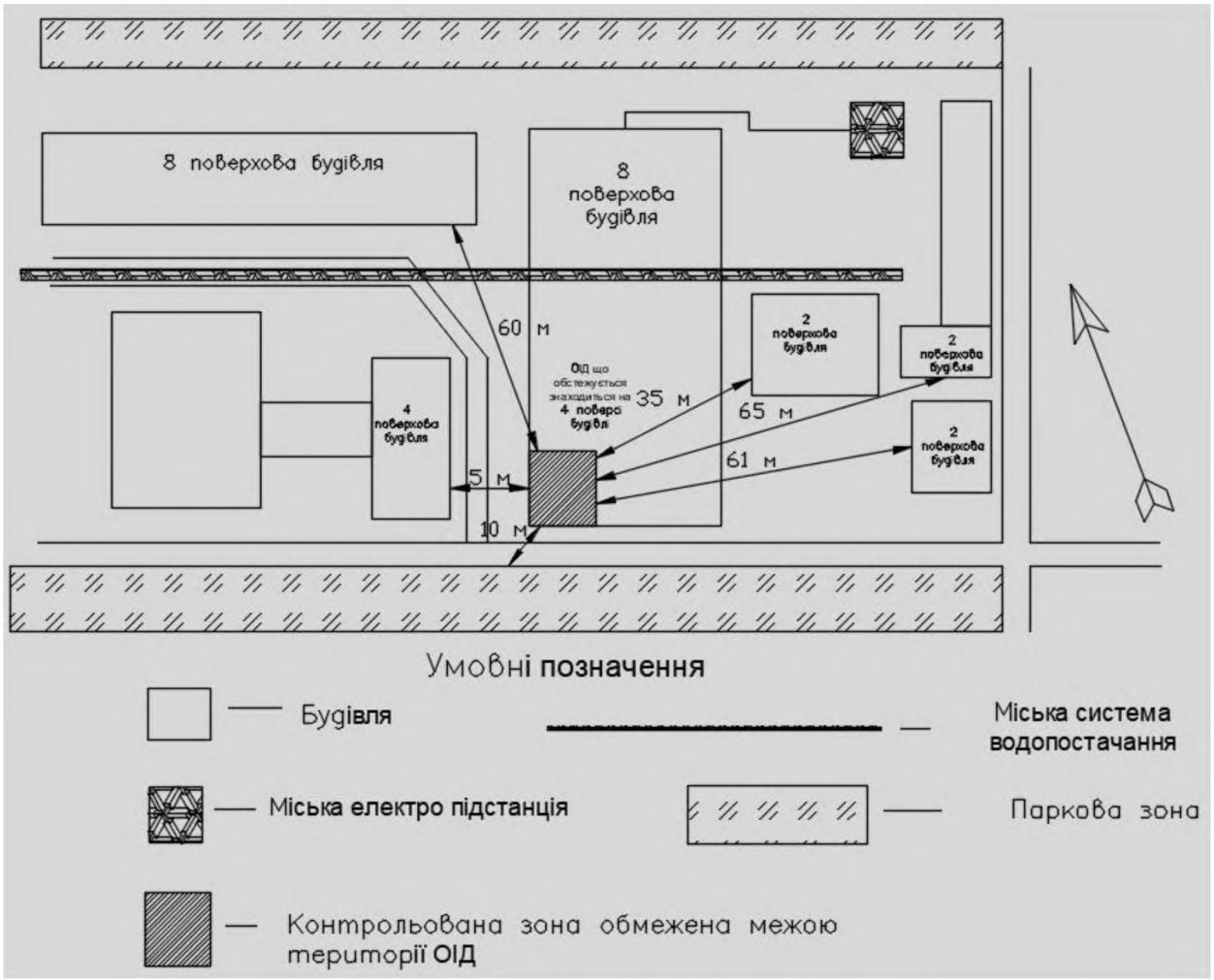

Рисунок 1.1. - Ситуаційний план

Інформація, що до характеристик будівель і споруд приводиться в табл. 1.1.

Таблиця 1.1. - Характеристика будівель та споруд.

№	Найменування	Кіль-кість повер-хів	Адреса	Від-стань до ОІД, м	Напрям
1	Жила будівля	2	Вул. Андрія Фабра, 16	61	Південний-схід
3	Адміністративна будівля	4	Вул. Старокозацька, 52	5	Північний-захід
4	Адміністративна будівля	2	Вул. Старокозацька, 50	35	Північний-схід
5	Жила будівля	3	Вул Андрія Фабра, 14	65	Схід
6	Жила будівля	8	Вул. Старокозацька, 52б	60	Північний-захід
7	Паркова зона			70	північ
8	Паркова зона			10	Південний-захід

ОІД, що обстежується, знаходиться на четвертому поверсі:

- стіни ОІД зроблені з пінобетонної цегли 220 мм., яка утеплена окремим спеціальним покриттям (таким як утеплюють будівлі) та зовні ще покрита декоративними алюмінієвими пластинами;
- підлога та стеля мають бетонні конструкції близько 30 см. товщини;
- в середині кімнати розмежовуються гіпсокартонними стінами;
- ОІД має один вхід\вихід, на якому встановлені посилені вхідні металеві двері шириною 90 см. та товщиною 7 см.

Режим доступу до будівлі в якій знаходиться ОІД контролюється завдяки КПП з охоронцем на першому поверсі будівлі, який здійснює пропуск з застосуванням системи контролю доступу, у вигляді турнікетної системи та за пред'явленням пропуску, а також веде спостереження через монітори на які транслюється відео з камер спостереження. Камери встановлені на фасаді будівлі і направлені на головний вхід. Також камери встановлені у підземному паркінгу

та направлені на в'їзд/виїзд, на двері ліфту шо веде на поверхи будівлі. Сторонні особи без перепустки пропускаються тільки за попередніми домовленостями з робітниками офісів.

До приміщення в, якому безпосередньо знаходиться ОІД, доступ в робочій час контролюється завдяки електромеханічному замку, який встановлений на вхідній двері в приміщення і відмикається завдяки магнітному ключу-карті, який є у всіх працівників офісу. Також на дверях стоїть дверний дзвінок з камерою, відео з якої виводиться на екран домофонної системи в середині офісу. Відвідувачів пропускають, використовуючи дистанційне відкриття з монітору домофонної системи, встановленої в середині приміщення біля вхідної двері офісу. Директор має ключі від кожного приміщення. Охоронець на КПП теж має ключі до вхідних дверей в приміщення, це потрібно для доступу у приміщення при виникненні надзвичайних ситуацій.

В неробочій час контроль доступу до приміщення забезпечується завдяки встановленій в приміщенні системі охорони. Доступ в середину приміщення додатково обмежується вхідними броньованими дверями, які мають циліндровий штифтовий замок із захисною накладкою. Такий замок зазвичай має середню секретність. Цей замок має не надто високу стійкість до злому, може розкриватись відмичками, або шляхом виламування циліндра розвідним ключем, чи ломом. Також на вхідних дверях стоїть електромеханічний замок який також додає надійності. А також всі двері всередині мають циліндровий штифтовий замок як і на вхідних дверях.

В ОІД три двері в середині пластикові не прозорі, двері які ведуть на балкон — скляні. Кожен робітник має ключі від вхідних дверей та магнітні картки для відкриття електромеханічного замку . Директор має ключі від кожного приміщення.

В приміщені є сім віконних отвори, вікна однокамерні, металопластикові. На всіх вікнах встановлені жалюзі. В основній кімнаті стоїть одне велике вікно, в кімнаті директора встановлено три вікна : одне глухе біля входу в кабінет ,одне з західної сторони і глухе вікно біля виходу на балкон. В кабінеті бухгалтера стоїть

два глухих вікна одне біля вхідних дверей в кабінет ,інше біля виходу на балкон. В переговорній стоять два глухих вікна біля виходу на балкон.

З східної сторони знаходиться сусіднє приміщення, яке розташовані перед вхідними дверима і представляє з себе сходовий проліт 3м на 4м і веде на нижні поверхи. З північної сторони через стіну знаходиться приміщення іншої організації.

На ОІД присутні такі системи: система електропостачання та освітлення на рис. 1.3, систем вентиляції та кондиціювання представлено на рис. 1.5, систем охоронної та пожежної сигналізації представлено на рис. 1.6. А також присутня автоматична телефонна станція лінії якої зображені на рис. 1.4 разом з лініями комп'ютерної мережі.

За межі ОІД, виходить лінії систем водопостачання, опалення, електроживлення, освітлення та інтернету.

Лінії освітлення та електроживлення йдуть спочатку до розподільчого щитка в офісі, потім до спільного етажної електрощитової розташованої у коридорі ОІД а далі до головного електричного щитка у підвальному приміщенні будівлі. З електричного щитка лінії освітлення та електроживлення йдуть в трансформаторну підстанцію, що знаходиться в парковій зоні на півночі.

В будівлю заведено оптичний кабель зв'язку який підключено до комутатора у підвалі будівлі і розведено до кожного поверху з клієнтами провайдера.

Підприємство використовує систему вентиляції і кондиціювання також для опалення, рис. 1.5.

Система охорони на ОІД була встановлена охоронною фірмою і обслуговується її фахівцями. Зв'язок з пультом охорони відбувається за допомогою GSM.

Генеральний план наведено на рис. 1.2.

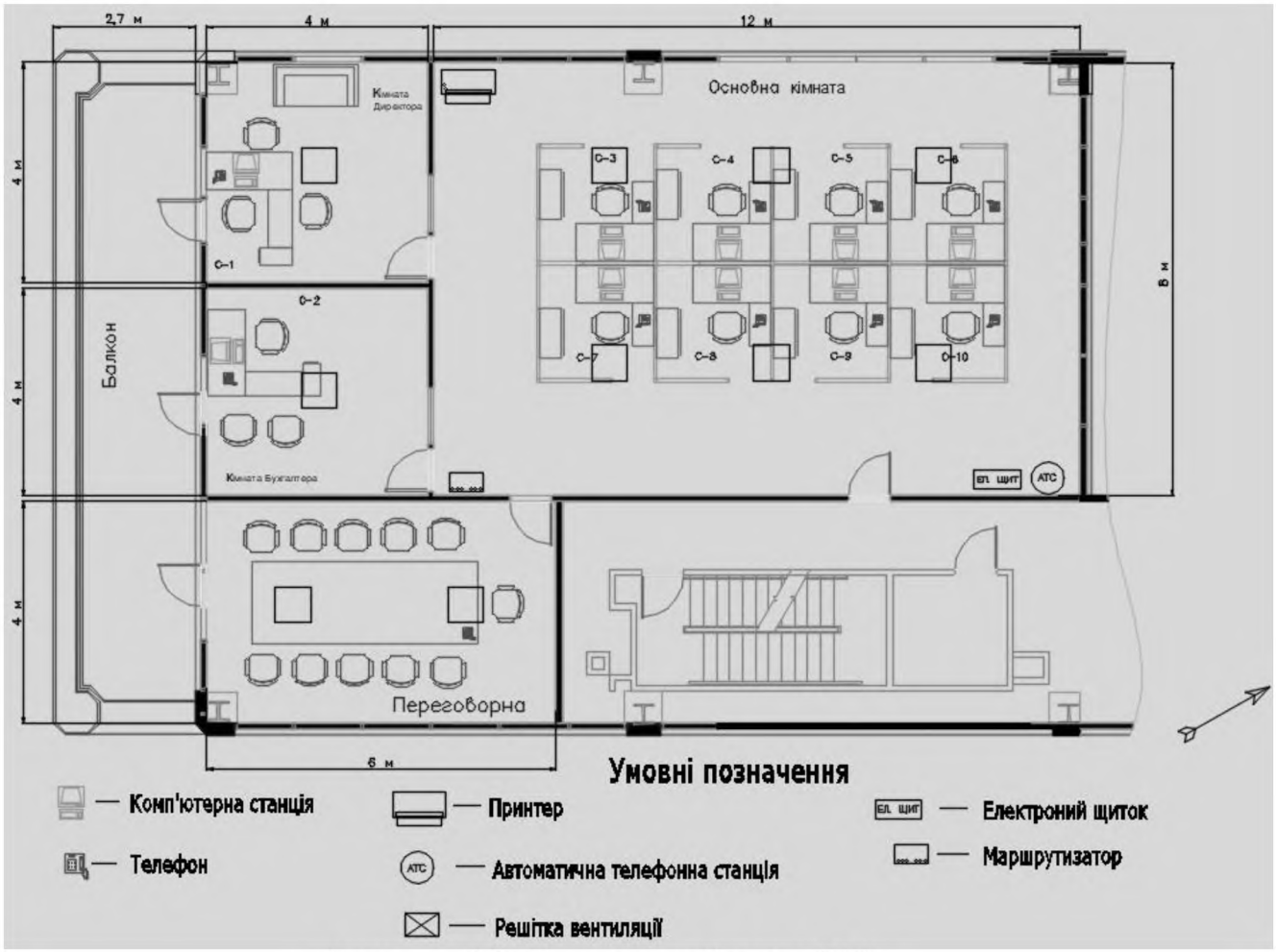

Рисунок 1.2. Генеральний план ОІД.

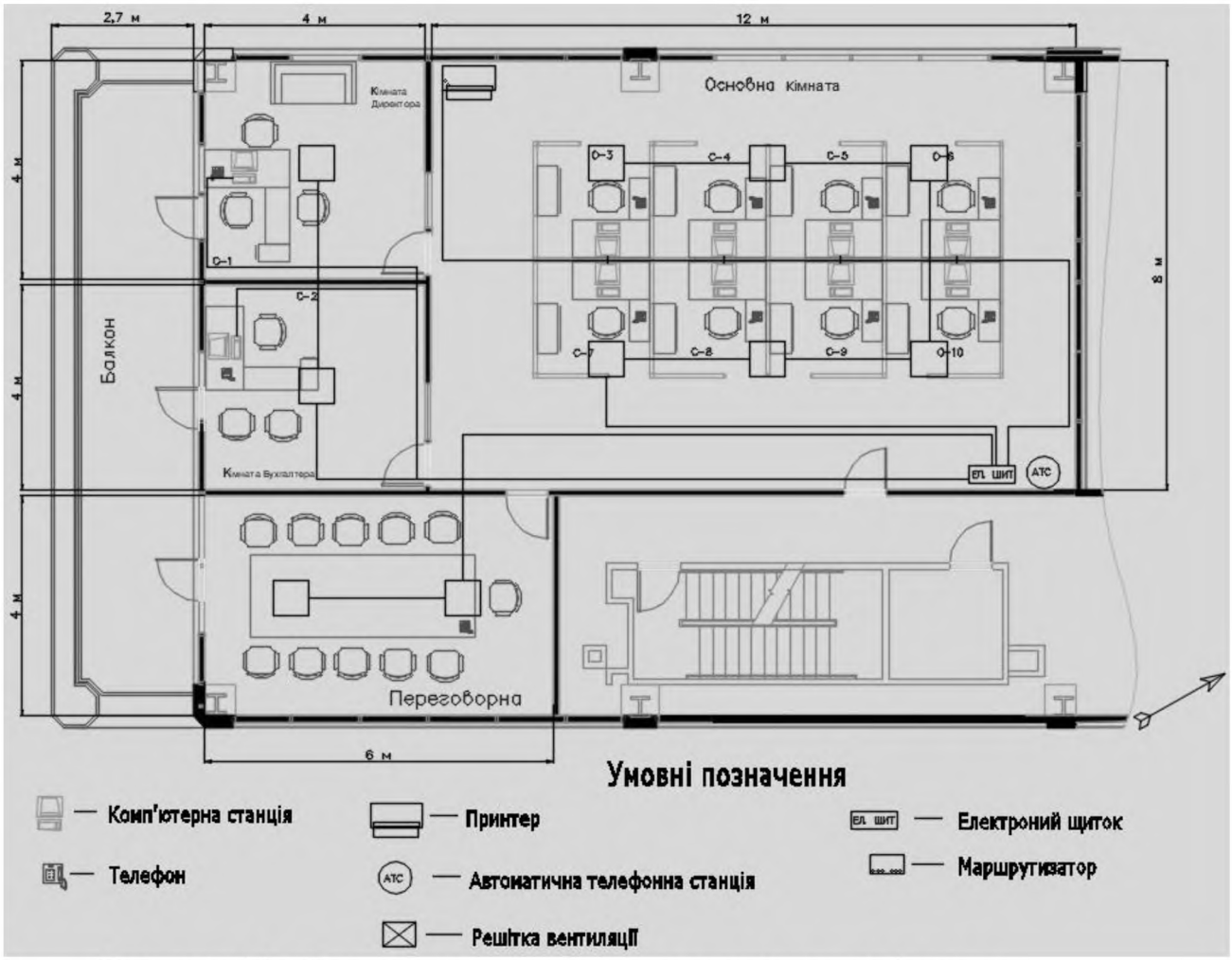

Рисунок 1.3. Схема системи електропостачання, освітлення .

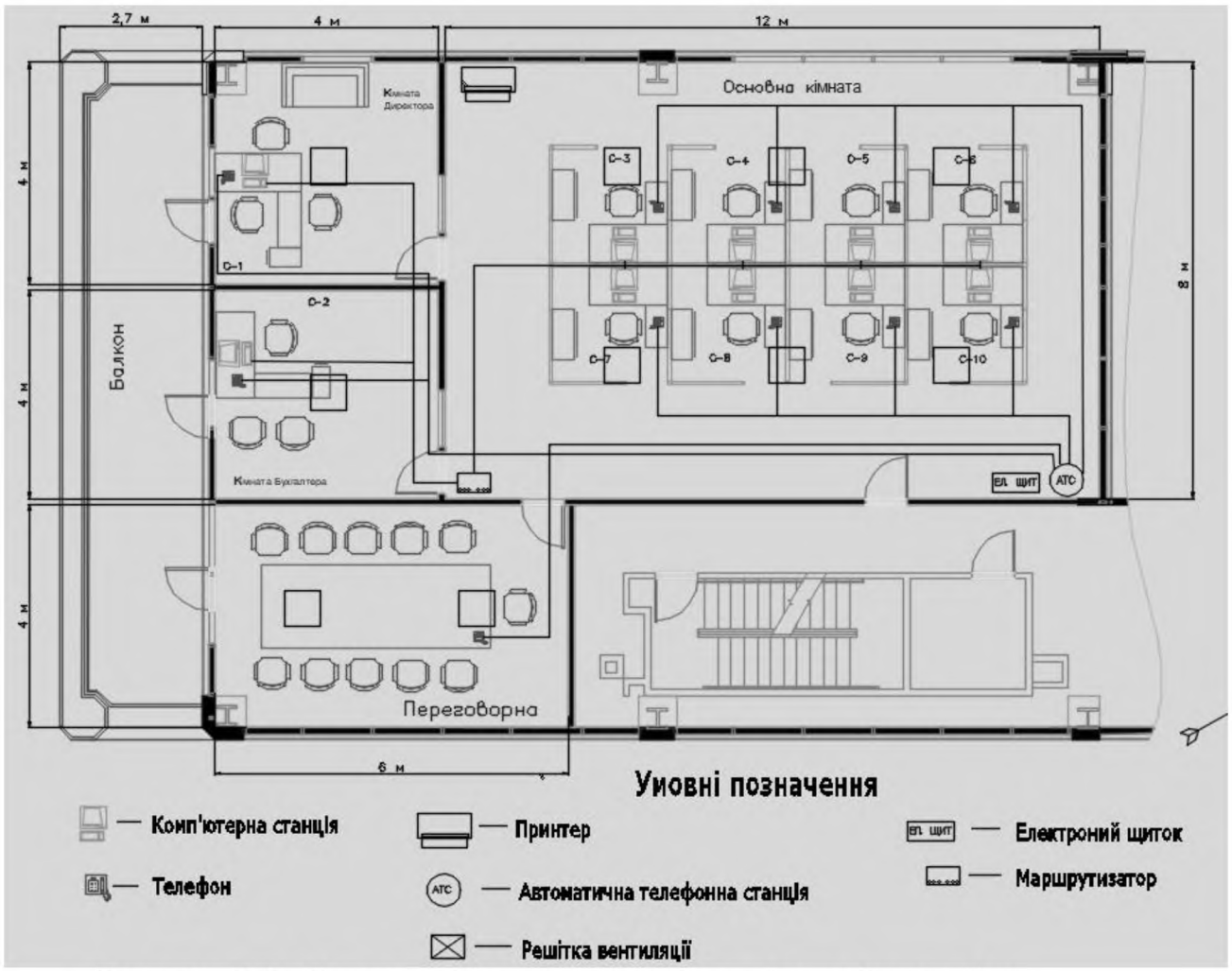

Рисунок 1.4. Схема ліній автоматичної телефонної станції та комп’ютерної мережі.

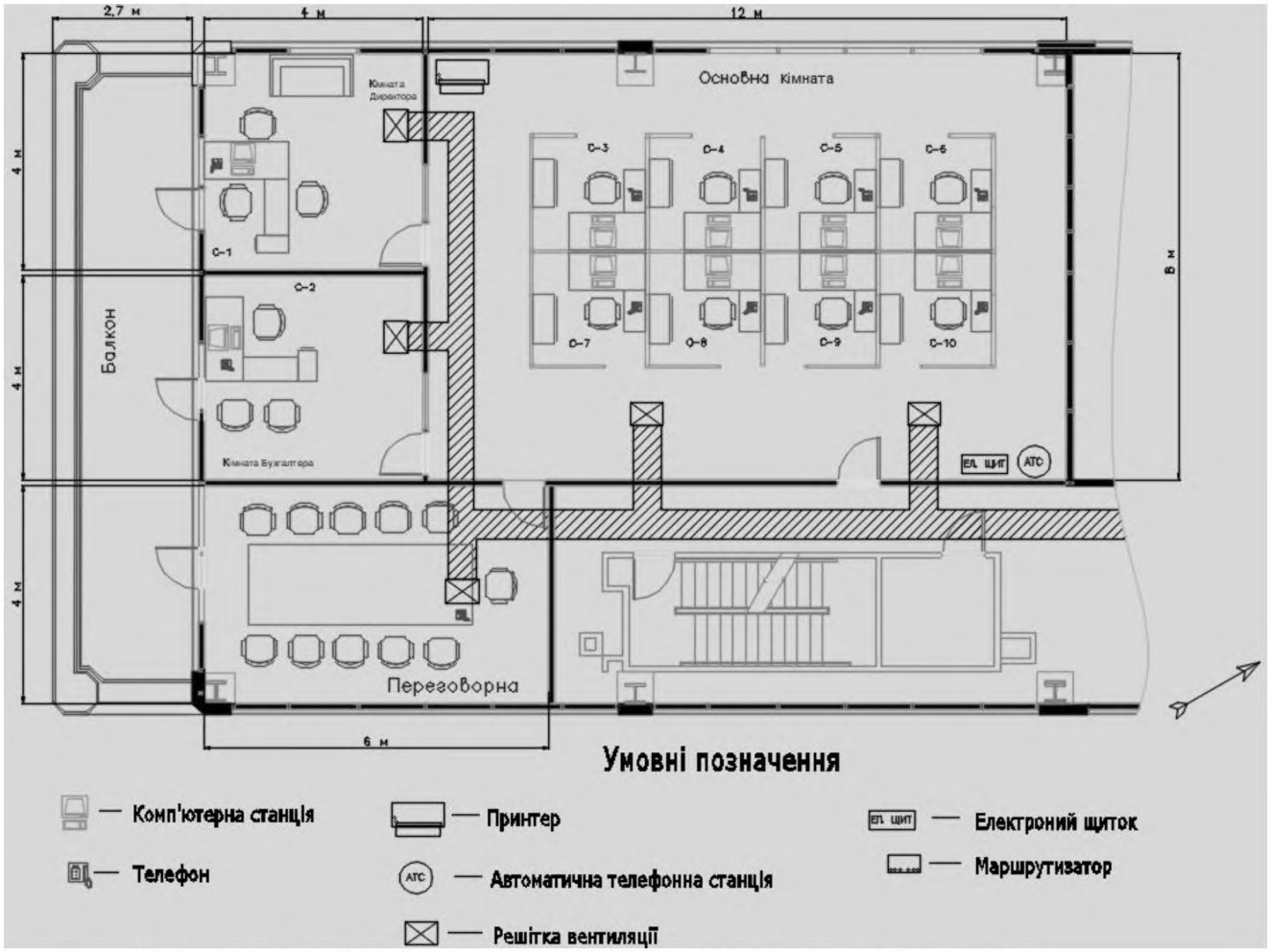

Рисунок 1.5. Схема системи вентиляції та кондиціювання.

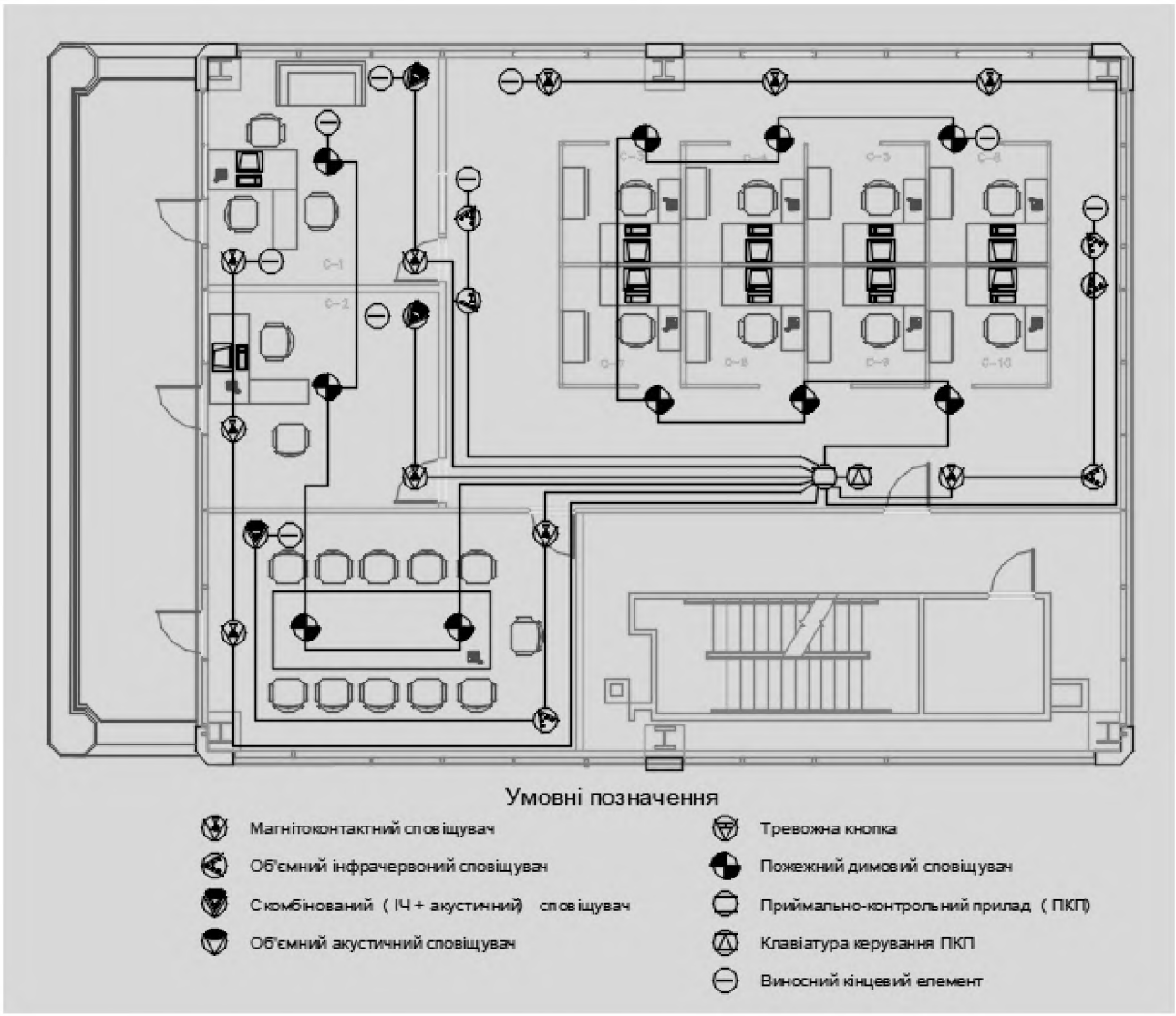

Рисунок 1.6. Схема системи охоронної та пожежної сигналізації.

Інформацію, що до основних технічних засобів підприємства та їх розташування описані в табл. 1.2

Таблиця 1.2. - Основні технічні засоби та їх розташування

№	Назва	Умовне позначення	Серійний номер	Розміщення	Відстань до меж ОІД, м
1	Маршрутизатор MikroTik RB3011UiAS-RM	R1	M125DO85455	Кімната директора	1.50

Продовження таблиці 1.2

№	Назва	Умовне позначення	Серійний номер	Розміщення	Відстань до меж ОІД, м
2	Монітор HP EliteDisplay E232	С1	125224T76RR	Кімната директора на столі	0,40
	Системний блок ARTLINE Business B27 v10		UTY13UT76R	Кімната директора на підлозі	0,40
	Клавіатура 2E KS 101		445656C	Кімната директора на столі	0,40
	Миша Jedel 602 Wireless		45I5467	Кімната директора на столі	0,40
3	Монітор HP EliteDisplay E232	С2	CC5224T76RR	Кімната бухгалтера на столі	0,40
	Системний блок ARTLINE Business B27 v10		1TY111T76R	Кімната бухгалтера на підлозі	0,40
	Клавіатура 2E KS 101		4555467	Кімната бухгалтера на столі	0,40
	Миша Jedel 602 Wireless		AAI5467	Кімната бухгалтера на столі	0,40

Продовження таблиці 1.2

№	Назва	Умовне позначення	Серійний номер	Розміщення	Відстань до меж ОІД, м
4	Монітор HP EliteDisplay E232	C3,C4	456AAR0013	Основна кімната на столі	1,50
	Системний блок ARTLINE Business B27 v10		56C52R0013	Основна кімната на підлозі	1,50
	Клавіатура Rapoo E1050		442256C	Основна кімната на столі	1,50
	Миша Jedel 602 Wireless		225I5467	Основна кімната на столі	1,50
5	Монітор HP EliteDisplay E232	C5,C6,C7	4561110013-16(C4-C7)	Основна кімната на столі	1,50
	Системний блок ARTLINE Business B27 v10		56C5770013-16 (C4-C7)	Основна кімната на підлозі	1,50
	Клавіатура Rapoo E1050		75116C1-4(C4-C7)	Основна кімната на столі	1,50
	Миша Jedel 602 Wireless		8995115-9(C4-C7)	Основна кімната на столі	1,50

Продовження таблиці 1.2

№	Назва	Умовне позначення	Серійний номер	Розміщення	Відстань до меж ОІД, м
6	Монітор HP EliteDisplay E232	C8,C9,C10	JNCAAR0013-15(C8-C10)	Основна кімната на столі	1,50
	Системний блок ARTLINE Business B27 v10		SSAAR00135-17(C8-C10)	Основна кімната на підлозі	1,50
	Клавіатура Rapoo E1050		335656C1-3(C8-C10)	Основна кімната на столі	1,50
	Миша Jedel 602 Wireless		233I5887-9(C8-C10)	Основна кімната на столі	1,50
7	Багатофункціональний пристрій Canon PIXMA E414	P1	JNCAAR0013	Основна кімната біля стінки на шухлядці.	0

Відомості про допоміжні технічні засоби підприємства та їх розташування описані в табл. 1.3

Таблиця 1.3. – Допоміжні технічні засоби та їх розташування

Засіб	Назва	Номер	Розташування
ПКП	INTEGRA-24	C23E40H96	Зліва від головного входу/виходу

Продовження таблиці 1.3

Засіб	Назва	Номер	Розташування
Клавіатура ПКП		C23E15H96	Зліва від головного входу/виходу
Магнітоконтактний	ЭЛЕКТРОН ЕСМК-1	UJG45HLG	Встановлений на головних дверях (основної кімнати)
Магнітоконтактний	ЭЛЕКТРОН ЕСМК-1	236iOI1	На вікні офісу (основної кімнати)
Магнітоконтактний	ЭЛЕКТРОН ЕСМК-1	380HKMW	На вікні офісу (основної кімнати)
Магнітоконтактний	ЭЛЕКТРОН ЕСМК-1	389HNM4	На вікні офісу (основної кімнати)
Магнітоконтактний	ЭЛЕКТРОН ЕСМК-1	C23E40H96	На дверях кімнати директора компанії
Магнітоконтактний	ЭЛЕКТРОН ЕСМК-1	C27658989	На дверях виходу на балкон у кімнати директора компанії
Магнітоконтактний	ЭЛЕКТРОН ЕСМК-1	HSC23E496	На дверях кімнати бухгалтера
Магнітоконтактний	ЭЛЕКТРОН ЕСМК-1	C267867969	На дверях виходу на балкон у кімнати бухгалтера компанії
Магнітоконтактний	ЭЛЕКТРОН ЕСМК-1	C23D12TE	На дверях кімнати переговорів
Магнітоконтактний	ЭЛЕКТРОН ЕСМК-1	C54448869	На дверях виходу на балкон у кімнати переговорів

Подовження таблиці 1.3

Засіб	Назва	Номер	Розташування
Пожежний датчик	Артон СПД-3.4 (ИПД-3.4)	H2172H91	Над робочим місцем (основної кімнати)
Пожежний датчик	Артон СПД-3.4 (ИПД-3.4)	H2172H92	Над робочим місцем (основної кімнати)
Пожежний датчик	Артон СПД-3.4 (ИПД-3.4)	H2172H93	Над робочим місцем (основної кімнати)
Пожежний датчик	Артон СПД-3.4 (ИПД-3.4)	H2172H94	Над робочим місцем (основної кімнати)
Пожежний датчик	Артон СПД-3.4 (ИПД-3.4)	H2172H95	Над робочим місцем (основної кімнати)
Пожежний датчик	Артон СПД-3.4 (ИПД-3.4)	H2172H96	Над робочим місцем (основної кімнати)
Пожежний датчик	Артон СПД-3.4 (ИПД-3.4)	H27234CH96	Над робочим місцем бухгалтера
Пожежний датчик	Артон СПД-3.4 (ИПД-3.4)	H7T4CH96	Над робочим місцем директора
Пожежний датчик	Артон СПД-3.4 (ИПД-3.4)	15T4CH96	Над столом в переговорній
Пожежний датчик	Артон СПД-3.4 (ИПД-3.4)	H704CH96	Над столом в переговорній
Інфрачервоний датчик	CROW SWAN PGB	NJJ37NQ151	В правому нижньому куті кімнати (основної кімнати)

Продовження таблиці 1.3

Засіб	Назва	Номер	Розташування
Інфрачервоний датчик	CROW SWAN PGB	NJJ62Q151	В основній кімнаті на північній стіні та направлений на вхідні двері
Інфрачервоний датчик	CROW SWAN PGB	NJJ345716	В основній кімнаті на північній стіні та направлений на вікна
Інфрачервоний датчик	CROW SWAN PGB	NJAHNJ2351	В основній кімнаті на південній стіні та направлений на вікна
Інфрачервоний датчик	CROW SWAN PGB	NJAHNJ2351	В основній кімнаті на південній стіні та направлений на двері переговорної
Інфрачервоний датчик	CROW SWAN PGB	NJJ3HJAJKLN151	В переговорній кімнаті в правому нижньому куті
Комбінований	SATEL NAVY	HJNKJQ150	В правому верхньому куті кімнати директора
Комбінований	SATEL NAVY	HJNKJQ164	В правому верхньому куті кімнати бухгалтера

Продовження таблиці 1.3

Засіб	Назва	Номер	Розташування
Телефон Panasonic	Panasonic KX-NT511ARUB	DDGLLJ6543	Телефони розташовані на столі у кожного працівника і в переговорній кімнаті (кількість 11 штук)
Автоматична телефонна станція	PANASONIC KX-HTS824	JNGFY00425	В нижньому правому куті основної кімнати

1.4.2 Обстеження обчислювальної системи

Доступ в відповідну мережу можливий зазвичай тільки за умови, що операційна система ПК буде завантажена з використанням логіна (облікового запису користувача), для якого авторизований.

Всі ПК об'єднані в локальну обчислювальну мережу. Всі користувачі об’єднані в одному домені Reni.

В локальній мережі існує підключення до мережі Internet. Канал зв’язку в межах корпоративної мережі та підключення до Internet забезпечує провайдер «Kyivstar», який надає послуги з побудови, надання та підтримки відомчої телекомунікаційної мережі у відповідності до Договорів між «Reni» та «Kyivstar».

Обладнання АС, за допомогою якого обробляється інформація на ОІД:

- робоча станція директора;
- робоча станція бухгалтера;
- робочі станції системного адміністратора;
- файловий сервер;
- робочі станції розробників;
- робочі станції тестувальників.

Спосіб з'єднання мережевих пристроїв за топологією відноситься до типу зірка. Всі комп'ютери мережі приєднані до центрального вузла, тобто маршрутизатора SMB, а від нього до мереживної карти комп`ютера.

На робочій станції С4 реалізований файловий RAID масив рівня 5. На нього працівники зберігають резервні копії своїх проектів . Станцію С4 також можно використовувати як звичайний робочу станцію для виконя робіт розробника або тестувальника. Ключ доступу до серверного масиву має директор та системний адміністратор. Для кожного працівника в середині масиву розмежований доступ до папок та файлів.

Всі комп’ютери в ІТС опломбовані, за договором гарантійного обслуговування.

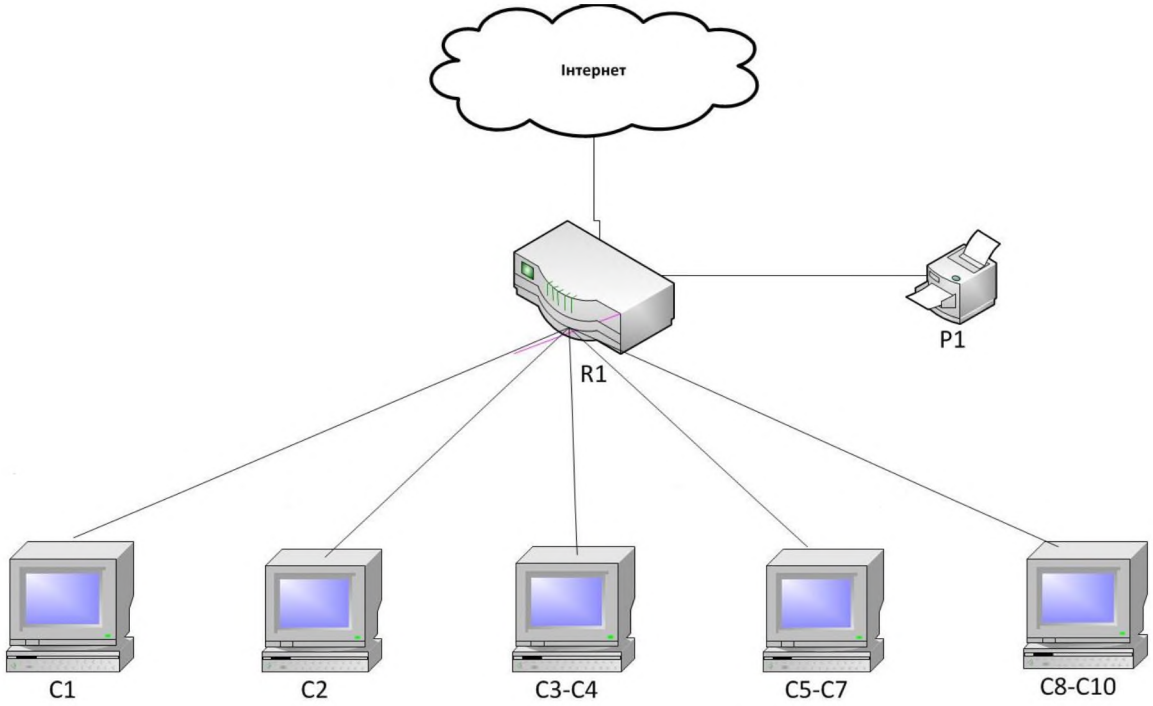

Рисунок 1.7. Структурна схема ІТС

Характеристика та перелік апаратного забезпечення наведено в табл. 1.4

Таблиця 1.4 - Характеристики апаратного забезпечення ОС

Назва в ІТС	Характеристика	Інвентар. номер
С1	Процесор:Intel Core i5-10400F (2.9 ГГц) RAM 8 ГБ SSD 120 ГБ HDD 1 ТБ Nvidia GeForce GT 730, 2 ГБ DVD ± RW/LAN	135670 135671 135672 135673 135674
С2	Процесор:Intel Core i5-10400F (2.9 ГГц) RAM 8 ГБ SSD 120 ГБ HDD 1 ТБ Nvidia GeForce GT 730, 2 ГБ DVD ± RW/LAN	175650 175651 175652 175653 175654
С3	Процесор: Intel Core i5-10400F (2.9 ГГц) RAM 8 ГБ SSD 120 ГБ HDD 1 ТБ Nvidia GeForce GT 730, 2 ГБ DVD ± RW/LAN	146550 146551 146552 146553 146554

Продовження таблиці 1.4

Назва в ІТС	Характеристика	Інвентар. номер
С4	Процесор: Intel Core i5-12400F (2.5GHz ГГц) RAM 16 ГБ HDD SAS 3.0 ТВ - 4 шт. Контролер RAID: MegaRAID SAS 9341-8i SGL SSD 240 ГБ Nvidia GeForce RTX 3050, 8 ГБ DVD ± RW/LAN	122700 122701 122702 122703,122704, 122705, 122706 122707 122708
С5	Процесор: Intel Core i5-12400F (2.5GHz ГГц) RAM 16 ГБ HDD 1 ТБ SSD 240 ГБ Nvidia GeForce RTX 3050, 8 ГБ DVD ± RW/LAN	168930 168931 168932 168933 168934
С6	Процесор: Intel Core i5-12400F (2.5GHz ГГц) RAM 16 ГБ HDD 1 ТБ SSD 240 ГБ Nvidia GeForce RTX 3050, 8 ГБ DVD ± RW/LAN	173650 173651 173652 173653 173654

Продовження таблиці 1.4

Назва в ІТС	Характеристика	Інвентар. номер
С7	Процесор: Intel Core i5-12400F (2.5GHz ГГц) RAM 16 ГБ HDD 1 ТБ SSD 240 ГБ Nvidia GeForce RTX 3050, 8 ГБ DVD ± RW/LAN	184910 184911 184912 184913 184914
С8	Процесор: Intel Core i5-12400F (2.5GHz ГГц) RAM 16 ГБ HDD 1 ТБ SSD 240 ГБ Nvidia GeForce RTX 3050, 8 ГБ DVD ± RW/LAN	164810 164811 164812 164813 164814
С9	Процесор: Intel Core i5-12400F (2.5GHz ГГц) RAM 16 ГБ HDD 1 ТБ SSD 240 ГБ Nvidia GeForce RTX 3050, 8 ГБ DVD ± RW/LAN	112340 112341 112342 112343 112344
С10	Процесор: Intel Core i5-12400F (2.5GHz ГГц) RAM 16 ГБ HDD 1 ТБ SSD 240 ГБ Nvidia GeForce RTX 3050, 8 ГБ DVD ± RW/LAN	133370 133371 133372 133373 133374

Програмне забезпечення яке встановлене на робочих станціях в ІТС

підприємства можна поділити на: системне наведено в табл. 1.5, прикладне наведено в табл. 1.6, спеціальне в табл. 1.7.

Таблиця 1.5 - Інвентаризаційна відомість системного програмного забезпечення ІТС.

№	Назва	Опис	Ліцензія	Де встановлена
1	Windows 10 Professional 10.0.17763.1 (build 1809)	Операційна система для персональних комп'ютерів і робочих станцій	Volume license	С1, С2, С3, С4, С5, С6, С7, С8, С9, С10
2	Windows Server 2019	Операційна система для серверів	Volume license	С4
3	ESET File Security (версія 7.1.12008)	Антивірусна програма	Commercial	С1, С2, С3, С4, С5, С6, С7, С8, С9, С10
4	WinRar (версія 5.80)	Архіватор файлів для 32- і 64-розрядних операційних систем Windows	Shareware	С1, С2, С3, С4, С5, С6, С7, С8, С9, С10

Таблиця 1.6. - Інвентаризаційна відомість прикладне програмного забезпечення ІТС.

№	Назва	Опис	Ліцензія	Де встановлена
1	Базовий пакет Microsoft Office 2019 Professional	ПЗ для роботи з різними видами документів, текстів, таблиць, базами даних тощо.	Volume license	С1, С2, С3, С4, С5, С6, С7, С8, С9, С10

Продовження таблиці 1.6

№	Назва	Опис	Ліцензія	Де встановлена
2	1С Підприємство 8.2. Базова версія	Програми, що дозволяють виконувати операції над даними, представленими в табличній формі	Volume license	С1, С2, С3, С4, С5, С6, С7, С8, С9, С10
3	Adobe Photoshop CS6 (версія 13.01)	Засоби створення нерухомих і рухомих зображень	Volume license	С3,С4,С5,С6,С7,С8,С9
4	Microsoft Edge (версія 44.18362.1.0)	Програми для роботи в комп'ютерній мережі	Freeware	С1, С2, С3, С4, С5, С6, С7, С8, С9, С10
5	Google Chrome (версія 80.0.3987)	Програми для роботи в комп'ютерній мережі	Freeware	С1, С2, С3, С4, С5, С6, С7, С8, С9, С10
6	Windows Media Player (версія 12.0.18362.418)	Програма для відтворення відео- та аудіофайлів	Freeware	С1, С2, С3, С4, С5, С6, С7, С8, С9, С10

Таблиця 1.7. - Інвентаризаційна відомість спеціального програмного забезпечення ІТС.

№	Назва	Опис	Ліцензія	Де встановлена
1	Visual Studio 2019 (версія 16.0)	Об'єктно-орієнтовані мови програмування	Volume license	С3,С4,С5,С6,С7,С8,С9

Продовження таблиці 1.7

№	Назва	Опис	Ліцензія	Де встановлена
2	TeamViewer (версія 15.4.4445)	Програми для роботи в комп'ютерній мережі через віддалений доступ	Freeware	С1, С2, С3, С4, С5, С6, С7, С8, С9, С10
3	Adobe Acrobat (версія 2019.008.20071)	Програма для роботи з pdf-файлами	Freeware	С1, С2, С3, С4, С5, С6, С7, С8, С9, С10
4	Skype (версія 14.56.102.0)	Програма забезпечує текстову, голосовий та відео зв’язок через Інтернет між комп'ютерами	Freeware	С1, С2, С3, С4, С5, С6, С7, С8, С9, С10
5	Viber (версія 12.6.0.41)	Програма забезпечує текстову, голосовий та відео зв’язок через Інтернет між комп'ютерами	Freeware	С1, С2, С3, С4, С5, С6, С7, С8, С9, С10
6	Eclipse (версія 4.23.0)	Програма забезпечує вільне інтегроване середовище розробки модульних кросплатформенних додатків.	Freeware	С3,С4,С5,С6, С7,С8,С9
7	IntelliJ IDEA Ultimate (версія 2022.2 EAP 222.2964.55)	Програма забезпечує комерційне інтегроване середовище розробки для різних мов програмування (Java, Python, Scala, PHP та ін.)	Commercial license	С3,С4,С5,С6, С7,С8,С9

Продовження таблиці 1.7

№	Назва	Опис	Ліцензія	Де встановлена
8	Figma Organization (конфігурація 2022 від 10.05.2022)	Онлайн сервіс забезпечує розробку інтерфейсів та прототипування.	Volume license	C1,C3,C4,C5, C6,C7,C8,C9

1.4.3 Характеристика середовища користувачів

Таблиця 1.8.- Характеристик користувачів

Працівник	Кількість працівників	Рівень кваліфікації	Роль в ІТС	Повно-важення керувати КСЗІ
Директор	1	Високо-кваліфіковані робітники	Адміністратор безпеки	+
Системний адміністратор	1	Високо-кваліфіковані робітники	Системний адміністратор	+
Бухгалтер	1	Високо-кваліфіковані робітники	Користувач	—
Розробники	3	Високо-кваліфіковані робітники	Користувач	—
Тестувальники	3	Високо-кваліфіковані робітники	Користувач	—

Керівником підприємства є директор. Директор має доступ до всієї інформації на підприємстві. До його обов`язків, стосовно об`єкта інформаційної діяльності (ОІД), входить:

- робота з документацією;
- розміщення персоналу;
- визначення напряму розвитку та стратегії підприємства;
- координування усіх видів діяльності підприємства;
- встановлення розмежування доступу до інформації;
- контроль, перегляд журналу подій;

- розробка технічного завдання ;

Бухгалтер має доступ до комерційної інформації, персональних даних. До його обов`язків, стосовно ОІД, входить:

- ведення бухгалтерського обліку;
- оформлення фінансових документів;
- складання усієї періодичної звітності;
- перерахунок податків та зборів за чинним законодавством;
- організація працевлаштування;
- виплата заробітної плати.

Системний адміністратор має доступ до усіх комп'ютерів в офісі. Має доступ до комерційної інформації. До його обов`язків, стосовно ОІД, входить:

- налаштування комп`ютерів, збір комп'ютерів
- встановлення програмного забезпечення;
- розмежування доступу до інформації;
- оновлення програм;
- оновлення антивірусів;
- перевірка цілісності;
- доступності локальної мережі;
- цілодобова перевірка серверів, їх доступності.

Розробники мають доступ до комерційної таємниці. Мають знання про плани та стратегію компанії. До його обов`язків, стосовно ОІД, входить:

- написання коду програм;
- розробка логічного функціонування програми;
- розробка дизайну програми.

Тестувальники мають доступ до технічної інформації, що становить комерційну таємницю. До його обов`язків, стосовно ОІД, входить:

- Тестування коду програмного забезпечення;
- Ведення переліку багів та помилок;
- Написання тестів для тестування програмного забезпечення.

Данні розподілу доступу до інформації наведено в розділі 1.2.4 в табл. 1.9

1.4.4 Матриця розмежування доступу до інформації.

Таблиця 1.9.- Матриця розмежування доступу до інформації

№ п/п	Опис документа	Режим доступу	Тип інформації	Вимоги до захисту	Директор	Бухгалтер	Системний адміністрато	Розробники	Тестувальники
1	Посадові інструкції	Відкрита	Відкрита	Д,Ц	Ч,З,В,К,М,ЗБ,Д	Ч	Ч	Ч	Ч
2	Технічні завдання	ІзОД	Конфіденційна	К,Ц,Д	Ч,З,В,К,М,ЗБ,Д	Ч	Ч	Ч	Ч
3	Бухгалтерські відомості	ІзОД	Конфіденційна	К,Ц,Д	Ч,З,В,К,М,ЗБ,Д	Ч,З,В,К,М,ЗБ,Д	-	-	-
4	Стратегія розвитку підприємства	ІзОД	Конфіденційна	К,Ц	Ч,З,В,К,М,ЗБ,Д	Ч	Ч	-	-

Продовження таблиці 1.9

№ п/п	Опис документа	Режим доступу	Тип інформації	Вимоги до захисту	Директор	Бухгалтер	Системний адміністрато	Розробники	Тестувальники
5	Архітектура ІТС	ІзОД	Відкрита	Ц, Д	Ч,З,В,К,М,ЗБ,Д	-	Ч,З,В,К,М,ЗБ,Д	-	-
6	Клієнтська база	ІзОД	Конфіденційна	К,Ц,Д	Ч,З,В,К,М,ЗБ,Д	Ч,З,В,К,М,ЗБ,Д	-	Ч	Ч
7	Дані про замовлення	ІзОД	Комерційна	К,Ц,Д	Ч,З,В,К,М,ЗБ,Д	Ч	-	-	-
8	Політика безпеки підприємства	ІзОД	Конфіденційна	К,Ц,Д	Ч,З,В,К,М,ЗБ,Д	Ч	Ч,З,В,К,М,ЗБ,Д	Ч	Ч
9	Кадрові дані	ІзОД	Персональні дані	К,Ц	Ч,З,В,К,М,ЗБ,Д	Ч,З,В,К,М,ЗБ,Д	Ч,З	-	-

Продовження таблиці 1.9

№ п/п	Опис документа	Режим доступу	Тип інформації	Вимоги до захисту	Директор	Бухгалтер	Системний адміністратор	Розробники	Тестувальники
10	Інформація про послуги та їх вартість		Відкрита	Ц,Д	Ч,З,В,К,М,ЗБ,Д	Ч,З,В,К,М,ЗБ,Д	-	-	-
11	Опис етапів створення алгоритмів програмного забезпечення	ІзОД	Конфіденційна	К,Ц,Д	Ч,З,В,К,М,ЗБ,Д	Ч	Ч,З,В,К,М,ЗБ	Ч,З,В,К,М,ЗБ	Ч,З,ЗБ,К
12	Політика конфіденційності ПЗ	ІзОД	Конфіденційна	К,Ц,Д	Ч,З,В,К,М,ЗБ,Д	Ч	Ч,З,В,К,М,ЗБ,Д	Ч	Ч

Продовження таблиці 1.9

№ п/п	Опис документа	Режим доступу	Тип інформації	Вимоги до захисту	Директор	Бухгалтер	Системний адміністрато	Розробники	Тестувальники
13	Опис дизайну та інтерфейсу	ІзОД	Конфіденційна	К, Ц	Ч,З,В,К,М,ЗБ,Д	-	-	Ч,З,В,К,М,ЗБ,Д	Ч,З,В,К,М,ЗБ,Д
14	Перелік засобів реалізації кодування	ІзОД	Конфіденційна	К,Ц,Д	Ч,З,В,К,М,ЗБ,Д	Ч	Ч,З,В,К,М,ЗБ,Д	Ч,З,В,К,М,ЗБ,Д	Ч,З,В,К,М,ЗБ,Д
15	Перелік встановлених помилок коду	ІзОД	Конфіденційна	К,Ц	Ч,З,В,К,М,ЗБ,Д	-	-	Ч,З,В,К,М,ЗБ,Д	Ч,З,В,К,М,ЗБ,Д
16	Опис технічної реалізації	Відкрита	Відкрита	Д,Ц	Ч,З,В,К,М,ЗБ,Д	-	-	Ч,З,В,К,М,ЗБ,Д	Ч,З,В,К,М,ЗБ,Д

Продовження таблиці 1.9

№ п/п	Опис документа	Режим доступу	Тип інформації	Вимоги до захисту	Директор	Бухгалтер	Системний адміністрато	Розробники	Тестувальники
17	Опис задачі для відділу тестування	ІзОД	Конфіденційна	К,Ц	Ч,З,В,К,М,ЗБ,Д	-	-	Ч,З,В,К,М,ЗБ,Д	Ч,З,В,К,М,ЗБ,Д
18	Технічне завдання на тестування	ІзОД	Конфіденційна	К,Ц,Д	Ч,З,В,К,М,ЗБ,Д	-	-	Ч,З,В,К,М,ЗБ,Д	Ч,З,В,К,М,ЗБ,Д
19	Інвентеризаційний список	ІзОД	Конфіденційна	К,Ц,Д	Ч,З,В,К,М,ЗБ,Д	Ч,З,В,К,М,ЗБ,Д	Ч	-	-
20	Журнал подій	ІзОД	Конфіденційна	К,Ц,Д	Ч,З,В,К,М,ЗБ,Д	-	Ч,З,В,К,М,ЗБ,Д	-	-

Продовження таблиці 1.9

№ п/п	Опис документа	Режим доступу	Тип інформації	Вимоги до захисту	Директор	Бухгалтер	Системний адміністрато	Розробники	Тестувальники
21	Фінальна збірка продукту	ІзОД	Конференційна	К,Ц,Д	Ч,З,В,К,М,ЗБ,Д	-	-	Ч,З,В,К,М,ЗБ,Д	Ч,З,В,К,М,ЗБ,Д

Умовні позначення:

Ч-читання, З – запис, В – видалення, К – копіювання, М – модифікація ЗБ - зберігання, Д – друкування.

1.4.5 Інформація що циркулює в ІТС

В табл. 1.10 наведено перелік та опис інформації яка циркулю в ІТС

Таблиця 1.10.- Інформація що циркулює в ІТС

№ п/п	Опис документа	Детально	Тип інформації	Тип зберігання	Вимоги до захисту
1	Посадові інструкції	Перелік вимог та обов`язків працівника	Відкрита	Текстова інформація в паперовому та електронному вигляді	Д,Ц

Продовження таблиці 1.10

№ п/п	Опис документа	Детально	Тип інформації	Тип зберігання	Вимоги до захисту
2	Технічні завдання	Постановка задачі, вимоги до готового продукту, строки реалізації, визначення мети створення, загальний опис та вимоги до ПЗ, вимоги до операційної системи (ОС) для якої призначена програма, створення блок-схеми	Конфіденційна	Текстова інформація зберігається в електронному вигляді	К,Ц,Д

Продовження таблиці 1.10

№ п/п	Опис документа	Детально	Тип інформації	Тип зберігання	Вимоги до захисту
3	Бухгалтерські відомості	Звітність за періоди, звітність із виплат аналогів, звіт із виплат заробітної плати, звіт із врахуванням прибутку підприємства, планування бюджету підприємства.	Конфіденційна	Текстова інформація у електронному та паперовому виглядах.	К,Ц,Д
4	Стратегія розвитку підприємства	Стратегічний план розвитку підприємства, заключення ділового партнерства	Конфіденційна	Текстовий документ в електронному та паперовому	К,Ц

Продовження таблиці 1.10

№ п/п	Опис документа	Детально	Тип інформації	Тип зберігання	Вимоги до захисту
5	Архітектура ІТС	Рішення про використання конкретних програм, конкретної ОС, вибір компонентів системи, спостереженість роботи серверів, рішення про реалізацію системи захисту даних, розподіл доступу згідно політики підприємства	Відкрита	Текстовий документ в електронному вигляді	Ц, Д
6	Клієнтська база	Клієнтські поштові адреса, e-mail адреса, назви кампаній, контакти замовників	Конфіденційна	Текстовий документ в електронному вигляді	К,Ц,Д
7	Дані про замовлення	Ідеї, способи реалізації, код реалізації	Комерційна	Текстовий документ в електронному та паперовому вигляді	К,Ц,Д
8	Політика безпеки підприємства	Забезпечення інформаційної безпеки, методи реалізації її.	Конфіденційна	Текстовий документ в електронному вигляді	К,Ц,Д

Продовження таблиці 1.10

№ п/п	Опис документа	Детально	Тип інформації	Тип зберігання	Вимоги до захисту
9	Кадрові дані	Накази, заяви, трудові книжки, контракти, графік відпусток	Персональні дані	Текстовий документ в паперовому вигляді та електронному вигляді.	К,Ц
10	Інформація про послуги та їх вартість	Перелік послуг, та їх вартість.	Відкрита	Текстовий документ в електронному вигляді.	Ц,Д
11	Опис етапів створення алгоритмів програмного забезпечення	Створення логіки реалізації, визначення потреб, вибір критеріїв для реалізації, визначення функціоналу програми, вибір типу програмуванняю	Конфіденційна	Текстовий документ в електронному вигляді.	К,Ц,Д

Продовження таблиці 1.10

№ п/п	Опис документа	Детально	Тип інформації	Тип зберігання	Вимоги до захисту
12	Політика конфіденційності ПЗ	Реалізація захисту даних користувача, його комп'ютера; надійний захист програми від видозмінення її первинного коду.	Конфіденційна	Текстовий документ у електронному вигляді.	К,Ц,Д
13	Опис дизайну та інтерфейсу	Створення мокапів проекту, вибір стилю оформлення, рішення про панель функціоналу, створення логотипу та дизайну іконки.	Конфіденційна	Графічний документ, що зберігається в електронному вигляді.	К, Ц

Продовження таблиці 1.10

№ п/п	Опис документа	Детально	Тип інформації	Тип зберігання	Вимоги до захисту
14	Перелік засобів реалізації кодування	Код програми, використані бібліотеки підключення, використані методи, засоби створення інтерфейсу користувача, засоби управління версіями, бази даних.	Конфіденційна	Документ, що зберігається в електронному вигляді	К,Ц,Д
15	Перелік встановлених помилок коду	Опис помилок коду програми, можливі витоку інформації, несправності	Конфіденційна	Код; Документ, що зберігається в електронному вигляді	К,Ц

Продовження таблиці 1.10

№ п/п	Опис документа	Детально	Тип інформації	Тип зберігання	Вимоги до захисту
16	Опис технічної реалізації	Вибір мови програмування, вибір головних критеріїв створення програми (швидкість роботи, кількість пам`яті, що ПЗ займає), опис модуля структури та перерахування створених/внесених змін до нього.	Відкрита	Текстовий документ, що зберігається в електронному вигляді	Д,Ц
17	Опис задачі для відділу тестування	Постановка задачі на тестування, роз`яснення щодо продукту	Конфіденційна	Документ, що зберігається в електронному вигляді	К,Ц

Продовження таблиці 1.10

№ п/п	Опис документа	Детально	Тип інформації	Тип зберігання	Вимоги до захисту
18	Технічне завдання на тестування	Опис перевірка програми на відповідність до технічного завдання, перевірка коректного відпрацювання функціоналу, код автотестів, опис скритих можливостей системи, аналіз коду	Конфіденційна	Код; Документ, що зберігається в електронному вигляді	К,Ц,Д
19	Інвентаризаційний список	Інвентаризаційні данні про всі технічні засоби	Конфіденційна	Документ, що зберігається в електронному та паперовому вигляді	К,Ц,Д

Продовження таблиці 1.10

№ п/п	Опис документа	Детально	Тип інформації	Тип зберігання	Вимоги до захисту
20	Журнал подій	Подробні данні про важливі програмні і апаратні події	Конфіденці йна	Документ, що зберігається в файловому вигляді	К,Ц,Д
21	Фінальна збірка продукту	Фінальний продукт який в собі містить програмний код та опис продукту, а також виконаний дизайн	Конференці йна	Документ зберігається в електронному вигляді, код, макет дизайну.	К,Ц,Д

1.4.6 Перелік політик безпеки які застосовані на підприємстві

1. Політка захисту паролів
2. Політика використання інтернету
3. Політика встановлення програмного забезпечення
4. Політика електронної пошти

1.5 Аналіз загроз інформації

[5] Згідно із НД-ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації комп'ютерних систем від несанкціонованого доступу»:

[5] «Модель загроз (model of threats) — абстрактний формалізований або неформалізований опис методів і засобів здійснення загроз.

Модель порушника (user violator model) — абстрактний формалізований або неформалізований опис порушника».

На даному етапі проводиться аналіз моделі ризиків, а саме побудова моделі загроз і моделі порушника, припущення можливих наслідків від реалізації загроз. Також визначається перелік критичних загроз, які є метою завдання створення КСЗІ.

Аналіз загроз і вразливостей складається з наступних етапів:

- модель порушника;
- модель загроз.

1.5.1 Модель порушника

До зовнішніх порушників відносяться особи, які знаходяться за поза підприємством. Це можуть бути конкуруючі підприємства та крадії або персонал з обслуговування приміщення, особи, яким не передбачено доступ до інформації з обмеженим доступом (ІзОД), але які мають доступ до приміщень, де розміщено компоненти ІТС і можуть отримати доступ до ІзОД, наприклад, прибиральники, електрики тощо.

До внутрішніх порушників відносяться особи, що мають можливість фізичного підключення до каналів зв'язку або інших складових мережі передачі даних, користувачі АС, персонал, який безпосередньо пов'язаний із забезпеченням функціонування ІТС.

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

А саме порушників класифікують за:

- За категоріями;
- За мотивами здійснення порушень;
- За рівнем кваліфікації та обізнаності щодо ІТС;
- За показником можливостей використання засобів та методів подолання системи захисту;
- За часом дії;
- За місцем дії.

Таблиця 1.11 - Модель порушника

Посада	Категорія порушення	Мотив порушення	Рівень обізнаності що до ІТС	Можливості щодо подолання я системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Директор	ПВ4	М1	К4	З3	Ч4	Д4	20
	4	1	4	3	4	4	
Системний адміністратор	ПВ4	М3	К4	З3	Ч4	Д3	21
	4	3	4	3	4	3	
Бухгалтер	ПВ1	М2	К2	З1	Ч3	Д2	11
	1	2	2	1	3	2	
Розробник	ПВ3	М3	К3	З3	Ч4	Д2	18
	3	3	3	3	4	2	
Тестувальник	ПВ3	М3	К3	З3	Ч4	Д2	18
	3	3	3	3	4	2	
Інформатор конкурента	ПЗ4	М4	К4	33	Ч4	Д2	21
	4	4	4	3	4	2	
Майстерня гарантійного обслуговування обладнання	ПЗ2	М3	К2	33	Ч1	Д3	14
	2	3	2	3	1	3	

Визначено, що найбільшу небезпеку становить співробітник ІТС, який виконує роль системного адміністратора. Дії особи на даній посаді мають відстежуватися, та суворо контролюватися оскільки вона є основним потенційним

порушником ІБ на ІТС даного підприємства. А також можливу небезпеку становить інформатор конкурента який під прикриттям був прийнятий на роботу у компанію на будь яку з посад. Для уникнення проникнення таких.

1.5.2 Модель загроз

Таблиця 1.12.- Модель загроз

№	Загроза	Вразливість	Збиток	Властивості інформації	Ймовірність
Загрози, пов'язані з внутрішніми діями працівників					
1	Неконтрольоване копіювання ІзОД на зовнішні носії інформації користувачі	Відсутність регламенту використання зовнішніх сторонніх носіїв. Відсутність блокування і контролю за портами USB.	Високий	К,Ц,Д	5
2	Несанкціоновані дії або помилки системних адміністраторів	Несанкціоновані або помилкові дії адміністраторів (неправильне встановлення або оновлення ПЗ, ОС, систем сигналізації, неправомірне відключення засобів захисту ІТС)	Високий	К,Ц,Д,С	4

Продовження таблиці 1.12

№	Загроза	Вразливість	Збиток	Властивості інформації	Ймовірність
3	Встановлення шкідливого ПЗ, технічні збої в роботі програм і компонентів ІТС	Порушення політики встановлення програмного забезпечення ; Зловживання встановлюванням ПЗ яке не пов'язане з службовими об'явками	Середній	К,Ц,Д,С	3
4	Зловживання правами системного адміністратора	Відсутність регулярних аудитів, неправильний розподіл прав	Високий	К,Ц,Д	4
Загрози, пов'язані з діями сторонніх людей					
5	Копіювання ,знищення інформації, створення технічних перешкод працівниками конкурентів під прикриттям	Відсутність контролю за використанням зовнішніх носіїв інформації, поблажливий вибір персоналу.	Середній	К,Д,Ц	4

Продовження таблиці 1.12

№	Загроза	Вразливість	Збиток	Властивості інформації	Ймовірність
6	Неправомірні дії агента під прикриттям підісланого конкурентом.	Необережний підбір співробітників. Викрадення, модифікація, копіювання інформації, працюючи на підприємств	Середній	К,Ц	3
7	Передача інформації стороннім особам та пристроям користувачами ІТС через Інтернет мережу	Відсутність трекінгових систем, які моніторять активність користувачів.	Середній	К,Ц,Д,С	5
Загрози, пов’язані з внутрішніми технічними проблемами					
8	Перехоплення інформації та підміна трафіку	Наявність незахищеного зовнішнього каналу.	Високий	К	5

Продовження таблиці 1.12

№	Загроза	Вразливість	Збиток	Властивості інформації	Ймовірність
9	Вихід з строю технічного обладнання	Збої та відмови системи електроживлення, часті скачки напруги.	Низький	Ц,Д	3
10	Вихід з строю носіїв інформації, серверу	Збої, пошкодження носіїв інформації, серверної частини підприємства.	Високий	Ц,Д	2
11	Викрадення інофрмації з внутрішніх носів співробітниками сервісного обслуговування	Відсутність можливості видалення носіїв інформації через опломбування робочих станцій і заміни їх комплектуючих через дію гарантійного договору.	Високий	К,Ц,Д	5
Загрози природного походження					
12	Природні катастрофи	Пожежа, повінь, землетрус, техногенні аварії.	Середній	Ц,Д	2

1. Неконтрольоване копіювання ІзОД на зовнішні носії інформації користувачами. Причина – корисливі дії. Можливі наслідки - втрата інформації, великі фінансові втрати.

2. Передача інформації стороннім особам та пристроям користувачами ІТС через Інтернет мережу. Причина - корисливі дії персоналу або навмисне перехоплення інформації сторонніми особами. Можливі наслідки - втрата конфіденційності, цілісності і доступності інформації.

3. Викрадення інформації з внутрішніх носів співробітниками сервісного обслуговування . Причина – корисливі дії. Можливі наслідки – втрата інформації, фінансові збитки, репутаційні збитки.

4. Можливий перехоплення та підміна трафіку через наявність незахищеного зовнішнього каналу. Причини – корисливі дії. Можливі наслідки – втрата інформації, фінансові збитки.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Профіль захищеності

Зважаючи на побудовану раніше модель загроз та порушників і загальну будову системи мною був обраний профіль захищеності 3 класу з підвищеними вимогами до забезпечення конфіденційності, цілісності і доступності оброблюваної інформації.

Відповідно до документа [8] для даної АС класу «3» обрано наступний профіль захищеності:

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

З рівнем гарантій до обраного профілю захищеності Г-3.

КД-2 Базова довірча конфіденційність. Реалізовано.

У КЗЗ даної ІТС присутні апаратні та людські ресурси, які мають змогу визначати користувачу або групі користувачів процеси, які належать до його домену, або конкретно до окремого користувача. Та визначають змогу мати або не мати права ініціювати процес. Стандартна система вибіркового керування доступу дозволяє реалізувати базовий рівень даної послуги. У поточній конфігурації системи, послуга реалізована завдяки спискам контролю доступу.

Відноситься до: усіх користувачів та інформаційних об'єктів.

КА-2. Базова адміністративна конфіденційність. Реалізовано.

КЗЗ даної ІТС має програмно-апаратні механізми, які здатні надати можливість адміністратору або особі з відповідними повноваженнями через процедури керування доменами визначати конкретних користувачів або групи користувачів, які мають права ініціювати процеси.

Відноситься до: усіх користувачів, процеси; інформаційні об'єкти; програмні засобі; зовнішні та внутрішні носії інформації.

КО-1. Повторне використання об’єкта. Реалізовано.

Реалізація цієї послуги унеможливлює отримання залишкової інформації з розділюваних об'єктів.

Данна послуга відноситься до: зовнішні та внутрішні носії інформації, сторінки оперативної пам'яті.

КВ-2. Базова конфіденційність при обміні. Не реалізовано.

Реалізація послуги забезпечує захист інформації, яка зберігається на внутрішніх чи зовнішніх носіях, від несанкціонованого ознайомлення у разі вилучення носіїв з-під контролю засобів захисту. А також забезпечує шифрування при передачі інформації зовнішніми не захищеними каналами.

Відноситься до: логічних дисків на внутрішніх та зовнішніх носіях, користувачів усіх категорій, інформації що передається зовнішніми каналами.

ЦД-1. Мінімальна довірча цілісність. Реалізовано.

Контроль дозволених процесів виконується ядром системи. Користувачі і домени мають чітко розмежованій доступ до об'єктів. Реалізація послуги забезпечує користувачеві можливість управляти потоками інформації від процесів, ініційованих іншими користувачами, до інформації, яка належать його домену.

ЦА-2. Базова адміністративна цілісність. Реалізовано.

В системі присутні програмно-апаратні механізми і осіб, які можуть взаємодіяти з даними ресурсами, керувати потоками інформації. Реалізація відбувається завдяки керуванню доступом до об’єктів на підставі атрибутів користувача та об’єкту. Атрибути призначаються при створенні об’єктів та користувачів.

Вона відноситься до: програмні засоби, інформаційні об'єкти, користувачів усіх категорій, процеси, зовнішні та внутрішні накопичувачі інформації.

ЦО-1. Обмежений відкат. Реалізовано

В КС э вбудовані функцій, які під час користування дозволяють зробити відкат нещодавніх дій і також роблять тимчасові копії документів або файлів з ІзОД. В програмному забезпеченні яке встановлено на робочих станціях також є функції ,які дозволяють робити відкат нещодавніх дій і роблять тимчасові копії. Також є можливість відміни послідовності операцій над захищеним об’єктом.

Послуга відноситься до: всіх послідовних операцій.

ЦВ-2. Базова цілісність при обміні. Реалізовано.

АС має програмно-апаратні механізми, які створюють умови імпорту та експорту. Адміністратори або користувачі з відповідними повноваженнями мають можливості створити умови на імпорт та експорт та присвоєння чи зміни рівня захищеності Утиліта перевірки вагової частки завантажених файлів у ESET File Security, а засобом перевірки системних файлів виступає вбудований в Windows SFC.exe.

Політика відноситься до: користувачів усіх категорій, логічних дисків на внутрішніх та зовнішніх носіях.

ДР-1. Квоти. Реалізовано.

Реалізація послуги унеможливлює захоплення користувачами надмірного об'єму ресурсів. КЗЗ завдяки стандартними засобами Windows надає можливість адміністратору, встановити обмеження на обсяг дискового простору що використовують користувачі для зберігання.

Данну послугу відносять до: користувачів усіх категорій, простору носіїв які використовують користувачами для зберігання.

ДВ-1. Ручне відновлення. Реалізовано.

У результаті збою КС в АС присутні особи з відповідними повноваженнями, які приводять КС до нормального стану або стану з обмеженими умовами у ручному режимі. У результаті виконання даної процедури КС тимчасово не доступний.

НР-2. Захищений журнал. Реалізовано.

В КС включені функції журналу подій безпеки в системі, завдяки інструментам вбудованим в Windows 10.

Параметри які фіксуються: дата, час, місце, тип події її успішність чи неуспішність зареєстрованої події.

Для забезпечення ведення аудиту подій безпеки адміністратору безпеки необхідно включити аудит подій безпеки і налаштувати події, які необхідно журнал подій реєструє: виведення документу на друк, зміна групи користувачів, автентифікація користувача в системі, зміна атрибутів доступу, зміна компонентів

захисту КС, збої активації корпоративної ліцензії, перегляд журналу безпеки, перевірка файлів і сайтів ESET Security, запуск ПЗ

НИ-2. Одиночна ідентифікація і автентифікація. Реалізовано.

Виконується за допомогою вбудованих функцій Windows 10: в локальній політиці безпеки та в редакторі локальної групової політики. Користувачі проходять автентифікацію під час введення паролю при вході в систему.

Дана політика відноситься до: усіх користувачів системи.

НК-1. Однонаправлений достовірний канал. Реалізовано.

Система має вбудовані функції ідентифікації і автентифікації користувача Windows 10 після запуску операційної системи за групою користувачів або окремим користувача в КС. Зв'язок з використанням даного каналу ініціалізується виключно користувачем.

Відноситься до: користувачів усіх категорій.

НО-2 Розподіл обов'язків адміністраторів. Реалізовано.

В системі присутні механізми, які за бажанням власника ІТС, керують діяльністю обов'язків адміністраторів. АС має особу, яка виконує функцію адміністратора системи та адміністратора безпеки. В локальній політиці безпеки Windows реалізуються функції розподілу обов’язків адміністратора і звичайного користувача завдяки визначенню прав користувачів.

Послуга відноситься до: користувачів усіх категорій.

НЦ-2. КЗЗ з гарантованою цілісністю. Реалізовано.

КЗЗ не має достатню кількість програмно-апаратних ресурсів для підтримки власних доменів від зовнішніх впливів, НСД та інших негативних випадків.

Реалізовано завдяки антивірусному ПЗ із механізмом пошуку вірусів, хробаків та інших, при старті ОС, Microsoft Defender.

НТ-2. Самотестування при старті. Реалізовано.

В КЗЗ присутні апаратні механізми, які реалізують дану політику, проте активація даної функції можлива за наказом власника ІТС.

НВ-1. Автентифікація вузла. Реалізовано.

КЗЗ присутні механізми для реєстрації вузла або вузлів, які імпортують або експортують об'єкти в КС. Але відсутні механізми які забезпечували автентифікацію при обміні через незхищені зовнішні канали.

2.2 Проектні рішення

2.2.1 Технічні заходи.

Проаналізувавши дані з табл. 1.11. модель порушника та табл. 1.12 модель загроз а також запропонований профіль захищеності і вже реалізованих послуг мною були висунуті такі засоби для реалізації проектних рішень.

Проаналізувавши перелік сертифікованих засобів ТЗІ наданий Державною службою спеціального зв'язку та захисту інформації України[11], я сформував табл. 2.1.

Таблиця 2.1.- Порівняння КЗЗ

	Засіб технічного захисту інформації від несанкціонованого доступу «Комплекс «Гриф» версії 4»	Система захисту інформації ЛОЗА™-2, версія 3 виробництва ТОВ «Науково-дослідний інститут «Автопром»	Система захисту інформації ЛОЗА™-1, версія 4 виробництва ТОВ «Науково-дослідний інститут «Автопром»	КЗЗ «Гриф-Мережа» версії 3, виробництва ТОВ «Інститут комп'ютерних технологій»
Клас АС	3	2	1	2
Довірча конфіденційність	-	КД-2	КД-2	-

Продовження таблиці 2.1

	«Комплекс «Гриф» версії 4»	ЛОЗА™-2,версія 3	ЛОЗА™-1, версія 4	КЗЗ «Гриф-Мережа» версії 3,
Адміністративна конфіденційність	КА-2	КА-2	КА-2	КА-2
Повторне використання об'єктів	КО-1	КО-1	КО-1	КО-1
Конфіденційність при обміні	КВ-2	-	-	-
Довірча цілісність	-	ЦД-1	ЦД-1	-
Адміністративна цілісність	ЦА-1	ЦА-1	ЦА-1	ЦА-2
Відкат	ЦО-1	-	-	ЦО-1
Цілісність при обміні	ЦВ-2	-	-	-
Використання ресурсів	ДР-1	-	-	ДР-1
Стійкість до відмов	ДС-1	ДС-1	ДС-1	ДС-1
Гаряча заміна	ДЗ-1	ДЗ-1	ДЗ-1	ДЗ-1
Відновлення після збоїв	ДВ-1	ДВ-1	ДВ-1	ДВ-1
Реєстрація	НР-3	НР-4	НР-4	НР-2
Достовірний канал	НК-1	НК-1	НК-1	НК-1

Продовження таблиці 2.1

	«Комплекс «Гриф» версії 4»	ЛОЗА™-2,версія 3	ЛОЗА™-1, версія 4	КЗЗ «Гриф-Мережа» версії 3,
Цілісність КЗЗ	НЦ-2	НЦ-2	НЦ-2	НЦ-2
Самотестування	НТ-2	НТ-2	НТ-2	НТ-2
Ідентифікація і автентифікація	НИ-3	НИ-2/НИ-3	НИ-2/НИ-3	НИ-3
Розподіл обов'язків	НО-2	НО-2	НО-2	НО-2

Виходячи з табл. 2.1 ми бачимо що данні засоби можуть встановлюватися на різні класи АС. Так, як на нашому підприємстві використовується АС класу 3. то нам підходить тільки КЗЗ «Комплекс «Гриф» версії 4».

Послуги які надає «Комплекс «Гриф» версії 4» а саме КВ-2 яка є критичною для ІТС. За допомогою послуг КВ-2 реалізується захист інформації, яка зберігається на внутрішніх чи зовнішніх носіях, від несанкціонованого доступу у разі вилучення носіїв з-під контролю засобів захисту.

Але послуга КВ-2 яку надає «Комплекс «Гриф» версії 4» не покриває захист та шифрування зовнішніх каналів інформації. Тому для убезпечення передачі даних через інтернет мережу потрібно використати додаткові інструменти шифрування даних, а саме додатки та розширення з технологією VPN. Ця технологія віртуальних приватних мереж була обрана мною через її достатньо просту реалізацію , а також за її надійність. Головними чинниками та можливостями за яким були обрані програми VPN це надійний захист конфіденційності. А також відповідність критеріям шифрування (AES-256), протоколам IPSec або L2TP, а також ліцензія VPN яка повинна розповсюджуватися на велику кількість пристроїв. Дані для порівняння наводяться в табл. 2.2.

Таблиця 2.2.- Порівняння VPN сервісів

	Express VPN	ZenMate	Ivacy	Private Internet Access	Surfshark	NordVPN
Потоколи	OpenVPN, L2TP/IPsec, PPTP	OpenVPN, IPSec,IKEv2, L2TP	OpenVP, L2TP, IKEv.	PPTP L2TP/IPSEC IKEV2 OPENVPN WIREGUARD	L2TP/IPSEC IKEV2 OPENVPN WIREGUARD	IKEv2/IPsec, OpenVPN, NordLynx
Тип шифрування	AES-256	AES-256	AES-256	AES-256	AES-256	AES-256
Кількість пристроїв на ліцензію	5	безліміт	5	10	безліміт	6
Додаток для ПК	+	+	+	+	+	+
Додаток для IOS/Android	+	+	+	+	+	+
Розширенуя для браузера	+	+	+	+	+	+
Кількість серверів	3000	3800	1000	29 650	3000	5800
Кількість країн	94	74	100	84	65	59
Ціна за місяць	$6.67	$2.41	$3.50	$11.95	$2.49	$6.99

Всі сервіси, з табл. 2.2, використовують шифрування AES-256, протоколи IPSec або L2TP, але безліміт на пристрої на одній ліцензії е лише у ZenMate та Surfshark. З цих двох додатків ZenMate має значну перевагу у більшій кількості серверів та кількості країн в яких вони розташовані, що значно підвищує його швидкість та якість роботи. Крім того, він має найнижчу ціну за місяць користування.

Постійне використання VPN для підключення працівників до корпоративної мережі дозволить: запобігти атакам, що використовують метод Man-in-the-Middle (MitM) (за допомогою перехоплення та ретранслювання відправляємої інформації).

2.2.2 Організаційні заходи.

Для забезпечення безпеки на ІТС ТОВ Рені були визначенні наступні організаційні заходи:

1. Контроль доступу користувачів до CD-і DVD-дисководів, жорстких дисків, зовнішніх USB-носіїв, USB-портів за допомогою програмного продукту — комплекс «Гриф», чим забезпечиться мінімізація занесення вірусу з боку зовнішніх носіїв та зменшиться вірогідність копіювання інформації;

2. Знищення інформації з створенням резервної копії, що зберігається на внутрішніх пристроях зберігання інформації, при списанні або відправці робочої станції в ремонт;

3. Ідентифікація зовнішніх носіїв на які здійснюється архівування даних, ідентифікація периферійних засобів вводу\виводу інформації (клавіатури, миші, принтери).

4. Обмеження доступу до соціальних мереж та засобів миттєвого обміну повідомленнями, а також до сайтів, які не зв'язані з робочим процесом програмними засобами;

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

6. Створення гостьової мережі для виходу в Інтернет задля унеможливлення несанкціонованого доступу до АС підприємства;

7. Впровадження квартальних семінарів та навчання персоналу , що спрямоване на покращення навичок роботи з ІТС.

РОЗДІЛ 3. ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ ДОЦІЛЬНОСТІ РОЗРОБКИ ПРОЕКТНИХ РІШЕНЬ РЕАЛІЗАЦІЇ НЕОБХІДНОГО РІВНЯ ЗАХИСТУ АС ТОВ «Reni»

3.1 Економічне обґрунтування доцільності впровадження проектних рішень

Для економічного обґрунтування доцільності впроваджень проектних рішень для ІТС ТОВ «Reni» потрібно провести розрахунки. На основі цих розрахунків буде визначатись економічна ефективність впровадження запропонованих рішень на підприємстві.

Економічна доцільність визначається:

- розрахунками капітальних витрат, що потребують впроваджені проектні рішення;
- розрахунками експлуатаційних витрат;
- розрахунками річного економічного ефекту від впровадження проектних рішень.

3.2 Розрахунок суми витрат на впровадження проектних рішень

3.2.1 Розрахунок трудомісткості впроваджень.

Спочатку розраховується трудомісткість впровадження проектних рішень, для цього потрібно скласти час, який знадобиться для кожної робочої операції:

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

- $t_{тз}$ - тривалість складання ТЗ на впровадження проектних рішень = 12 годин;
- $t_{в}$ - тривалість розробки концепції безпеки інформації у організації = 8 годин;
- $t_{а}$ - тривалість процесу аналізу ризиків = 6 годин;
- $t_{вз}$ - тривалість визначення вимог заходів, методів та засобів захисту = 2

годин;

- $t_{озб}$ - тривалість виробу основних рішень з забезпечення безпеки інформації = 10 годин;
- $t_{товр}$ - тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організацій = 16 години;
- $t_д$ - тривалість документального оформлення політики безпеки = 8 годин.

$$t = 12 + 8 + 6 + 2 + 10 + 16 + 8 = 62, \text{год}, \quad (3.1)$$

3.2.2 Розрахунок суми витрат на реалізацію обраних проектних рішень.

Сума витрат на впровадження обраних рішень (Kpn) складається з витрат на:

- Заробітну плату спеціаліста з кібербезпеки — Ззп, грн;
- Вартості витрат машинного часу, що необхідний для реалізації проектних рішень — Змч.

$$К_{рп} = З_{зп} + З_{мч} = 7311, \text{грн} \quad (3.2)$$

Заробітна плата спеціаліста складається з основної та додаткової заробітної плати, соціальних виплат та визначається за формулою:

$$З_{зп} = t * З_{іб} = 62 * 75 = 4650, \text{грн} \quad (3.3)$$

де t — загальна тривалість розробки політики безпеки інформації = 330 годин;

$З_{іб}$ — середньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями = 12000 / 160 = 75, грн/годину

Вартість машинного часу для розробки проектних рішень на ІТК визначається за формулою:

$$З_{зп} = t * С_{мч} = 2661, \text{грн}, \quad (3.4)$$

де t — трудомісткість підготовки документації на ІТК =4 години;

$С_{мч}$ — вартість 1 години машинного часу ПК, грн./година (5,6 грн).

Відповідно до розроблених рекомендацій, планується використання ліцензійних програмних засобів, як вже встановлених, так і нових.

Розрахована вартість розробки проектних рішень Kpn є складовою одноразових капітальних витрат разом з витратами на придбання програмних засобів, як рекомендовані для використання.

Отже фіксована сума капітальних витрат на розробку обраних проектних рішень складає:

$$К = К_{рп} + К_{зпз} + К_{аз} + К_{навч} + К_{н} = 97643, \text{ грн}, \quad (3.5)$$

$$К = 7311 + 90332 + 0 + 0 + 0 = 97643, \text{ грн}, \quad (3.5)$$

де *К* — вартість розробки проекту впроваджень рішень та залучення для цього зовнішніх спеціалістів, грн;

Кзпз — вартість закупівлі ліцензійного основного і додаткового програмного забезпечення (ПЗ), 90332 грн.;

Крп — вартість розробки проектних рішень, 7311 грн;

Каз — вартість закупівлі апаратного забезпечення та допоміжних матеріалів = 0 грн;

Кнавч вартість витрати на навчання технічних фахівців і обслуговуючого персоналу = 0 грн;

Кн — витрати на встановлення обладнання та налагодження системи інформаційної безпеки = 0 грн.

3.3 Розрахунок поточних (експлуатаційних) витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об’єкта проектування за визначений період, що виражені у грошовій формі.[13]

Формула річних поточних виплат:

$$С = С_в + С_к + С_{ак}, \text{ грн} \quad (3.6)$$

де, $С_в$ – витрати на модернізацію проектних рішень безпеки;

$С_к$ – витрати на керування системою інформаційної безпеки;

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

Витрати на керування системою інформаційної безпеки розраховується за формулою:

$$С_к = С_н + С_а + С_з + С_{єв} + С_е + С_{єл} + С_о + С_{тос}, \text{ грн} \quad (3.7)$$

$С_н$ – витрати на навчання адміністративного персоналу й кінцевих користувачів;

$С_а$ – річний фонд амортизаційних відрахувань;

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

$С_е$ – вартість електроенергії;

$С_о$ – витрати на залучення сторонніх організацій;

$С_{тос}$ – витрати на технічне й організаційне адміністрування та сервіс.

Річний фонд амортизаційних відрахувань розраховується за допомогою *прямолінійного метода*. Нарахування амортизації передбачає рівномірний розподіл вартості, яка амортизується, на строк корисного використання ПЗ.

Вартість закупівлі «Комплексу «Гриф» версії 4» складає 8948 грн. Строк використання складає 10 роки , залишкова вартість 0 грн.

Річний фонд амортизаційних відрахувань «Комплексу «Гриф» версії 4» складає:

$$С_а(ГРИФ) = \frac{89480-0}{10} = 8948, \text{ грн} \quad (3.7)$$

Вартість річної підписки сервісу VPN ZenMate - 852 грн\рік. Строк використання складає 1 рік , залишкова вартість 0 грн.

Річний фонд амортизаційних відрахувань VPN ZenMate складає:

$$С_а(VPN) = \frac{852}{1} = 852 \text{ грн} \quad (3.7)$$

Разом, річний фонд амортизаційних відрахувань складає:

$$С_а = 8948 + 852 = 9800, \text{ грн} \quad (3.7)$$

Річний фонд заробітної плати інженерно-технічного персоналу розраховується по формулі:

$$С_з = З_{осн} + З_{дод}, \text{ грн} \quad (3.8)$$

де $З_{осн}$ та $З_{дод}$ – є основною та додатковою заробітною платою відповідно, грн/рік.

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

Основна заробітна плата спеціалісті з інформаційної безпеки на місяць складає 12000 грн/міс та 144000 грн/рік. Додаткова заробітна плата – 1500 грн/міс та 18000 грн/рік. Виконання робіт щодо впровадження системи захисту інформації на підприємстві потребує залучення спеціаліста інформаційної безпеки на 0,1 ставки. Отже:

$$С_з = (144000 + 18000) * 0{,}1 = 16200, \text{ грн} \quad (3.9)$$

Ставка ЄСВ для всіх категорій платників з 01.012022 складає 22%.

$$С_{єв} = 16200 * 0{,}22 = 3564, \text{ грн} \quad (3.10)$$

Вартість електроенергії розраховується за формулою:

$$С_{ел} = P * F_P * Ц_е, \text{ грн} \quad (3.11)$$

де, Р – встановлена потужність апаратури інформаційної безпеки, кВт;

$F_р$ – річний фонд робочого часу системи інформаційної безпеки;

$Ц_е$ – тариф на електроенергію, грн/кВт*годин.

$$C_{ел} = 0,6 * 7 * 2160 * 1,68 = 15240,96, \text{грн} \quad (3.11)$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат – 2%.

$$C_{тос} = 9800 * 0,02 = 196, \text{грн} \quad (3.12)$$

Можна розрахувати витрати на керування системи інформаційної безпеки:

$$C_к = 9800 + 16200 + 3564 + 15240,96 + 196 = 45000,96, \text{грн} \quad (3.13)$$

Таким чином;

$$C = 45000,96 \text{ грн} \quad (3.14)$$

3.4 Оцінка збитків у разі виникнення загроз

3.4.1 Оцінка величини збитку

Ця оцінка проводиться для визначення обсягів матеріальних збитків, виходячи з ймовірності реалізації конкретної загрози й можливих матеріальних втрат від неї.

Заробітна плата працівників підприємства зазначена в табл. 3.1.

Таблиця 3.1 - Заробітна плата працівників підприємства.

Посада	Розмір заробітної плати в місяць, грн
Директор	45000
Системний адміністратор	20000
Бухгалтер	25000
Розробник 1	30000
Розробник 2	30000
Розробник 3	30000
Тестувальник 1	15000

Продовження таблиці 3.1

Посада	Розмір заробітної плати в місяць, грн
Тестувальник 2	15000
Тестувальник 2	15000

Загальна сума заробітних плат працівників підприємства становить 225000 грн.

Необхідні вихідні дані для розрахунку:

$t_п$ – час простою вузла або сегмента мережі підприємства внаслідок атаки, 6 годин;

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

$t_{ви}$ – час повторного введення загубленої інформації працівниками, 1 година;

$З_о$ – заробітна плата обслуговуючого персоналу, 17000 грн на місяць;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 225000 грн на місяць;

$Ч_о$ – чисельність обслуговуючого персоналу, 1 особа;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 9 осіб;

О – обсяг продажів атакованого вузла або сегмента корпоративної мережі, 6000000 грн у рік;

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

I – число атакованих вузлів або сегментів корпоративної мережі, 1;

N – середнє число атак на рік 4.

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

$$U = П_п + П_в + V \tag{3.15}$$

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;

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

Витрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі розраховується за формулою:

$$П_п = \frac{\sum Зс}{F} * t_п \quad (3.16)$$

де, F – місячний фонд робочого часу (при 45-и годинному робочому тижні становить 198 годин)

$$П_п = \frac{225000*4}{198} * 6 = 27272{,}73, \text{ грн} \quad (3.16)$$

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають такі складові;

$$П_в = П_{ви} + П_{пв} + П_{зч} \quad (3.17)$$

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 розраховуються за формулою:

$$П_{ви} = \frac{\sum Зс}{F} * t_{ви} \quad (3.18)$$

$$П_{ви} = \frac{225000*4}{198} * 1 = 4545{,}45, \text{ грн} \quad (3.18)$$

Витрати для відновлення вузла або сегмента корпоративної мережі розраховується за формуло:

$$П_{пв} = \frac{\sum Зо}{F} * t_в \quad (3.19)$$

$$П_{пв} = \frac{17000*1}{198} * 3 = 257{,}58, грн \quad (3.19)$$

Отже упущена вигода дорівнює;

$$П_{в} = 4545{,}45 + 257{,}58 = 4803{,}03, грн \quad (3.17)$$

Витрати на зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента розраховується за формулою:

$$V = \frac{O}{F_r} * (t_п + t_в + t_{ви}) \quad (3.20)$$

де, $F_г$ – річних фонд часу роботи організації, 1800 годин.

$$V = \frac{6000000}{1800} * (6 + 3 + 1) = 33333{,}33, грн \quad (3.20)$$

Упущена вигода від простою дорівнює:

$$U = 27272{,}73 + 4803{,}03 + 33333{,}33 = 65409{,}09, грн \quad (3.15)$$

Таким чином, загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складає:

$$B = \sum i \sum n\, U \quad (3.21)$$

$$B = 1 * 4 * 65409{,}09 = 261636{,}37, грн \quad (3.21)$$

Отже загальний збиток від атаки на вузол або сегмент корпоративної мережі організації дорівнює 261636,37 грн

3.4.2 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B * R - C \quad (3.22)$$

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

мережі, грн;

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

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

$$E = 261636{,}37 * 0{,}24 - 45000{,}96 = 17791{,}77 \text{ грн} \quad (3.22)$$

Таким чином, загальний ефект від впровадження системи інформаційної безпеки становить:

$$E = 17791{,}77 \text{ грн} \quad (3.22)$$

3.5 Визначення та аналіз показників економічної ефективності

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

- сукупна вартість володіння (ТСО) – використовується, коли величину відверненого збитку від атаки на вузол або сегмент корпоративної мережі важко або неможливо визначити у вартісній формі;
- коефіцієнт повернення інвестицій (ROSI) – показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки;
- термін окупності капітальних інвестицій (T_o) – показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки.[11]

Щодо інформаційної безпеки говорять не про прибуток, а про запобігання можливих витрат від атаки на сегмент або вузол корпоративної мережі, а отже

$$ROSI = \frac{E}{K} \quad (3.23)$$

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

грн;

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

Таким чином,

$$ROSI = \frac{17791,76}{97643} = 0,18, \text{ частки одиниці} \quad (3.23)$$

Термін окупності капітальних інвестицій (T_o) розраховується за формулою:

$$T_o = \frac{K}{E} = \frac{1}{ROSI} \quad (3.24)$$

$$T_o = \frac{1}{0,18} = 5,56 \text{ років} \quad (3.24)$$

Таким чином, капітальні інвестиції окупляться приблизно за 8,3 місяців.

3.6 Висновки до економічного розділу

В цьому розділі було визначено доцільність впровадження запропонованих рішень безпеки інформації інформаційно-телекомунікаційної системи ТОВ «Reni». Було проведено наступні розрахунки:

1. Капітальні витрати на впровадження на експлуатацію політики безпеки інформації становить 97643 грн;
2. Повна вартість річних експлуатаційних витрат становить 45000,96 грн;
3. Загальний збиток від атаки становить 261636,37 грн;
4. Загальний ефект від впровадження системи інформаційної безпеки становить 17791,76 грн;
5. Термін окупності капітальних інвестицій становить 5,56 років.

Отже запропоновані рішення для забезпечення безпеки ІТС ТОВ «Reni» може вважатися цілком економічно доцільними.

ВИСНОВКИ

У першому розділі кваліфікаційної роботи були проаналізовані загальні відомості про підприємство «Reni» та були визначені підстави для створення КСЗІ на ньому.

В ході проведення аналізу були обстежені середовища функціонування ІТС: фізичне середовище, обчислювальна система, інформаційне та середовище користувачів. Була розроблена модель порушника та модель загроз.

Спираючись на модель загроз та вразливостей був обраний профіль захищеності. Згідно з обраним профілем захищеності були описані послуги, які вже є на даному підприємстві. І визначені послуги які необхідно реалізувати додатково задля забезпечення необхідного рівня захищеності АС.

Запропоновано проектні рішення стосовно реалізації необхідного рівня захисту. А саме впровадження використання «Комплексу «Гриф» версії 4» та використання сервісу VPN ZenMate. Також били визначенні додаткові організаційні заходи.

Проектні рішення запропоновані для ТОВ «Reni» є економічно доцільними, оскільки коефіцієнт повернення інвестицій ROSI складає 0,18 частки одиниці, що означає окупність капітальних вкладень, на впровадження запропонованих рішень інформаційної безпеки підприємства, за 5,56 років. Отримане значення коефіцієнту повернення інвестицій значно вище дохідності альтернативного вкладення коштів.

Впровадження VPN ZenMate дозволить забезпечити достатній рівень безпеки передачі інформації. А саме безпеку від можливого перехоплення інформації при передачі її зовнішнім незахищеним каналом. А також забезпечить шифрування переданої інформації завдяки виконанню стандарту AES-256 та протоколам IPSec. Використання комплексу «Гриф» версії 4 дозволить забезпечити реалізацію керування знімних або незнімних носіями, захищеними логічними дисками, вся інформація на яких зберігається у зашифрованому

вигляді. Також забезпечить розмежування доступу до їх вмісту з використанням механізмів "прозорого" розшифрування (шифрування) даних у момент їх читання (запису), що дозволить забезпечити захист конфіденційності збереженої інформації навіть у випадку крадіжки робочої станції або відповідних носіїв.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України "Про інформацію" [Електронний ресурс] // 2657-XII. 01.01.2017. Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2657- 12.
2. НД ТЗІ 1.6-005-2013 "Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці" [Електронний ресурс].— 2013. Режим доступу до ресурсу: https://tzi.com.ua/downloads/1.6-005-2013.pdf
3. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" [Електронний ресурс] // 80/94-ВР. — 19.04.2014. Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/80/94-вр.
4. ДСТУ 3396.2-97 "Захист інформації. Технічний захист інформації. Терміни та визначення." [Електронний ресурс]. — 1998. Режим доступу до ресурсу: https://tzi.com.ua/478.html
5. НД ТЗІ 1.1-003-99 "Термінологія в галузізахисту інформації в комп'ютерних системах від несанкціонованого доступу" [Електронний ресурс]. 1999. Режим доступу до ресурсу: https://tzi.com.ua/downloads/1.1-003-99.pdf.
6. НД ТЗІ 3.7-003-05 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі" [Електронний ресурс]. — 2005. Режим доступу до ресурсу: https://tzi.com.ua/downloads/3.7-003-2005.pdfє
7. НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу" [Електронний ресурс]. 1999. Режим доступу до ресурсу: https://tzi.ua/ru/nd tz 2.5-004-99.html .

8. НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від “ 28 ” квітня 1999 р. № 22 . Режим доступу до ресурсу: https://tzi.com.ua/downloads/2.5-005%20-99.pdf
9. НД ТЗІ 1.1-002-99 "Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступ" [Електронний ресурс]. від 28.12.2012 .Режим доступу до ресурсу:yhttps://tzi.com.ua/downloads/1.1-002-99.pdf
10. НД ТЗІ 1.4-001-2000 " Типове положення про службу захисту інформації в автоматизованій системі " [Електронний ресурс] – 2000 – Режим доступу до ресурсу: https://tzi.com.ua/downloads/1.4-001-2000.pdf
11. " Засоби ТЗІ, які мають експертний висновок про відповідність до вимог технічного захисту інформації " [Електронний ресурс] – 07.02.2022 – Режим доступу до ресурсу: https://cip.gov.ua/ua/news/zasobi-tzi-yaki-mayut-ekspertnii-visnovok-pro-vidpovidnist-do-vimog-tekhnichnogo-zakhistu-informaciyi
12. Програмні продукти виробництва ТОВ «Інститут комп’ютерних технологій» [Електронний ресурс]- Режим доступу до ресурсу: http://www.ict.com.ua/?lng=1&sec=19
13. Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека / Упорядн.: Д.П. Пілова. – Дніпро: Національний технічний університет «Дніпровська політехніка», 2019. – 16 с.
14. Методичні рекомендації до виконання кваліфікаційних робіт бакалаврів спеціальності 125 Кібербезпека / Упоряд.: О.В. Герасіна, Д.С. Тимофєєв, О.В. Кручінін, Ю.А. Мілінчук – Дніпро: НТУ «ДП», 2020. – 47 с.

ДОДАТКИ

Додаток А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість аркушів	Примітки
Документація				
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	Розділ 1. Стан питання. Постановка задачі	54	
6	А4	Розділ 2. Спеціальна частина	10	
7	А4	Розділ 3. Економічна частина	11	
8	А4	Висновок	2	
9	А4	Перелік посилань	2	
10	А4	Додаток А. Відомість матеріалів кваліфікаційної роботи	1	
11	А4	Додаток Б. Перелік документів на оптичному носії	1	
12	А4	Додаток В. Відгук керівника кваліфікаційної роботи	2	
13	А4	Додаток Г. Відгук керівника економічного розділу	1	
14	А4	Додаток Д. Політики безпеки які застосовані на підприємстві	1	

Додаток Б. Перелік документів на оптичному носі

1. Хричов_ОВ_125-18-2_ПЗ.doc
2. Хричов_ОВ_125-18-2_ПЗ.pdf
3. Хричов_ОВ_125-18-2_ПЗ.pdf.p7s
4. Хричов_ОВ_125-18-2_презентація.pptx

Додаток В. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125-18-2

Хричова Олександра Вадимовича

на тему: «Комплексна система захисту інформації інформаційно-телекомунікаційної системи ТОВ «Reni»»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на_____сторінках.

Метою кваліфікаційної роботи є забезпечення заданого рівня безпеки інформації, яка обробляється в ІТС ТОВ «Reni».

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: обстеження середовищ функціонування ІТС, розробка моделі порушника, визначення актуальних загроз, формування вимог до захисту інформації та розробка проектних рішень їх реалізації.

Запропоновано правила доступу до зовнішніх носіїв, доступу до Інтернет. Розроблені проектні рішення: з впровадження додаткового КЗЗ та системи VPN.

Практичне значення результатів кваліфікаційної роботи полягає у адаптації запропонованих рішень до особливостей ІТС та самого ТОВ «Reni».

До недоліків відноситься:

- недостатньо обґрунтована модель загроз та профіль захищеності;
- відсутність комплексного підходу та недостатність обґрунтування проектних рішень.

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

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

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

Кваліфікаційна робота заслуговує оцінки «_____».

Керівник кваліфікаційної роботи, професор **Корнієнко В.І.**

Керівник спец. розділу, ст. викладач **Кручінін О.В.**

Додаток Г. Відгук керівника економічної частини

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 90 б. («відмінно»).

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (ініціали, прізвище)

Додаток Д. Політики безпеки які застосовані на підприємстві

ПОЛІТИКА ЗАХИСТУ ПАРОЛІВ

1. Опис

Паролі є важливим аспектом безпеки комп'ютера. Неправильно обраний пароль може призвести до несанкціонованого доступу та / або експлуатації ресурсів. Весь персонал, які мають доступ до систем, несуть відповідальність за вжиття відповідних заходів, як зазначено нижче, для вибору та захисту своїх паролів.

2. Мета

Метою цієї політики є встановлення стандарту для створення стійких паролів та захисту цих паролів.

3. Сфера застосування

Ця політика стосується всього персоналу, який несе відповідальність за обліковий запис (або будь-який вид доступу, який підтримує або вимагає пароль).

4. Політика

4.1 Створення пароля

- Користувачі повинні використовувати окремий унікальний пароль для кожного з своїх робочих облікових записів. Користувачі не можуть використовувати будь-які пов'язані з роботою паролі для власних особистих облікових записів.

- Облікові записи користувачів, які мають привілеї на рівні системи, надані через членство в групах повинні мати унікальний пароль з усіх інших облікових записів, що зберігаються цим користувачем, для доступу до прав на рівні системи.

4.2 Захист паролем

- Паролі не повинні бути доступними жодному іншому, включаючи керівників та колег. Усі паролі слід розглядати як чутливі, конфіденційну інформацію Корпоративна інформаційна безпека визнає, що застарілі програми не підтримують проксі-системи. Будь ласка, зверніться до технічної довідки для додаткової інформації.

- Паролі не повинні вставлятися в електронні листи, справи Альянсу або інші форми електронного зв'язку, а також не розкриваються по телефону нікому.

- Паролі можуть зберігатися лише в уповноважених організацією.

- Не використовуйте функцію "Запам'ятати пароль" у програмах (наприклад, веб-браузери).

- Будь-який користувач, який підозрює, що його / її пароль може бути скомпрометований, повинен повідомити про інцидент та змінити всі паролі.

ПОЛІТИКА ВИКОРИСТАННЯ ІНТЕРНЕТУ

1. Опис

Доступ до інтернету персоналу, який не відповідає діловим потребам, призводить до неправильного використання ресурсів. Це може негативно вплинути на продуктивність через час, який витрачений на персональне використання інтернету, або його «серфінг». Крім того, компанія може зіткнутися з втратою репутація через некоректну діяльність в інтернеті.

2. Мета

Метою даної політики є визначення правильного використання інтернету співробітникам ТОВ «Reni» .

3. Сфера застосування

Політика використання інтернету застосовується до всіх співробітників компанії, які мають доступ до інтернету через обчислювальні або мережеві

ресурси ТОВ «Reni». Очікується, що користувачі інтернетом ознайомлені з цією політикою та дотримуються її вимог.

4. Політика

4.1. Використання ресурсів

Доступ до інтернету повинен бути затверджений власником компанії, та надаватися лише в разі виявлення потреб для бізнесу. Інтернет-послуги будуть надаватися лише на основі поточних обов'язків працівника. Якщо працівник змінює службові функції, новий запит на доступ до інтернету повинен бути поданий протягом 3 днів. Доступ до інтернету окремих працівників періодично переглядаються системними адміністраторами, щоб забезпечити наявність постійних потреб.

4.2. Дозволене використання

Інтернет використовується лише з метою підтримки ділової діяльності, необхідної для використання робочих функцій. Усі користувачі повинні дотримуватися корпоративних принципів щодо використання ресурсів та інтернету.

Дозволене використання інтернету для виконання робочих функцій включає:

- зв'язок між працівниками та не працівникам в комерційних цілях;
- завантаження програмних оновлень, патчів;
- огляд робочих веб-сайтів для довідки, навчання та допомоги в вирішенні робочих питань;

4.3. Заборонене використання

Забороняється придбання, зберігання та розповсюдження даних, які є незаконними, порнографічними або які негативно відображають расу, секс, чи вірування.

Компанія також забороняє ведення підприємницької діяльності, політичної діяльності, збір інформації на підприємстві, участь у шахрайській діяльності, навмисне розповсюдження неправдивих або наклепницьких матеріалів.

Інші види діяльності, які категорично заборонені:

- доступ до інформації компанії, яка не входить до сфери роботи співробітника. Це включає в себе неавторизоване читання інформації про клієнтів, несанкціонований доступ до персональної інформації, та доступ до будь-якої інформації, яка не потрібна задля належного виконання робочих функцій;
- зловживання, розголошення без належного дозволу або зміна інформації про клієнтів або персонал. Це включає внесення неавторизованих змін у файли персоналу, чи обмін електронними даними клієнтів чи персоналу;
- будь-яка поведінка, яка спричиняє або сприяє кримінальному злочину, призводить до цивільної відповідальності або іншим чином порушує будь-які положення та законодавства;
- використання, передача, копіювання або добровільне отримання матеріалу, який порушує авторські права, торгівельні марки, комерційні таємниці чи патенти будь-якої особи чи організації. Припущено, що всі матеріали в інтернеті захищені авторськими правами та / або запатентовані, якщо спеціальні повідомлення не встановлюють інше;
- передача будь-якої конфіденційної інформації без належного дозволу;
- будь-яка форма азартних ігор.

Якщо спеціально не дозволено власником компанії, жорстко забороняється також така діяльність:

- неавторизоване завантаження будь-яких умовно-безкоштовних програм або файлів для використання без дозволу системного адміністратора;
- будь-яке замовлення товарів чи послуг в інтернеті;
- участь в будь-якому онлайн конкурсі чи акції.

Пропускна спроможність інтернету у межах компанії – загальний, кінцевий ресурс. Користувачі повинні розумно використовувати його таким чином, щоб це не вплинуло на інших працівників.

5. Винятки

Будь-яке виключення з цієї політики має бути затверджене директором компанії ТОВ «Reni» заздалегідь.

6. Відповідальність

Працівник, який порушив цю політику, може бути притягнутий до покарання у виді штрафу, догани, а в тяжких випадках може призвести до звільнення.

ПОЛІТИКА ВСТАНОВЛЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

1. Огляд

Дозвіл працівникам встановлювати програмне забезпечення на обчислювальні машини компанії відкриває організацію до необґрунтованих загроз. Приклади проблем, які можуть реалізуватися через цю загрозу: конфлікт версії файлів або бібліотек DLL, які можуть перешкоджати запуску програм; введення шкідливого програмного забезпечення з інфікованих програм; встановлення неліцензованого програмного забезпечення; встановлення програм, які можуть використовуватися для зламу мережі організації.

2. Мета

Мета цієї політики полягає у визначенні вимог щодо програмного забезпечення, яке встановлюється на комп'ютерах, що належать компанії. Мінімізація ризику втрати функціональності робочих програм, втрати ІзОД, що зберігається на комп'ютерах компанії. Зменшення ризику введення шкідливого програмного забезпечення у систему.

3. Сфера застосування

Ця політика застосовується до всіх співробітників ТОВ «Reni». Ця політика охоплює усі комп'ютери, смартфони, планшети та інші обчислювальні пристрої, що належать і працюють у межах компанії.

4. Політика

- Працівники не можуть встановлювати програмне забезпечення на комп'ютери, що працюють в мережі компанії.
- Запити на встановлення програмного забезпечення повинні схвалюватися систем адміністратором.
- Програмне забезпечення повинно бути обране із затвердженого списку програм, який ведеться систем адміністратором, за винятком випадків,

коли вибір у списку відповідає вимогам запитувача.

- Системний адміністратор отримує та слідкує за ліцензіями програмного забезпечення, перевіряє на конфлікти та сумісність, а також виконує встановлення та оновлення програм.

5. Винятки

Будь-яке виключення з політики моє бути затверджене системним адміністратором та директором ТОВ «Reni» .

6. Відповідальність

Працівник, який порушив цю політику, може бути притягнутий до покарання у виді штрафу, догани, а в тяжких випадках може призвести до звільнення.

ПОЛІТИКА ЕЛЕКТРОННОЇ ПОШТИ

1. Огляд

Електронна пошта широко використовується у компанії і часто є основним методом спілкування підприємства з партнерами. У той же час, неправильне використання електронної пошти може поставити багато ризиків юридичного характеру, конфіденційності та безпеки, тому для користувачів важливо розуміти належне використання електронних засобів зв'язку.

2. Мета

Мета цієї політики полягає у забезпеченні належного використання системи електронної пошти ТОВ «Reni» та інформування користувачів про те, що ТОВ «Reni» вважає прийнятним та неприйнятним використання поштової системи. Ця політика визначає мінімальні вимоги до використання електронної пошти.

3. Сфера застосування

Ця політика охоплює належне використання будь-якого електронного листа, надісланого з адреси електронної пошти ТОВ «Reni» і застосовується до всіх працівників.

4. Інструкція політики

- використання електронної пошти повинне відповідати політиці та процедурам етичної поведінки, безпеці, відповідності діючим законам та належній діловій практиці.

- поштові облікові засоби ТОВ «Reni» повинні використовуватися в першу чергу для цілей ТОВ «Reni» .

- особисте спілкування, яке не пов'язане з комерційним використанням електронної пошти, заборонено;

- електронна пошта ТОВ «Reni» не повинна використовуватися для створення або розповсюдження будь-яких зловмисних або образливих повідомлень, включаючи нав'язливі коментарі про расу, стать, колір волосся, інвалідність, вік, сексуальну орієнтацію, порнографію, релігійні переконання та практику, політичні переконання або національне походження.

- користувачам забороняється автоматично пересилати повідомлення електронної адреси ТОВ «Reni» до сторонньої електронної пошти. Окремі повідомлення, які пересилаються користувачем, не повинні містити конфіденційну інформації.

- електронна листи на електронній пошті ТОВ «Reni» повинні зберігатися, лише якщо вони відповідають незакінченому діловому листуванню. У всіх інших випадках інформація не повинна зберігатися на електронній пошті.

5. Відповідальність

Відповідальний за виконання політики безпеки є директор підприємства. Контроль та виконання лягають на нього.

6. Дії при порушенні

Працівник, який порушив цю політику, може бути предметом дисциплінарної відповідальності, включаючи припинення його роботи.