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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Брижатої Наталії Юріївни*

академічної групи *125-16-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплексна система захисту інформації відділу розробки сільськогосподарської техніки ТОВ «Промислова Група «Корсунь»*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.е.н., доц. Герасіна О.В.			
розділів:				
спеціальний	ст. викл. Тимофєєв Д.С.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Тимофєєв Д.С.			

Дніпро
2020

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Брижатій Наталії Юріївні*** **академічної групи** ***125-16-2***
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Комплексна система захисту інформації відділу розробки сільськогосподарської техніки ТОВ «Промислова Група «Корсунь»***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 26.05.2020 № 275-с

Розділ	Зміст	Термін виконання
Розділ 1	Проаналізувати стан інформаційної безпеки та особливості організації захисту інформації на підприємствах, які займаються розробкою сільськогосподарської техніки	29.03.2020
Розділ 2	Обстеження на ОІД, аналіз середовища функціонування, аналіз ризиків, розробка основних положень КСЗІ.	24.05.2020
Розділ 3	Економічна доцільність впровадження КСЗІ, розрахунок витрат та ефекта впровадження КСЗІ.	10.06.2020

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

Дата видачі: 08.01.2020р.

Дата подання до екзаменаційної комісії: 15.06.2020р.

Прийнято до виконання _____ Брижата Н. Ю.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 76 с., 5 рис. 27 табл., 7 додатків, 20 джерел.

Об’єкт дослідження: інформаційно-телекомунікаційна система відділу розробки сільськогосподарської техніки ТОВ «Промислова Група «Корсунь».

Предмет дослідження: комплексна система захисту інформації.

Мета роботи: підвищення ефективності рівня захіщенності в ІТС відділу розробки сільськогосподарської техніки ТОВ «Промислова Група «Корсунь».

Методи розробки: спостереження, порівняння, аналіз, опис.

Актуальність теми визначається необхідністю захисту інформації в інформаційно-телекомунікаційній системі ТОВ «Промислова Група «Корсунь».

В першому розділі кваліфікаційної роботи надано загальний аналіз проблем забезпечення безпеки інформації України, розглянуто стан інформаційної безпеки на підприємствах, які займаються розробкою сільськогосподарської техніки.

В другому розділі кваліфікаційної роботи виконана розробка КСЗІ. Наведено загальні відомості про об’єкт інформаційної діяльності. Проведено обстеження об’єкту інформаційної діяльності, категоріювання інформаційно-телекомунікаційної системи, обрано профіль захищеності. Визначені основні загрози.

В третьому розділі кваліфікаційної роботи розраховано доцільність впровадження та використання КСЗІ , економічну ефективність впровадження її елементів в інформаційно-телекомунікаційну систему на об’єкті інформаційної діяльності.

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

РЕФЕРАТ

Пояснительная записка: 67 с., 5 рис. 27 табл., 7 приложений, 20 источников.

Объект исследования: информационно-телекоммуникационная система отдела разработки сельскохозяйственной техники ООО «Промышленная Группа «Корсунь».

Цель работы: разработка и внедрение КСЗИ для ИТС отдела разработки сельскохозяйственной техники ООО «Промышленная Группа «Корсунь».

Методы разработки: наблюдение, сравнение, анализ, описание.

Актуальность темы определяется необходимостью защиты информации в информационно-телекоммуникационной системе ООО «Промышленная Группа Корсунь».

В первом разделе квалификационной работы предоставлено общий анализ проблем обеспечения безопасности информации Украины, рассмотрено состояние информационной безопасности на предприятиях, занимающихся разработкой сельскохозяйственной техники.

Во втором разделе квалификационной работы рассмотрена необходимость разработки КСЗИ, состояние информационной безопасности в настоящее время. Приведены общие сведения об объекте информационной деятельности. Проведено обследование объекта информационной деятельности, категорирование информационно-телекоммуникационной системы, подобрано профиль защищенности. Рассчитаны коэффициенты вероятности реализации угроз, разработанные комплексные системы защиты информации на предприятии.

В третьем разделе квалификационной работы рассчитаны целесообразность внедрения и использования КСЗИ, экономическую эффективность внедрения ее элементов в информационно-телекоммуникационную систему на объекте информационной деятельности.

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

ABSTRACT

Explanatory note: 67 pp., 5 figs. 25 tablets, 7 appendix, 20 sources.

Object of research: information and telecommunication system of the department of development of agricultural machinery of LLC Industrial Group "Korsun`".

Purpose: development and implementation of CIPS (comprehensive information protection system) for ITS of the department of development of agricultural machinery of Industrial Group "Korsun`".

Development methods: observation, comparison, analysis, description.

The relevance of the topic is determined by the need to protect information in the information and telecommunications system of LLC "Industrial Group Korsun".

The first section of the qualification work provides a general analysis of the problems of information security of Ukraine, the state of information security at enterprises engaged in the development of agricultural machinery.

The second section of the qualification work considers the need to develop KSZI, the state of information security at present. General information about the object of information activity is given. The object of information activity was surveyed, the information and telecommunication system was categorized, the security profile was selected. Coefficients of probability of realization of threats are calculated, complex systems of protection of the information for the enterprise are developed.

In the third section of the qualification work the expediency of introduction and use of CIPS, economic efficiency of introduction of its elements in information and telecommunication system on object of information activity is calculated.

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

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

В роботі використовуються такі позначення і скорочення**:**

АС - автоматизована система;

ДСТУ - державний стандарт України;

ІзОД — інформація з обмеженим доступом;

ІТС – інформаційно-телекомунікаційна система;

КЗЗ — комплекс засобів захисту;

КС — комп'ютерна система;

КСЗІ — комплексна система захисту інформації;

НД — нормативний документ;

НД ТЗІ - нормативний документ системи технічного захисту інформації;

НСД — несанкціонований доступ;

ОІД – об’єкт інформаційної діяльності;

ОС — обчислювальна система;

ПЗ — програмне забезпечення;

ЗМІСТ

ВСТУП

Розвинуте сільськогосподарське машинобудування є індикатором розвитку АПК (агропромислового комплексу) будь-якої країни. Висока механізація праці є запорукою зростання обсягів і якості виготовленої сільгосппродукції. У той же час неповна забезпеченість галузі необхідною кількістю сільськогосподарської техніки є серйозним бар'єром для розвитку сільського господарства. Україна володіє унікальним аграрним потенціалом - будучи одним з найбільших зерносіючих і зернопереробних регіонів світу. Майбутнє сільського господарства України - у використанні високопродуктивних і високорентабельних технологій, які, в свою чергу, є основою для досягнення конкурентоспроможності українського продовольства. Сьогодні всі основні етапи розробки сільськогосподарської техніки припадає на комп'ютерні системи. Але для безпечного функціонування підприємства потрібно забезпечувати безпеку інформації. За оцінками експертів Асоціації підприємств промислової автоматизації України (АППАУ і національного руху «Індустрія 4.0 (І 4.0) в Україні, за швидкістю та об'ємами впровадження І 4.0 Україна, маючи для цього великий і подекуди унікальний потенціал, все ж поки демонструє порівняно скромні результати і відстає від всіх своїх основних сусідів у Північній та Східній Європі, включаючи РФ та Казахстан. Проте у коротко- та середньостроковій перспективі це жодним чином не нівелює гостроту викликів, пов'язаних з модернізацією національної системи кібербезпеки згідно з потребами розвитку цифрової економіки та суспільства. На даному етапі в Україні відчувається, зокрема, певний дефіцит відповідного нормопроектного забезпечення, особливо на тлі розвинених країн. Нині держава має чинний закон «Про основні засади забезпечення кібербезпеки України», стратегію кібербезпеки України і «Концепцію розвитку цифрової економіки та суспільства України на 2018-2020 роки».

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

Наприкінці червня 2017 року Україна зазнала кібератаки вірусом-здирником Petya.A, яка завдала шкоди об’єктам “критичної інфраструктури” майже на півмільярда доларів. Серед постраждалих: “Ощадбанк” і “Укргазбанк”, Укрзалізниця, міжнародні аеропорти “Київ” і “Бориспіль”, Укрпошта, Київський метрополітен та Чорнобильська атомна електростанція.

Кібератака Petya.A добряче шокувала суспільство. Хоча вона не завдала невиправних збитків, саме тоді стало зрозуміло, наскільки ефективна зброя є в руках ворога, аби паралізувати усю країну. Стало також зрозуміло, що наступна масштабна кібератака може призвести і до людських жертв: за допомогою комп’ютера, сидячі за тисячі кілометрів від об’єкту, тепер можна і електропостачання перекрити для цілого регіону, заслонки греблі підняти на водосховищі, дезорганізувати авіарух. Тоді ж багато хто виступав з заявами, мовляв, нам треба заново будувати систему кіберзахисту в країні, і обіцянками таку систему швидко створити.

Підводячи підсумки 2019 року, ми відзначаємо такі тенденції:

- Кількість унікальних кіберінцидентів продовжило рости і на 11% перевищило показники аналогічного періоду в 2018 році;
- Стає більше шкідливого ПО, яке поєднує в собі функції троянів декількох типів. Гнучка модульна архітектура робить його універсальним. Наприклад, зловредів може демонструвати рекламу і одночасно з цим красти призначені для користувача дані;
- Продовжує зменшуватися частка прихованого Майнінг (7% проти 9% в IV кварталі 2018 року). Хакери почали модернізувати Майнер до рівня багатофункціональних троянів. Потрапивши в систему з низькими обчислювальними ресурсами, де Майнінг малоефективний, такий троян активує функції шпигунського ПЗ і крадедані;

- Зростає число заражень шифрувальником (24% проти 9% в IV кварталі 2018 року). Досить часто даний тип шкідливого ПЗ використовується в комбінації з фішингом, причому зловмисники винаходять нові способи обдурити користувачів і спонукати їх заплатити викуп;
- Медичні установи - найпоширеніші жертви троянів-шифрувальників. Можливо, керівництво організацій охорони здоров'я більш охоче погоджується заплатити викуп, ніж інші компанії, адже на кону виявляються життя і здоров'я людей;
- Кібератаки на державу головним чином спрямовані або на крадіжку даних, для чого зловмисники використовують унікальне шпигунське ПЗ власної розробки, або на злом урядових веб-ресурсів з метою заразити їх відвідувачів шкідливим ПЗ;
- Розповсюдження шкідливих програм - головна загроза для великих промислових компаній. Атакуючи сферу промисловості, зловмисники найчастіше зацікавлені в комерційну таємницю. У зв'язку з цим не можна виключати, що атаки шифрувальників на промисловість спрямовані на приховування слідів раніших інцидентів;
- Багатомільйонні витоки облікових записів ставлять під загрозу онлайн-сервіси. Зловмисники охоче використовують дані, які опинилися у відкритому доступі, для атак типу credentials stuffing;
- Атаки на веб-сайти з впровадженням шкідливого JavaScript-коду (JS-сніфферов), який краде дані банківських карт, ставлять під загрозу користувачів інтернет-магазинів і онлайн-сервісів з функцією оплати послуг.

У 2019 році зростання частки атак, спрямованих на отримання даних триває. Тепер більше половини хакерських атак відбуваються з метою розкрадання інформації. Зловмисники зацікавлені в найрізноманітніших даних - від особистого листування до комерційної таємниці. Але як і раніше найбільш високо цінуються облікові дані, персональні дані і дані платіжних карт.

На рисунку 1.1 зазначені основні мотиви порушників.

Рисунок 1.1 Мотиви порушників

На рисунку 1.2 показані основні типи цінної інформації що була об’єктом атаки.

На рисунку 1.3 описані основні категорії жертв кібератак.

- Рисунок 1.2 Основні типи цінної інформації

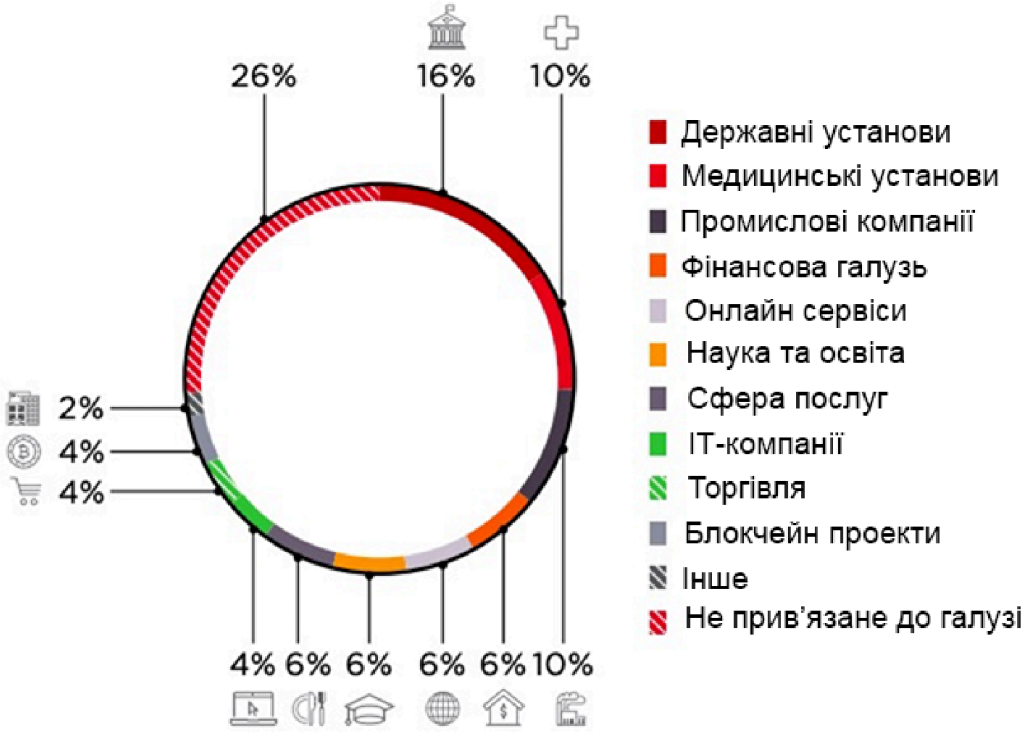


Рисунок 1.3 Категорії жертв кібератак

У 2019 року частка цілеспрямованих атак знизилася в порівнянні з 2018 роком і склала 47% проти 62%. Це пов'язано зі збільшенням частки атак, які не прив'язані до конкретної галузі; в основному мова йде про масові шкідливих кампаніях. Частка кіберінцідентів, у результаті яких постраждали приватні особи, практично не змінилася (21% проти 22% у 2018 року). Серед юридичних осіб найбільш часто зловмисники атакують державні організації, медичні установи, промислові компанії, банки та інші організації фінансової сфери.

В таблиці 1.1 наведена статистична характеристика кібератак в Україні.

Таблиця 1.1 Статистична характеристика кібератак

Розподілення кібератак		Державні установи	Медицинські утсанови	Промислові компанії	Фінансова галузь	Онлайн сервіси	Наука та освіта	Сфера послуг	ІТ компанії	Торгівля	Блокчейн проекти	Інше	Не прив’язане до
Всього атак		45	17	28	28	16	16	11	17	10	74	5	70
Об’єкт	Інфраструктура	29	14	27	17	7	7	10	10	2	17	6	2
	Веб-ресурс	13	2		8	9	3	1	5	5	8	2	3
	Користувачі	2	1	1	3		1		2	1	28	2	
	Мобільні притсрої	1									18		
Метод	Банкомати / термінали						5			2			
	Несанкціонований доступ	20	11	22	13	2	10	6	5	5	40	3	1
	Соціальна інженерія	10	10	20	9			1	4	2	42	3	

Продовження таблиці 1.1

	Розподілення кібератак	Державні установи	Медицинські утсанови	Промислові компанії	Фінансова галузь	Онлайн сервіси	Наука та освіта	Сфера послуг	ІТ компанії	Торгівля	Блокчейн проекти	Інше	Не прив’язане до галузі
	Перебір паролей		1		7	4	3	5	5		5	2	2
	Хакінг	7	2	6	2	3	2	2	4		5	5	1
	Єксплуатація веб вразливостей	13				5	1	2	2	6	3		2
	Інше	10	2			4		2	1		4		
Мотив	Фінансова вигода	8	4	3	9		3	3	5	2	33	4	2
	Отримання даних	18	10	24	19	9	12	7	8	7	33	6	2
	Хактивізм	18	3			7	1	1	4	1	8		1
	Кібервійна	1		1									

1.2 Аналіз нормативно-правового забезпечення захисту інформації

Під поняттям нормативно-правового забезпечення слід розуміти сукупність правових норм, що визначають порядок створення, правовий статус і функціонування захищених інформаційно-комунікаційних систем і мереж, регламентують порядок одержання, перетворення та використання інформації і інформаційних ресурсів.

Розробка КСЗІ ґрунтується у відповідності до вимог чинного законодавства України та на основі нормативно-правових документів, серед яких можна виділити:

- Закон України "Про інформацію»;
- Закон України "Про захист інформації в автоматизованих системах";
- НД ТЗІ 1.1-002-99: Загальні положення з захисту інформації в комп'ютерних системах від НСД (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. № 22);
- НД ТЗІ 1.1-003-99: Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. № 22);
- НД ТЗІ 1.4-001-2000: Типове положення про службу захисту інформації в автоматизованій системі (введено в дію Наказом ДСТСЗІ СБУ від 04.12.2000 р. № 53);
- НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. № 22).;
- ДСТУ ISO/IEC 27001:2015 - Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT)- На заміну ДСТУ ISO/IEC 27001:2010
- ДСТУ ISO/IEC 27005:2015 - Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT).
- стандарти ДСТУ ISO/IEC, що основані на міжнародних стандартах і відповідно до вимог, що висуваються до захисту інформації на підприємстві;
- 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.

1.3 Постановка задачі

На основі проаналізованих проблем у пункті 1.1, у якому були встановлені основні проблеми кібербезпеки підприємства сільгоспмашинобудування, ставимо задачу реалізувати КСЗІ в розділі 2.

Для розробки КСЗІ потрібно:

- Ознайомитись з особливостями підприємства;
- Проаналізувати фізичні характеристики об’єкту;
- Проаналізувати логічну характеристику об’єкту;
- Проаналізувати види інформації та особливості взаємодії інформації на об’єкті;
- Обрати профіль захищенності;
- Підібрати методи захисту.

1.4 Висновки до першого розділу

У першому розділі кваліфікаційної роботі було описано стан інформаційної захищенності в галузі сільського господарства в країні, наведені основні проблеми країни в плані кібербезпеки, проаналізована нормативно-правова база, що регулюють відносини у сфері інформаційних відносин у державі, поставлена задача для подальшої роботи кваліфікаційної роботи.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальні відомості про підприємство

Товариство з обмеженою відповідальністю «Промислова Група «Корсунь» займається розробкою та виготовленням сільськогосподарьскої техніки, надає також послуги ремонтування та розробки виробів з металу.

Основними напрямами діяльності є розробка борон, культиваторів, глибокорозпушувачів, котків, станків, ремонт ґрунтообробної техніки, ремонт тракторів та інші. Підприємство працює на базі колишнього верстатобудівничого заводу ім. Богдана Хмельницького.

Об’єктом іформаційної діяльності (надалі ОІД) є ІТС відділу розробки сількогосподарської техніки ТОВ "Промислова Група «Корсунь».

2.2 Обґрунтування необхідності створення КСЗІ

Підставою для необхідності створення КСЗІ є нормативно-правові акти, що розглянуті в Розділі 1, де вказані вимоги, які встановлюють обов’язковість обмеження доступу до певних видів інформації. Згідно з актом категоріювання об'єкту (Додаток Б), інформація яка обробляється на підприємстві не потребує обов'язкового захисту, але на підставі проведеного аналізу власником інформації, яким виступає директор, прийняте рішення щодо створення КСЗІ та видано наказ «Про визначення відповідального за забезпечення технічного захисту інформації та створення КСЗІ на ТОВ «Промислова Група «Корсунь»» (Додаток В).

На підприємстві наявна інформації, яка підлягає автоматизованій обробці та потребує захисту і забезпечення конфіденційності, цілісності та доступності відповідно до вимог нормативно-правових актів, розглянутих у розділі 1.

2.3 Організаційна структура підприємства

Кількість співробітникив компанії: 98 чоловік. Підприємство має виробничі площадки у місті Єрки Катеринопільсого району Черкаської області, де працює 37 чоловік, інші працюють у місті Корсунь-Шевченківський.

ОІД знаходиться в Адміністративній будівлі підприємства, тому його слід проаналізувати більш детально.

До складу Адміністративної будівлі входять такі відділи:

- Бухгалтерія;
- Інженерний відділ;
- Головне правління;
- Відділ маркетингу;
- Логістичний відділ;
- Приміщення для проводження навчання;
- Технічні приміщення (склади, їдальні, прибиральні).

Так як ОІД є інженерний відділ компанії, тому його треба описати більш детально. Інженерний відділ налічує 7 співробітників, які мають чітку ієрархію та розподілення обов'язків.

У відділі присутні:

- Генеральний інженер;
- Генеральний технолог;
- Інженер 1 категорії ;
- Інженер 2 категорії ;
- Інженер 2 категорії ;
- Технолог 1 категорії ;
- Технолог 2 категорії.

На рисунку 2.1 представлена структурна схема ІТС.

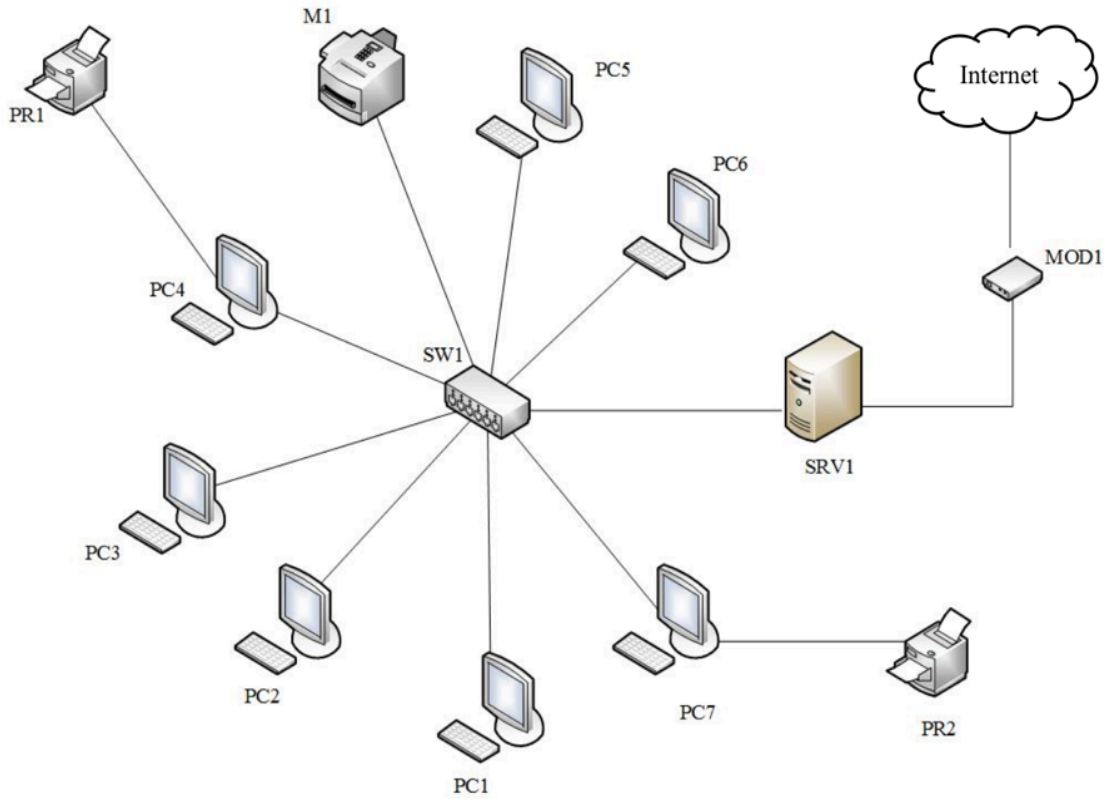


Рисунок 2.1. Структурна схема ІТС

2.4 Аналіз оброблюваної інформації

У відділі співробітниками обробляється інформація з обмеженим доступом: розробки планів оптимізації виробництва, інженерні моделі, креслення, документація з технології виробництва, звіти закупівель, документація зборки, програмні коди для програмування обладнання та інші. Вся документація існує у двох видах матеріальному та електронному, остання створюється працівниками на робочих станціях з інстальованим ПЗ, матеріальні копії створюються шляхом розмноження на принтері. Електронні копії зберігаються на робочій станції працівника та на центральому сервері. Після втрати чинності документи знищуються, облік місця та режиму зберігання носіїв інформації, а також її переміщення на підприємстві не відстежується.

Детальний перелік інформації, правовий режим, вид зберігання та вимогу до захисту наведено у таблиці 2.4.1.

К – вимоги до конфіденційності

Ц – вимога до цілісності

Д – вимога до доступності

Таблиця 2.1 Перелік основної інформації

№	Інформація	Вид зберігання	Режим доступу	Правовий режим	Вимоги до захисту
1	Розробки планів оптимізації виробництва	Електронний, паперовий	ІЗоД	Комерційна таємниця	КЦД
2	Звіти закупівель	Електронний, паперовий	ІЗоД	Комерційна таємниця	КЦД
3	Документація зборки	Електронний, паперовий	ІЗоД	Комерційна таємниця	КЦД
4	Інженерні моделі	Електронний	ІЗоД	Комерційна таємниця	КЦД
5	Креслення	Електронний, паперовий	ІЗоД	Комерційна таємниця	КЦД
6	Програмні коди для програмування обладнання	Електронний	ІЗоД	Комерційна таємниця	КЦД
7	Документація з технології обробки метелу	Електронний, паперовий	ІЗоД	Комерційна таємниця	КЦД
8	Документація з технології зварювання метелу	Електронний, паперовий	ІЗоД	Комерційна таємниця	КЦД
9	Норми виробництва	Електронний, паперовий	ІЗоД	Комерційна таємниця	КЦД
10	Стратегічний план розвитку	Електронний, паперовий	ІЗоД	Комерційна таємниця	КЦД
11	Звітність з дифіциту	Електронний, паперовий	ІЗоД	Комерційна таємниця	КЦД

Продовження таблиці 2.1

№	Інформація	Вид зберігання	Режим доступу	Правовий режим	Вимоги до захисту
12	Звідність з складів матеріалу	Електронний, паперовий	ІЗоД	Комерційна таємниця	КЦД
13	Технічні завдання інженерам	Електронний, паперовий	ІЗоД	Комерційна таємниця	КЦД
14	Технічні завдання технологам	Електронний, паперовий	ІЗоД	Комерційна таємниця	КЦД
15	Технічні завдання конструкторам	Електронний, паперовий	ІЗоД	Комерційна таємниця	КЦД
16	Документи постачання	Електронний, паперовий	ІЗоД	Комерційна таємниця	КЦД
17	Інформація про діяльність відділів	Електронний, паперовий	Відкрита	-	Ц

Таблиця 2.2 Матриця доступу до інформації

Інформація	Посада						
	Генеральний інженер	Генеральний технолог	Інженер 1 категорії	Інженер 2 категорії	Інженер 2 категорії	Технолог 1 категорії	Технолог 2 категорії
1	CRWDP	CRWDP	RW	R	R	RW	R
2	CRWDP	RP	RP	R	R	R	R
3	CRWDP	RP	CRWDP	RWP	RWP	RP	RP
4	CRWD	R	RWP	RWP	RWP	RW	R
5	CRWDP	CRWP	RWP	RWP	RWP	RWP	RWP
6	CRWD	R	R	R	CRWD	R	R
7	CRWDP	CRWDP	RWP	RW	RW	R	-
8	CRWDP	CRWDP	R	R	R	CRWDP	RW
9	CRWDP	CRWDP	RW	R	R	RW	R
10	CRWDP	RWP	RW	R	R	RW	R
11	CRWDP	CRWDP	CRWDP	R	R	CRWDP	R

Продовження до таблиці 2.2

Інформація	Посада						
	Генеральний інженер	Генеральний технолог	Інженер 1 категорії	Інженер 2 категорії	Інженер 2 категорії	Технолог 1 категорії	Технолог 2 категорії
12	CRWDP	RWP	RP	-	-	RP	-
13	CRWDP	-	RWP	R	R	-	-
14	-	CRWDP	-	-	-	RWP	R
15	CRWDP	CRWDP	RWP	RWP	RWP	CRWDP	RWP
16	CRWDP	R	R	R	-	R	-
17	-	-	-	-	-	-	-

C – create (право на створювання); R – read (право на зчитування); W – write (право на редагування); D – delete (право на видалення); P - print (право на друк).

На рисунку 2.2 показана схема інформаційних потоків.

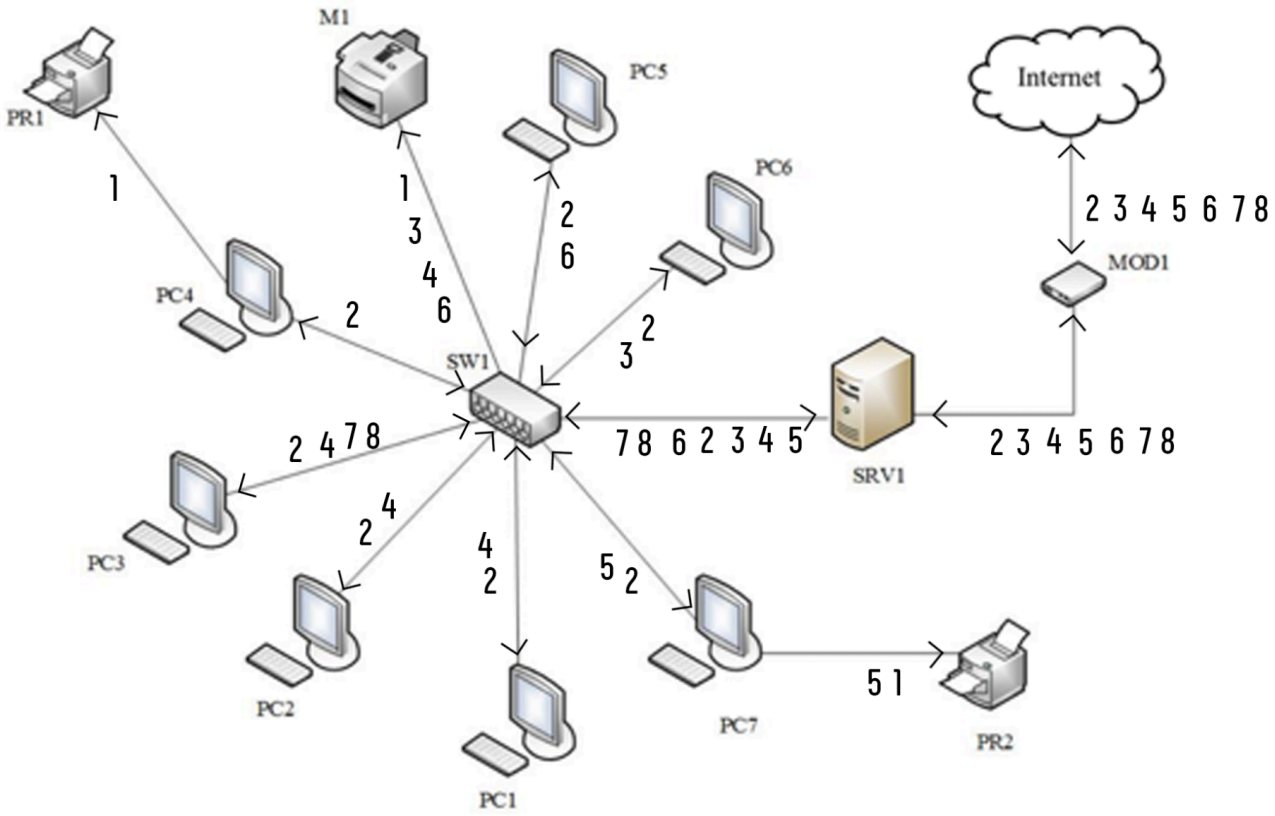


Рисунок 2.2 Схема інформаційних потоків.

2.5 Обстеження об’єкту інформаційної діяльності

Відділ розробки сільгосптехніки є об’єктом інформаційної діяльності, що досліджується в кваліфікаційній роботі. ОІД є складовою адміністративного відділу Компанії «Промислова Група «Корсунь», за адресою: Черкаська обл., м. Корсунь-Шевченківський, вул. Правобережна, 83. Приміщення ОІД знаходиться на 2 поверсі Адміністративної будівлі, займає 2 приміщеня.

Режим роботи підприємства:

Час роботи: 08.00 – 17.00

Перерва: с 12.00 до 13.00

Робочі дні: понеділок – п’ятниця.

За фізичну охорону ОІД відповідає власний відділ безпеки, що забезпечує фізичну охорону на території всього заводу. Графік роботи фізичної охорони складається з трьох змін:

- Перша зміна: 7:00 - 16:00;
- Друга зміна: 16:00 - 00:00;
- Третя зміна: 00:00 - 7:00.

На території заводу під час роботи не відбувається патрулювання охорони, вся охорона працює на КПП та на пультах охорониприміщень. На поверсі де знаходиться ОІД розташовані декілька камер в коридорах. Також кожна кімната підключена до пульта управління і сповіщення сигналізації. Кожному працівникові видається унікальний ідентифікатор, за допомогою, якого він може потрапити на територію заводу через прохідний КПП з еклектронним турнікетом.

Пропускний режим.

КЗ на північному заході обмежена:

- Ворота (КПП проїздний);
- Паркан (2.30м).

КЗ на півночі обмежений:

- завнішнім фасадом будівель 1,2,3,4;
- Ворота (проїздний КПП 2);

- Паркан (2.30м).

КЗ на північному сході обмежена:

- фасад будівлі 13;
- Паркан (2.30м);
- Частина рельефу (підйом 3м).

КЗ на півдні обмежена:

- Частина рельефу (підйом 3м).

КЗ на південному заході обмежена:

- Частина рельефу (підйом 3м);
- Паркан (2.30м).

На підприємстві вхід на територію здійснюється через КПП. Утворено 2 КПП:

- Прохідні КПП;
- Проїздні КПП.

Прохідні ПКК - пункти, на яких встановлені електронні пропускні системи, металодетектори та охорона. Доступ на територію підприємства здійсньюється через пропуски або за заявою. Всі співробітники вносяться в електрониий реєстр. Всі відвідувачі підприемства вносяться в журнал відвідувань.

Проїздні КПП - пункти, на яких встановлені системи відеоспостереження, охорона, шлакбаум, ручний металодетектор. Доступ на територію підприємства здійсньюєть через пропуски або за заявою. Всі співробітники вносяться в електрониий реєстр. Всі відвідувачі підприемства вносяться в журнал відвідувань. При в’їзді та виїзді здійснюється обшук транспортних засобів.

На ситуаційному плані на рисунку відображено положення об’єкту інформаційної діяльності відносно об’єктів місцевості.

Навпроти головного входу з північної сторони, на відстані 120м, розташований міст через річку.

Навпроти головного входу з північно-західної сторони, на відстані 80м, розташований паркувальний майданчик з прилеглим магазином будівельних матеріалів.

Зі Східної сторони на відстані 450 м, знаходиться ГЕС. З південної сторони підприємство межує з полями та лісополосою. На південно-західній стороні, на відстані 50 м знаходиться будівля ЦТДМ. На південно-сході, на відстані 400 м знаходяться складські приміщення.

Місце розташування ОІД зображено в додатку А.

Таблиця 2.3 Пояснення до ситуаційного плану.

№ будівлі	Назва об’єкту	Опис об’єкту
1	Адміністративна будівля	Будівля виконана з цегли, 4 поверхи.
2	Перший механічний цех	Цегляна будівля, 1 поверх (висота 11м)
3	Другий механічний цех	Цегляна будівля, 1 поверх (висота 11м)
4	Склад прийому та збеігання матеріаллів	Ангар з металевих листівб 1 поверх(висота 7м)
5	Цех заготовчий	Цегляна будівля, 1 поверх (5м)
6	Цех гідравлічного обробітку	Цегляна будівля, 1 поверх (5м)
7	Бібліотека та інструментальний цех	Цегляна будівля, 3 поверхи: -1 поверх, інструментальний цех, висота (4м); -2-3 поверх, бібліотека;
8	Інутрументалний цех	Цегляна будівля, 1 поверх (5м)
9	Зварювальний цех	Цегляна будівля, 1 поверх (7м)
10	Відділ машинної плазмової заготовки, склад техніки	Цегляна будівля з размежувальною металевою стіно, 1 поверх (11м)
11	Відділ зборки, склад техніки	Цегляна будівля з размежувальною металевою стіно, 1 поверх (11м)
12	Центральний розподілювач, генераторна	Цегляна будівля, 1 поверх (2,5м)
13	Цех деревообробки	Цегляна будівля, 1 поверх (5м)

Прилеглі вулиці відносно КЗ вказані у таблиці 2.4.

Табліця 2.4 Прилеглі вулиці відносно КЗ.

Назва	Опис
Вул. Правобережна	Вулиця розташована на півночі від ОІД. Трафік низький, приблізно від 40-100 машин нв годину.

Комунікаційні системи КЗ вказані у таблиці 2.5.

Система комунікації	Вихід за межі КЗ	Характеристика
Система електро-постачання	+	Підключена до трансформаторної підстанції, яка не має сторонніх споживачів і знаходиться за межами КЗ
Система опалення	+	Автономна система, проходить через адміністартивну будівлю та знаходиться в межах КЗ
Система каналізації	+	Підключена до міської мережі, яка знаходиться за межами КЗ
Система водопостачання	+	Підключена до автономної станції, яка знаходиться в межах КЗ
Телефонна лінія та Інтернет	+	Підключені до АТС «Фрегат"
Система вентиляції	+	Приточно-витяжна

Таблиця 2.6. Комунікаційні системи КЗ

Система комунікації	Вихід за межі КЗ	Характеристика
Система сигналізації	-	Складається з датчиків відкриття (магнітно-контактний датчик), датчиків руху (пасивні інфрачервоні) та системи кабелів
Система кондиціонування	-	Спліт-система, що складається з двох блоків: зовнішнього та внутрішнього
Протипожежна система	-	Складається з системи оповіщувачів та датчиків, дані з яких обробляються протипожежним прийомно-контрольним пристроєм, що знаходиться на пості реєстратури
Кабелі компютерної мережі	+	Кабель локальної мережі комп'ютерів являє собою неекранована вита пара (1000BASE-T) категорії 5е
Опалення	-	Труби опалення виконані з поліпропіленового матеріалу. Це унеможливлює витік інформації по вібро-акустичному каналу

Фізичні характеристики будівлі:

- Зовнішні стіни – біла цегла, завтовшки 700 мм;
- Внутрішні стіни – біла цегла, завтовшки 160 мм;
- Дах будівлі викладений руберойдом та шифером. Вхід на дах здійснюється через пожежну драбину на останньому поверсі;
- Підлога – залізобетонні плити перекриття, завтовшки 350 мм, укриті лінолеумом та паркетом;

• Двері головного входу мають розміри 5000 мм х 2000 мм, виконані зі скла завтовшки 4мм, оздоблені 2 врізними замками з різними ключами; міжкімнатні двері мають розміри 1200 мм х 2000 мм, виконані з ламінованого МДФ, кожна міжкімнатна дверь має один врізний замок;

• Вікна приміщення виконані з металопластику, 2080 мм х 1420 мм ,та мають 2 пакети скла, кожне вікно має можливість видкриватись у 2-х положеннях:

A. Повне відкривання;

B. Провітрювання;

• Територія, навколо будівлі закрита, обмежена забором (в ролі забору виступає фасади будівлі та окремі будови. Паркан виконан з білої цегли завтовшки 160 мм);

• Вхід на територію здійснюється через КПП: 1 - проїздний КПП, 2-прохідний КПП;

• Перебування транспорту на цій території обмежено, контролюється;

• Територію навколо будівлі впорядковано, вона має асфальтне покриття.

Опис технічних засобів, що використовуються на підприємстві наведений у таблиці 2.7.

Таблиця 2.7 Опис технічних засобів, що використовуються на підприємстві

Назва ОТЗ/ДТЗС	Розміщення	Мінімальна відстань до КЗ /м	Інвентарний номер	ОТС/ДТЗС
PC1	Головна частина офісу відділу інженерів	1,3	638452897351	ОТС
PC2	Головна частина офісу відділу інженерів	1,3	638452897352	ОТС

Продовження таблиці 2.7

Назва ОТЗ/ДТЗС	Розміщення	Мінімальна відстань до КЗ /м	Інвентарний номер	ОТС/ДТЗС
РС3	Головна частина офісу відділу інженерії	1,3	638452897353	ОТС
Прінтер HP DeskJet Ink Advantage	Головна частина офісу відділу інженерії	1,3	35223463345524	ОТС
Комутатор	Головна частина офісу відділу інженерії	7	35223463345523	ДТЗС
Модем	Головна частина офісу відділу інженерії	7	35223463345522	ДТЗС
Кондиціонер	Головна частина офісу відділу інженерії	4,5	25937625639075	ДТЗС
3 освітлювальні прилади	Головна частина офісу відділу інженерії	3	25937625639076 25937625639077 25937625639078	ДТЗС
РС5	Кімната технологів відділу інженерії	1,3	638452897354	ОТС
РС6	Кімната технологів відділу інженерії	1,3	638452897355	ОТС

Продовження таблиці 2.7

Назва ОТЗ/ДТЗС	Розміщення	Мінімальна відстань до КЗ /м	Інвентарний номер	ОТС/ДТЗС
Кондиціонер	Кімната технологів відділу інженерії	2,4	25937625639074	ДТЗС
РС4	Кімната головного інженену відділу інженерії	12,7	638452897356	ОТС
РС7	Кімната головного технолога відділу інженерії	13,4	638452897357	ОТС
Кондиціонер	Кімната головного інженену відділу інженерії	14	25937625639073	ДТЗС
Кондиціонер	Кімната головного технолога відділу інженерії	11,2	25937625639072	ДТЗС
Чайник	Кімната відпочинку відділу інженерії	-	25937625639071	ДТЗС
Мікрохвильова піч	Кімната відпочинку відділу інженерії	13	352234633455677	ДТЗС

2.6 Опис обчислювальної системи

Опис обчислювальних систем, що використовуються на ОІД наведено в таблиці 2.8.

Таблиця 2.8 Опис обчислювальної системи

Назва	Характеристика	Умовні позначення	Кількість
Принтери	Модель: HP DeskJet Ink Advantage 2135 (F5S29C)	PR1-PR2	2
Комутатор	Модель: Cisco SB SRW224G4-K9-EU	SW1	1
ADSL модем	Модель: TP-LINK TD-8616	Mod1	1
Робоча станція	Intel Core i9-9900K 3.6GHz/8GT/s/16MB / RAM 32 ГБ / SSD 1 ТБ / GeForce RTX 2060 / LAN / Без ОДД / Windows 10 Pro 64-bit	PC1-PC7	7
Сервер	HPE ProLiant ML10 Gen9 : Intel Xeon Quad-Core E3-1225 v5 (3.3 - 3.7 ГГц)/ 8 ГБ/ 2 x 2 ТБ (3.5", SATA 3, 7200 об/мин) HPE LFF	SRV1	1

Програмне забезпечення обчислювальних систем наведено у таблиці 2.9.

Таблиця 2.9 Програмне забезпечення обчислювальних систем

Розміщення	Тип	Назва
Сервер БД	Операційна система	Microsoft Windows Server 2016 R2 10.0.14393
	ПЗ для роботи з документами	Microsoft Office 2016 build 16.0.6366.2062

	ПЗ для автоматизації бухгалтерського обліку	1С:Бухгалтерія 8.1
	Антивірус	ESET SmartSecurity 6
Робочі станції	Операційна система	Microsoft Windows 10 Enterprise Edition Service Pack 1 19041.264
	ПЗ для роботи з документами	Microsoft Office 2016 build 16.0.6366.2062
	Веб-браузер	Google Chrome 55.0.2883.87
	ПЗ для автоматизації бухгалтерського обліку	1С:Бухгалтерія 8.1 клієнт
	Антивірус	Avast Premier 19.8.2393 Final
	ПЗ для моделювання	SolidWorks Visual 2019

2.7 Аналіз загроз та вразливостей

Здійснення аналізу ризиків (опрацювання моделі загроз і моделі порушника, можливих наслідків від реалізації потенційних загроз, величини можливих збитків та ін.) та визначення переліку суттєвих загроз є метою етапу формування завдання на створення КСЗІ.

Аналіз ризиків інформаційної безпеки розроблений на основі документу ДСТУ ISO/IEC 27005:2015 - Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT) з урахуванням особливостей діяльності підприємства.

Представлений аналіз включає в себе:

- модель порушника;
- модель загроз;
- ідентифікація наслідків реалізації загроз;
- оцінку ризиків та ймовірності їх появи.

2.7.1. Модель порушника

Порушником є особа, яка здійснює спробу несанкціонованого доступу до об’єктів захисту (ознайомлення, модифікація, знищення, зміна режимів використання чи функціонування тощо).

Потенційними порушниками є: особи, які знаходяться за межами ІТС, мають можливість фізичного підключення до каналів зв’язку або інших складових мережі передачі даних; користувачі АС; персонал, який безпосередньо пов'язані із забезпеченням функціонування ІТС; особи, яким не передбачено доступ до ІзОД, але які мають доступ до приміщень, де розміщено компоненти ІТС і можуть отримати доступ до ІзОД;

Категорії порушників, що використовуються при створенні моделі, наведено в таблиці 2.6.1.1. У таблицях наведено специфікації моделі порушника за мотивами здійснення порушень, за рівнем кваліфікації та обізнаності щодо ІТС, за показником можливостей використання засобів ІТС для реалізації загроз, за часом та місцем дії. Сукупність цих характеристик визначає профіль порушника.

Рейтингова оцінка рівня загроз:

Рейтінгова оцінка	Опис
1	незначний
2	низький
3	середній
4	високий
5	неприпустимо високий

Виходячи із результатів аналізу характеристики інформації, яка обробляється, категорій порушників, які мають потенційну можливість порушення конфіденційності та цілісності інформації вважаються найбільш: небезпечними, доступності - менш небезпечними, а спостережності - найменш небезпечними.

Таблиця 2.10 Категорії порушників

Позначення	Визначення категорії	Потенціальний рівень загроз
П1	Авторизовані користувачі ІТС, яким надано право доступу до ІзОД	5
П2	Авторизовані користувачі, яким надано повноваження контролювати дії користувачів та персоналу та забезпечувати управління ІТС	4
П3	Особи, які забезпечують працездатність ІТС	2
П4	Особи, яким не передбачено доступ до ІзОД, але які мають доступ до приміщень, де розміщено ІТС і потенційно можуть отримати доступ до ІзОД	2
П5	Особи, які знаходяться за межами ІТС, мають можливість фізичного підключення до каналів зв’язку та можуть здійснити дії щодо порушення діючої в ІТС	5

Таблиця 2.11 Специфікація моделі порушника за місцем дії

Позначення	Визначення категорії	Потенціальний рівень загроз
Д1	Усередині приміщення, але без доступа до технічних засобів ІТС	3
Д2	З робочих місць користувачів та персоналу ІТС, а також місць розміщення обладнання ІТС, де обробляється інформація, яка підлягає захисту	4
Д3	Без доступу до приміщень, в тому числі з зовнішніх каналів зв’язку, з можливістю застосування технічних засобів здобуття інформації оптичними, акустичними каналами.	2

Таблиця 2.12 Специфікація моделі порушника за рівнем кваліфікації та обізнаності

Позначення	Визначення категорії	Потенціальний рівень загроз
К1	Не володіє знаннями та інформацією про порядок функціонування ІТС, не має навичок щодо користування штатними засобами обробки інформації системи та захисту інформації	1
К2	Має навички щодо користування ПК на рівні користувача	3
К3	Володіє базовими знаннями щодо функціонування програмного забезпечення і операційних систем, а також практичними навичками роботи з засобами обробки інформації	4
К4	Володіє знаннями щодо: функціонування засобів та механізмів обробки інформації та її захисту, що використовуються на ІТС та їх недоліків.	5

Таблиця 2.13 Специфікація моделі порушника за показником можливостей використання засобів ІТС для реалізації загроз

Позначення	Визначення категорії	Потенціальний рівень загроз
З1	Має фізичний доступ до компонентів ІТС, але не є авторизованим користувачем ІТС	2
З2	Має можливість запуску програм, що реалізують функції обробки інформації	3
З3	Має можливість керування функціонуванням ІТС, тобто конфігурує програмне забезпечення ІТС.	4

Таблиця 2.14 Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Визначення категорії	Потенціальний рівень загроз
М1	Безвідповідальність (недбалість, ненавмисне порушення)	3
М2	Корислива цілеспрямованість (зловмисне порушення)	5

Таблиця 2.15 Специфікація моделі порушника за часом дії

Позначення	Визначення категорії	Потенціальний рівень загроз
Ч1	Під час бездіяльності компонентів системи (під час планових перерв у роботі, неробочий час)	3
Ч2	Під час функціонування ІТС	5
Ч3	Під час перерв у роботі для обслуговування та ремонту	2

Профілі порушників всіх категорій наведено в таблиці, у колонці «Рівень загроз» наведено рейтингову оцінку загроз порушника з відповідними характеристиками.

Таблиця 2.16 Профілі можливостей порушників

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума
Головний інженер	П2	М2	К1	З1	Ч3	Д2	18
Головний технолог	П2	М2	К2	З1	Ч3	Д2	20
Інженер 1 категорії	П2	М2	К2	З1	Ч3	Д2	20
Інженер 2 категорії-1	П1	М1/М2	К2	З1	Ч3	Д2	21

Продовження таблиці 2.16

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума
Технолог 1 категорії	П2	М1/М2	К3	З3	Ч3	Д3	21
Технолог 2 категорії	П1	М1/М2	К2	З1	Ч3	Д2	21
Інженер 2 категорії-2	П1	М1/М2	К2	З1	Ч3	Д2	21
Адміністратор	П4	М1/М2	К4	З3	Ч3	Д3	20

З таблиці 2.16 видно, що найбільшу загрозу, що має відношення до проблеми захисту інформації, становлять: інженера 1 та 2 категорії, технологи 1 та 2 категорії. Тому організація роботи цих особ повинна бути найбільш контрольованою, оскільки вони є основними потенційними порушниками безпеки інформації.

2.7.2. Модель загроз

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

1) Порушення конфіденційності інформації (К) - отримання інформації користувачами або процесами всупереч встановленим правилам розмежування доступу до інформації.

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

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

4) Втрата спостережності (керованості системою) (С) - порушення процедур ідентифікації та автентифікації адміністраторів або процесів і надання їм повноважень, втрата контролю за їх діяльністю, можливість відмови від отримання або пересилання повідомлень.

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

Таблиця 2.17 Шкала оцінки ймовірності реалізації загрози

Оцінка ймовірності	Характеристика
1	Виникнення інциденту практично неможливо
2	Виникнення інциденту малоймовірне
3	Виникнення інциденту ймовірне до 1 разу на 3 місяці
4	Виникнення інциденту ймовірне до 1 разу на тиждень
5	Виникнення інциденту ймовірне до 1 разу на добу

Зроблено якісну оцінку ймовірності реалізації загрози та визначено сукупний рівень загрози. Результати аналізу викладені в таблиці 2.18.

Таблиця 2.18 Результати аналізу загроз та вразливостей інформації в ІТС

№	Вид загрози	Вразливість	Ймовірність	Що порушує	Рівень загрози	Джерело	Загальна оцінка загрози
1. Навмисні загрози (антропогенні та техногенні)							

Продовження таблиці 2.18

№	Вид загрози	Вразливість	Ймовірність	Що порушує	Рівень загрози	Джерело	Загальна оцінка загрози
1.1	Фізичний НСД до ІзОД	Вразлива система охорони; Поганий контроль за системами відеоспостереження; Поганий контроль за режимом КЗ;	1	КЦДС	4	Внутрішнє	2,5
1.2	Порушення правил розмежування доступу	Зловживання повноважень адміністраторі в системи; Помилки при розмежуванні доступу;	4	КЦДС	3	Внутрішнє	3,5
1.3	Порушення КЦД внаслідок навмисних дій користувача	Відсутність резервного копіювання; Порушені правила розмежування доступу; Помилкові дії персоналу внаслідок некомпетенстності;	3	КЦДС	4	Внутрішнє	3,5

Продовження таблиці 2.18

№	Вид загрози	Вразливість	Ймовірність	Що порушує	Рівень загрози	Джерело	Загальна оцінка загрози
1.4	Навмисне порушення систем життєзаьезпечення	Погана система охорони; Відстуність котнролю за примізеннями та вузлами життєзабезпечення;	2	КЦДС	4	Внутрішнє	3
1.5	Впровадження і використання комп'ютерних вірусів, закладних програм для порушення безпеки даних	Відсутність Антивірусних програмних засобів; Наявність неконтрольованих каналів витоку інформації;	4	КЦДС	3	Внутрішнє	3,5
1.6	Соціальна інженерія з корисливою метою	Погано підібраний персонал; Низіка заробітна платня та мотивації співробітників	3	КЦДС	5	Зовнішнє	4
1.7	Зловживання атрибутами доступу за для НСД до ІзОД	Відстуність Політики розмежування доступу; Порушення правил розмежування доступу;	2	КЦДС	2	Внутрішнє	2

Продовження таблиці 2.18

1.8	Неправомірне використання КС	Відсутність політики інформаційної безпеки, або саме пункту «Порядок використання КС»;	4	КЦДС	2	Внутрішнє	3
1.9	Навмисне порушення цілісності та працездатності КС	Вразлива система охорони; Поганий контроль за системами відеоспостереження; Відсутнсіть планової та позапланової інвентаризації КС; Відустність контролю цілісності компонентів КС;	3	КЦДС	4	Внутрішнє	3,5

Продовження таблиці 2.18

№	Вид загрози	Вразливість	Ймовірність	Що порушує	Рівень загрози	Джерело	Загальна оцінка загрози
1.10	Втручання та/або зміна ПЗ(видалення, блокування, встановлення, редагування, архівування)	Відстуність або вразливість системи розмежування прав користувачей; Піратське ПЗ; Недосконаліст ь системи розмежування доступом;	2	КЦДС	4	Внутрішнє	3
1.11	Доступ до даних, сервера	Недосконаліст ь системи розмежування доступом; Наявність неконтрольова них каналів передачі даних;	2	КЦДС	3	Внутрішнє/Зовнішнє	2,5
1.12	Відсутність контролю доступу до приміщення	Відстуність правил сберігання ключей; Відустність системи відеоспостере ження; Відстуність журналу відвідувачей на КПП;	4	КЦДС	2	Внутрішнє	3

Продовження таблиці 2.18

2. Випадкові загрози							
2.1	Ненавмисні дії користувачів, що призводять до відмови функціонування мережі чи окремих її елементів, пошкодження обладнання.	Низький рівень кваліфікації користувачей; Доступ до елементів, які не використовуються у бізнес процесах; Відстуність спеціалістів, які забезпечують працездатність мережі, її елементів, обладнання;	2	КЦДС	3	Внутрішнє	2,5
2.2	Порушення цілісності інформації, що зберігається, внаслідок ненавмисних дій користувачів	Некомпетентність персоналу з питання користування КС; Застарілі ПЗ; Відсутність резервного копіювання;	3	КЦДС	3	Внутрішнє	3
2.3	Ненавмисне пошкодження носіїв інформації чи інформації, яка зберігається на цих носіях	Відстуність резеврого копіювання;	4	КЦДС	4	Внутрішнє	4

Продовження таблиці 2.18

№	Вид загрози	Вразливість	Ймовірність	Що порушує	Рівень загрози	Джерело	Загальна оцінка загрози
2.4	Випадкове зараження програмних засобів комп'ютерними вірусами	Відсутність або застарілість антивірусного ПЗ;	3	КЦДС	2	Внутрішнє	2,5
2.5	Використання ПЗ, які заборонені політикою безпеки	Відсутність політики безпеки або розділу у політиці безпеки про регулювання дозволених ПЗ; Відсутність системи адміністрування дозволених ПЗ;	3	КЦДС	4	Внутрішнє	3,5
2.6	Порушенні цілісності інформації, що зберігається внаслідок апаратного або програмного збою	Відсутність резервного копіювання; Використання піратських ПЗ;	2	ЦД	4	Внутрішнє	3
3. Стихійні фактори							

Продовження таблиці 2.18

№	Вид загрози	Вразливість	Ймовірність	Що порушує	Рівень загрози	Джерело	Загальна оцінка загрози
3.1	Землетрус	Пошкодження фундаменту; Застарілі лініїї забезпечення;	1	ЦД	3	Зовнішнє	2
3.2	Повінь	Старе приміщення; Пошкодження фундаменту;	1	ЦД	3	Зовнішнє	2
3.3	Пожежа	Наявність легкозаймистих речовин; Відсутність противопожежної системи;	2	ЦД	3	Зовнішнє	2,5
3.4	Грозові розряди	Відсутність заземлення; Відсутність стабілізаторів напруги; Відсутність громоотводів;	1	ЦД	3	Зовнішнє	2

Найбільш актуальними загрозами для ОІД вважаються:

• Порушення правил розмежування доступу;

• Порушення КЦД внаслідок навмисних дій користувача;

• Впровадження і використання комп'ютерних вірусів, закладних програм для порушення безпеки даних;

• Соціальна інженерія з корисливою метою;

• Навмисне порушення цілісності та працездатності КС;

• Ненавмисне пошкодження носіїв інформації чи інформації, яка зберігається на цих носіях;

• Використання ПЗ, яке заборонені політикою безпеки;

• Порушення цілісності інформації, що зберігається внаслідок апаратного або програмного збою;

• Навмисне порушення систем життєзабезпечення;

• Неправомірне використання КС;

• Втручання та/або зміна ПЗ (видалення, блокування, встановлення, редагування, архівування);

• Залишити доступ до приміщення;

• Порушення цілісності інформації, що зберігається, внаслідок ненавмисних дій користувачів;

• Порушенні цілісності інформації, що зберігається внаслідок апаратного або програмного збою.

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

Для оцінки ризиків використані такі шкали:

Таблиця 2.19 Шкала оцінювання впливу реалізації загрози на конфіденційність

Оцінка рівня наслідків	Характеристика
1	Практично не призводить до розкриття конфіденційної інформації
2	Призводить до розкриття окремих документів, які відносяться до ІзОД та/або персональних даних і не призводить до фінансових втрат
3	Призводить до розкриття окремих документів, які відносяться до ІзОД та/або персональних даних і призводить до незначних фінансових втрат
4	Призводить до розкриття окремих документів, які відносяться до ІзОД та/або персональних данихі призводить до значних фінансових втрат, може призвести до зупинки роботи системи підприємства
5	Призводить до зупинки роботи системи, порушення вимог нормативно-правової бази

Таблиця 2.20 Шкала оцінювання впливу реалізації загрози на доступність

Оцінка рівня наслідків	Характеристика
1	Практично не впливає на доступність
2	Вплив на доступність незначний (не більше 1/10 від максимально допустимого часу простою)
3	Вплив на доступність середній (не більше 1/4 від максимально допустимого часу простою)
4	Вплив на доступність значний (до максимально допустимого часу простою)
5	Призводить до зупинки роботи системи на тривалий час, який перевищує максимально допустимий час простою)

Таблиця 2.21 Шкала оцінювання впливу реалізації загрози на спостережність

Оцінка рівня наслідків	Характеристика
1	Практично не впливає
2	Вплив незначний
3	Призводить до неможливості відстежити частину дій користувачів в системі
4	Призводить до неможливості відстежити дії користувачів і адміністраторів системи
5	Призводить до неможливості відстежити дії всіх кроситувачів і адміністратора системи, може призвести до зупинки роботи системи на тривалий час

Таблиця 2.22 Шкала оцінювання впливу реалізації загрози на цілісність

Оцінка рівня наслідків	Характеристика
1	Практично не призводить до наслідків з фінансовими втратами
2	Призводить до незначних фінансовихвтрат
3	Призводить до значнихфінансових втрат
4	Призводить до великихфінансових втрат і може призвести до зупинки роботи системи підприємства
5	Призводить до зупинки роботи системи, порушення вимог нормативно-правової бази

Оцінка збитків, що можуть бути нанесені ІТС внаслідок реалізації загроз, складається з величин очікуваних збитків від втрати інформацією кожної з властивостей (конфіденційності, цілісності або доступності) або від втрати керованості системи внаслідок реалізації загрози.

Величина збитків:

1. відсутня;
2. низька;

3. середня;
4. висока;
5. неприпустимо висока.

Для оцінки ризиків використана комбінація кількісних та якісних методів. Це дає змогу розрахувати доцільність впровадження політики безпеки, адже вартість заходів безпеки, не мають бути більшими, ніж фінансові втрати інциденту інформаційної безпеки.

Надалі представлени аналіз ріня ризику для основних типів інформації, обробляємої в ОІД.

У табліці 2.23 представлен рівень ризику для

Таблиця 2.23 Оцінка ризику

№	Загроза	Вразливість	Оцінка ймовірності реалізації загрози з	Оцінка реалізації загрози на цілісність	Оцінка реалізації загрози на конфіден-ційність	Оцінка реалізації загрози на доступ-ність	Оцінка величини можливих збитків	Рівень ризику за окремою парою загроза/ вразливість
1	Порушення правил розмежування доступом	Зловживання повноважень адміністраторі в системи;	2	1	3	1	3	18
2	Порушення КЦД внаслідок навмисних дій користувача	Помилкові дії персоналу внаслідок некомпетенст ності;	3	3	4	2	4	288

Продовження таблиці 2.23

№	Загроза	Вразливість	Оцінка ймовірності реалізації загрози з	Оцінка реалізації загрози на цілісність	Оцінка реалізації загрози на конфіден-ційність	Оцінка реалізації загрози на доступ-ність	Оцінка величини можливих збитків	Рівень ризику за окремою парою загроза/ вразливість
3	Впровадження і використання комп'ютерних вірусів, закладних програм для порушення безпеки даних	Відсутність Антивірусних програмних засобів;	2	3	3	2	4	144
4	Соціальна інженерія з корисливою метою	Низіка заробітна платня та мотивації співробітників;	1	1	3	1	5	15
5	Навмисне порушення цілісності та працездатності КС	Відсутність політики інформаційної безпеки, а саме пункту «Порядок використання КС»;	2	4	1	4	4	128

Продовження таблиці 2.23

№	Загроза	Вразливість	Оцінка ймовірності реалізації загрози з	Оцінка реалізації загрози на цілісність	Оцінка реалізації загрози на конфіден-ційність	Оцінка реалізації загрози на доступ-ність	Оцінка величини можливих збитків	Рівень ризику за окремою парою загроза/ вразливість
6	Ненавмисне пошкодження носіїв інформації чи інформації, яка зберігається на цих носіях	Відустність контролю цілісності компонентів КС;	2	4	1	5	3	120
7	Використання ПЗ, які заборонені політикою безпеки	Відсутність політики безпеки або розділу у політиці безпеки про регулювання дозволених ПЗ;	3	1	2	2	2	24

Продовження таблиці 2.23

№	Загроза	Вразливість	Оцінка ймовірності реалізації	Оцінка реалізації загрози на цілісність	Оцінка реалізації загрози на конфіден-ційність	Оцінка реалізації загрози на доступ-ність	Оцінка величини можливих збитків	Рівень ризику за окремою парою загроза/ вразливість
8	Порушенні цілісності інформації, що зберігається внаслідок апаратного або програмного збою	Відсутність резервного копіювання;	2	3	1	1	3	18
9	Навмисне порушення систем життєзаьезпечення	Погана система охорони;	1	2	1	1	4	8
10	Неправомірне використання КС	Відсутність політики інформаційної безпеки, або саме пункту «Порядок використання КС»;	2	1	2	1	2	8

Продовження таблиці 2.23

№	Загроза	Вразливість	Оцінка ймовірності реалізації загрози з	Оцінка реалізації загрози на цілісність	Оцінка реалізації загрози на конфіден-ційність	Оцінка реалізації загрози на доступ-ність	Оцінка величини можливих збитків	Рівень ризику за окремою парою загроза/ вразливість
11	Втручання та/або зміна ПЗ (видалення, блокування,встановлення, редагування, архівування)	Відстуність або вразливість системи розмежування прав користувачей;	1	2	1	5	4	40
12	Залишити доступ до приміщення	Відустність системи відеоспостереження;	2	1	3	2	2	24
13	Порушення цілісності інформації, що зберігається внаслідок апаратного або програмного збою	Некомпетентність персоналу з питання користування КС;	1	4	1	2	2	16

Продовження таблиці 2.23

№	Загроза	Вразливість	Оцінка ймовірності реалізації	Оцінка реалізації загрози на цілісність	Оцінка реалізації загрози на конфіден-ційність	Оцінка реалізації загрози на доступ-ність	Оцінка величини можливих збитків	Рівень ризику за окремою парою загроза/ вразливість
14	Порушення цілісності інформації, що зберігається, внаслідок ненавмисних дій користувачів	Відсутність резервного копіювання;	1	4	1	2	3	24

За отриманим максимальним рівнем ризику за окремою парою, складена шкала оцінки ризику для можливості класифікувати ризики за рівнем прийнятності. Шкала оцінки ризику:

- <30 - малий рівень ризику;
- 31-99 - припустимий рівень ризику;
- 100 > - критичний рівень ризику.

Виконавши оцінку ризиків, було виділено критичні загрози, серед яких:

- Ненавмисне пошкодження носіїв інформації чи інформації, яка зберігається на цих носіях;
- Порушення КЦД внаслідок навмисних дій користувача;
- Впровадження і використання комп'ютерних вірусів, закладних програм для порушення безпеки даних;
- Навмисне порушення цілісності та працездатності КС.

2.8 Профіль захищеності

Проаналізувавши основні характеристики ІТС об’єкту кваліфікаційної роботи та вимог до властивостей інформації, відповідно до НД ТЗІ 2.5-004-99 зі змінами згідно наказу Адміністрації Держспецзв’язку від 28.12.2012 № 806 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу».

АС відноситься до класу «3» — розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності.

Істотна відміна від попереднього класу — необхідність передачі інформації через незахищене середовище або, в загальному випадку, наявність вузлів, що реалізують різну політику безпеки.

Обраний профіль захищенності:

3.КЦ.1 = { КД-2, КВ-1, ЦД-1, ЦВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НВ-1 }

Таблиця 2.24 Профіль захищеності

№	Послуга	Назва послуги	Опис послуги
1	КД-2	Базова довірча конфіденційність	Ця послуга дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування. Атрибути доступу об'єктів і користувачів повинні містити інформацію, що використовується КЗЗ для розмежування доступу до об'єктів з боку конкретного користувача. Додатково повинна існувати можливість встановлювати, які користувачі можуть активізувати конкретний процес, що дозволяє одержати можливість обмеженого керування потоками інформації. Керування правами доступу на даному рівні має невисоку вибірковість. Користувач, домену якого належить об'єкт (процес) може вказати, які групи користувачів і, можливо, які конкретні користувачі мають право одержувати інформацію від об'єкта (ініціювати процес).

Продовження таблиці 2.24

№	Послуга	Назва послуги	Опис послуги
2	КВ-1	Мінімальна конфіденційність при обміні	Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Забезпечує захист від несанкціонованого ознайомлення за рахунок пасивного спостереження за лініями зв'язку або розкрадання носіїв інформації. Прикладом реалізації може служити програмне шифрування файлів перед їх передачею каналами зв'язку або прозоре шифрування файлів перед їх записуванням на диск.
3	ЦД-1	Мінімальна довірча цілісність	Ця послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування. На даному рівні користувач, домену якого належить об'єкт, може накладати обмеження на доступ до об'єктів з боку інших користувачів. Керування правами має грубу вибірковість. Для такої системи можна побудувати часткову матрицю доступу користувачів до захищених об'єктів.

Продовження таблиці 2.24

4	ЦВ-1	Мінімальна цілісність при обміні	Ця послуга забезпечує мінімальний захист. На включення даного рівня в свій рейтинг може претендувати система, що дозволить на підставі цифрового підпису перевіряти цілісність функціонуючого на ЕОМ ПЗ, або система електронної пошти, що забезпечує цифровий підпис повідомлень.
5	НР-2	Захищений журнал	Ця послуга дозволяє контролювати небезпечні для КС дії. Вибір фізичного носія, що використовується для зберігання даних реєстрації, повинен відповідати способу використання і обсягу даних. Будь-яке переміщення таких даних має виконуватись способом, що гарантує їх безпеку. Одним із найбезпечніших, хоч і досить дорогих рішень, є використання носіїв з одноразовим записом. В будь-якому випадку рівень захищеності даних реєстрації має бути не нижче, ніж рівень захищеності даних користувачів, яку забезпечують реалізовані послуги конфіденційності і цілісності. Повинні бути вироблені угоди щодо планування і ведення архівів даних реєстрації. Засоби аналізу — це засоби, що виконують більш складну, ніж перегляд, оцінку журналу реєстрації з метою виявлення можливих порушень політики безпеки. Ці засоби повинні надавати адміністратору можливість виконання сортування, фільтрації за певними критеріями та інших подібних операцій. КЗЗ повинен надавати

			адміністратору можливість вибирати події, що реєструються. Це може бути досягнено або через "передвибірки", або "поствибірки". Передвиборка подій, що реєструються, дозволяє виділити під час ініціалізації системи з всієї множини доступних для реєстрації подій підмножину тих, що необхідно реєструвати в журналі. Використовуючи передвибірку, адміністратор може зменшити кількість реально реєстрованих подій і, отже, розмір остаточного журнального файлу. Недоліком предвибірки є те, що ті події, які не були вибрані, не можуть уже пізніше бути проаналізовані, навіть, якщо постає така необхідність. Перевага поствибірки полягає в гнучкості можливості аналізу "пост-фактум", проте така організація ведення журнального файла вимагає виділення значного обсягу пам'яті для даних реєстрації.

Продовження таблиці 2.24

6	НИ-2	Одиночна ідентифікація і автентифікація	Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, який намагається одержати доступ до КС. Хоч поняття ідентифікація і автентифікація відрізняються, на практиці обидва ці процеси важко буває поділити. Важливо, щоб в кінцевому підсумку були підстави стверджувати, що система має справу з конкретним відомим їй користувачем. Пароль, персональний номер або інша подібна інформація є прикладом того, що називається "дещо, відоме користувачеві". Даний тип автентифікації є простим у реалізації і достатньо ефективним. Проте його ефективність обмежена простотою його повторення: достатньо просто обчислити або вгадати інформацію автентифікації, а для її дублювання не вимагається спеціального устаткування чи можливостей.
7	НК-1	Однонаправлений достовірний канал	Дана послуга дозволяє гарантувати, що користувач взаємодіє безпосередньо з КЗЗ і ніякий інший користувач або процес не може втручатись у взаємодію (підслухати або модифікувати інформацію, що передається). Рівні даної послуги ранжируються в залежності від того, чи має КЗЗ можливість ініціювати захищений обмін, чи це є прерогативою користувача.

Продовження таблиці 2.24

8	НВ-1	Автентифікація вузла	Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ранжируються на підставі повноти реалізації.

2.9 Визначення методів та засобів захисту.

Основним критерієм вибору методів захисту було:

• Використовувати методи захисту відповідно до п. 17 Положення про технічний захист інформації в Україні, затвердженого Указом Президента України від 27 вересня 1999 р. № 1229. Перелік призначений для використання суб'єктами системи технічного захисту інформації (ТЗІ) під час розроблення, модернізації та впровадження комплексів ТЗІ на об’єктах інформаційної діяльності (ОІД) та комплексних систем захисту інформації (КСЗІ) в автоматизованих системах (АС);

• Використовувати економічно обґрунтовані методи захисту;

• Дотримуватись принципів логічності.

Проаналізувавши основні загрози та вразливості об’єкту з таблиці 2.24, були обрані наступні методи захисту:

Таблиця 2.25 Загрози та вразливості об’єкту

Номер загрози з таблиці 2.20	Назва, позначення засобу та його технічних умов (за наявності)	Призначення засобу
1	Курси підвищення кваліфікації	Організаційний метод, направлений на підвищення обізнаності щодо ІТС у співробітників компанії.
2	Програмний продукт антивірусного захисту «Panzor Cloud Antivirus» версії 1.01.3223,	Призначене для захисту робочих станцій користувачів від дій шкідливого програмного забезпечення та реагуванні на виявлення даних програм та інформації, а також мережевих атак. Відповідає вимогам нормативних документів системи технічного захисту інформації в Україні в обсязі функцій, зазначених у документі «Програмний продукт антивірусного захисту «Panzor Cloud Antivirus». Технічні вимоги за критеріями технічного захисту інформації» № И2908-04 від 29.08.2017 року, сукупність яких визначається функціональним профілем КА-2, ЦА-1, ЦО-1, ЦВ-1, ДС-1, ДЗ-1, ДВ-1, НР-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-2, НВ-1 з рівнем гарантій Г-2 оцінки коректності їх реалізації згідно з НД ТЗІ.2.5-004-99. Дійсний з 25.09.2017 до 25.09.2020
3	Програмний продукт захисту інформації «Safetica Full DLP» версії 8.340	Відповідає вимогам нормативних документів з технічного захисту інформації в обсязі функцій, зазначених у документі «Програмний продукт захисту інформації Safetica Full DLP версії 8.х. Технічні вимоги за критеріями технічного захисту інформації». Дійсний з 28.09.2018 до 28.09.2021

Продовження таблиці 2.25

4	Організаційні заходи, політика інформаційної безпеки	Створення політики або впровадження в існуючу політику пунктів про «Порядок використання КС». Приклад політики у ДОДАТКУ 5
5	Організаційні заходи, інвентаризація	Впровадження планових та позапланових інвентаризацій КС компанії. Приклад політики у ДОДАТКУ 6
6	Організаційні заходи, політика інформаційної безпеки	Створення політики або впровадження в існуючу політику пунктів про дозволені ПЗ
7	Резервне копіювання	Планове або позапланове резервне копіювання інформації
8	Захищений програмний комплекс "Система відеоспостереження CaMaP" (версія 1.012)	Відповідає вимогам нормативних документів з технічного захисту інформації в обсязі функцій, зазначених у документі "Захищений програмний комплекс "Система відеоспостереження CaMaP". Технічне завдання» Дійсний з 06.03.2018 до 06.03.2021
9	Організаційні заходи, політика інформаційної безпеки	Створення політики або впровадження в існуючу політику пунктів про «Порядок використання КС»
10	Захищений програмний комплекс "Система відеоспостереження CaMaP" (версія 1.012)	Відповідає вимогам нормативних документів з технічного захисту інформації в обсязі функцій, зазначених у документі "Захищений програмний комплекс "Система відеоспостереження CaMaP". Технічне завдання» Дійсний з 06.03.2018 до 06.03.2021
11	Курси підвищення кваліфікації	Організаційний метод, направлений на підвищення обізнаності щодо ІТС у співробітників компанії.
12	Резервне копіювання	Планове або позапланове резервне копіювання інформації
13	Політика інформаційної безпеки	Політика розмежування доступом
14	Політика інформаційної безпеки	Антивірусна політика безпеки

1)Політика антивірусного захисту

Опис: Політика включає в себе інструкції для користувачів із застосування антивірусного ПЗ.

Метою цієї політики: захист системи від комп'ютерних вірусів.

Галузь застосування: політика відноситься до всіх робітників підприємства, хто є користувачами системи.

Проаналізувавши рейтинги та оцінки антивірусів, обрати серед доступних найефективніший. Антивірусне програмне забезпечення має бути встановлене на всіх робочих станціях та ноутбуках системи та постійно оновлюватись. Варто слідкувати за терміном дії ліцензії та продовжувати її заздалегідь.

Рекомендації для уникнення проблем з зараженням вірусами:

- на початку роботи з системою, переконатися, що антивірусне ПЗ увімкнено;
- завжди сканувати носії інформації та підозрілі файли або файли з невідомого джерела на наявність вірусів;
- зберігати резервні копії важливих даних в безпечному місці;
- ніколи не завантажувати файли з невідомих чи підозрілих джерел;
- не відкривати невідомі вам файли, що прикріплені до електронної пошти від невідомого, підозрілого або ненадійного джерела. Видаляти ці вкладення відразу, «подвійним видаленням», шляхом спорожнення кошика.

2)Політика розмежування прав доступу

Опис: Політика розмежування прав доступу регламентує правила доступу користувачів і процесів до пасивних об'єктів.

Мета: надати доступ до інформації користувачам, яким він необхідний згідно з посадовими інструкціями.

Галузь застосування: Відноситься до всіх користувачів системи.

Інструкція політики

Відповідно до НД ТЗІ 1.4-001-2000, мають виконуватися наступні дії:

- кожне робоче місце повинно мати свого користувача, який несе відповідальність за його працездатність та за дотримання всіх вимог і

процедур, пов’язаних з обробкою інформації та її захистом. Користувач повинен бути забезпечений відповідними інструкціями і навчений всім вимогам і процедурам;

- для попередження неавторизованого доступу до даних, ПЗ, інших ресурсів, керування механізмами захисту здійснюється адміністратором системи;
- за всі зміни ПЗ, створення резервних і архівних копій несе відповідальність адміністратор. Такі роботи виконуються за його дозволом;
- кожний користувач має свій унікальний ідентифікатор і пароль. Право видачі цих атрибутів надається адміністратору. Атрибути для адміністраторів надає адміністратор безпеки ІТС. Видача атрибутів дозволяється тільки після документальної реєстрації особи як користувача;
- користувачі проходять процедуру автентифікації для отримання доступу до ресурсів ІТС;
- атрибути користувачів змінюються двічі на рік , а невикористовуванні і скомпрометовані – видаляються.

Контроль за ПРД можливий при створенні матриці керування доступом: виділяють об’єкти та суб’єкти доступу. Суб'єктами інформаційних відносин є особи, об'єктом інформаційних відносин є інформація.

Підібрані методи забезпечення захищенності інформації відповідають державній стандартизації та захищають від основних загроз.

2.10 Висновки до розділу 2:

У рамках другого розділу роботи було виконано обстеження на ОІД, розглянуто: обчислювальну систему, інформаційне середовище, фізичне середовище, середовище користувачів. Проведено аналіз та оцінку ризиків інформаційної безпеки і виділено значущі загрози. За результатами обстеження на ОІД та аналізу інформаційних ризиків, визначено недосконалості інформаційно-

телекомунікаційної системи підприємства. Недоліки можуть стати причинами появи вразливостей системи та завдати збитків підприємству.

За результатами з проведеним аналізом, запропоновані до впровадження методи та засоби захисту інформації для забезпечення ефективної роботи всіх складових системи.

Аналіз ризиків після впровадження запропонованих політик вказує на зниження рівня ризиків на систему через виявлені загрози.

3 ЕКОНОМІЧНИЙ РОЗДІЛ

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

Економічна доцільність визначається розрахунками:

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

Таблиця 3.1 Використані програмні, інженерно-технічні та адміністративні засоби

Panzor Cloud Antivirus	1 100 підписка на 3 роки
Safetica Full DLP	1 325 (10 ліцензій)
Система відеоспостереження CaMaP	13 200
Курси підвищення кваліфікації	1 000 на чоловіка – всього 7 000
Всього	22 625

3.1 Розрахунок капітальних витрат

3.1.1 Визначення трудомісткості розробки КСЗІ

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

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

де ttз - тривалість складання ТЗ на розробку ПБІ = 21 годин;

$t_в$ - тривалість розробки концепції безпеки інформації у організації = 18 годин;

t_a - тривалість процесу аналізу ризиків = 15 годин;

$t_{вз}$ - тривалість визначення виімог заходів, методів та засобів захисту = 12 годин;

$t_{озб}$ - тривалість виробу основних рішень з забезепечення БІ = 7 годин;

$t_{овр}$ - тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організацій = 12 годин;

$t_д$ - тривалість документального оформлення ПБ = 15 годин.

Отже, t = 21 + 18 + 15 + 12 + 7 + 12 + 15 = 100 годин

3.1.2 Розрахунок витрат на створення елементів КСЗІ

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

$$К_{рп} = З_{зп} + З_{мч} .$$

$$К_{рп} = З_{зп} + З_{мч} = 7700 + 462 = 8162 \text{ грн}$$

$$З_{зп} = t * З_{іб} = 100 * 77 = 7700 \text{ грн}$$

де t – загальна тривалість розробки КСЗІ, годин;

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

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

$$З_{мч} = t * С_{мч} = 100 * 4{,}62 = 462 \text{ грн}$$

де t – трудомісткість підготовки документації на ПК, годин;

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

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = P \cdot t_{нал} \cdot C_e + \frac{Ф_{зал} \cdot Н_а}{F_р} + \frac{К_{лпз} \cdot Н_{апз}}{F_р}, \text{ грн;}$$

$$С_{мч}=0{,}8 * 3 * 1{,}68 + ((2838{,}5 * 0{,}27)/1920) + ((2425 * 0{,}16)/1920) = 4{,}62 \text{ грн}$$

Відповідно до розроблених рекомендації щодо застосування розробки в підприємства ТОВ «Промислова Група «Корсунь» планується використання програмних засобів, які вже встановлені на підприємстві.

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

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

$$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} = 30787грн$$

$$К = 8162 + 2425 + 0 + 13200 + 7000 + 0 = 30787 \text{ грн}$$

де $К_{рп}$ – вартість розробки КСЗІ та залучення для цього зовнішніх консультантів = 8162 грн

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ) = 2425 грн

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

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів = 13200 грн

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу = 7000 грн

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки = 0 грн

3.2 Розрахунок експлуатаційних витрат

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

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

- вартість Upgrade-відновлення й модернізації системи (Св);

- витрати на керування системою в цілому (Ск);

- витрати, викликані активністю користувачів системи інформаційної безпеки (Сак - "активність користувача").

Річні експлуатаційні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_в + С_к + С_{ак}, \quad грн$$

$$С = 0 + 53452,3 + 0 = 53452,3 \text{ грн}$$

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

$С_к$ - витрати на керування системою в цілому = 53452,3 грн;

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

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

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

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються $= С_н = 1000$ грн

Річний фонд амортизаційних відрахувань $С_а$:

$С_а = К * 0,25$

$С_а = 30787 * 0,25 = 7696,75$ грн

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

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

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

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

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 7700 грн. Додаткова заробітна плата – 10% від основної заробітної плати. Виконання роботи щодо налаштувань інфраструктури безпечних підключень мобільних користувачів до інтрамережі підприємства потребує залучення спеціаліста інформаційної безпеки на 0,25 ставки. Отже,

$$С_з = (7700 * 12 + 7700 * 12 * 0,1)* 0,25 = 25410 \text{ грн}$$

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

$$С_{єв} = 25410 *0,22 = 5590,2 \text{ грн}$$

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

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

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=0,8 кВт);

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

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

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

$$С_{ел} = 0,8 * 1920 * 1,68 = 2580,48 \text{ грн}$$

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

$$С_{тос} = 30787 * 0,01 = 307,87 \text{ грн}$$

Витрати на керування системою інформаційної безпеки визначаються:

$С_к = 1000 + 7696,75 + 25410 + 2580,48 + 0 + 307,87 + 5590,2 = 42585,3$ грн

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають 42585,3 грн.

3.3 Оцінка величини збитку

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

Необхідні вихідні дані для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 3 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 2 години;

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

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 7500 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 6900 грн./міс.;

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

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 7 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 4000 тис. грн. у рік;

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

I – число атакованих сегментів корпоративної мережі, 1;

N – середнє число атак на рік, 6.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V,$$

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

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

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

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

$$П_п = ((6900 * 12) / 176) * 3 = 1411{,}36 \text{ грн}$$

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

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

$$П_в = П_{ви} + П_{пв} + П_{зч},$$

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

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

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

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

$$П_{ви} = ((7400 * 12) / 176) * 2 = 1009 \text{ грн.}$$

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

$$П_{пв} = ((6000 * 1) / 176) * 3 = 102{,}27 \text{ грн}$$

Витрати на заміни встаткування або запасних частин можуть скласти 700 грн.

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

$$П_в = 1009 + 102{,}27 + 700 = 1811{,}27 \text{ грн}$$

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

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

$$V = (4000000 / 2080) * (3 + 3 + 2) = 15384{,}6 \text{ грн}$$

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

$$U = 1411{,}36 + 1811{,}27 + 15384{,}6 = 18607{,}23 \text{ грн}$$

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

$$B = 1 * 6 * 42585,3 = 255511,8 \text{ грн}$$

3.4 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B \cdot R - C \text{ грн.},$$

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

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці = 64%;

С – щорічні витрати на експлуатацію системи інформаційної безпеки.

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

$$E = 255511,8 * 0,64 - 42585,3 = 120942,25 \text{ грн}$$

3.5 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

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

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

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

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

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = 120942,25 / 30787 = 3,9 \text{ частки одиниці,}$$

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

$$ROSI > (N_{деп} – N_{інф})/100),$$

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

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

Розрахункове значення коефіцієнта повернення інвестицій:

$$0,58 > (23 – 14)/100 = 0,58 > 0,09.$$

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

$$T = 1/3,9 = 0,2 \text{ років.}$$

3.6 Висновки до 3 розділу:

Згідно з отриманими даними під час розрахунку економічної частини - капітальні затрати становлять 30787 грн, експлуатаційні - 42585,3 грн. Згідно з підрахунками, створені елементи КСЗІ є доцільними з економічної точки зору.

Загальний збиток від атаки на вузол або сегмент корпоративної мережі організації склав 255511,8 грн. Загальний ефект від впровадження системи інформаційної безпеки склав 120942,25 грн. Згідно с коефіцієнтом ROSI який становить 3,9 - створені елементи КСЗІ є цілком доцільними. Термін окупності елементів КСЗІ становить 0,2 роки = 2,4 місяці.

ВИСНОВКИ

У першому розділі кваліфікаційної роботі було проаналізовано стан інформаційної захищенності в галузі сільського господарства в країні, визначені основні проблеми країни в сфері кібербезпеки, проаналізована нормативно-правова база, що регулює відносини у інформаційній сфері. Виконана постановка завдачі.

У рамках другого розділу роботи було виконано обстеження на ОІД, розглянуто: обчислювальну систему, інформаційне середовище, фізичне середовище, середовище користувачів. Проведено аналіз та оцінку ризиків інформаційної безпеки і виділено значущі загрози. За результатами обстеження на ОІД та аналізу інформаційних ризиків, виділено недосконалості інформаційно-телекомунікаційної системи підприємства. Недоліки можуть спричинити використання вразливостей системи та произвести до завдання збитків підприємству.

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

Згідно з отриманими даними під час розрахунку економічної частини - капітальні затрати становлять 30787 грн, експлуатаційні - 42585,3 грн. Згідно з підрахунками, створені елементи КСЗІ є доцільними з економічної точки зору.

Загальний збиток від атаки на вузол або сегмент корпоративної мережі організації склав 255511,8 грн. Загальний ефект від впровадження системи інформаційної безпеки склав 120942,25 грн. Згідно с коефіцієнтом ROSI який становить 3,9 - створені елементи КСЗІ є цілком доцільними. Термін окупності елементів КСЗІ становить 0,2 роки = 2,4 місяці.

ПЕРЕЛІК ПОСИЛАНЬ

1. Кібербезпека в умовах розгортання четверної промислової революції [Електронний ресурс]. Режим доступу до ресурсу: https://niss.gov.ua/en/node/135
2. Закон України «Про інформацію» від 02.10.1992 No2657-XII // Відомості Верховної Ради України. - 1992. - No 48. [Електронний ресурс]. Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2657-12 Класифікація “інформації в законодавстві України”.
3. Закон України “Про захист персональних даних” від 01.06.2010 No 2297-VI // Відомості Верховної Ради України. - 2010. - No 5[Електронний ресурс]. Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2297-17.
4. НД ТЗІ 1.1-002-99: Загальні положення з захисту інформації в комп’ютерних системах від НСД (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. № 22); [Електронний ресурс]. Режим доступу до ресурсу: http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46074&cat_id=38835
5. НД ТЗІ 1.4-001-2000: Типове положення про службу захисту інформації в автоматизованій системі (введено в дію Наказом ДСТСЗІ СБУ від 04.12.2000 р. № 53); [Електронний ресурс]. Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=102122&showHidden=0
6. НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу» (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. № 22).; [Електронний ресурс]. Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article;jsessionid=15FDA2B2745B1390AC937214804F2E76?showHidden=1&art_id=102089&cat_id=89734&ctime=1344502332348
7. НД ТЗІ 3.7-001-99: Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі (введено в дію Наказом ДСТСЗІ СБУ від 28.04.199 р. № 22) [2-4,6-

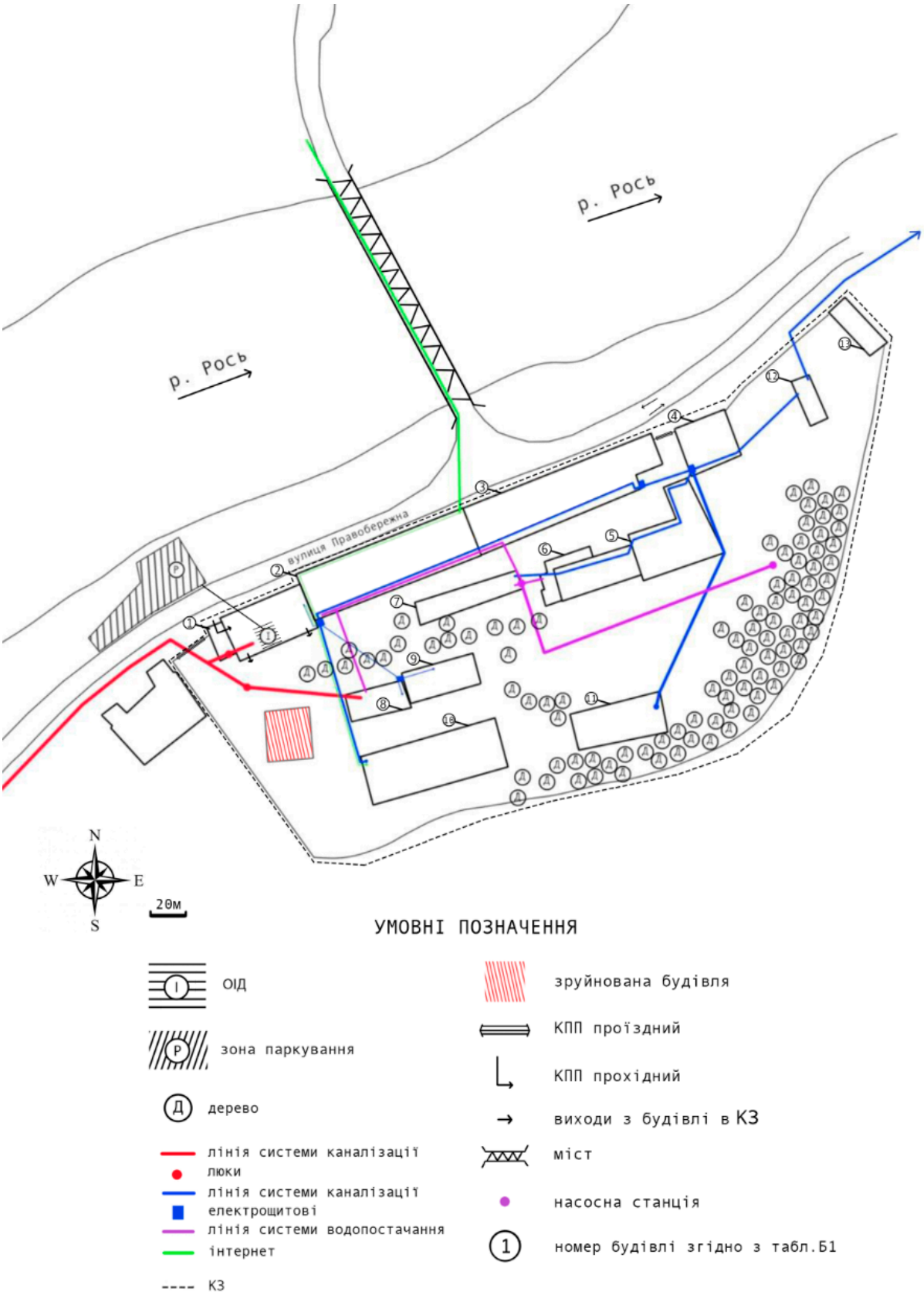
8,9]. [Електронний ресурс]. Режим доступу до ресурсу: http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46074&cat_id=38835

8. ДСТУ ISO/IEC 27002:2015 [Електронний ресурс] // ДСТУ. - 2015. - Режим доступу до ресурсу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66911.
9. Етапи створення КСЗІ [Електронний ресурс] - Режим доступу до ресурсу: http://www.vaas.gov.ua/news/zaxist-informacijnix-sistem-vazhlive- zavdannya-sogodennya/.
10. Закон України "Про захист інформації в інформаційно- телекомунікаційних системах" від 05.07.1994 No80-VI // Відомості Верховної Ради України. - 1994. - No 80. [Електронний ресурс]. - Режим доступу: http://zakon4.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
11. Закон України "Про захист інформації в автоматизованих системах" від 05.07.1994 No80-VI // Відомості Верховної Ради України. - 1994 р., N 31. [Електронний ресурс]. - Режим доступу https://zakon.rada.gov.ua/laws/show/2594-15
12. Асоціаційя підприємств промислової автоматизації України (АППАУ). [Електронний ресурс]. - Режим доступу: https://appau.org.ua/en/
13. Індустрія 4.0 (І 4.0) в Україні. [Електронний ресурс]. - Режим доступу: https://www.proxis.ua
14. Методичні вказівки до виконання економічної чатини дипломного проекту зі спеціальності 125 Кібербезпека/Упорядн. Д. П. Пілова. – Дніпро: Національний технічний університет «Дніпровська політехніка», 2019.
15. Поняття нормативно-правове забезпечення. [Електронний ресурс]. - Режим доступу: https://lpnu.ua
16. Методичні рекомендації до виконання дипломних робіт (проектів) бакалаврів та магістрів спеціальностей 125 Кібербезпека, 172 Телекомунікації та радіотехніка / О.Ю. Гусєв, О.В. Герасіна, О.М. Алексеев, О.В. Кручинін – Дніпро: НГУ, 2018. – 52 с.

17. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.2–004–99. – Київ: ДСТСЗІ СБ України, 1999. – 55 с.
18. НД ТЗІ 2.5-004 - Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. - [Чинний від 28.04.1999] - К. : ДСТСЗІ СБУ, 1999. - No22 - (Нормативний документ системи технічного захисту інформації).
19. НД ТЗІ 2.5-005 - Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. - [Чинний від 28.04.2000] - К. : ДСТСЗІ СБУ, 2000. - No22- (Нормативний документ системи технічного захисту інформації).
20. НД ТЗІ 1.1-002-99: Загальні положення з захисту інформації в комп'ютерних системах від НСД (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. № 22); [Електронний ресурс]. Режим доступу до ресурсу: http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46074&cat_id=38835

Додаток А

Рисунок 1 Ситуаційний план



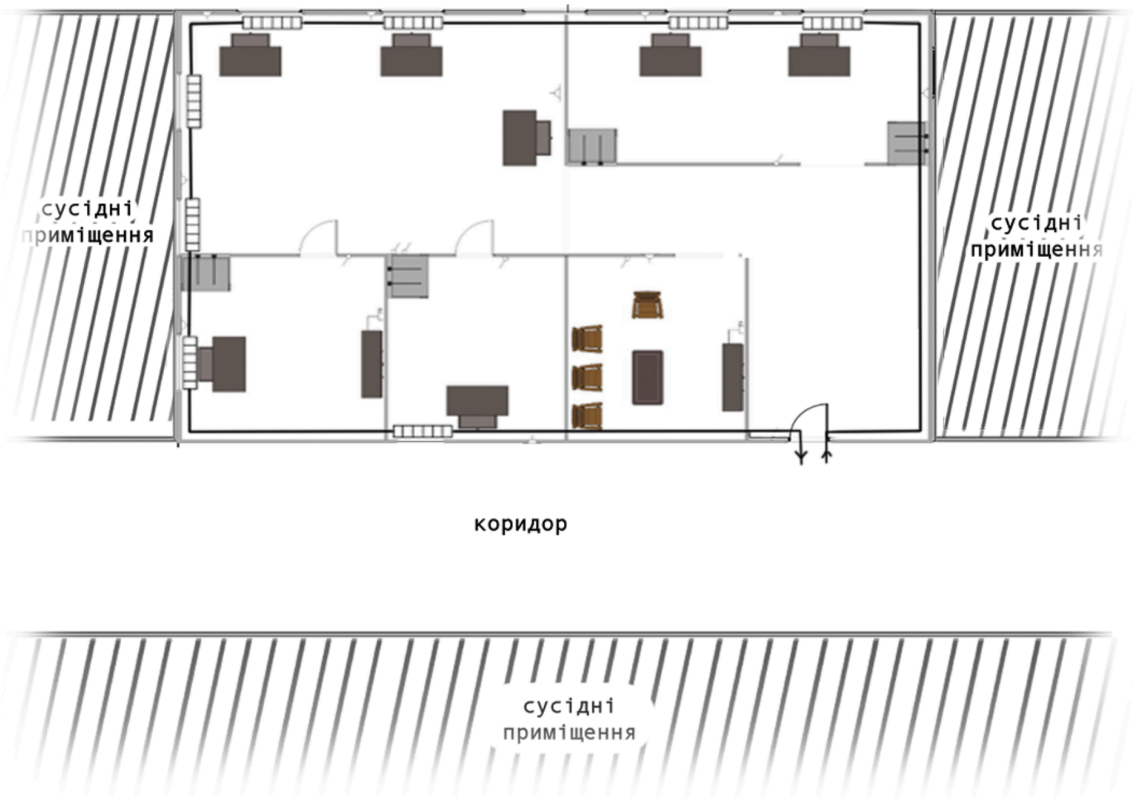


Рисунок 2. Схема системи опалення ОІД

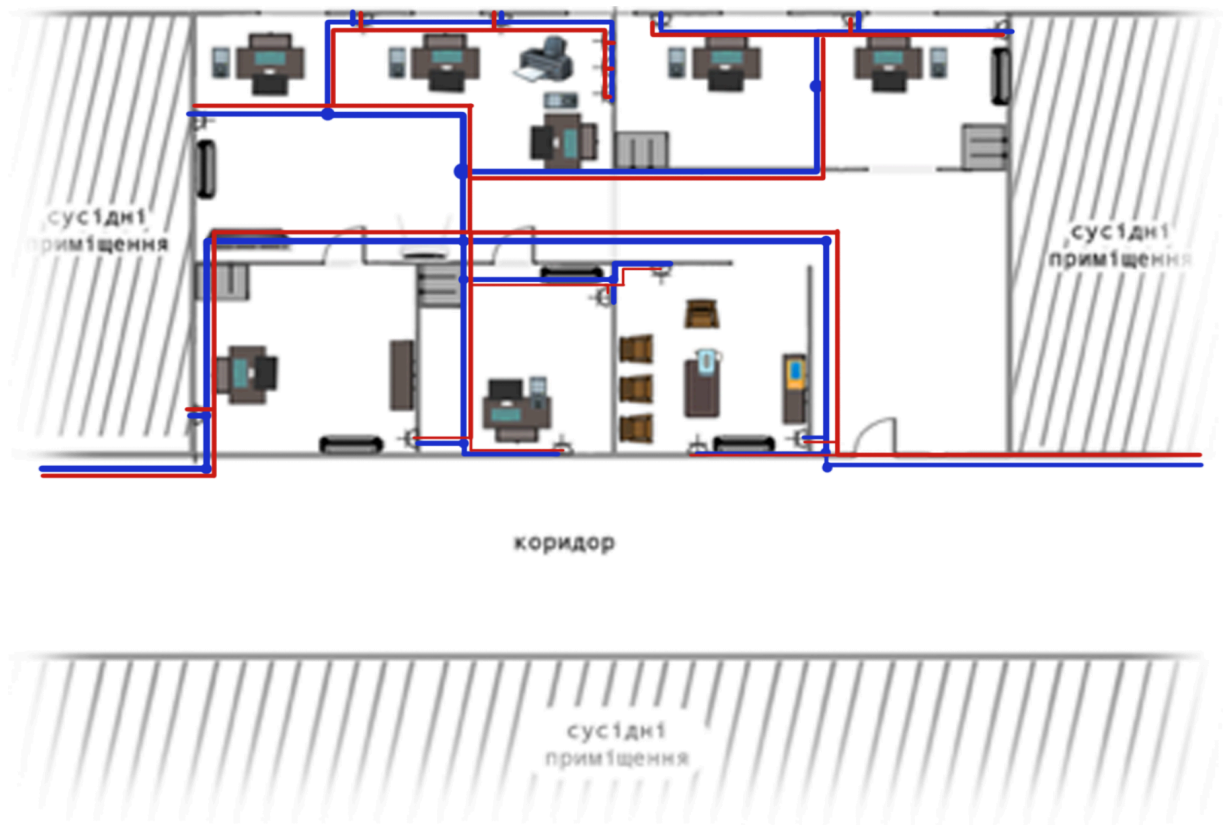


Рисунок 3. Схема електропостачання

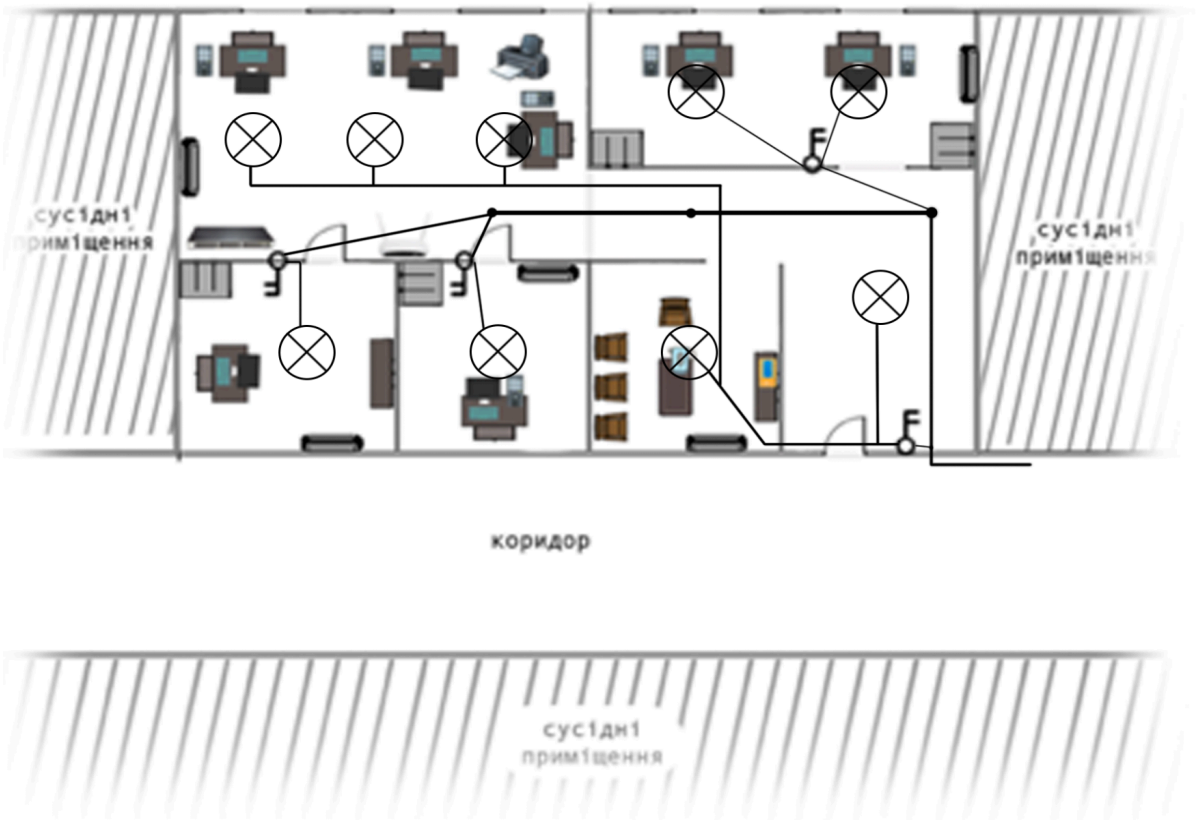


Рисунок 4. Схема освітлення

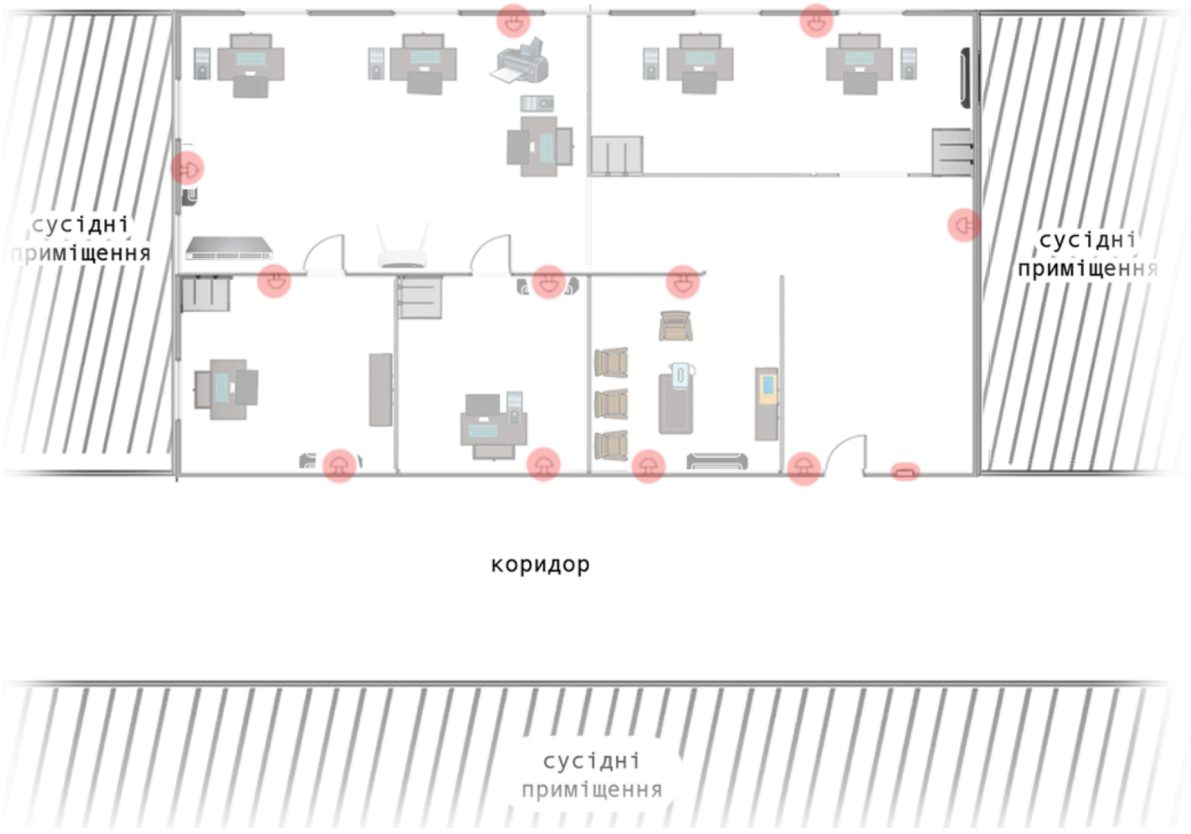


Рисунок 5. Схема системи сигналізації

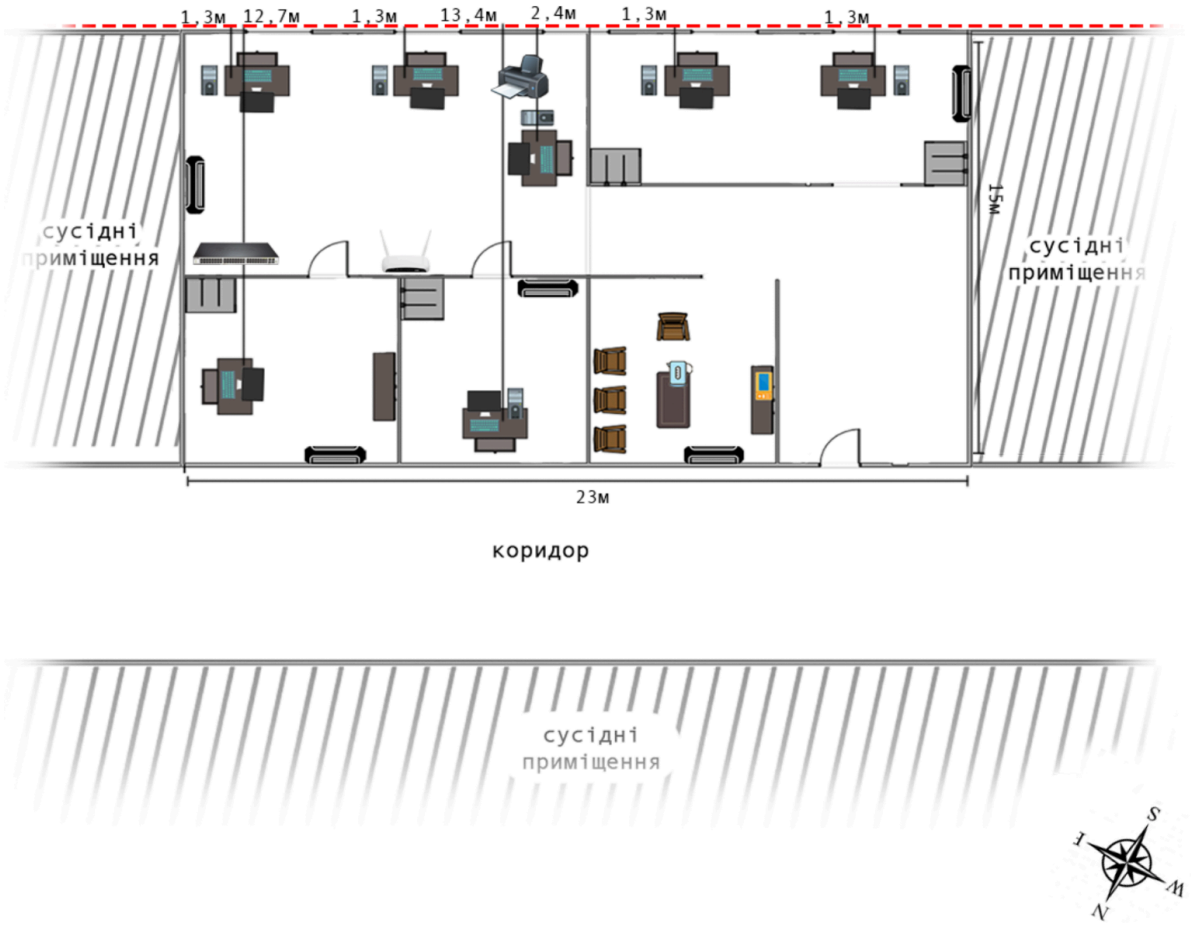


Рисунок 6. Схема основних та допоміжних технічних засобів

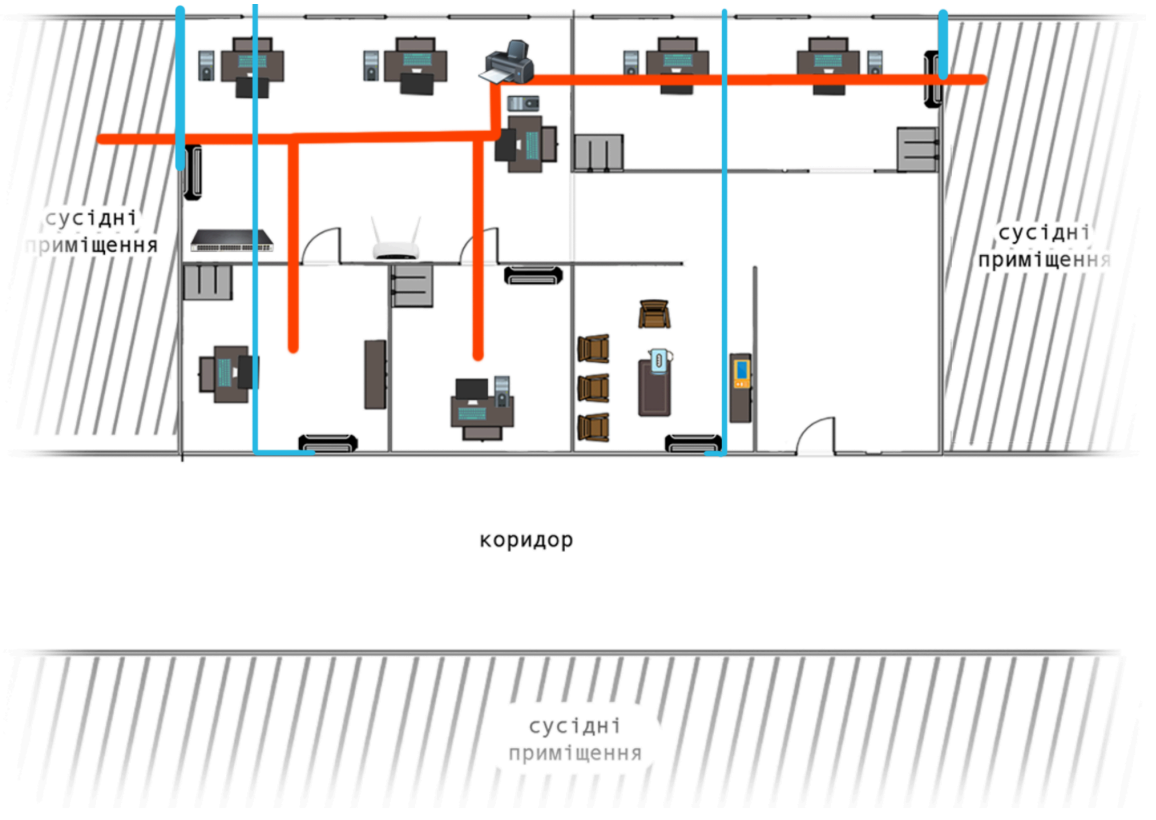


Рисунок 7. Схема системи вентіиляції та кондиціонування

Додаток Б

Гриф обмеження доступу

Прим. № ___

ЗАТВЕРДЖУЮ

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

_директор Людва І. Ю.

(посада, підпис, ініціали, прізвище)

01. 03. 2020

М.П.

АКТ

категоріювання __ТОВ «Промислова Група Корсунь»

(найменування об’єкта категоріювання)

1. Підстава для категоріювання _____

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

_____

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

_____

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

2. Вид категоріювання _____первинне _____

(первинне, чергове, позачергове)

_____

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

3. На ОІД здійснюється обробка інформації технічними засобами _____

(обробка інформації технічними засобами та/або озвучування інформації)

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

_____ конфіденційна інформація _____

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

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

Голова комісії _____ _С.І.Подскальнюк_____

(підпис) (ініціали, прізвище)

Члени комісії: _____ _Т.М. Табала_____

(підпис) (ініціали, прізвище)

____.____. 20___

Додаток В

Н А К А З

м. Корсунь-Шевченківський

01.03.2020 № 101

Про створення комплексної системи
захисту інформації в автоматизованій
системі ІТС ТОВ «Промислова Група
Корсунь»

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

НАКАЗУЮ:

1. Створити комплексну систему захисту інформації в автоматизованій системі для обробки інформації з обмеженим доступом.

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

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

Директор І. Ю. Людва

Додаток Г. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	1 Розділ	7	
6	А4	2 Розділ	46	
7	А4	3 Розділ	11	
8	А4	Висновки	1	
9	А4	Список посилань	3	
10	А4	Додаток А	4	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	
14	А4	Додаток Ґ	1	
15	А4	Додаток Д	1	
16	А4	Додаток Е	1	

Додаток Ґ. Перелік документів на оптичному носії

1 Пояснювальна_записка_Брижата.docx

2 Пояснювальна_записка_Брижата.pdf

3 Презентація_Брижата.pptx

Додаток Д. Відгуки керівників розділів

Відгук керівника економічного розділу:

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

Додаток Е. ВІДГУК

Керівник

ДОДАТОК Є. Відгук керівника кваліфікаційної роботи

ВІДГУК

на кваліфікаційну роботу студентки групи 125-16-2 Брижатої Наталії Юріївни

на тему: «Комплексна система захисту інформації відділу розробки сільськогосподарської техніки ТОВ «Промислова Група «Корсунь»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 11, 60 та 70 сторінках.

Метою кваліфікаційної роботи є підвищення ефективності рівня захіщенності в ІТС відділу розробки сільськогосподарської техніки ТОВ «Промислова Група «Корсунь».

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: аналіз стану інформаційної безпеки та особливості організації захисту інформації на підприємствах, які займаються розробкою сільськогосподарської техніки, аналіз нормативно-правової бази у сфері захисту інформації, аналіз інформаційних ризиків після впровадження КСЗІ.

Практичне значення результатів кваліфікаційної роботи полягає у підвищенні ефективності процесу ідентифікації інформаційних активів, за рахунок розробки рекомендацій для проведення ідентифікації.

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

За час дипломування Карпенко Є.О. проявила 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 Керівник спец. розділу