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 *Зубкова Михайла Юрійовича*

академічної групи *125-20-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплексна система захисту інформації інформаційно-комунікаційної системи ФОП "СТО 911"*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	проф. Магро В.І.			
розділів:				
спеціальний	ст. викл. Кручінін О.В.			
економічний	к.е.н., доц. Пілова Д.П.	90	відмінно	
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2024

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту *Зубкову Михайлу Юрійовичу* **академічної групи** *125-20-2*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Комплексна система захисту інформації інформаційно-комунікаційної системи ФОП "СТО 911"***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 23.05.2024 № 469-с

Розділ	**Зміст**	**Термін виконання**
Розділ 1	Обстеження ІКС «СТО 911», аналіз потенційних загроз безпеки	15.03.2024
Розділ 2	Формування вимог захисту в ІКС, розробка профілю захищеності, політик безпеки та інженерних рішень	10.05.2024
Розділ 3	Економічне обґрунтування доцільності впровадження запропонованих рішень кваліфікаційної роботи	11.06.2024

Завдання видано _____ _____
(підпис керівника) (ім'я, прізвище)

Дата видачі: 15.03.2024р.

Дата подання до екзаменаційної комісії: 28.06.2024р.

Прийнято до виконання _____ Михайло ЗУБКОВ
(підпис студента) (ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 83 с., 6 рис., 15 табл., 6 додатків, 10 джерел.

Об'єкт розробки: ІКС «СТО 911».

Предмет розробки: Комплексна система захисту інформації.

Мета кваліфікаційної роботи: підвищення рівня захищеності інформації, яка обробляється в інформаційно-комунікаційній системі ФОП «СТО 911».

Перший розділ містить обґрунтування необхідності створення КСЗІ для ІКС досліджуваного підприємства та опис результатів обстеження фізичного та інформаційного середовища та обчислювальної техніки ІКС.

В другому розділі формуються вимоги до рівня захисту інформації, досліджується стан виконання окремих послуг безпеки, виконується формулювання організаційних та технічних рішень для забезпечення безпеки інформації.

Третій розділ є обґрунтуванням економічної доцільності створення КСЗІ для ІКС підприємства. Виконуються розрахунки вартості реалізації запропонованих проєктних рішень та потенційні втрати унаслідок реалізації загроз.

Практична цінність розробки полягає у зменшені вірогідності реалізації загроз інформаційної безпеки та уникненню потенційних втрат унаслідок реалізації цих загроз.

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА СИСТЕМА, ІНФОРМАЦІЙНА БЕЗПЕКА, ПОЛІТИК БЕЗПЕКИ, МОДЕЛЬ ПОРУШНИКА, КІБЕРБЕЗПЕКА

ABSTRACT

Explanatory Note: 83 pages, 6 pictures, 15 tables, 6 apps, 10 references.

Object of Development: ICS "STO 911".

Subject of Development: Comprehensive information protection system.

Purpose of the Qualification Work: Improving the level of information security in the information and communication system of the private enterprise "STO 911".

The first section contains the justification for the need to create a comprehensive information protection system for the ICS of the studied enterprise and describes the results of the examination of the physical and information environment and the computing equipment of the ICS.

In the second section, the requirements for the level of information protection are formulated, the state of implementation of certain security services is investigated, and organizational and technical solutions for ensuring information security are formulated.

The third section justifies the economic feasibility of creating a comprehensive information security system for the enterprise's ICS. The costs of implementing the proposed project solutions and potential losses due to threat realization are calculated.

The practical value of the development lies in reducing the likelihood of information security threats and avoiding potential losses due to the realization of these threats.

COMPREHENSIVE INFORMATION SECURITY SYSTEM, INFORMATION AND COMMUNICATION SYSTEM, INFORMATION SECURITY, SECURITY POLICY, THREAT MODEL, CYBERSECURITY

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ДБЖ – джерело безперебійного живлення;

ДСТУ – державний стандарт України;

ЗУ – Закон України;

ІБ – інформаційна безпека;

ІС – інформаційна система;

ІКС – інформаційно-комунікаційна система;

ІзОД – інформація з обмеженим доступом;

КЗ – контрольована зона;

КЗЗ – комплекс засобів захисту;

КСЗІ – комплексна система захисту інформації;

НСД – несанкціонований доступ;

НД ТЗІ – нормативний документ із технічного захисту інформації;

ОІД – об’єкт інформаційної діяльності;

ОС – операційна система;

ПК – персональний комп’ютер.

ЗМІСТ

с.

ВСТУП

У двадцять першому сторіччі неможливо уявити життя без комп'ютерної техніки та усіх похідних з неї. З кожним роком комп'ютеризація суспільства стає все ширшою та поглинає все більше побутових завдань, вирішення яких ручним способом ще вчора здавалось буденним і не уявлялось можливості автоматизації цих процесів. Швидкість цього процесу збільшується по геометричній прогресії. Найбільшу цінність несуть не фізичні активи, а інформаційні.

Чим більш складною та комплексною стає комп'ютерна система, тим більше з'являється вразливостей, при використанні котрих злочинці можуть скомпрометувати інформацію. Роблячи висновок з першого абзацу, безпека інформації виходить на перші позиції по важливості у сучасному світі.

Якщо раніше комп'ютерні технології були доступними лише найбільш забезпеченим підприємствам та найважливішим державним установам, то зараз без досягнень інформаційних технологій не обходиться жодне виробництво та жоден об'єкт інформаційної діяльності (далі – ОІД). Теж саме стосується і зловмисників – гаджети стають все більш потужними та доступними. В таких умовах, захист інформації стає не забаганкою, а потребою.

Не дивлячись на це, багатьма управлінцями нехтується важливість забезпечення безпеки інформації, і, як наслідок, інформаційно-комунікаційні системи (далі – ІКС) майже всіх підприємств мають фатальні вразливості, які можуть перерости у не менш фатальні збитки.

Мета кваліфікаційної роботи – дослідити середовище існування конкретного ОІД та його ІКС, висунути вимоги відносно ступеню захищеності та запропонувати проєктні рішення для реалізації потреб захисту інформації, попутно обґрунтувавши економічну доцільність запропонованих заходів.

РОЗДІЛ І. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Підстави для створення КСЗІ

На момент написання кваліфікаційної роботи, Україна знаходиться більше двох років у стані активної війни з сусідньою державою. Як було зазначено у вступі до кваліфікаційної роботи, комп'ютеризація та впровадження інформаційних технологій не обходить жодну сферу життя. Очевидно, що військова галузь, яка протягом усього доступного для пізнання часу, була найбільш забезпеченою досягненнями сучасних технологій і слугувала полігоном для тестування та «обкатки» нових, експериментальних рішень. Було б дуже наївно вважати, що під час війни не будуть використовуватись усі переваги своїх, та вразливості чужих інформаційних технологій.

В таких умовах, інформаційна безпека стає ще більш актуальною, а її завдання стають складнішими і більш комплексними. З'являється все більше зловмисників, що мають ідеологічні мотиви. Крім того, вже існуючи зловмисники, мотивовані матеріальним збагаченням, можуть бути закликані до активних дій за допомогою долучення бюджетів країни-ворога.

Наприклад, по даним Державної служби спеціального зв'язку та захисту інформації України, в 2024 році було зафіксовано щонайменше дві величезні кібератаки на комп'ютери робітників бухгалтерських відділів [1].

Очевидно, що хакерські атаки мають своєю ціллю не тільки державну інформаційну інфраструктуру, а й приватні підприємства. Нехтувати захистом інформації в таких умовах фактично неможливо.

Згідно шостого пункту НД ТЗІ 3.7-003-2005, підставою для визначення необхідності створення КСЗІ є норми та вимоги чинного законодавства, які встановлюють обов'язковість обмеження доступу до певних видів інформації або забезпечення її цілісності чи доступності, або прийняте власником інформації рішення щодо цього, якщо нормативно-правові акти надають йому право діяти на власний розсуд.

Вихідні дані для обґрунтування необхідності створення КСЗІ у загальному випадку одержуються за результатами:

- аналізу нормативно-правових актів (державних, відомчих та таких, що діють в межах установи, організації, підприємства), на підставі яких може встановлюватися обмеження доступу до певних видів інформації чи заборона такого обмеження, або визначатися необхідність забезпечення захисту інформації згідно з іншими критеріями;
- визначення наявності у складі інформації, яка підлягає автоматизованій обробці, таких її видів, що потребують обмеження доступу до неї або забезпечення цілісності чи доступності відповідно до вимог нормативно-правових актів;
- оцінки можливих переваг (фінансово-економічних, соціальних тощо) експлуатації ІКС у разі створення КСЗІ. На підставі проведеного аналізу приймається рішення про необхідність створення КСЗІ [2].

Рішення про необхідність впровадження КСЗІ прийнято керівництвом підприємства. Головним чинником прийняття такого рішення впевненість у тому, що достатній рівень захисту інформації значно зменшить ризики фінансових та репутаційних збитків для підприємства. Головним чинником, що вплинув на вибір в користь саме КСЗІ, а не Системи Управління Інформаційною Безпекою, є плани керівництва по розширенню виробництва та початку обслуговування спеціальної техніки.

1.2 Обстеження ІКС

1.2.1 Загальні відомості

«Сервіс технічного обслуговування «СТО 911» являє собою підприємство по діагностиці та ремонту автомобілів у м. Дніпро.

Форма власності - ФОП, площа та будівля орендовані у власника нерухомості.

Основними напрямами діяльності є:

- діагностика автомобілів;
- ремонт автомобілів;
- продаж автомобільних товарів.

Штат працівників складає: 2 керівники, менеджер по роботі з клієнтами, менеджер по роботі з закупками, 10 механіків, логіст, бухгалтер на віддалені, завгосп, інструменталіст, прибиральниця офісу, 2 нічні сторожі.

1.2.2 Фізичне середовище

Ситуаційний план представлено нижче на рис. 1.1.

Рисунок 1.1 – Схема ситуаційного плану

Об’єкт інформаційної діяльності розташовано в одноповерховій промисловій будівлі та прибудові до неї, що виконує функції офісу за адресою вулиця Каруни, 135А. Територія навколо об’єкту вкрита бетоном, на задньому дворі переважає ґрунтова поверхня.

На північному сході від об'єкту дослідження знаходиться невелике кафе, сервіс надання послуг по реєстрації транспортних засобів. Між кафе та сервісом реєстрації розташована парковка для відвідувачів сервісу. Через дорогу знаходиться будівля Дому культури, що нині знаходиться у власності християнської общини.

На сході від об’єкту знаходиться великий піщаний пустир, частково покритий деревами. За пустирем на відстані 190м знаходиться 9-поверховий будинок.

На півдні від об’єкту розташований гаражний кооператив. До нього веде єдина дорога уздовж периметру об’єкту.

На заході від об’єкту знаходиться прилегла вулиця, з якої можна попасти на територію об’єкту. За цією вулицею на відстані 10 м знаходиться шосе, за яким на відстані 30 м знаходиться залізна дорога.

В таб. 1.1 представлений перелік сусідніх будівель.

Таблиця 1.1. – Характеристика прилеглих будівель та споруд

№	Найменування	Кількість поверхів	Адреса	Відстань від ОІД
1	ОІД	1	вул. Каруни, 135а	-
2	Сервіс реєстрації автомобілів	2	пр. Мануйлівський, 2	30м
3	Кафе «Drive»	1	пр. Мануйлівський, 2	45м
4	АЗС «Нефтек»	1	пр. Мануйлівський, 2а	100м
5	Сторожова гаражного кооперативу	1	вул. Каруни, 137	60м
6	Дім культури	2	пр. Мануйлівський, 1	105м

Продовження таблиці 1.1

№	Найменування	Кількість поверхів	Адреса	Відстань від ОІД
7	Житловий будинок	9	пр. Мануйлівський, 2б	190м

На рис. 1.2 представлено фрагмент генерального плану, а саме офісну частину, або ж приймальню СТО. Фактично, ОІД розповсюджується на всю територію технічного цеху та приймальні, бо для потреб комп'ютерної діагностики потрібно підносити робочі ноутбуки, які є частиною інформаційно-комунікаційної системи, безпосередньо до автомобіля, що проходить діагностику. На рис. 1.3 зображену схему ліній комунікацій на фрагменті генерального плану.

КЗ представлена стінами, дверима, вікнами, підлогою та стелею офісної частини будівлі. У час роботи доступ до КЗ контролюється працівниками, несанкціоновані особи визивають інтерес зі сторони персоналу та мають обґрунтувати своє знаходження на території об'єкту.

ОІД займає усю територію будівлі, так як обчислювальна техніка використовується як в офісній частині будівлі, так і у технічному ангарі. Доступ до території ОІД фактично має будь яка людина. До офісної частини можна потрапити лише через технічне приміщення.

Оскільки підприємство є станцією технічного огляду, клієнти повинні мати вільний доступ до території. Працівники не можуть забезпечити повне дотримання режиму через зайнятість роботою.

Повна площа ОІД - 440м^2, площа офісну - 60м^2. Зовнішні стіни складаються з цегли, укладеної у 1.5 шара, товщиною 400 мм. Внутрішні стіни з цегли в 1 шар, товщиною 250 мм. Фундамент будівлі бетонний, дах складається з гофрованого металу.

Вікна та двері офісу металопластикові. Для в'їзду транспортних засобів на територію СТО використовуються залізні ворота висотою 4м та шириною 3,6м.

Рисунок 1.2 – Фрагмент генерального плану

Рисунок 1.3 – схема ліній комунікацій на фрагменті генерального плану

По периметру та всередині будівлі встановлені камери спостереження та об ’ємнісні датчики, на дверях встановлено електромагнітні датчики. Сліпих зон засобів виявлення не спостерігається.

По праву руку від воріт паркану встановлена сторожове приміщення. З нього є огляд на шляхи підходу до будівлі. Поряд з сторожовою знаходиться загородження з охоронними собаками, що лають на незнайомців.

За територію підприємства винесені лінії електропостачання, водопостачання та оптоволоконний кабель інтернет-підключення. Труби водопостачання заходять зі сторони шосе, електропостачання та

оптоволоконний кабель проведено через пустир від найближчого багатоповерхового будинку (будівля №7 на сит. плані). На стовпі поряд з будинком встановлено невеликий масляний трансформатор.

Об'єкт не має підключення до системи каналізації, відходи зливаються у зливну яму.

Прибиранням на території офісу та складу займається прибиральниця. На промисловій території фактично не прибираються. За інструментами слідкує інструменталіст. Їх роботу контролює завгосп.

Документи та інші цінні папери зберігаються у шафі під замком. Також присутня окрема шафа для зберігання пристроїв комп'ютерної діагностики автомобілів. Вона розташована у наступній залі за приймальною. Доступ до шафи мають лише управлінці та 2 механіки, уповноважені для роботи по діагностиці.

До офісу, або ж приймальні, мають доступ усі працівники. Там розміщені майже всі елементи ІКС.

Пристрої підключаються до мережі по WI-FI. Специфіка електронної діагностики вимагає прямого підключення автомобілю через спеціальний діагностичний інтерфейс до комп'ютера через спеціальне технічне обладнання. У свою чергу, на комп'ютері встановлено ПЗ призначене для діагностики. Через вищевказані фактори, для забезпечення робочого циклу по обслідуванню, діагностиці та ремонту автомобіля, використовуються переносні ноутбуки та відповідні пристрої, що до них підключаються. Через необхідність прямого підключення, ноутбуки мають знаходитись максимально близько до автомобіля, що проходить діагностику. Через це, межа ОІД фактично покриває усю територію підприємства.

1.2.3 Обчислювальна система:

Комп'ютерна система складається з мережевого обладнання, офісних ПК, мережевого принтеру та ноутбуків для діагностики. На рис. 1.4 можна побачити структурну схему ІКС.

В групу мережевого обладнання входить медіаконвертор, маршрутизатор, концентратор та ретранслятор. На територію ОІД проведено оптоволоконний кабель, в віддаленій частині офісу знаходиться медіаконвертор, що перетворює оптичний сигнал на електричний. Далі по витій парі інтернет підключається до маршрутизатору, що створює WI-FI мережу. З маршрутизатору проведено кручену пару до концентратора, з якого у свою чергу розведено кабелі до стаціонарних комп'ютерів та принтеру. Наявний ретранслятор сигналу в сторожовому приміщені за межею основної будівлі.

Ноутбуки підключаються до мережі Інтернет за допомогою бездротового підключення.

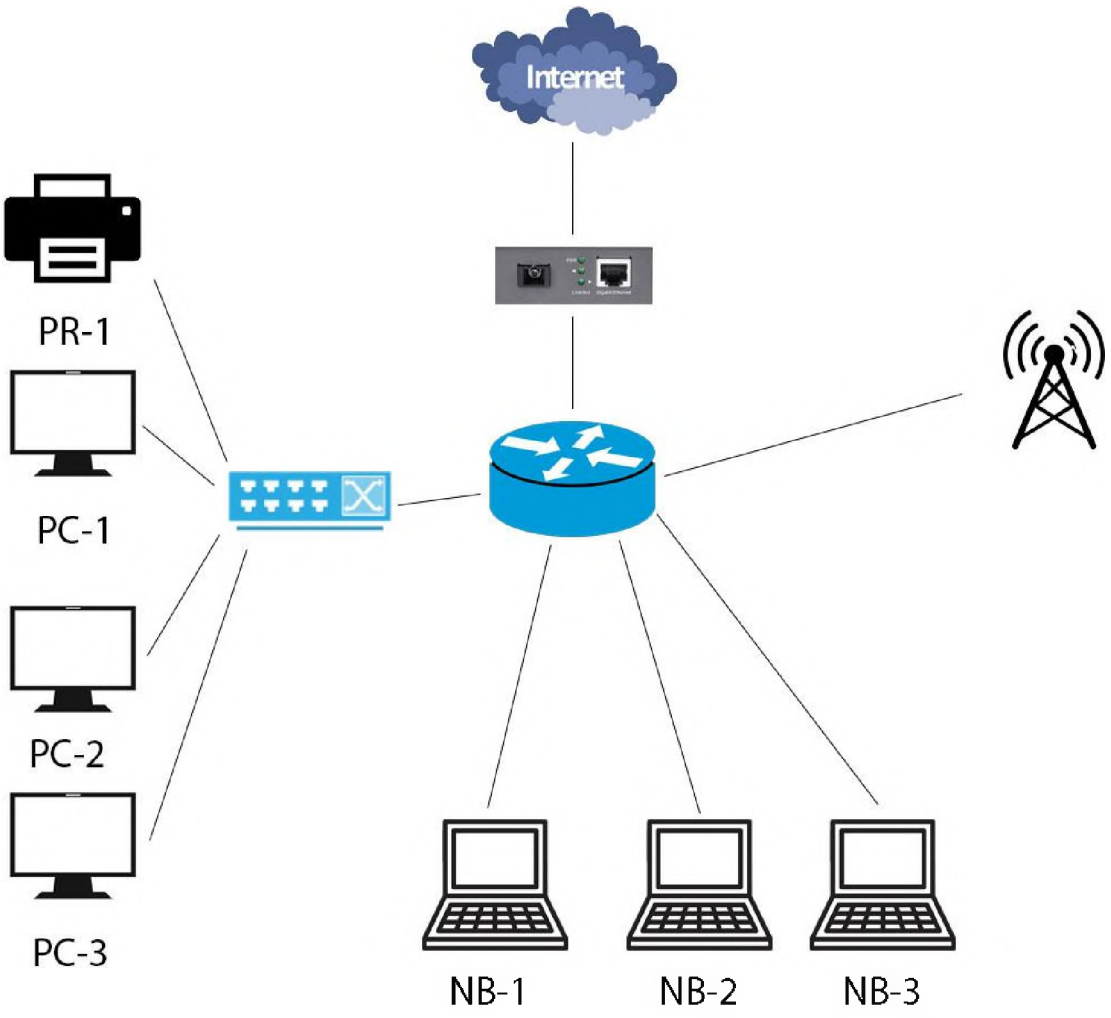

Рисунок 1.4 – Структурна схема інформаційно-комунікаційної системи

Рисунок 1.5 – Позначення на структурній схемі інформаційно-комунікаційної системи

Також варто зазначити, що по бездротовому зв'язку, до мережі WI-FI можуть підключатись усі співробітники підприємства, навіть ті, що не є штатними користувачами ІКС.

В додатку Б наведено перелік основних технічних засобів інформаційно-комунікаційної системи досліджуваного об'єкту.

В таблиці 1.2 представлено перелік допоміжних технічних засобів ІКС.

Таблиця 1.2 Додаткові технічні засоби ІКС

№	Пристрій	Модель	Характеристика	Серійний номер	Відстань до КЗ
1	Миша комп'ютерна бездротова (3 шт.)	Logitech B100	Дротове підключення, оптичний сенсор	МРС-1	2м
				МРС-2	3м
				МРС -3	1м
2	Клавіатура комп'ютерна (3 шт.)	Logitech K120	Дротове підключення	КВРС-1	2м
				КВРС-2	3м
				КВРС-3	1м

В таблиці 1.3 представлений перелік ПЗ, встановленого на ПК в системі.

Таблиця 1.3 Програмне забезпечення ІКС

Тип	Назва	Опис	Ліцензія	Встановлено на пристрій
Системне ПЗ	Windows 10 Pro 22H2	Операційна система	Електрона ліцензія	PC-1, PC-2, PC-3, NB-1
	Windows 7 Ultimate	Операційна система	Електрона ліцензія	NB-2
Системне ПЗ	Windows Vista Ultimate	Операційна система	Електрона ліцензія	NB-3
	Драйвери	Драйвери для коректної роботи пристроїв	Пропрієтарна ліцензія	PC-1, PC-2, PC-3, NB-1, NB-2, NB-3
Прикладне	Microsoft Office 365 for Business	Комплект офісного ПЗ	Електрона ліцензія	PC-1, PC-2, PC-3, NB-1, NB-2, NB-3
Спеціалізоване	Chrome	Вебпереглядач	Електрона ліцензія	PC-1, PC-2, PC-3, NB-1, NB-2, NB-3
	Telegram	Мессенджер	Електрона ліцензія	PC-1, PC-2, PC-3, NB-1, NB-2, NB-3
	Viber	Мессенджер	Електрона ліцензія	PC-1, PC-2, PC-3, NB-1, NB-2, NB-3
	TeamViewer	Віддалений доступ до ПК	Електрона ліцензія	PC-1, PC-2, PC-3, NB-1, NB-2, NB-3
	AnyDesk	Віддалений робочий стіл	Електрона ліцензія	NB-1, NB-2, NB-3

Продовження таблиці 1.3

Тип	Назва	Опис	Ліцензія	Встановлено на пристрій
	XENTRY OpenShell	ПЗ для діагностики	Корпоративна ліцензія	NB-1
	ISTA BMW	ПЗ для діагностики	Корпоративна ліцензія	NB-2
	Renault CAN CLIP	ПЗ для діагностики	Корпоративна ліцензія	NB-3

Постійний системний адміністратор у системі відсутній. Персонал компанії власноруч обслуговує систему у рамках своєї компетенції у роботі з комп'ютерною технікою. У разі виникнення задачі, що її вирішення не під силу робітникам, керівництво долучає знайомого системного адміністратора за фіксовану суму в залежності від складності завдання. Адміністратор не має власного облікового запису у системі. Адміністратор прибуває до підприємства і вирішує проблему, але при можливості усунення проблеми дистанційно, він підключається до відповідного комп'ютеру за допомогою TeamViewer.

1.2.4 Інформаційне середовище

Було досліджено інформаційне середовище. Уся інформація, що циркулює в ІКС підприємства була відсортована за типами. Перелік інформації та вимог до захисту інформації цього типу, наведено в таблиці 1.4.

Таблиця 1.4 − Інформація, що циркулює на досліджуваному об'єкті

№	Інформація	Режим доступу	Правовий режим	Носій інформації	Вимоги до захисту		
					К	Ц	Д
1	Інформація про клієнтів та їх ТС	ІзОД	Конфіденційна	Електронні носії	4	3	1

Продовження таблиці 1.4

2	Фінансова інформація	ІзОД	Конфіденційна	Електронні та паперові носії	4	3	2
3	Інформація про закупівлі	ІзОД	Конфіденційна	Електронні та паперові носії	3	3	2
4	Інформація про забезпечення	ІзОД	Конфіденційна	Електронні носії	2	1	1
5	Діагностична інформація	ІзОД	Конфіденційна	Електронні носії	3	3	1
6	Технологічна інформація	ІзОД	Конфіденційна	Електронні та паперові носії	4	4	3
7	Довідкова інформація	Відкрита	Відкрита	Електронні та паперові носії	2	3	2

Рівні конфіденційності інформації:

- К1 – інформація не вважається конфіденційною, її розкриття не призведе до серйозних збитків;
- К2 – розкриття інформації особам, яким не передбачається доступ, завдасть несуттєвих збитків у випадку;
- К3 – розкриття інформації особам, яким не передбачається доступ, завдасть суттєвих збитків;
- К4 – розкриття інформації особам, яким не передбачається доступ, завдасть суттєвих збитків, в тому числі фінансових;
- К5 – розкриття інформації особам, яким не передбачається доступ, завдає значних збитків, може призвести до тимчасової або повної зупинки роботи.

Рівні цілісності інформації:

- Ц1 – втрата цілісності не призведе до збитків, можна знехтувати;
- Ц2 − втрата цілісності призводить до несуттєвих збитків;

- Ц3 – втрата цілісності призводить до суттєвих збитків;
- Ц4 – втрата цілісності призводить до суттєвих, фінансових або репутаційних, збитків;
- Ц5 – втрата цілісності інформації завдає значних збитків, може призвести до тимчасової або повної зупинки роботи.

Рівні доступу інформації:

- Д1 – втрата доступності не призведе до збитків, можна знехтувати;
- Д2 – втрата доступності призводить до несуттєвих збитків;
- Д3 – втрата доступності призводить до суттєвих збитків;
- Д4 – втрата доступності призводить до суттєвих, фінансових або репутаційних, збитків;
- Д5 – втрата доступності інформації завдає значних збитків, може призвести до тимчасової або повної зупинки роботи.

Уся інформація, що безпосередньо зв'язана з промисловим циклом обслуговування клієнтів фіксується, та оброблюється за допомогою потужностей сервісу CarBook. Це український сервіс, розроблений спеціально для потреб вітчизняних станцій технічного огляду, або ж СТО. В ньому ведеться облік клієнтів, транспортних засобів, ведеться бухгалтерський підрахунок, тощо.

Інформація про клієнтів, їх персональні дані, інформація про їх транспортні засоби, їх стан та виконані роботи зберігається, як сказано вище, на віддаленому сервері сервісу CarBook. Доступ до цієї інформації мають керівники, менеджер, бухгалтер та логіст.

Інформація про інструменти зберігається у Google таблиці. Доступ до цієї інформації мають керівники, менеджер, інструменталіст та логіст. Також, оскільки на СТО дуже великий об'єм інструментарію та велика кількість робітників, які можуть його використовувати; він зберігається на настінних тримачах, на яких намальовано форму та назву інструменту, для того щоб в процесі роботи можна було швидко орієнтуватись у зайнятості певного інструменту, та щоб можна було зручно і швидко повернути на своє місце конкретний інструмент. Оскільки кожен інструмент має своє чітко визначене

місце і місцезнаходження, можна вважити, що полиці з силуетами є фізичним носієм інформації про інструменти.

Фінансова інформація створюються та оброблюється бухгалтером на основі даних з сервісу CarBook та початково знаходиться в електронній формі. Однак, за потреби, вони можуть бути роздруковані. Роздруковані документи зберігаються у кімнаті керівника.

Під діагностичною інформацією розуміються відомості про стан конкретного транспортного засобу, збої в роботі, попередження, тощо. Ця інформація створюється лише в момент електронної діагностики автомобіля на спеціалізованому ноутбуці, після чого вона відправляється на ПК менеджера для друку на принтері. Для відправки цієї інформації використовується окремий чат в додатку Viber.

Інформація про забезпечення це вся інформація, що стосується забезпечення виробничого циклу усіма необхідними умовами для безперебійної роботи, однак не має прямого відношення безпосередньо до процесу ремонту автомобілів. Наприклад такою інформацією є договори про забезпечення СТО розхідниками, інформація про прибирання, інформація про хімчистку робочих комбінезонів, інформація про комунальні послуги, тощо.

Також у ІКС представлена довідкова інформація. До неї відносяться друковані, або електронні довідники, інструкції по ремонту, списки запчастин, тощо. Головним чином вона представлена у вигляді віддаленого робочого стола з різними вкладками у відповідності до типу шуканої інформації. Також є деякі паперові довідники. Сама інформація не є ІзОД, бо фактично хто завгодно може купити ці довідники у вільному доступі. Однак, на ОІД вона знаходиться поза зоною доступу клієнту сервісу.

1.2.5 Середовище користувачів

Штатними працівниками є безпосередньо механіки, менеджери, керівники, логіст та бухгалтер на віддалені. Серед механіків, користувачами ІКС є один, бо лише він та один з двох керівників мають відповідні навички та освіту для виконання електронної діагностики. Рядові механіки, що не мають такої

кваліфікації фактично не використовують ресурси ІКС. Позаштатними є завгосп, інструменталіст, прибиральниця та сторожі. Завгосп керує роботою прибиральниці, інструменталіста та частково сторожів. Прибиральниця приходить увечері п'ятниці, щоб прибратись у офісній частині будівлі. Інструменталіст приходить двічі на тиждень щоб прослідкувати за станом інструментів, за потреби повернути їх на місця. Сторожі працюють позмінно через день. Вони приходять за 20 хвилин до закриття СТО та займають своє місце у сторожовій будівлі.

Керівники займаються безпосередньо управлінням підприємством, керують виробничими процесами, представляють підприємство, можуть виконувати частину роботи менеджерів, тощо. Один з керівників та один з механіків є фактично старшими механіком, що виконує найтяжчі та найважливіші завдання. Лише в нього та одного з механіків є достатній рівень кваліфікації для виконання електронної діагностики автомобілів.

Серед трьох менеджерів два займаються закупівлею, замовленням деталей, відправленням на ремонт окремих частин автомобілів, що потребують спеціалізованого обладнання для ремонту, закупівлю інструментів, розхідників, тощо. Третій менеджер виконує функції обслуговування клієнтів. Він відповідає на дзвінки, приймає клієнтів, що звертаються в очному форматі. Через відносно невелику зайнятість, він допомагає за можливості іншим працівникам, тестує автомобілі в реальних умовах, переганяє ТС.

В обов'язки логіста входить забезпечення виробництва. Він займається доставкою деталей на об'єкт або з об'єкту, доставляє товари забезпечення, переганяє автомобілі на «схід-розвал», тощо.

В обов'язки бухгалтера входить повне ведення бухгалтерського обліку. Під цим розуміється контроль фінансових процесів, підготовка звітностей, облік коштів, розрахування витрат та доходів, підрахунок заробітної плати, тощо.

В таблиці 1.5 представлена матриця доступу співробітників до інформації.

Таблиця 1.5 – Матриця розмежування доступу

Посада	1	2	3	4	5	6	7
Керівник	В Д З Р С Ч	В Д З Р С Ч	В Д З Р С Ч	В Д З Р С Ч	В Д З Р С Ч	В Д З Р С Ч	В Д З Р С Ч
Старший механік	-	-	-	-	В Д Р С Ч	-	Д З Ч
Менеджер	В Д З Р С Ч	Д Ч	В Д З Р С Ч	В Д З Р С Ч	Д Ч	В Д З Р С Ч	Д З Ч
Логіст	-	-	Ч С Р	В Д З Р С Ч	-	-	-
Бухгалтер	-	В Д З Р С Ч	-	-	-	-	-

Умовні позначення в таблиці 1.7:

- В – видалення
- Д – друк
- З – зберігання
- Р – редагування
- С – створення
- Ч – читання

1.2.6 Модель порушника

Відповідно до НД ТЗІ 1.1-002-99 від 28.12.201, порушник - особа, яка може одержати доступ до роботи з включеними до складу КС засобами. Залежності до знаходження у або поза середовищем користувачів, порушників можна поділити на внутрішніх та зовнішніх. В таблиці 1.6 наведено моделі порушників.

Таблиця 1.6 – Модель порушника

Назва	Мотив	Кваліфікація	Можливості	Час дії	Місце дії	Сума загроз
Внутрішні порушники						
Керівник	М1	К3	З4	Ч3	Д4	14
Менеджер	М3	К3	З2	Ч2	Д3	13
Старший мех.	М3	К2	З2	Ч1	Д2	10
Логіст	М3	К2	З2	Ч1	Д2	10
Інструменталіст	М2	К1	З1	Ч1	Д1	6
Механіки	М2	К1	З1	Ч1	Д1	6
Бухгалтер	М3	К2	З4	Ч2	Д1	12
Системний адміністратор	М3	К4	З4	Ч3	Д4	18
Зовнішні порушники						
Хакери	М3	К4	З4	Ч1	Д1	13
Обслуговуючий персонал	М2	К1	З1	Ч1	Д2	7
Агенти конкурентів	М3	К2	З1	Ч2	Д1	9

Категоризація порушників за мотивом здійснення порушення:

- М1 – безвідповідальність (недбалість);
- М2 – самоствердження;
- М3 – Корисливий інтерес [3].

Категоризація порушників за рівнем кваліфікації та обізнаності щодо ІКС:

- К1 – Володіє низьким рівнем знань, не має навичок користування засобами ІКС
- К2 – Володіє навичками та знаннями користування ПК на рівні користувача;

- К3 – володіє базовими навичками та знаннями стосовно функціонування штатних для ІКС програмного забезпечення й операційних систем;
- К4 – володіє навичками та знаннями стосовно функціонування штатних для ІКС програмного забезпечення й операційних систем, а також їх недоліками [3].

Категоризація порушників за можливістю використання засобів ІКС для реалізації загроз:

- З1 – може отримувати мінімальну інформацію методом підслуховування,

підглядування, тощо;

- З2 - може отримувати інформацію пасивним способом використовуючи

технічні засоби, не модифікує інформацію;

- З3 – може отримувати інформацію, використовуючи лише штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів);
- З4 – використовує технічні засоби для активного впливу на ІКС, може

модифікувати інформацію на ІКС, дезорганізовувати систему [3].

Категоризація порушників за часом дії:

- Ч1 – під час призупинки компонентів системи (під час технічних або планових перерв у роботі, у неробочій час);
- Ч2 – під час функціонування ІКС, або її компонентів;
- Ч3 – як під час функціонування, так і під час зупинки роботи ІКС для обслуговування та ремонту [3].

Категоризація порушників за місцем дії:

- Д1 – усередині приміщень, але без доступу до технічних засобів ІКС;
- Д2 – з робочих місць користувачів;
- Д3 - З доступом у зону зберігання баз даних, архівів тощо;

- Д4 - З доступом у зону керування засобами забезпечення безпеки ІКС [3].

Аналізуючи матрицю моделей порушників можна зробити висновок, що найбільшу загрозу для безпеки ІКС становлять: системний адміністратор, керівники та менеджери.

1.2.7 Аналіз загроз для інформації в ІКС

Розділяючи загрози безпеці інформації за джерелом походження, можна виділити 3 основні групи:

- Антропогенні (людського походження);
- Техногенні (технічного походження);
- Стихійні (природного походження).

В додатку Г наведено найбільш ймовірні загрози по кожному з пунктів вище.

Таблиця 1.7 – Розподілення рівня загроз за ступенем небезпеки

Загроза	Рівень загрози				Ступінь небезпеки
	Ймовірність	Збитки			
		К	Ц	Д	
Несанкціонований доступ до ІКС	3	4	3	3	40
Несанкціоноване копіювання ІзОД	3	4	1	1	24
Підглядання та підслуховування ІзОД	2	2	1	1	10
Відсутність інтернет-підключення через збої роботи провайдера	3	1	3	4	32
Перепади напруги	2	1	4	4	24
Займання легкозаймистих речовин	1	5	5	5	20

Означення ймовірності реалізації загроз в таб 1.13:

1 – мала або відсутня ймовірність (0-10%);

2 – невірогідна (10-20%);

3 – можлива (20-40%);

4 – достатня вірогідність (40-60%);

5 – висока вірогідність (60-100%).

Ступінь небезпеки розраховано за формулою 1.1.

$$C_н = \frac{I*(К+Ц+Д)}{75} * 100 \quad (1.1)$$

1.3 Висновок

Провівши обстеження інформаційно-комунікаційної системи об'єкту інформаційної діяльності, дослідивши усі середовища існування системи, стало очевидно, що на даний момент, організація інформаційної безпеки не може забезпечити належний рівень безпеки інформації. Провівши аналіз моделі порушника, було виявлено, що найбільшу загрозу для функціонування системи становлять в першу чергу внутрішні користувачі системи з високим рівнем доступу до останньої, такі як системний адміністратор, керівники, менеджери. Також, велику загрозу становлять хакери, так як система не відрізняється великим ступнем захисту. Однак, через малу матеріальну віддачу відносно витрачених зусиль на компрометацію системи, атака хакерів на інформаційну систему є досить маловірогідною.

РОЗДІЛ ІІ. СПЕЦІАЛЬНИЙ РОЗДІЛ

2.1 Формування вимог захисту інформації в ІКС

2.1.1 Визначення вимог до захисту інформації

Система, що розглядається в роботі, за всіма ознаками є автоматизованою системою 3 класу.

Після аналізу загроз для інформаційної безпеки, можна визначити вимоги до захисту інформації на об’єкті інформаційної діяльності.

Умовно, об’єкти, що потребують захисту, можна поділити на декілька груп:

1) Дані, що зберігаються на віддаленому сервері бази даних CarBook;

2) Дані, що зберігаються на електронних носіях ПК та ноутбуків;

3) Дані, що зберігається на паперових носіях (фінансові звітності, юридична інформація, довідники по ремонту).

Далі представлено послуги безпеки, які мають бути реалізовані задля забезпечення належного рівня захисту інформації.

Умова: КД-2 – Базова довірча конфіденційність

Відноситься до множин об’єктів: 3

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта. Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта. Необхідні умови: НИ-1 [4].

Умова: КА-2 – Базова адміністративна конфіденційність

Відноситься до множин об’єктів: 1,2.

Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження. Необхідні умови: НО-1, НИ-1 [4].

Умова: КО-1 – Повторне використання об’єктів.

Відноситься до множин об’єктів: оперативна пам’ять комп’ютера.

Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані.

Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною [4].

Умова: КВ-2 – Базова конфіденційність при обміні.

Відноситься до множин об’єктів: 1, 2, 3.

Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуються, і спроможність користувачів і/або процесів керувати рівнем захищеності.

КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається.

Запити на призначення або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження.

Запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу.

Запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу. Необхідні умови: НО-1 [4].

Умова: ЦД-1 – Мінімальна довірча цілісність

Відноситься до множин об’єктів: 3.

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

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

КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт. Необхідні умови: НИ-1 [4].

Умова: ЦА-2 – Базова адміністративна цілісність

Відноситься до множин об’єктів: 1, 2

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

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

КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретні процеси і/або групи процесів, які мають право модифікувати об'єкт.

КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного процесу шляхом керування належністю користувачів і процесів до відповідних доменів визначити – конкретних користувачів і/або групи користувачів, які мають право ініціювати процес. Необхідні умови: НО-1, НИ-1 [4].

Умова: ЦО-1 –Обмежений відкат

Відноситься до множин об’єктів: 1, 2, 3

Множина об’єктів, до яких відноситься умова: множина 1

Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу. Необхідні умови: НИ-1 [4].

Умова: ЦВ-2 – Базова цілісність при обміні

Відноситься до множин об’єктів: 3.

КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається, а також фактів його видалення або дублювання, Запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу, Запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу, Запити на присвоєння або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження. Необхідні умови: НО-1 [4].

Умова: ДР-1 –Квоти

Відноситься до множин об’єктів: простір хмарного сервісу CarBook.

Політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу.

Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження. Необхідна умова: НО-1 [4].

Умова: ДВ-1 – Ручне відновлення

Відноситься до множин об’єктів: 1, 2, 3.

Після відмови КС або переривання обслуговування КЗЗ повинен перевести КС до стану, із якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження. Необхідна умова: НО-1 [4].

Умова: НР-2 – Захищений журнал.

КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки.

Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події.

КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування. Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації. Необхідні умови: НИ-1, НО-1 [4].

Умова: НИ-2 – Одиночна ідентифікація та автентифікація.

Атрибути користувачів: інсталяція та запуск ПЗ, зміна системних файлів, перегляд журнал подій, а також дозвіл на перегляд, редагування, видалення та виконання.

Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен автентифікувати цього користувача з використанням захищеного механізму. Необхідні умови: НК-1 [4].

Умова: НК-1 – Однонаправлений достовірний канал

Достовірний зв'язок повинен реалізуватися автентифікацією користувачів (складний пароль) і наданням доступу до АС тим користувачам, які мають для цього необхідні повноваження.

Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем. Необхідні умови: немає [4].

Умова: НО-2 – Розподіл обов’язків адміністратора

Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції.

Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі. Необхідні умови: НИ-1 [4].

Умова: НЦ-2 – КЗЗ з контролем цілісності.

КЗЗ повинно забезпечити перевірку цілісності ПЗ за допомогою засобів автоматичної перевірки і оновлення.

В разі виявлення порушення цілісності будь-якого із своїх компонентів КЗЗ повинен повідомити адміністратора і або автоматично відновити відповідність компонента еталону або перевести КС до стану, з якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження.

Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ. Необхідні умови: НР-1, НО-1 [4].

Умова: НТ-2 – КЗЗ з контролем цілісності.

Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ. КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження, при ініціалізації КЗЗ. Необхідні умови: НО-1 [4].

Умова: НВ-1 –Автентифікація вузла.

КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації. Необхідні умови: немає [4].

2.1.2 Профіль захищеності

На основі обраних умов послуг безпеки, можна виділити профіль захищеності 3.КЦД.2 = { КД-2, КА-2, КО-1, КВ-2, ЦД-1, ЦА-2, ЦО-1, ЦВ-2, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }, тобто профіль захищеності для систем 3 класу, з підвищеними вимогами до забезпечення конфіденційності, цілісності і доступності оброблюваної інформації 2-го рівня [9].

Далі буде проаналізовано реалізацію послуг безпеки, визначених в пункті вище.

КД-2 – Мінімальна довірча конфіденційність – частково реалізована. На комп'ютерах та в базі даних наявні облікові записи з паролями, однак в робочому процесі, один співробітник може попросити іншого виконати певну дію зі свого робочого місця з автентифікованим записом першого користувача.

КА-2 – Базова адміністративна конфіденційність – не реалізована. Зміна доступу до об'єктів відбувається не за запитом адміністратора.

КО-1 – Повторне використання об'єктів – не реалізована. Оперативна пам'ять комп'ютера не очищується.

КВ-2 –Базова конфіденційність при обміні – реалізована. Обмін інформацією відбувається за допомогою захищених протоколів HTTPS та SSL.

ЦД-1 – Мінімальна довірча цілісність – реалізована. На ПК та у базі даних CarBook є розмежування доступу до ІзОД між різними користувачами з різними обліковими записами, унікальними паролями та різним рівнем доступу

ЦО-1 – Обмежений відкат –реалізована. В системі та використовуваних додатках є можливість відновлення змін у файлах, що містять ІзОД.

ЦВ-1 – Мінімальна цілісність при обміні – реалізована. Обмін інформацією здійснюється за допомогою захищених інтернет протоколів HTTPS та SSL

ДР-1 – Квоти – реалізована. На сервері бази даних CarBook під кожний запис клієнта виділяється 100 МБ дискового простору. На робочих станціях встановлено ліміт по можливому використанню ресурсів жорсткого диску користувачем.

ДВ-1 – Ручне відмовлення – реалізована. В ОС Windows є можливість відновити роботу системи вручну.

НР-2 – Захищений журнал – частково реалізована. В ОС Windows є можливість вести журнал подій та обмежити доступ до нього, однак ця функція не використовується.

НИ-2 – Одиночна ідентифікація і автентифікація – частково реалізована. Під час запуску ОС Windows відбувається ідентифікація та автентифікація за допомогою логіну та паролю, однак немає чітко описаної політики паролів.

НК-1 – Однонаправлений достовірний канал – реалізована. Під час запуску ОС Windows відбувається ідентифікація та автентифікація за допомогою логіну та паролю, що вводиться користувачем з клавіатури. На кришці корпусу наявні наліпки (пломби), що контролюють цілісність корпусу ПК.

НО-2 - Розподіл обов'язків адміністраторів – частково реалізована. В системі є обліковий запис адміністратора, однак неможливо розділити обов'язки та права системного адміністратора та адміністратора безпеки

НЦ-2 – КЗЗ з гарантованою цілісністю – реалізована. Система перевіряє цілісність під час ініціалізації системи.

НВ-1 – Автентифікація вузла – реалізована. З'єднання з інтернетом відбувається через вебпереглядач Google Chrome за захищеним протоколом HTTPS.

В результаті аналізу КС було виявлено:

- послуги, що реалізовано:, КВ-2, ЦД-1, ЦО-1, ДР-1, ЦВ-1ДВ-1, НК-1, НЦ-2, НВ-1;
- послуги, що реалізовано частково: КД-2, НР-2, НО-2, НИ-2;
- послуги, що не реалізовано: КА-2, КО-1.

Витік інформації технічними каналами витоку інформації(Акустичний, віброакустичний, акустоелектричний, оптико-електронний та параметричні канали витоку інформації) в цій роботі не розглядається через відсутність акустичної інформації на ОІД, та недоцільність її перехвату порушниками через співвідношення отриманої вигоди та витрачених засобів.

2.2 Організаційні заходи

Відповідно до НД ТЗІ 1.1-003-99, Комплексна система захисту інформації; КСЗІ – сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС [5]. Для забезпечення належного рівня захисту інформації та впровадження на підприємстві КСЗІ, треба вжити відповідно організаційних та інженерно-технічних заходів. Далі буде запропоновано заходи, що мають забезпечити стан безпеки для інформаційних ресурсів підприємства.

2.2.1 Розробка елементів політики безпеки

Основними організаційними заходами по забезпеченню належного рівня захисту інформації є різноманітні політики безпеки. Оскільки в ОІД є велика кількість користувачів обчислювальної техніки, що не мають високого рівня володіння цією технікою, потрібно прописувати політики безпеки таким чином, щоб користувачі навіть з низьким рівнем освіченості змогли зрозуміти зміст політики та виконували його. Це підвисить загальний рівень безпеки, бо зведе до мінімуму фактор виникнення помилок внаслідок необережності та необдуманості дій. Далі представлено приклади політик безпеки, які доречно впровадити на даному ОІД.

Політика безпеки щодо захисту ПК від вірусів

Дана політика безпеки розроблена задля забезпечення захисту інформації в ІКС підприємства і стосується усіх співробітників компанії.

На всіх ПК повинне буде встановлене антивірусне програмне забезпечення. У випадку сумнівів щодо коректної роботи антивірусного ПЗ, звертайтеся до системного адміністратора. Працівники мають перевіряти наявність оновлень антивірусного ПЗ та завантажувати і встановлювати їх у разі наявності. Системний адміністратор має виконувати раз на тиждень сканування ПК співробітників та перевіряти їх коректну роботу.

Забороняється спілкування з третіми персонами у робочий час та надання їм персональної інформації або інформації про підприємство. Категорично забороняється відкривати підозрілі електроні листи з незнайомих адрес, переходити по підозрілим та/або невідомим посиланням.

Рекомендується переглядати лише сайти з безпечним з'єднанням. Категорично забороняється завантажування будь яких файлів, програм, тощо. Якщо завантаження файлів є критичним для ведення професійної діяльності, перед завантаженням потрібно повідомити про це системного адміністратора.

Забороняється використання зовнішніх носіїв інформації, окрім тих, що знаходяться на обліку підприємства. За можливості, рекомендується виконувати задачі без залучення зовнішніх носіїв інформації.

Положення про використання всесвітньої мережі Інтернет

Мета: Підвищення рівня інформаційної безпеки за допомогою освіти користувачів комп'ютерної системи та за допомогою впровадження низки правил, що їх повинні дотримуватись співробітників.

Область застосування: Це положення поширюється на всіх співробітників, підрядників та інших осіб, які мають доступ до мережі Інтернет через офісну інфраструктуру компанії.

Положення: використання мережі інтернет дозволяється співробітникам для безпосереднього виконання службових зобов'язань, або для пошуку відомостей, статей, тощо, потрібних для підтримання робочого процесу. Використання інтернету для власних цілей співробітників, для спілкування з третіми особами (якщо це не входить в обов'язки співробітника) забороняється. Виключенням є використання мережі для спілкування, освіти, прослуховування музики на легальних сервісах у час перерви.

Відповідальність: за порушення пунктів даного положення, до співробітників буде застосоване дисциплінарне покарання: позбавлення премії, штраф, пониження в посаді, звільнення. Суворість покарання розглядається керівництвом підприємства в залежності від важкості порушення та збитків, до яких воно привело.

Відповідальним за впровадження та донесення пунктів положення до працівників призначається системний адміністратор.

Положення про резервне копіювання

Мета: Підвищення рівня відмовостійкості інформаційної системи підприємства за допомогою впровадження. Введення правил поводження та порядку дій в ситуації

Область дії: Положення поширюється на всіх працівників інформаційно-комунікаційної системи підприємства. Положення стосується інформації про клієнтів та фінансових звітностей.

Відповідальні особи: Системний адміністратор.

Положення:

- впровадження механізму резервного копіювання найважливішої інформації;
- встановлення відповідального за виконання резервного копіювання;
- встановлення найважливіших видів інформації, що підлягають резервному копіюванню;
- встановлення порядку дій по відновленню інформації в випадку її руйнування;
- донесення пунктів положення до співробітників та вимагання дотримання пунктів положення;

Відповідальність: за порушення пунктів даного положення, до співробітників буде застосоване дисциплінарне покарання: позбавлення премії, штраф, пониження в посаді, звільнення. Суворість покарання розглядається керівництвом підприємства в залежності від важкості порушення та збитків, до яких воно привело.

Політика паролів

Політика паролів використовується для підвищення стійкості до підбору паролів. Вона визначається такими параметрами конфігурації:

- кількість неповторюваних паролів;
- максимальний термін дії пароля;
- мінімальна довжина пароля;
- паролі повинні задовольняти вимогам щодо складності.

Параметр кількість неповторюваних паролів обмежує можливість користувачів використовувати старі паролі під час зміни пароля.

Параметр максимальний термін дії пароля визначає термін, після закінчення якого система змушує користувача змінити пароль.

Параметр мінімальна довжина пароля не дозволяє використовувати занадто короткі паролі.

Параметр паролі повинні задовольняти вимогам щодо складності змушує користувача використовувати досить складні паролі.

Складність пароля означає виконання таких вимог:

- пароль не повинен містити в собі ім’я або повне ім’я користувача;
- пароль має містити символи хоча б із трьох наборів із наведених чотирьох:
  - прописні літери латинського, російського та українського алфавітів;
  - строкові літери латинського, російського та українського алфавітів;
  - цифри;
  - спеціальні символи: ~ ` ! @ # $ % ^ & * ( ) _ - + = | \ { }. [6]

2.2.2 Обґрунтування реалізації умов послуг безпеки

КД-2 – Мінімальна довірча конфіденційність

Для реалізації цієї послуги потрібно заборонити працівникам виконувати роботу поза своїми РС. Для цього потрібно прописати політику користування обліковими записами. Далі буде запропоновано варіант такої політики.

Політика користування робочими комп’ютерами

Дана політика створена для підвищення рівня захищеності інформації з обмеженим доступом від несанкціонованого доступу.

Кожен користувач інформаційної системи підприємства має мати свій персональний обліковий запис на робочій станції, за якою він закріплений. Користувач має входити до свого облікового запису під час початку роботи та виходити після закінчення роботи. Якщо доводиться залишити своє робоче місце без нагляду, потрібно зберегти зміни і вийти з облікового запису. Забороняється давати користуватись своїм робочим місцем з автетифікованим обліковим записом іншим робітникам.

КА-2 – Базова адміністративна конфіденційність

Головним заходом має бути наймання системного адміністратора на постійну роботу, а не запрошення його по факту виникнення питання стосовно

системи. Йому не обов'язково знаходитись на об'єкті постійно, досить щотижневих візитів для перевірки та підтримання системи у надійному стані.

Для долучення постійного системного адміністратора є декілька причин:

- більша вмотивованість;
- глибше знання та розуміння особливостей конкретної ІКС;
- гарантії виконання роботи за допомогою трудового контракту.

Оскільки на даний момент, системний адміністратор залучається лише за умови виникнення проблем у системі та запиту на отримання його послуг від керівництва, він не може в повній степені забезпечити належний стан захисту інформації та безперебійної роботи системи. Наприклад, у випадку інциденту у роботі інформаційної системи підприємство зробить запит допомоги до спеціаліста, а він може відмовити за власних причин. Це може зупинити роботу підприємства на значний сирок.

У випадку наймання адміністратора на офіційному рівні, буде укладено трудовий договір, в якому будуть чітко прописані умови роботи та вимоги від спеціаліста. Це дозволить отримати безвідказну допомогу у випадку виникнення проблем в інформаційній системі. Також, у ході регулярного відвідування об'єкту та ознайомлення з роботою даної системи, адміністратор здобуде більш повне розуміння специфіки наявного обладнання та програмного забезпечення, фізичного влаштування системи, тощо. Також, регулярна перевірка комп'ютерного обладнання підвищить надійність системи, зробить можливим своєчасне усунення проблем у роботі системи.

Наймання системного адміністратора на повну ставку не є доречним, тому що ІКС досліджуваного об'єкту інформаційної діяльності не є досить розгалуженою, не потребує постійного спостерігання. Вихід з ладу більшості компонентів не є безповоротнім. Наймання такого адміністратор буде дорожчим для підприємства і не дасть суттєвих переваг перед варіантом з щотижневим відвідуванням адміністратором офісу.

КО-1 – Повторне використання об'єктів

Для автоматизованого очищення пам'яті від процесу, що використовував ІзОД, можна використати вбудований функціонал Windows 10 Pro, а саме утиліту «Планувальник задач» та програму "Mem Reduct".

НР-2 – Захищений журнал

Для реалізації цієї послуги можна скористатись вбудованим функціоналом ОС Windows 10 Pro. Відповідальним за ведення журналу буде адміністратор з безпеки.

НИ-2 – Одиночна ідентифікація і автентифікація

Щоб повністю реалізувати цю вимогу послуги безпеки, потрібно створити політику використання паролів. Така політика описана в пункті 2.2.1.

Про специфіку його роботи буде викладено в реалізації послуги НО-2.

НО-2 - Розподіл обов'язків адміністраторів

Системний адміністратор на даний момент при підключені має повні права на всі види інформації. Якщо прийняти на роботу адміністратора і залишити такими самими його права, то він фактично отримає повний контроль над системою та інформацією

Для цього потрібно виконати вимоги функції НО-2 та розділити обов'язки системного адміністратора та адміністратора з безпеки. Найбільш надійним рішенням було б залучення окремого працівника, що є кваліфікованим спеціалістом в сфері інформаційної безпеки, однак через специфіку підприємства, таке рішення буде занадто витратним і не дасть суттєвого результату.

Для зменшення витрат на окремого працівника, що буде виконувати ці функції, можна надати ці права вже наявному працівнику, що є надійним з точки зору керівництва та має хоча б середній рівень кваліфікації в роботі з комп'ютером. Найбільш очевидною кандидатурою є логіст. В нього середній рівень володіння комп'ютером і він не надто навантажений іншими робочими обов'язками.

Після наймання на роботу адміністратора з безпеки, повноваження системного адміністратора будуть дещо урізані:

- системний адміністратор має інсталювати та видаляти ПЗ лише під наглядом адміністратора з безпеки;
- внесення змін в журнал безпеки має відбуватись лише адміністратором з безпеки;
- впровадження та слідкування за дотриманням політики паролів знаходиться під юрисдикцією адміністратора з безпеки.

В обов'язки адміністратора безпеки входить:

- ведення журналу подій;
- впровадження та дотримання політики паролів;
- дотримання інших політик та положень, що стосуються інформаційної безпеки підприємства.

Через зміни в середовищі користувачів, а саме наймання двох адміністраторів, потрібно впровадити зміни в розмежування доступу до інформації.

Таблиця 2.1 – Матриця розмежування доступу

Посада	1	2	3	4	5	6	7	8*
Керівник	Д З Р С Ч	Д З Р С Ч	В Д З Р С Ч	В Д З Р С Ч	В Д З Р С Ч	В Д З Р С Ч	В Д З Р С Ч	-
Старший механік	-	-	-	-	В Д Р С Ч	-	Д З Ч	-
Менеджер	З Р С Ч	Д Ч	В Д З Р С Ч	В Д З Р С Ч	Д Ч	Ч	Д З Ч	-
Логіст**	-	-	Ч С Р	В Д З Р С Ч	-	-	З Ч	-

Продовження таблиці 2.1

Посада	1	2	3	4	5	6	7	8*
Бухгалтер	-	В Д З Р С Ч	-	-	-	-	З Ч	-
Системний адміністратор	-	-	-	-	-	В Д З Р С Ч	З Ч	-
Адміністратор з безпеки	-	-	-	-	-	-	З Ч	В Д З Р С Ч

* - Тип інформації 8 – журнал подій безпеки.

** - Логіст виконує обов’язки адміністратора з безпеки.

Умовні позначення атрибутів розмежування доступу.

- В – видалення
- Д – друк
- З – зберігання
- Р – редагування
- С – створення
- Ч – читання

НР-2 – Захищений журнал

Хоча в ОС Windows допускається можливість вести журнал подій та захистити його від несанкціонованого доступу, однак немає чітких правил щодо того, які саме події потрібно заносити в журнал, а які ні. За основу для списку подій обов'язкових до реєстрації обрано список з 11 пункту Постанови Кабінету Міністрів України від 29 березня 2006 «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах» [8] та додано додаткові події.

- факти входу/виходу або спроби входу/виходу в/з ОС користувачів будь-яких категорій;
- факти реєстрації/видалення або спроби реєстрації/видалення облікових записів користувачів будь-яких категорій;
- факти зміни даних автентифікації користувачів будь-яких категорій;
- факти присвоєння/зміни прав доступу користувачів до захищених ресурсів;
- факти порушення встановлених прав доступу користувачів;
- факти отримання або спроби отримання користувачем будь-якої категорії доступу до будь-якого ПЗ, що використовуються для обробки захищених інформаційних об'єктів;
- факти отримання доступу та виконання певних дій або спроби отримання користувачем будь-якої категорії доступу до будь-яких захищених інформаційних об'єктів;
- факти порушення прав доступу користувачів до захищених ресурсів;
- факти перезавантаження, вимкнення ПК та виникнення інших системних подій;
- Події, пов'язані зі спостереженням за процесами (запуск, завершення).

Усі ці події можливо фіксувати за допомогою журналу подій, вбудованому в ОС Windows.

2.3 Організація системного адміністрування

На робочих комп'ютерах встановлено ПЗ для віддаленого доступу "TeamViewer" та "AnyDesk". Воно використовується для надання послуг системного адміністратора віддалено. Для того, щоб системний адміністратор міг надавати послуги віддалено, кожен з користувачів має бути наявний обліковий запис адміністратора для внесення змін в систему. Таке розмежування доступу не надає належного рівню захищеності інформації і є загрозою для безпеки.

Заради підвищення рівня захищеності інформації, що циркулює в ІКС підприємства, пропонується використовувати додаток від компанії Microsoft під назвою System Center Configuration Manager. Це комплексне ПЗ для автоматизації процесів на пристроях, що використовують ОС Windows.

Для вирішення задачі по віддаленому адмініструванні потрібно інсталювати ПЗ на всі комп'ютери ІКС, змінити налаштування клієнту та після цього змінити, налаштування у секції Remote Tools, що безпосередньо відповідають за правилам віддаленого підключення. Можна використати налаштування за замовчуванням, як на рис 2.1.

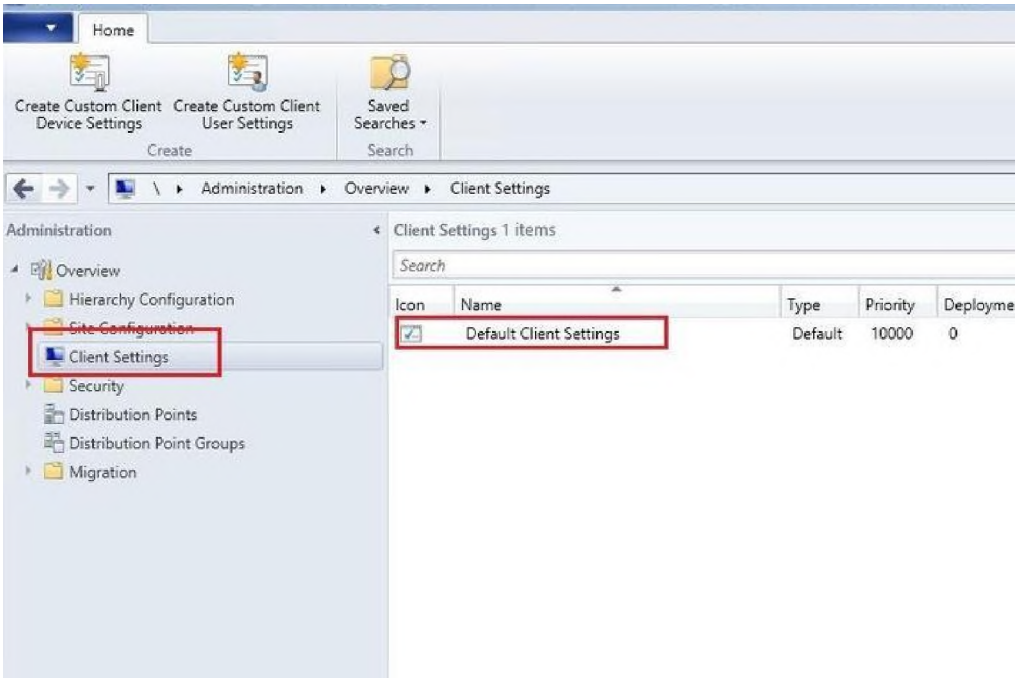

Рисунок 2.1 – стандартні налаштування підключення

Рекомендується підключатись у режимі Remote Assistance, а не Remote Control, так як в такому режимі адміністратор не має можливості керувати комп'ютером, а лише отримує трансляцію робочого стола користувача. Оскільки користувачі системи володіють комп'ютером на середньому або вище рівнях, для них не буде складною задачею виконувати вказівки адміністратора. А при роботі в режимі Remote Control адміністратор має доступ до інструментів управління комп'ютером і має можливість таким чином перевищити свої повноваження. До того ж, у цьому режимі є можливість підключитись до

системи без повідомлення та навіть у час просто ПК, що створює велику загрозу для інформації.

2.4 Реалізація резервного копіювання

Хоча й специфіка підприємства та організації інформаційного середовища є такою, що основна частина інформаційних ресурсів зберігається на віддаленому сервері сервісу CarBook, однак є можливою така ситуація, що за певних обставин дані можуть бути видалені звідти. Також варто пам'ятати що деяка частина даних все ще зберігається локально на носіях інформації комп'ютерів.

Для запобігання втрати даних, доречним є впровадження системи для резервного копіювання даних. Серед найбільш очевидних рішень є придбання RAID масиву або придбання підписки на хмарний сервіс для зберігання даних. Далі буде проаналізовано вигоду конкретних рішень та вибір найбільш актуального для даного об'єкту.

Серед переваг рішення придбання RAID масиву можна одразу виділити

- швидкість роботи;
- швидке відновлення даних;
- високу надійність та відмовостійкість;
- відсутність потреби в постійному вкладанню грошей.

Недоліками системи RAID є:

- висока вартість придбання NAS приводу та потреби придбання жорстких дисків;
- складність в організації системи;
- потреба в висококваліфікованому спеціалісту для підтримання роботи системи;
- підвищення затрат електроенергії;
- вразливість до фізичного знищення.

Перевагами хмарного резервного копіювання є:

- можливість виконати відновлення даних на будь який пристрій;

- відсутність загрози фізичного руйнування носіїв інформації та відповідно даних;
- простота у користуванні;
- теоретично необмежений дисковий простір;
- висока надійність зберігання даних в безпеці;
- відсутність великих стартових витрат.

Недоліками хмарного резервного копіювання даних є:

- потреба в стабільному інтернет-підключенні для копіювання та відновлення даних;
- довше відновлення;
- повільніша робота;
- передача даних у «треті руки»;
- високі витрат у довгостроковій перспективі;

Ураховуючи усі переваги та недоліки кожного з варіантів реалізації резервного копіювання, прийнято рішення у придбані підписки на хмарний сервіс. Головними чинниками, що вплинули на це рішення є те, що на підприємстві відсутні кваліфіковані для роботи з технологією RAID працівники, а постійне замовлення спеціалістів для встановлення та обслуговування системи стають фактично постійною оплатою функціонування системи. Також варто розуміти, що через режим роботи СТО, коли відвідувачі підприємства мають доступ до приміщення, в якому знаходиться обладнання ІКС, ризики для фізичної цілісності RAID масиву та відповідно даних, що в ньому зберігаються, стають більшими.

В той же час, переваги цієї системи не є настільки значущими для конкретного об’єкту. Дані, що підлягають резервному копіюванню не є такими, що постійно циркулюють в системі, тому швидкість роботи не є вирішальним фактором.

Хмарне сховище ж представляє більше переваг через те, що щомісячне списання не є значущою сумою в рамках інших щомісячних витрат підприємства і керівництво готово піти на більшу суму витрат в довгостроковій перспективі

Також, хмарні сервіси є досить надійним ресурсом, який більше підходить для зберігання архівних даних. Вірогідність втрати даних на фізичних носіях є відносно низькою, тому низька швидкість відновлення даних не є проблемою, з якою доведеться стикатися постійно. Відсутність фізичного обладнання для зберігання даних підвищує їх безпеку і відвідування клієнтами підприємства офісу не є загрозою для цілісності даних.

Однак для підтримання резервації даних на хмарний сервіс, потрібно мати стабільне Інтернет-підключення, про що буде написано в пункті 2.5.

На ринку хмарних сховищ є досить багато різних рішень, в тому числі для потреб бізнесу. В таблиці 2.2 розглянуто найпопулярніші рішення.

Таблиця 2.2 – Сервіси хмарного сховища

№	Назва сервісу	Ціна місячної плати для бізнесу за користувача	Об'єм пам'яті на кожного користувача
1	Google Drive	Від 6$	30 ГБ
2	Microsoft OneDrive	Від 5$	1 ТБ
3	DropBox	Від 12.50$	3 ТБ
4	IDrive	Від 74.50$*	5 ТБ
5	Box	Від 5$	100 ГБ**

* – варіант оплати лише на рік.

** – об'єм пам'яті на трьох користувачів.

Google Drive є досить зручним у користуванні, підтримує інструменти Microsoft Office, має зручну інтеграцію різних пристроїв та зручність при обміні та одним з найдешевших варіантів. Однак, це рішення має великі недоліки, що роблять цей варіант не найкращим вибором. Наприклад, об'єм пам'яті на кожного користувача є найменшим серед усіх рішень. Також великі питання визиває надійність та захищеність даних. Також, є досить критичний ліміт на розмір файлів, а саме 50 МБ для файлів та 20 МБ для таблиць.

Microsoft OneDrive має найнижчий тариф на користувача серед усіх запропонованих рішень. Варто відмітити високу захищеність даних, підтримку багатофакторної автентифікації, вбудований захист від програм-вимагачів. Однак у цього рішення маються недоліки у вигляді неможливості виділити окремі папки для синхронізації та залежність від додатків екосистеми Microsoft. Також, OneDrive має відносну невелику пропускну швидкість під час синхронізації даних.

DropBox є одним за найперших сервісів, що почали надавати послуги хмарного зберігання даних для широкого кола користувачів. В першу чергу варто відзначити найбільшу вартість тарифу серед конкурентів, однак сервіс надає мабуть найбільшу кількість функцій та можливостей, таких як:

- просте налаштування синхронізації;
- можливість копіювати обрані файли та папки;
- можливість перегляду файлів без завантаження;
- захищеність даних;
- інтеграція з великою кількістю додатків.

IDrive надає найбільший дисковий простір серед усіх конкурентів і має найвигідніше відношення ГБ/$. Однак, в сервісі відсутня можливість оплачувати підписку щомісячно і вимагається оплата відразу на рік вперед. Також, маються доволі суворі обмеження на зберігання файлів.

Перевагами сервісу Box є інтеграція з додатками пакету Office, інтеграція з багатьма додатками, можливість сумісної роботи над файлами, контроль версій. Також, дані шифруються закритим ключем і наявна можливість підключення багатофакторної автентифікації. Однак недоліки, такі як обмеження на розмір та імена файлів і один з найменших об'ємів пам'яті на користувача, переважують переваги [6].

Проаналізувавши приведені вище переваги та недоліки різних сервісів, обрано сервіс DropBox, як одне з найбільших імен у сфері хмарних сховищ, яке зароблено роками надання надійних послуг. Переваги у вигляді можливості резервного копіювання окремих файлів та папок є значним аргументом у

порівняні з другим найкращим рішенням у вигляді сервісу OneDrive. Також, об'єм наданої пам'яті є одним з найбільших.

2.5 Організація резервування каналу Інтернет

Оскільки резервне копіювання даних буде відбуватись на сервіс хмарного сховища, потрібно подбати про резервну лінію підключення послуг Інтернету у випадку виходу з ладу ліній підключення основного провайдеру, збої у роботі провайдеру, тощо.

На адрес підприємства є можливість провести резервну лінію від одного провайдера – «Фрегат». Вартість підключення є 1000 грн за тарифом для приватного сектора та щомісячна плата 30 грн/місяць. Значною перевагою є проведення ліній за технологією PON, що зробить наявність підключення до Інтернету незалежним від наявності електроенергії в місці дислокації розподільного обладнання провайдеру.

Для виконання перемикання на резервну лінію Інтернет-підключення, можна використати MultiWAN маршрутизатор, або перемикати вручну.

Так як головним ресурсом, що використовує Інтернет трафік є база даних CarBook, а вона зберігає усі зміни в реальному часі, в миттєвому перемиканні ліній Інтернету немає потреби. До того ж, маршрутизатори з двома або більше WAN-портами є досить складним обладнанням, що його потребують складні комп'ютерні системи. Тому, окрім наявності декількох WAN-портів, пристрій навантажений багатьма функціями, які не є обов'язковими на даному об'єкті і не дадуть суттєвого приросту ефективності виробництва.

Через вище описані фактори, такі маршрутизатори є надто коштовним обладнанням. Саме тому керівництвом прийнято рішення, що перемикання лінії Інтернету буде відбуватись вручну. Відповідальним за перемикання назначений менеджер, так як він завжди знаходиться поруч з обладнанням і може відновити підключення в найменші терміни.

2.6 Забезпечення безперебійного живлення

Щоб захистити комп'ютери від перепадів напруги, що є досить вірогідною подією в скрутний час для енергетики країни, вирішено придбати джерело безперебійного живлення для стаціонарних комп'ютерів, що використовуються на підприємстві.

В таблиці 2.3 наведено найпопулярніші моделі ДБЖ в онлайн маркеті.

Таблиця 2.3 – Перелік варіантів ДБЖ для закупівлі

№	Модель	Потужність	Час автономної роботи при піковій потужності	Вартість
1	Powercom BNT-1000AP Schuko USB	1000 ВА / 600 Вт	10-20 хвилин	7485 грн
2	Powercom RPT-1000A Schuko	1000 ВА / 600 Вт	12 хвилин	3744 грн
3	Powercom IMD-825AP LCD Schuko	495 Вт	10 хвилин	5823 грн

В наявності є три комп'ютери з блоками живлення на 150 Вт. Час, потрібний для завершення роботи з документами в разі перепаду напруги – 10 хвилин.

Як видно з таблиці 2.3, третій варіант надає потужність лише на 45 Вт вище споживаною. До того ж, серед трьох роз'ємів лише два мають можливості заструмлення від батареї.

Другий варіант виглядає найбільш вигідним зі сторони вартості товару та відповідності потребам, однак це ДБЖ має погані відгуки користувачів, що пишуть про погану якість виготовлення. Також наявна велика кількість відгуків про заводський брак.

Таким чином, обрано перший варіант, що є найдорожчим, однак він вигідно виділяється серед представлених на ринку пропозицій своє якістю.

Для реалізації безпечного збереження даних та вимкнення комп'ютерів потрібно під'єднати ДБП до одного з комп'ютерів та налаштувати утиліту на безпечний вихід в разі перепаду напруги.

Існує багато додатків по роботі з UPS. Далі розглянуто такі рішення, як NUT, та UPSmon.

Таблиця 2.4 – Порівняння додатків для налаштування UPS

Характеристика	NUT	APC PoweChute	UPSmon
Підтримка ДБЖ від різних виробників	Широкий спектр ДБЖ від різних виробників	ДБЖ від виробника APC	Широкий спектр ДБЖ від різних виробників
ОС	Linux, FreeBSD, macOS, Windows	Linux, Windows	Linux, Windows
Інтерфейс	Файли конфігурацій	Файли конфігурацій	Файли конфігурацій, графічний
Тип моніторингу	Мережевий	Мережевий	Локальний та мережевий
Вартість	Безкоштовно	Безкоштовно*	Безкоштовно

* - розповсюджується безкоштовно разом з обладнанням виробника APC

Оскільки обрано обладнання від компанії Powercom, додаток APC PowerChute не підходить через несумісність з ДБЖ іншого виробника.

Додаток NUT має більшу гнучкість налаштування, однак не має графічного інтерфейсу, що ускладнює роботу з ДБЖ. До того ж, відсутня можливість локального моніторингу.

У свою чергу, додаток UPSmon є продуктом безпосередньо виробника обраного ДБЖ, що гарантує найбільшу сумісність ПЗ та обладнання. Має всі ті ж функції, що і NUT, і окрім цього має графічний інтерфейс, що дозволяє швидко і зручно налаштувати ДБЖ. Також, присутня можливість локального моніторингу, що дозволяє отримувати інформацію про стан роботи ДБЖ у найшвидші терміни та з великою надійністю.

2.7 Висновок

Проаналізувавши реалізацію вимог послуг безпеки, що відповідають обраному профілю захищеності 3.КЦД 2, визначено, що велика кількість послуг реалізуються лише частково або не реалізується взагалі. Проведена робота дозволила виявити такі послуги та розробити план дій по їх реалізації.

Порівнюючи рівень захищеності інформації в ІКС до та після впровадження запропонованих рішень, стає наочним результат проведеної роботи по покращенню захисту інформації.

Такі загрози для безпеки, що мають декілька шляхів для вирішення були проаналізовані, були висунуті рішення для зменшення або ліквідації цих загроз. В ситуаціях, де можливо обрати один з декількох варіантів для вирішення проблеми, рішення були оцінені та вибрані оптимальні, такі як наймання системного адміністратора, резервування лінії Інтернет-підключення та придбання джерела безперебійного електроживлення.

РОЗДІЛ ІІІ. ЕКОНОМІЧНИЙ РОЗДІЛ

Метою впровадження КСЗІ на підприємстві є підвищення рівню захищеності інформації, щоб понизити вірогідність реалізації загроз та, як наслідок, не допустити втрати матеріальних або інформаційних активів.

Однак, окрім ліквідації або зменшення вірогідності реалізації загроз інформаційної безпеки, для підприємства важлива фінансові витрати на роботу. Для ефективності вжитих заходів, витрати на розробку КСЗІ та впровадженню рішень для її реалізації мають бути меншими за потенційні втрати, якщо загрози реалізуються.

В економічному розділі кваліфікаційної роботи буде підраховано вартість створення КСЗІ, витрати на заробітну платню спеціалісту, вартість впровадження рішень по посиленню захищеності інформації на підприємстві, та проаналізовано відношення витрат на розробку до збитків у випадку реалізації загроз.

3.1 Визначення витрат на розробку КСЗІ

Трудомісткість розробки політики безпеки інформації визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного спеціаліста з інформаційної безпеки) [10]. Трудомісткість розробки визначено за формулою 3.1.

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

де $t_{тз}$ – тривалість складання технічного завдання на розробку політики безпеки інформації;

$t_{в}$ – загальна трудомісткість розробки елементів політики безпеки. tв - тривалість розробки концепції безпеки інформації у організації; ta - тривалість процесу аналізу ризиків;

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

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

інформації;

$t_{овр}$ – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації;

$t_д$– тривалість документального оформлення політики безпеки.

Таким чином, трудомісткість розробки КСЗІ становить:

$$54 + 18 + 40 + 24 + 64 + 150 = 350 \text{ год}$$

Витрати на впровадження КСЗІ можна описати, як суму проєктних рішень та заробітної платні спеціаліста з інформаційної безпеки:

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

де $К_{рп}$ – це витрати на формування проєктних рішень;

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

$З_{мч}$ – вартість витрат машинного часу, що необхідні для формування проєктних рішень.

Заробітну платню фахівця можна розрахувати за допомогою множенню погодинної оплати праці на трудомісткість праці.

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

де t - загальна тривалість розробки політики безпеки, годин;

Зіб – середньо годинна заробітна плата фахівця з інформаційної безпеки з нарахуваннями, грн/годину.

Середню оплату праці фахівця можна оцінити в 75 грн/год. Підставивши тривалість розробки політики безпеки та погодинну оплату праці в формулу 3.3 можна отримати заробітну плату працівника:

$$З_{зп} = 350 \text{ год} * 75 \text{ грн/год} = 26250 \text{ грн}$$

$$З_{зп} = 26250 \text{ грн}$$

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

$$C_{мч} = P * t_{нал} * C_e + \frac{Ф_{зал} * Н_a}{F_p} + \frac{K_{лпз} * Н_{апз}}{F_P}, \quad \text{грн}, \tag{3.4}$$

де P – встановлена потужність ПК, кВт;

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

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

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

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

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

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

Залишкова вартість ПК визначається на основі фактичного терміном його експлуатації як різниця між початковою вартістю та зносом під час користування пристроєм.

P = 0, 065 кВт;

Се = 4,32 грн/кВт год;

Ліцензійне програмне забезпечення:

- Windows 11 Pro – 7899 грн;
- Microsoft Office 365 2021 – 3899 грн;

Загалом: 7899 грн + 3899 грн = 11798 грн

Вартість ПК = 25000 грн;

Мінімальний строк корисної служби = 24 місяці;

Накопичена амортизація = $\frac{25000}{24} \times 12 = 12500$ *грн*

Залишкова вартість: $25000 - 12500 = 12500$ грн.

Річна норма амортизації на ПК = 0,5

Річна норма амортизації на ліцензійне програмне забезпечення = 0,5

$$C_{\text{мч}} = 0{,}06 * 2 * 4{,}32 + \frac{12500 * 0{,}5}{1920} + \frac{11798 * 0{,}5}{1920} = 0{,}52 + 3{,}25 + 3{,}1 = 6{,}87 \text{ грн}$$

Підставляючи отримане значення в формулу 3.4 отримано вартість машинного часу для розробки КСЗІ.

$$З_{\text{мч}} = 350 * 6{,}87 = 2404 \text{ грн}$$

Таким чином, загальні витрати на розробку КСЗІ складають:

$$К_{\text{рп}} = 26250 + 2404 = 28654 \text{ грн}$$

Капітальні витрати на розробку та впровадження КСЗІ можна порахувати за формулою 3.5.

$$К = К_{\text{рп}} + К_{\text{аз}}, \text{ грн,} \qquad (3.5)$$

де $К_{рп}$ – вартість розробки КСЗІ, тис. грн.;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та додаткового обладнання, тис. грн.

Для впровадження КСЗІ потрібно зробити такі одноразові трати, як:

- Джерело безперебійного живлення Powercom BNT-1000AP Schuko USB - 7485 грн;
- Проведення резервної лінії Інтернет підключення – 1000 грн.

Сумарні витрати:

$$К_{аз} = 7485 + 1000 = 8485 \text{ грн}$$

Підставивши у формулу 3.5 значення, підраховано повні капітальні витрати на розробку та впровадження КСЗІ:

$$К = 28654 + 8485 = 37139 \text{ грн}$$

3.2 Розрахунок експлуатаційних витрат

Експлуатаційній витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проєктування за визначений період (тиждень, місяць, рік тощо), що виражені у грошовому вигляді [10].

Підрахувати експлуатаційні витрати можна за формулою 3.6.

$$С = С_а + С_з + С_е + С_{єв} + С_і \text{ , грн,} \quad (3.6)$$

де $С_а$ – річний фонд амортизаційних відрахувань;

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

$С_е$ – вартість електроенергії, що споживається апаратурою;

$С_і$ – вартість оплати інтернет послуг;

Річний фонд амортизаційних відрахувань можна обчислити за формулою

3.7.

$$С_а = Са = Ф_п/Т \ , \ \text{грн}, \qquad (3.7)$$

де *Фп* – первісна вартість придбаного обладнання;

Т – мінімальний термін корисного використання (дорівнює 5 років для апаратного забезпечення).

$$С_а = \frac{7485}{5} = 1697 \text{ грн}$$

Річний фонд заробітної плати інженерно-технічного персоналу можна обчислити за формулою 3.8.

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

де $З_{осн}$– основна заробітна плата, що визначається, виходячи з місячного посадового окладу;

$З_{дод}$– додаткова заробітна плата, що визначається в розмірі 8-10% від основної заробітної плати.

Фонд оплати праці потрібно розділити на 2 співробітників – найманого системного адміністратора, що буде один раз на тиждень відвідувати об’єкт та на збільшення оплати праці для логіста, до обов’язків якого додається виконання функції адміністратора з безпеки.

$$З_{осн} = З_{осн\,1} + З_{осн\,2} = 10000 + 3000 = 13000 \text{ грн}$$
$$З_{дод} = З_{дод\,1} + З_{дод\,2} = 900 + 270 = 1170 \text{ грн}$$

Таким чином, підставивши значення в формулу 3.8 та помноживши

результат на 12 місяців, можна отримати річний фонд оплати праці:

$$С_з = (З_{осн} + З_{дод}) \times 12 = 14170 \times 12 = 170040 \text{ грн}$$

Розмір єдиного внеску на загальнообов'язкове державне соціальне страхування визначається на підставі встановленого чинним законодавством відсотка від суми основної та додаткової заробітної плати (за узгодженням з керівником економічної частини кваліфікаційної роботи було встановлено 22%).

Звідси:

$$Сєв = 0,22 * Сз = 0,22 * 170040 = 37408 \text{ грн}$$

За формулою 3.9 можна підрахувати обсяг споживаної технічними засобами, впровадженими під час проєктування КСЗІ, електроенергії.

$$С_{ел} = Р * F_р * Ц_е, \text{ грн}, \quad (3.9)$$

де P – встановлена потужність апаратури інформаційної безпеки, кВт (становить 1,2 кВт)

$F_р$– річний фонд робочого часу системи інформаційної безпеки (за 40-годинного робочого дня становить 1920)

$Ц_е$ – тариф на електроенергію, грн/кВт*годин (становить 4, 32 грн/кВт*годин)

Річна вартість електроенергії, що споживається апаратурою, становить:

$$С_{ел} = 1,2 * 1920 * 4,32 = 9953 \text{ грн}$$

Для знаходження вартості утримання резервної лінії інтернету використано формулу 3. 10.

$$C_i = 12 * Ц_i, \quad \text{грн}, \tag{3.10}$$

Де $Ц_i$ – ціна місячної оплати послуг провайдера.

Підставивши тариф інтернету у формулу 3.10, можна отримати річний фонд оплати резервної лінії інтернету:

$$C_i = 12 * 30 = 360 \text{ грн}$$

Підставляючи дані у формулу 3.6, можна підрахувати повний обсяг експлуатаційних витрат.

$$C = 4691 + 170040 + 37408 + 9953 + 360 = 222452 \text{ грн}$$

3.3 Оцінка величини збитку у разі реалізації загрози

Кінцевим результатом впровадження й проведення заходів щодо забезпечення інформаційної безпеки є величина відвернених втрат, що розраховуються, враховуючи ймовірність виникнення інциденту інформаційної безпеки і ймовірних економічних втрат. Ця величина – це та частка прибутку, що може бути втрачена [10].

Для розрахунку збитків від реалізації загроз, можна використати формулу 3.11.

$$U = П_п + П_в + V, \quad \text{грн}, \tag{3.11}$$

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

$П_в$ – вартість відновлення працездатності вузла (заміна

конфігурацій, оновлення та переустановлення ПЗ тощо);

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

Для розрахунку показників $П_п$, $П_в$ та V використано формули 3.12, 3.13 та 3.14 відповідно.

$$П_п = \frac{\sum З_с}{F} * t_п \text{ , грн,} \quad (3.12)$$

де F – місячний фонд робочого часу

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

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

$$П_в = П_{ві} + П_{пв} + П_{зч}, \text{ грн,} \quad (3.13)$$

де $П_{ві}$ – витрати на повторне введення інформації, грн;

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

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

$$П_{ві} = \frac{\sum З_с}{F} * t_{ві} \text{ , грн,} \quad (3.14)$$

де *F* – місячний фонд робочого часу

Зс – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн/місяць

$t_{ві}$ – час повторного введення пошкодженої або загубленої інформації працівниками атакованого вузла або сегмента корпоративної мережі,

годин.

$$П_{пв} = \frac{\sum З_о}{F} * t_в , \quad грн, \tag{3.15}$$

де F – місячний фонд робочого часу

$З_о$ – заробітна плата обслуговуючого персоналу, грн/місяць

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

$$V = \frac{O}{F} * (t_п + t_в + t_{ві}) , \quad грн, \tag{3.16}$$

де F – місячний фонд робочого часу;

O – обсяг продажів атакованого вузла або сегмента корпоративної мережі грн на місяць;

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

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

$t_{ві}$ – час повторного введення пошкодженої або загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин.

В таблиці 3.2 представлені дані для розрахунку значень вище.

Таблиця 3.1 – Вихідні дані для розрахунку збитків від реалізації загроз

Умовні позначення	Величина
$t_п$ (час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин)	6 годин

Продовження таблиці 3.1

$t_в$ (час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин)	10 годин
$t_{ві}$ (час повторного введення пошкодженої або загубленої інформації працівниками атакованого вузла або сегмента корпоративної мережі, годин)	9 годин
$З_о$ (заробітна плата обслуговуючого персоналу, грн на місяць)	36000 грн/місяць
$З_с$ (заробітна плата працівників атакованого вузла або сегмента корпоративної мережі, грн на місяць)	390000 грн/місяць
О (обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн на рік)	5400000 грн
$П_{зч}$ (вартість заміни встаткування або запасних частин, грн)	8000 грн
I (число атакованих вузлів або сегментів корпоративної мережі)	1 шт.
N (середнє число атак на рік)	2 шт.
F (місячний фонд робочого часу)	176 годин
F_r (річний фонд робочого часу)	2080 годин (за 2022 рік)

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

$$П_п = \frac{\sum З_с}{F} * t_п = \frac{39000}{176} * 6 = 13295 \text{ грн}$$

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

$$П_в = П_{ві} + П_{пв} + П_{зч},$$

Де:

$$П_{ві} = \frac{\sum З_с}{F} * t_{ви} = \frac{390000}{176} * 9 = 19943 \text{ грн}$$

$$П_{пв} = \frac{\sum З_о}{F} * t_в = \frac{390000}{176} * 10 = 22159 \text{ грн}$$

Звідси:

$$П_в = 19943 + 22159 + 8000 = 50102 \text{ грн}$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі визначаються, враховуючи середньо годинний обсяг продажів і сумарний час простою атакованого вузла або сегмента корпоративної мережі, і становлять:

$$V = \frac{O}{F} * (t_п + t_в + t_{ві}) = \frac{5400000}{2080} * (6 + 10 + 9) = 64903 \text{ грн}$$

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

$$U = 13295 + 50102 + 64903 = 128300 \text{ грн}$$

Загальний збиток від атаки на вузол або сегмент корпоративної мережі закладу освіти розраховується за формулою 3.17.

$$B=\Sigma_i\Sigma_n U \ , \ \text{грн}, \qquad (3.17)$$

$$B = 1 * 3 * 128300 = 384000 \text{ грн}$$

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

$$E = B * R - C \ , \ \text{грн}, \qquad (3.18)$$

де B– загальний збиток від атаки на вузол корпоративної мережі, грн;

R– очікування ймовірність атаки на вузол або сегмент корпоративної мережі, частки одиниць (55%);

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

Підставивши значення у формулу 3.18 отримано значення:

$$E = 384900 * 0{,}65 - 222452 = 27733 \text{ грн}$$

3.4 Визначення та аналіз показників економічної ефективності запропонованих в проєктних рішень

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

- Сукупна вартість володіння (ТСО);
- Коефіцієнт повернення інвестицій ROSI (Return on Investment for

Security);

- Термін окупності капітальних інвестицій *To*.

Показний сукупної вартості володіння (ТСО) використовується, якщо величину відверненого збитку від атаки на вузол або сегмент корпоративної мережі неможливо прорахувати у вартісній формі. В рамках даної кваліфікаційної роботи значення ТСО не використовується, бо було розраховано величину відверненого збитку.

Коефіцієнт ROSI показує, скільки коштів (у гривнях) додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

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

$$ROSI = \frac{E}{K} \tag{3.19}$$

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

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

Звідси,

$$\text{ROSI} = \frac{27733}{37139} = 0{,}74$$

Проєкт системи інформаційної безпеки визнається доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції. Керівництвом прийнято

рішення фінансувати проєкт за допомогою реінвестування коштів. Доцільність вжитих заходів можна вирахувати за формулою 3.19.

$$ROSI > \frac{(N_{деп} - N_{інф})}{100} \quad (3.19)$$

де $N_{деп}$– річна депозитна ставка (13%)

$N_{інф}$ – річний рівень інфляції (3%)

Оскільки 0,74 > 0,10, проєкт вважається економічно доцільним.

Термін окупності капітальний інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки, і розраховується за такою формулою:

$$T_o = \frac{К}{Е} = \frac{1}{ROSI}, \text{ років} \quad (3.19)$$

Таким чином, термін окупності:

$$T_o = \frac{37629}{27733} = 1{,}36 \text{ років} \approx 1 \text{ рік } 4 \text{ місяців}$$

3.5 Висновок

Метою економічного розділу є підтвердження доцільності впровадження запропонованих в попередньому розділі проєктних рішень.

В ході виконання економічного завдання, було підраховано показники, як:

- ROSI = 0,74
- T_o(термін окупності) ≈ 1 рік 4 місяців

Проаналізувавши показник ROSI, можна зробити висновок, що запропонований проєкт є економічно доцільним і поверне вкладені інвестиції, а термін окупності показує, що інвестиції повернуться через 1 рік та 4 місяця. Тому

підприємство, впроваджуючи його, не тільки захистить власний бренд від репутаційних втрат, а ще й зможе зберегти матеріальні активи, посиливши свій захист від потенційних загроз інформаційної безпеки.

ВИСНОВКИ

Причиною для створення комплексної системи захисту інформації для підприємства «СТО 911» є потенційна загроза для інформаційної безпеки підприємства.

Метою впровадження КСЗІ на базі даного підприємства є підвищення загального рівня захищеності інформаційних активів підприємства, його захист від потенційних матеріальних та репутаційних збитків у разі реалізації загроз інформаційної безпеки.

В першому розділі кваліфікаційної роботи було виконано обстеження об'єкту інформаційної діяльності, була досліджена обчислювальна техніка підприємства, фізичне, інформаційне та середовище користувачів. Після цього було проведено створення моделей порушників інформаційної безпеки, та загроз для безпеки інформації. Після цього стало очевидно, що рівень захищеності інформації не відповідає належному.

Виходячи з результатів обстеження, в другому розділі було сформовано вимоги до захисту інформації та обрано профіль захищеності, що відповідає потребам підприємства. В ході аналізу виконання вимог послуг безпеки відповідного рівня захищеності, стало очевидно, що значна кількість послуг безпеки виконуються частково, або не виконуються зовсім. Для реалізації цих послуг було запропоновано рішення.

Після цього було розраховано економічну доцільність запропонованих заходів по підвищенню захищеності інформації. Показники ефективності вкладання коштів, такі як ROSI, показали, що вкладені кошти в розробку та впровадження КСЗІ є ефективною інвестицією і повернуться менш ніж через півтора роки, що є досить високим показником доцільності впровадження заходів.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. CERT-UA попереджає про збільшення кількості кібератак проти бухгалтерів. URL: https://cip.gov.ua/ua/news/cert-ua-poperedzhaye-pro-zbilshennya-kilkosti-kiberatak-proti-bukhgalteriv

2. НД ТЗІ 3.7-003-2005 – Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системи. – ДСТСЗІ СБ України, Київ. URL: https://tzi.com.ua/downloads/3.7-003-2005.pdf

3. Аналіз і дослідження моделі порушника безпеки інформації для захищеного вузла Інтернет-доступу – Комаров М.Ю., Ониськова А.В., Гончар С.Ф.

4. НД ТЗІ 2.5-004-99 – Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу – ДСТСЗІ СБ України – Київ. URL: https://tzi.com.ua/downloads/2.5-004-99.pdf

5. НД ТЗІ 1.1-003-99 – Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу ДСТСЗІ СБ України – Київ. URL: https://tzi.ua/assets/files/1.1_003_99.pdf

6. Система захисту інформації Лоза-1. Версія 4.4.0. Інструкція адміністратора безпеки. URL: http://avtoprom.kiev.ua/avtoprom/sites/default/files/LOZA-1_4_SecAdmin.pdf

7. Найкращі хмарні сховища для бізнесу та особистого використання. URL: https://blog.colobridge.net/uk/2024/03/top-cloud-storage-2024-ua/

8. Постанова Кабінету Міністрів України від 29 березня 2006 «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах». URL: https://zakononline.com.ua/documents/show/269716___702814

9. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу URL: https://tzi.com.ua/downloads/2.5-005%20-99.pdf

10. Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека / Упорядн.: Д.П. Пілова. – Дніпро: Національний технічний університет «Дніпровська політехніка», 2019. – 16 с.

ДОДАТОК А. ВІДОМІСТЬ МАТЕРІАЛІВ КВАЛІФІКАЦІЙНОЇ РОБОТИ

№	Формат	Найменування	Кількість листів
Найменування			
1	А4	Реферат	2
2	А4	Список умовних скорочень	1
3	А4	Зміст	2
4	А4	Вступ	1
5	А4	Розділ І	21
6	А4	Розділ ІІ	26
7	А4	Розділ ІІІ	16
8	А4	Висновки	1
9	А4	Перелік використаних джерел	2
10	А4	ДОДАТОК А	1
11	А4	ДОДАТОК Б	2
12	А4	ДОДАТОК В	2
13	А4	ДОДАТОК Г	1
14	А4	ДОДАТОК Ґ	2
15	А4	ДОДАТОК Д	1

ДОДАТОК Б. ПЕРЕЛІК ОСНОВНИХ ТЕХНІЧНИХ ЗАСОБІВ

Таблиця Б.1 – перелік основних технічних засобів ІКС

№	Тип	Модель	Характеристики	Серійний та інвентаризаційний номери	Відстань до КЗ
1	Персональний компьютер PC-1	Viper XT-1	Процесор Intel i5, ОЗУ 4GB, Жорсткий диск 480 GB SSD, відеокарта Intel UHD, монітор LG 22m35AA	Системний блок PC456-1, монітор 1230-1	2м
2	Персональний компьютер PC-1	Viper XT-1	Процесор Intel i5, ОЗУ 4GB, Жорсткий диск 480GB SSD, відеокарта Intel UHD, монітор LG 22m35AA	Системний блок PC456-2, монітор 1230-2	2м
3	Персональний компьютер PC-1	Viper XT-1	Процесор Intel i5, ОЗУ 4GB, Жорсткий диск 480 GB SSD, відеокарта Intel UHD, монітор LG 22m35AA	Системний блок PC456-3, монітор 1230-3	1м
4	Ноутбук NB-1	Lenovo ThinkPad T470	Процесор Intel i5, ОЗУ 4GB, Жорсткий диск 256GB SSD, відеокарта Intel UHD	PC321-1	-
5	Ноутбук NB-2	Lenovo ThinkPad T470	Процесор Intel i5, ОЗУ 4GB, Жорсткий диск 256GB SSD, відеокарта Intel UHD	PC321-2	-

Продовження таблиці Б.1

6	Ноутбук NB-3	Lenovo ThinkPad T470	Процесор Intel i5, ОЗУ 4GB, Жорсткий диск 256GB SSD, відеокарта Intel UHD	PC321-3	-
7	Багатофункціональний пристрій PR-1	HP LaserJet Pro MFP M125nw	Чорно-білий друк, формати A4, A5	RP865-100	1м
8	Маршрутизатор	Keenetic Viva KN-1910 SKIPPER	1 WAN порт, 4 LAN порти, стандарт WI-FI AC1300, частоти роботи 2,4МГц та 5МГц, швидкість LAN портів 1ГБіт/с	RT624-1	2м
9	Концентратор	Mercusys MS108G	8 портів RJ45,	MC23-1	2м
10	Медіа конвертор	TKO-WS01/02-20	швидкість портів 1ГБіт/с	NG745-1	2м

ДОДАТОК В. ПЕРЕЛІК ОСНОВНИХ ЗАГРОЗ ДЛЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Антропогенні загрози

Таблиця В.1 – Характеристика антропогенних загроз

№	Джерело загрози	Загроза	Вразливість	Наслідки
1	Користувачі системи	Несанкціонований доступ до ІКС	Не суворе дотримання системи керування доступом	Загроза для конфіденційності, цілісності та доступності інформації
2	Користувачі системи	Несанкціоноване копіювання ІзОД	Відсутність чіткого розмежування доступу користувачів	Загроза для конфіденційності інформації
3	Сторонні особи	Підглядання, підслуховування ІзОД	Відсутність режиму доступу відвідувачів до ОІД	Загроза для конфіденційності інформації
4	Сторонні особи	Псування технічних засобів КС	Відсутність режиму доступу відвідувачів до ОІД	Загроза для конфіденційності, цілісності та доступності інформації
5	Системний адміністратор	Несанкціонований доступ до ІКС	Відсутність системи облікових записів	Загроза для конфіденційності, цілісності та доступності інформації

Техногенні загрози

Таблиця В.2 – Характеристика техногенних загроз

№	Джерело загрози	Загроза	Вразливість	Наслідки
1	Єдина лінія підключення інтернету	Зупинка деяких інформаційних процесів	Збої роботи провайдера інтернет послуг	Уповільнення або зупинка потоків інформації в ІКС
2	Перепади напруги	Неполадки в системі електропостачання	Відсутність джерел безперебійного живлення, стабілізаторів, тощо.	Вихід зі строю технічного обладнання, руйнування даних внаслідок екстреного вимкнення

Стихійні загрози

Таблиця В.3 – Характеристика стихійних загроз

№	Джерело загрози	Загроза	Вразливість	Наслідки
1	Займання легкозаймистих речовин	Фізичне знищення технічних засобів, обладнання, паперових носіїв	Використання в робочому процесі речовин, що можуть зайнятися і почати пожежу	Крах ОІД

ДОДАТОК Г. ПЕРЕЛІК ДОКУМЕНТІВ НА ОПТИЧНОМУ НОСІЇ

ЗубковМЮ_125_20_2_ПЗ.docx

ЗубковМЮ_125_20_2_ПЗ.pdf

ЗубковМЮ_125_20_2_ПРЕЗ.pptx

ДОДАТОК Ґ. ВІГУК КЕРІВНИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ

ВІДГУК

на кваліфікаційну роботу бакалавра на тему:

«Комплексна система захисту інформації інформаційно-комунікаційної системи ФОП «СТО 911»

студента групи 125-20-2

Зубкова Михайла Юрійовича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 83 сторінках та містить 6 рисунків, 15 таблиць, 10 джерел та 8 додатків.

Метою кваліфікаційної роботи є забезпечення заданого рівня безпеки інформації, яка обробляється в ІКС ФОП «СТО 911».

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

Запропоновано матрицю розмежування доступу, розроблені положення політики безпеки щодо: реєстрації подій, розмежування повноважень адміністраторів, віддаленого адміністрування, резервного живлення та резервного копіювання. Розроблені проектні рішення впровадження резервного копіювання та реалізації резервного електроживлення.

Практичне значення результатів кваліфікаційної роботи полягає у адаптації запропонованих рішень до особливостей ФОП «СТО 911».

До недоліків відноситься недостатньо обґрунтована модель загроз та профіль захищеності.

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

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

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

Кваліфікаційна робота заслуговує оцінки «_____».

Керівник кваліфікаційної роботи, професор Магро В.І.

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

ДОДАТОК Д . ВІДГУК КЕРІВНИКА ЕКОНОМІЧНОЇ ЧАСТИНИ

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

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (ініціали, прізвище)