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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Біжка Івана Сергійовича*

академічної групи *125-18-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему Комплексна система захисту інформації інформаційно- телекомунікаційної системи сільськогосподарського підприємства «Чумаки»

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.т.н., проф. Корнієнко В.І.			
розділів:				
спеціальний	ст. викл. Кручінін О.В.			
економічний	к.е.н., доц. Романюк Н.М.	82	добре	

Рецензент				

Нормоконтролер	ст. викл. Тимофєєв Д.С.			

Дніпро
2022

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту ***Біжко І. С.*** **академічної групи** ***125-18-1***
(прізвище та ініціали) (шифр)

спеціальності ***125 Кібербезпека***

спеціалізації

за освітньо-професійною програмою ***Кібербезпека***

на тему Комплексна система захисту інформації інформаційно- телекомунікаційної системи СПП «Чумаки»

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

Розділ	**Зміст**	**Термін**
Розділ 1	*Обстеження інформаційно-телекомунікаційної системи СПП «Чумаки» аналіз потенційних загроз, фромування вимог та визначення послуг безпеки, які реалізовані*	10.05.2022
Розділ 2	*Аналіз існуючого стану послуг безпеки в ІТС, розробка проектних рішень*	20.05.2022
Розділ 3	*Економічне обгрунтування доцільності впровадження запропонованих рішень кваліфікаційної роботи*	10.06.2022

Завдання видано _____ Корнієнко В.І.
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: 20.01.2022

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Біжко І. С.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 69 с., 5 рис., 26 табл., 9 джерел.

Об'єкт розробки: інформаційно- телекомунікаційна система підприємства СПП «Чумаки».

Предмет розробки*:* комплексна система система захисту інформаційно-телекомунікаційної системи підприємства СПП «Чумаки».

Метою роботи є забезпечення необхідного рівня захисту інформації, яка обробляється в інформаційно-телекомунікаційній системі (ІТС) підприємства СПП «Чумаки».

Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі:

1. Проведення обстеження ІТС для визначення рівня захисту інформації в інформаційно-телекомунікаційній системі СПП «Чумаки»;
2. Розробка моделі порушника та визначення актуальних загроз ІТС;
3. Формулювання вимог щодо рівня захищеності інформації СПП «Чумаки».
4. Розробка проектних рішень щодо реалізації вимог захищеності
5. Доведення економічної ефективності впровадження комплексної системи захсту інформації СПП «Чумаки».

В економічній частині здійснені розрахунки капітальних витрат на внесення основних елементів політики безпеки інформації та визначена доцільність їх впровадження

Практична цінність роботи полягає у підвищенні ефективності захисту інформації в інформаційно-телекомунікаційній системі, за допомогою адаптованих проектних рішень до умов підприємства СПП «Чумаки».

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ТЕХНОЛОГІЯ ОБРОБКИ ІНФОРМАЦІЇ, МОДЕЛЬ ПОРУШНИКА, МОДЕЛЬ ЗАГРОЗ,ЕКОНОМІЧНА ЕФЕКТИВНІСТЬ

ABSTRACT

Explanatory note: 69 pp., 5 Fig., 26 Tab., 9 Sources.

The object of development: information and telecommunication system of the agricultural enterprise Chumaky.

The subject of development: a complex system of protection of information and telecommunication system of the enterprise of AE Chumaky.

The purpose of the work is to develop elements of a comprehensive system of protection of information and telecommunication system of the enterprise AE "Chumaky".

To achieve this goal in the qualification work the following tasks are solved:

1. Conducting an ITS survey to determine the level of information protection in the information and telecommunications system of AE "Chumaky";

2. Development of the violator model and identification of current ITS threats;

3. Formulation of requirements for the level of information security of AE "Chumaky".

4. Development of design solutions for the implementation of security requirements

5. Proving the economic efficiency of the implementation of a comprehensive information protection system of AE "Chumaky".

In the economic part, calculations of capital expenditures for the introduction of the main elements of information security policy and the feasibility of their implementation

The practical value of the work is to increase the effectiveness of information protection in the information and telecommunication system, with the help of adapted design solutions to the conditions of the enterprise AE "Chumaky".

COMPREHENSIVE INFORMATION PROTECTION SYSTEM, INFORMATION PROCESSING TECHNOLOGY, INFRINGEMENT MODEL, THREAT MODEL, ECONOMIC EFFICIENCY

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ОС – обчислювальна система;

ІТС – інформаційно-телекомунікаційна система;

КСЗІ – комплексна система захисту інформації;

НД – нормативний документ;

НД ТЗІ – нормативний документ системи технічного захисту інформації;

ІзОД– інформація з обмеженим доступом;

ОІД– об’єкт інформаційної діяльності;

ПЗ- програмне забезпечення;

ПК- персональний комп’ютер;

НСД – несанкціонований доступ;

ТЗІ – технічний захист інформації;

ОП – оперативна пам’ять;

Зміст

ВСТУП

Безпека інформації в інформаційно-телекомунікаційній системі на сьогоднішній день дуже важлива. Велика кількість підприємств, які займаються сільским господарством, або іншими виробництвами все більше інтегрують нові елементи не лише автоматизації бухгалтерського обліку, та обігу документів, а й в тому числі елементів автоматизації технологічного процесу, питання безпеки для них також є актуальними, звісно чим більший стає бізнес, тим більше стає ризиків при реалізації загроз інформаційної безпеки, та як правило на великих підприємствах вже є запроваджені процедури комплексної системи захисту інформації. Тому задача забезпечення безпеки інформації яка обробляється в ІТС в середніх, та малих підприємствах є дуже актуальною. Нажаль на сьогоднішній день не всі власники організацій приділяють цьому значення. Робота як правило ведеться не систематизовано без комплексного підходу рішення цього питання, тому створення цих систем без систематизованого комплексного підходу, не буде працювати як слід і буде матиме свої вразливості, які зможуть призводити до втрати інфоррмації. Створення комплексу системи захисту інформації буде забезпечувати системність, постійність супроводу, тому задача створення КСЗІ для таких підприємств є актуальною

1.СТАН ПИТАННЯ.ПОСТАНОВКА ЗАДАЧІ

1.1 Загальні відомості про сільськогосподарське підприємство (СПП) «Чумаки»

Сільськогосподарське підприємство «Чумаки» засноване в 2001 р., загальна площа земель підприємства складає 4995 га, які використовуються для вирощування продукції рослинництва, другим напрямком виробництва є тваринництво, а саме виробництво та реалізація молока, вирощування тварин на забій, та реалізація племенного молодняка загальна кількість 1211 голів.

Адреса офісу компанії: Дніпропетровська область , Дніпрвський район с. Чумаки вул. Шкільна 10. Також у власності підприємства є ферма за адресою Дніпропетровська область, Дніпрвський район с.Горянівське, вул Лугова 1 , склад за адресою Дніпропетровська область, Дніпрвський район с. Маївка пров Мирний 17. Також підприємству належать 10 полів загальною площею 4900 га які знаходяться в с. Зоря Дніпропетровської області , Дніпрвського району

Схема взаємодії між підрозділами підприємства зображена на рис. 1.1

Рисунок 1.1 – Структура підприємства

Штат підприємства включає в себе 103 особи.

Організаційна структура підприємства зображена на рис. 1.2.

Директор: Управління виробництвом контроль, розподілення фінансових потоків, самостійно обирає план реалізувації продукції і затвердження плану закупівлі, затвердження кадрових рішень.

Заступник директора з тваринництва: виробництво продукції тваринництва, годівля утримання і відтворення стада, кормозаготівля додержання техноголічного процесу продукції тваринництва. Має в підпорядкуванні: головного технолога з виробництва продукції тваринництва, ветеринарного лікаря, ветеринарного фельдшера, зоотехніка, шість операторів машинного доїння, бригадира, оператора комбікормового заводу, сім працівників по догляду за тваринами, чотири слюсара-ремонтника.

Заступник директора з виробництва: виробництво продукції рослинництва , процес оброблення грунту, внесення мінеральних і органічних добрив , посів культур, оброблення засобами захисту рослин , збирання урожаю, облення грунту і внесення мінеральних доброив під урожай наступного року. Має в підпорядкуванні: головного агронома та агронома.

Головний інженер: відповідає за утримання машино тракторного парку, ремонт усіх технічних засобів,закупівлю запасних частин , облік і закупівлю технічних засобів. Має в підпорядкуванні: енергетика, завідуючого автопарком, старшого механіка, дев'ять водіїв, дванадцять механізаторів та слюсара.

Інженер з охорони праці: контроль за дотримуванням умов праці відповідно до чинного законодавства, закупівля спеціального одягу , спеціальних засобів, навчання прцівників з техніки безпеки.

Головний бухгалтер: контроль ведення бухгалтерського обліку , нарахування заробітної плати , орендної плати за використпння земельного паю, сплати податків і зборів до держ бютжету. Має в підпорядкуванні: чотирьох бухгалтерів, сім обліковців та спеціаліста в роботі з пайовиками.

Керівник служба безпеки: охорона території і збереження майнав і цілісності підприємства. Має в підпорядкуванні: замісника керівника служби безпеки та двадцять два спеціаліста служби безпеки.

Юрист-консультант: контроль оформлення юридичних договорів, представлення інтересів підприємства в судах і дотримання всіх мір і вимог законодавства при веденні господарчої діяльності підприємства.

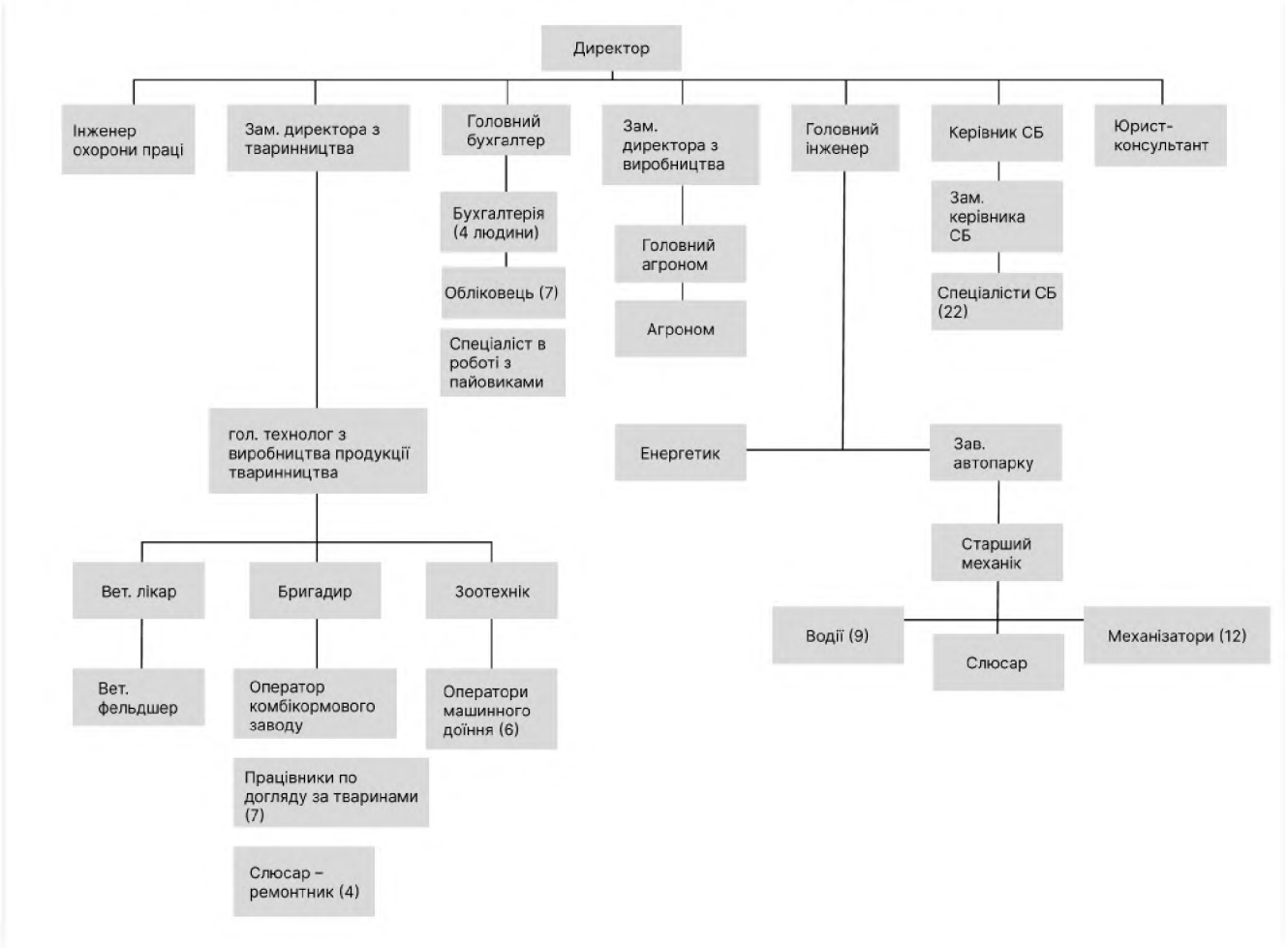


Рисунок 1.2 – Організаційна структура підприємства

1.2 Обгрунтування необхідності створення КСЗІ

Згідно НД ТЗІ процес створення КСЗІ полягає у здійсненні комплексу взаємоузгоджених заходів, спрямованих на розроблення і впровадження інформаційної технології, яка забезпечує обробку інформації в ІТС згідно з вимогами, встановленими нормативно-правовими актами та НД у сфері захисту інформації.[6]

Відповідно до статті 9 Закону України «Про захист інформації в інформаційно-комунікаційних системах» власник системи, в якій обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога

щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним. [2]

Відповідно до статті 5 Закону України «Про захист персональних даних» об’єктами захисту є персональні дані. Персональні дані можуть бути віднесені до конфіденційної інформації про особу законом або відповідною особою. Не є конфіденційною інформацією персональні дані, що стосуються здійснення особою, уповноваженою на виконання функцій держави або місцевого самоврядування, посадових або службових повноважень. [3]

Відповідно до статті 1 Закону України «Про інформацію» захист інформації - сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї; інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді; [5]

Згідно пукту 2 статті 21 Закону України «Про інформацію» Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом.[1]

Відносини, пов'язані з правовим режимом конфіденційної інформації, регулюються законом.

На підприємстві наявна конфіденційна інформація з обмеженням доступу до окремих видів інформації та інформація яка повинна зберігати цілісність та бути захищеною відповідно до нормативно-правових вимог нормативно-правових актів, які можуть формувати вимоги до захисту або обмеження доступу до окремих видів інформації.

А саме інформація про: урожайність, удій, ціну реалізації, прибуток, ціну основнного обладнання, зарплата, особисті данні співробітників. На даний

момент питання створення КСЗІ найбільш актуальним є для офісу компанії, так як там розміщена вся інформація.

1.3 Обстеження середовищ функціювання ІТС.

Об’єкт інформаційної діяльності знвходиться за адресою Дніпропетровська область, Дніпровський район, село Чумаки, вулиця Шкільна 10.

1.3.1 Фізичне середовище

Офісна будівля знаходиться біля проїжджої частини та має три поверхи і збудована з цегли та бетонних конструкцій. Дах будівлі виконаний з металочерепиці, який є стійким до вогню. Ситуаційний план зображено на рис1.3.

Характеристика будівель і споруд, що знаходяться навколо ОІД описана в табл. 1.1

Рисунок 1.3 – Ситуаційний план

Таблиця 1.1 - Характеристика будівель і споруд, що знаходяться навколо ОІД

№	Найменування	Кількість поверхів	Адреса	Відстань
1	Громадська будівля	1	С. Чумаки, вул. Шкільна, 9	22 м
2	Адміністративна будівля	1	С. Чумаки, вул. Шкільна,13	22 м
3	Школа	2	С. Чумаки, вул. Шкільна, 14	29 м
4	Громадська будівля	2	С. Чумаки, вул. Шкільна, 12	90 м

КЗ обмежена периметром будівлі: підлога , стіни, стеля, вікна, двері. Центральний вхід в будівлю контролюється охороною, яка знаходиться на КПП, має можливість за допомогою електричного замка відкривати двері. Охоронці охороняють будівлю з використанням технічних засобів охоронної сигналізації. Доступ в будівлю дозволяється лише співробітникам офісу, та охороні лише в робочий час, в неробочий час по узгодженню з керівництвом. Неподалеку від КЗ знаходиться велика бетонна стіна висотою 3 метра. Вікна першого поверху знаходяться досить високо, через що підглядання з вулиці не можливе.

Система електропостачання підключена до будівлі кабелем, повітряним способом комунікації.

Зі сторони південного заходу територія обладнана парковкою, на якій є можливість перегляду камер спостереження в записі. Режим контролю доступу до робочих приміщень відсутній. Обладнаних місць для зберігання носіїв інформації немає. В кабінеті директора і головного бухгалтера є сейфи для зберігання цінних речей та документів. Для зберігання документів також використовують шафи, або ящики столів.

Розміщення працівників в офісі вказано в табл. 1.2

Таблиця 1.2 – Розміщення працівників в офісі

№ кабінету	Поверх	Назва кабінету
1	1	Бухгалтерія
2	1	Обліковці
3	1	Головний бухгалтер
4	1	Кімната для перемовин
5	1	Інженер охорони праці
6	2	Юрист-консультант
7	2	Заст. Директора з тваринництва
8	2	Заст. Директора з виробництва
9	2	Директор
10	2	Керівник СБ
11	1	Серверна

Фрагмент генерального плану зображено на рис.1.4

Рисунок 1.4 – Фрагмент генерального плану

Дві шафи що знаходяться в кабінеті бухгалтерії біля входу використовуються для зберігання особистих речей та верхнього одягу.

Фрагмент основних технічних засобів описано в табл. 1.3. Фрагмент допоміжних технічних засобів описано в табл. 1.4. Табл. 1.5 – Специфікація апаратного забезпечення сервера. Табл. 1.6 – Специфікація апаратного забезпечення (фрагмент). Програмне забезпечення описано в табл. 1.7

Таблиця 1.3 – Основні технічні засоби (фрагмент)

№	**Назва**	**Марка**	**Модель**	**Серійний номер**	**Розміщення**	**Відстань ОІД в м.**	**№ Каб**
1	PC монітор (ПК1)	LG	22m38a-B	703NTCZBG419	На столі	1,6	1
2	PC монітор (ПК2)	LG	22m38a-B	0mo0IdB28Epv	На столі	3,4	1
3	PC монітор (ПК3)	LG	22m38a-B	WO6S3Bae94Zn	На столі	5,0	1
4	PC монітор (ПК4)	LG	22m38a-B	n9nBkGJG503g	На столі	2,1	1
5	PC монітор (ПК5)	LG	22m38a-B	pPBb9mU337ra	На столі	4,0	1
6	PC блок (ПК1)	DELL	OptiPlex 3010 SFF	7B7hw7fQCN3e	На столі	1,6	1
7	PC блок (ПК2)	DELL	OptiPlex 3010 SFF	2nOtVi0Q5tJ1	На столі	3,5	1
8	PC блок (ПК3)	DELL	OptiPlex 3010 SFF	n3oWQ9j95QES	На столі	4,9	1
9	PC блок (ПК4)	DELL	OptiPlex 3010 SFF	xfwi4A99p4VN	На столі	2,1	1
10	PC блок (ПК5)	DELL	OptiPlex 3010 SFF	WJ9YS0V0qU4A	На столі	3,9	1
11	Принтер	Canon	PIXMA G1520	e3KkuT3M1X0x	На столі	2,0	1
12	Принтер	Canon	PIXMA G1520	e3KkuT3M1X0x	На столі	1,2	1

Продовження таблиці 1.3

№	Назва	Марка	Модель	Серійний номер	Розміщення	Відстань ОІД в м.	№ Каб
13	Клавіатура	Logitech	MK120	Va5inB8Ho5u0	На столі	1,5	1
14	Клавіатура	Logitech	MK120	sL3MD5TqFuFJ	На столі	3,4	1
15	Клавіатура	Logitech	MK120	N5LDpCYN4cf7	На столі	5,0	1
16	Клавіатура	Logitech	MK120	LpcqUwC7w9ZQ	На столі	2,1	1
17	Клавіатура	Logitech	MK120	RQxJCEg42Y4x	На столі	4,0	1

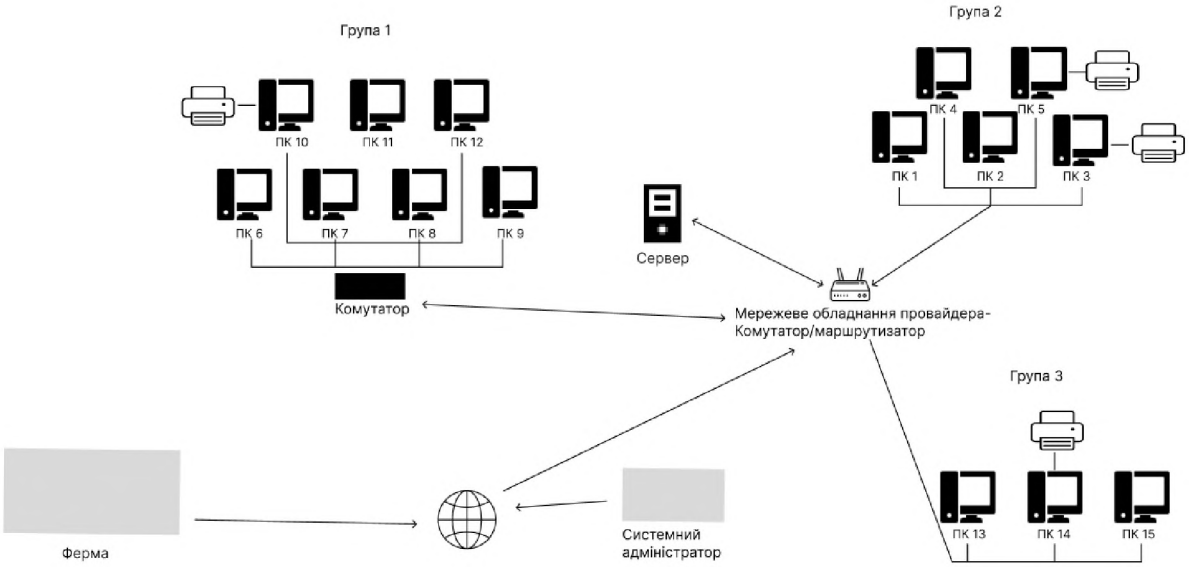
Таблиця 1.4 – Допоміжні технічні засоби

№	Назва	Марка	Модель	Серійний номер	Розміщення	Відстань ОІД в м.
1	Кондиціонер	Hyundai	ARN12HSSUAWF1	W1Q3H2uY2DmF	На стіні	0,1
5	Настільна лампа	Splendid Rey	N203B WT	91Ud1MwC6JZs	На столі	3,1
6	Комп'ютерна миша(5)	Logitech	910-001794	MWG1om028ogi	На столі	1,5
7	Енергозберігаюча лампа (4)	Brille	E27 PL-SP 24W/864 techno Br	6AM9Xh	На стелі	2

1.3.2 Обчислювальна система

Схематичне зображення взаємозв'язку комп'ютерів вказано на рис 1.4

Рисунок 1.4 – Схематичне зображення взаємозв'язку комп'ютерів



Локальна обчислювальна система складається з 15 комп'ютерів і серверу який використовується для зберігання файлів,резервних копій та керуванням базами данни. Комп'ютерна система однорангова, усі комп'ютери і сервери підключені крученою парою, яка розташовується над навісною стелею, до комутатора. На підприємстві розміщенний сервер DELL R730xd. Специфікація апаратного забезпечення серверу вказана в табл. 1.5. RAID масиви на сервері відсутні.

Таблиця 1.5 – Специфікація апаратного забезпечення сервера

№	Назва	Марка	Модель	Серійний номер
1	Процессор	Intel	E5-2630L v3 1.80-2.90 GHz	UorZb2BDlx6L
2	Процессор	Intel	1.80 GHz E5-2630L v3/55W 8 Cores/20MB Cache/DDR4 1866MHz	DbyV2ncWqSGX
3	Контролери SAS/SATA	Dell	H730 + 1GB (0KMCCD)	nnE1tOteAOGH
4	Блок живлення	Dell	750W AC Platinum Hot Plug Power Supply	gSaD3goAAlPS

Продовження таблиці 1.5

№	Назва	Марка	Модель	Серійний номер
5	Блок живлення	Dell	750W AC Platinum Hot Plug Power Supply	MQGZzkC27jp4

Таблиця 1.6 – Специфікація апаратного забезпечення робочих місць (фрагмент)

№	Назва	Марка	Модель	Серійний номер
ПК1				
1	Процессор	Intel	Pentium 4 2.4A	DqA4yCsfHuyu
2	ОЗУ	Crucial	DDR4-3200 8192MB PC4-25600 Ballistix Black	aAAVuc8Aw252
3	Жорсткий диск	Transcend	StoreJet 25M3C 4TB TS4TSJ25M3C 2.5	xpRaJkSX8dPw
4	Материнська плата	ASUS	P5LD2-VM/S	zPeQ2w6TSjZ2
ПК2				
5	Процессор	Intel	Pentium 4 2.4A	gT3Jset6QkWx
6	ОЗУ	Crucial	DDR4-3200 8192MB PC4-25600 Ballistix Black	RqrRJXBL2nRS
7	Жорсткий диск	Transcend	StoreJet 25M3C 4TB TS4TSJ25M3C 2.5	RN39Sbn2Edph
8	Материнська плата	ASUS	P5LD2-VM/S	MmU3BAvZPEhR
ПК3				
9	Процессор	Intel	Pentium 4 2.4A	zUcP47FaFc39
10	ОЗУ	Crucial	DDR4-3200 8192MB PC4-25600 Ballistix Black	jhZrKJC4Mnmt
11	Жорсткий диск	Transcend	StoreJet 25M3C 4TB TS4TSJ25M3C 2.5	Qt7w8gmRG54K
12	Материнська плата	ASUS	P5LD2-VM/S	fEwnDTefaUuy

Продовження таблиці 1.6

№	Назва	Марка	Модель	Серійний номер
ПК4				
13	Процессор	Intel	Pentium 4 2.4A	wu9xKUs97mUq
14	ОЗУ	Crucial	DDR4-3200 8192MB PC4-25600 Ballistix Black	pj2SWWMm75rw
15	Жорсткий диск	Transcend	StoreJet 25M3C 4TB TS4TSJ25M3C 2.5	Vc3JtSc9mA5Y
16	Материнська плата	ASUS	P5LD2-VM/S	MuBCQbBTSVjG
ПК5				
17	Процессор	Intel	Pentium 4 2.4A	V54JE7zn5Yxc
18	ОЗУ	Crucial	DDR4-3200 8192MB PC4-25600 Ballistix Black	3jSnUk2sBXNA
19	Жорсткий диск	Transcend	StoreJet 25M3C 4TB TS4TSJ25M3C 2.5	3KycYrx9nzhg
20	Материнська плата	ASUS	P5LD2-VM/S	yCCNcSj44urf

Таблиця 1.7 – Програмне забезпечення

№	Назва програмного забезпечення	Ліцензія	Тип програмного забеспечення	Де встановлено
1	AnyDesk 6.2.6	Безкоштовна	прикладне	ПК1, ПК2… ПК15
2	Teamviewer 15.30.3	Безкоштовна	прикладне	ПК1, ПК2… ПК15
3	1с бухгалтерія 8.3	Комерційна до (13.10.2022)	прикладне	ПК1, ПК2… ПК15
4	Клиент-банк	Безкоштовна	прикладне	ПК1, ПК2… ПК15
5	Opera 75.0.3969.171	Безкоштовна	прикладне	ПК1, ПК2… ПК15
6	Google Chrome 102.0.5005.61/63	Безкоштовна	прикладне	ПК1, ПК2… ПК15

Продовження таблиці 1.7

№	Назва програмного забезпечення	Ліцензія	Тип програмного забеспечення	Де встановлено
7	WinRAR 6.11	Безкоштовна	прикладне	ПК1, ПК2… ПК15
8	Avast 21.6.2474	Комерційна до (20.09.2022)	спеціалізоване	ПК1, ПК2… ПК15
9	Uniform Agri 5.4	Комераційна	прикладне	ПК1, ПК2… ПК15
10	Dairy Plan 5.2	Комерційна	прикладне	ПК1, ПК2… ПК15
11	Windows 10 Pro	Комерційна	системне	ПК1, ПК2… ПК15
12	Пакет програм Microsoft Office 2019 Home & Business	Комерційна	прикладне	ПК1, ПК2… ПК15
13	MS SQL Server 15.0.2000.5	Комерційна	системне	Сервер
14	Студия управления MS SQL Server	Комерційна	системне	Сервер
15	Windows 10 Server 2019	Комерційна	системне	Сервер

Програма Uniform Agri використовується для управління доїльним апаратом та розподілу кормів. Програма Dairy Plan використовується для контролю за тваринами, там зберігається база даних тварин.

1.3.3 Інформаційне середовище

Класифікація інформації в ІТС вказано в табл. 1.8

Таблиця 1.8 – Класифікація інформації в ІТС

Інформація	Вид представлення в ІТС	Режим доступу	Правовий режим	Вимоги до захисту
1. Інформація про співробітників, копії персональних данних працівників.	Паперовий, електронний	ІзОД	Конфіденційна	К Ц Д

Продовження таблиці 1.8

Інформація	Вид представлення в ІТС	Режим доступу	Правовий режим	Вимоги до захисту
2. Інформація про контракти.	Паперовий, електронний	ІзОД	Комерційна таємниця	К Ц Д
3. Бухгалтерські звіти.	Паперовий, електронний	ІзОД	Комерційна	К Ц Д
4. Інформація про прибуток.	Паперовий, електронний	ІзОД	Комерційна таємниця	К Ц Д
5. Інформація про урожайність.	Паперовий, електронний	ІзОД	Комерційна таємниця	К Ц Д
6. Інформація про удій.	Паперовий, електронний	ІзОД	Комерційна таємниця	К Ц Д
7. Організаційно-розпорядчі документи.	Паперовий, електорнний	ІзОД	Конфіденційна	К Ц Д
8. Вартість основного обладнання.	Паперовий, електорнний	Відкрита	Відкрита	Ц Д
9. Технологія вирощування зернових культур.	Електорнний	ІзОД	Комерційна таємниця	К Ц Д
10. Технологія годування тварин.	Електорнний	ІзОД	Комерційна таємниця	К Ц Д
11. Інформація про рівень безпеки підприємства.	Електронний	ІзОД	Конфіденційна	К Ц Д
12. Технологічна інформація	Електронний	ІзОД	Конфіденційна	К Ц Д

(облікові записи, журнал подій, реєстр тощо)				

Умовні позначення вимог до захисту:

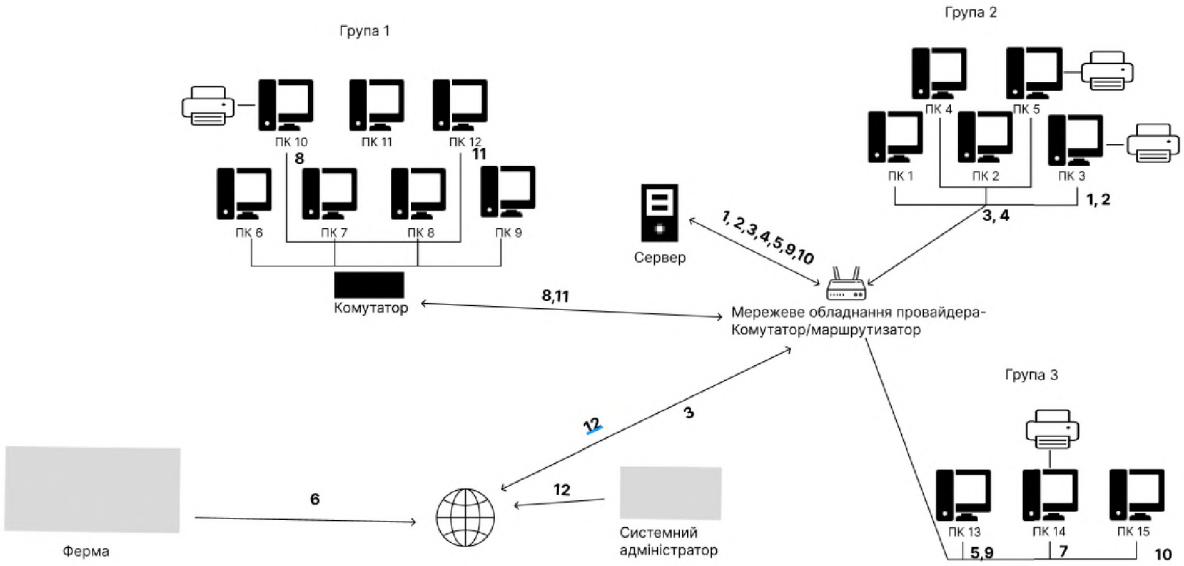
К – конфиденційність

Ц – цілісність

Д – доступність

Інформаційні потоки вказані в рис 1.5

Рисунок 1.5 – Інформаційні потоки



Технологія обробки інформації на підприємстві:

Інформація про співробітників, копії персональних данних працівників. Додається в електронному вигляді під час найму працівника на роботу головним бухгалтером. В паперовому вигляді зберігається в шафі, яка знаходиться в кабінеті у головного бухгалтера. Інформація може змінюватися, видалятися головним бухгалтером власноруч, або після звернення працівника.

Інформація про контракти після узгодження з директором, та підписання контакту в кімнаті перемовин інформація вноситься в електронний вигляд головним бухгалтером, в паперовому вигляді інформація зберігається в керівника

підрозділу у якого заключали контракт, або в директора. Копії передаються юристу-консультанту.

Бухгалтерські звіти сторюються, видаляються та редагуються бухгалтерами під керівництвом головного бухгалтера, включаючи виплату заробітно плати та премії, в паперовому вигляді документи знаходяться в кабінеті бухгалтерії в шафі.

Інформація про прибуток створюється бухгалтерією в електронному вигляді, в паперовому вигляді передається головному бухгалтеру і зберігається у нього в кабінеті.

Інформація про урожайність створюється заступником директора з виробництва та обліковцями в електронному вигляді, в паперовому зберігається кабінеті заступника директора з виробництва.

Інформація про удій створюється заступником директора з тваринництва та обліковцями елктронному вигляді, зберігається в столі в кабінеті заступника директора з тваринництва

Організаційно-розпорядчі документи створюються директором, підписуються усіма працівниками підприємства, та дублюється в електронному вигляді на електронну пошту підрозділів.

Вартість основного обладнання створюється обліковцями та головним інженером, в паперовому вигляді зберігається в кабінеті обліковців

Технологія вирощування зернових культур створюється заступником директора з виробництва, головним агрономом та агрономом, може редагуватись та видалятись.

Технологія годування тварин створюється заступником директора з тваринництва та головним технологом з виробництва продукції тваринництва, може редагуватись лише під керівництвом заступника директора з тваринництва, передається до ознайомлення обліковцям.

Інформація про рівень безпеки підприємства створюється керівником служби безпеки та заступником служби безпеки, узгоджується з директором, може передаватись на ознайомлення спеціалістам служби безпеки, та керівникам відділень.

Технологічна інформація створюється змінюється і видаляється системним адміністратором. Паролі видаються всім користувачам і зберігаються у системного адміністратора.

1.3.4 Середовище користувачів

Характеристика користувачів підприємства описана у табл. 1.9. Матрицю розмежування доступу вказано в табл. 1.10

Таблиця 1.9 – Характеристика користувачів підприємства

Посада	Роль в системі	Рівень кваліфікації	Кількість працівників
Директор	Користувач	Середній	1
Зас. Директора з виробництва	Користувач	Середній	1
Зас. Директора з тваринництва	Користувач	Середній	1
Бухгалтер	Користувач	Середній	4
Головний бухгалтер	Користувач	Середній	1
Обліковець	Користувач	Середній	7
Керівник СБ	Користувач	Середній	1
Зас. Керівника СБ	Користувач	Середній	1
Юрист – консультант	Користувач	Середній	1
Системний адміністратор (Зовнішній співробітник за договором)	Системний адміністратор	Високий	1

У підприємства є договір з ФОП «Главацький Олександр Вікторович» за яким він зобов’язується раз в квартал проводити обов’язкове обстеження ПЗ та

системного обладнання локально, у разі необхідності налагоджувати збої в системі, та проводити заміну, налаштування обладнання, а також віддалено контролювати коректність роботи окремих програм. Системний адміністратор може для підключення дистанційно використовувати програму AnyDesk або Teamviewer.

Таблиця 1.10 – Матриця розмежування доступу

Об'єкт	Інформація*												Повноваження Інсталювання ПЗ	Доступ до ресурсів
Користувач	1	2	3	4	5	6	7	8	9	10	11	12		
Директор	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	Ч	ЧС РВ ЕД	ЧС РВ ЕД	-	Так	ПК 1-15
Зас. Директора з виробн.	Ч	ЧС РВ ЕД	-	Ч	ЧС РВ ЕД	-	ЧС РВ ЕД	-	ЧС РВ ЕД	-	Ч	-	Так	ПК 13
Зас. Директора з тварин.	Ч	ЧС РВ ЕД	-	Ч	ЧЕ Д	ЧС РВ ЕД	ЧС РВ ЕД	-	-	ЧС РВ ЕД	Ч	-	Так	ПК 14
Бухгалтер	-	Ч	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	-	-	-	-	-	Так	ПК 1-4
Головний бухгалтер	ЧС РВ ЕД	Ч	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	Ч	-	-	Ч	-	Так	ПК 5
Обліковець	-	Ч	Ч	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	-	-	Так	ПК 9-12
Керівник СБ	ЧС РВ ЕД	ЧС РВ ЕД	-	Ч	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	Ч	Ч	ЧС РВ ЕД	-	Так	ПК 6

Продовження таблиці 1.10

Користувач	1	2	3	4	5	6	7	8	9	10	11	12		
Зас. Керівника СБ	Ч	Ч	-	Ч	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	Ч	Ч	ЧС РВ ЕД	-	Так	ПК 7
Юрист – консультант	ЧС РВ ЕД	Ч РВ ЕД	-	-	-	-	ЧС РВ ЕД	-	-	-	Ч	-	Так	ПК 8
Системний адміністратор	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	Так	ПК 1-15 Сервер

*Номера інформації наведено згідно з табл. 1.8.

Умовні позначення доступу до інформації.

Ч- читання.

С-створення нових файлів.

Р-редагування.

В-видалення.

Е-імпорт або експорт.

Д-друк.

1.4 Аналіз актуальних загроз

1.4.1 Аналіз моделі порушників

Порушник – особа (користувач) яка намагається здійснити спробу несанкціонованого доступу до інформації.

Враховуючи особливості середовища можна визначити декілька груп потенційних порушників:

- Внутрішні по відношенню до ІТС.
- Зовнішні по відношенню до ІТС.

Також будемо розглядати порушників за такою класифікацією:

- Мотив за яким може бути скоєний несанкціонований доступ.
- Рівень кваліфікації потенційного порушника.
- Можливість подолання захисту.
- Класифікація порушення за місцем.
- Класифікація порушення за часом дії.

Розглянемо мотив за яким може бути скоєний несанкціонований доступ. Виявимо Рівень кваліфікації потенційного порушника. Розглянемо можливість подолання захисту та визначимо де і коли буде найбільш незахищенною система для різних груп.

В табл. 1.11 ми розглянемо категорії порушників. В табл. 1.12 розглянемо мотив порушнення. В табл. 1.13 специфікацію порушника за за рівнем кваліфікації та обізнаності в роботі з ІТС. В табл. 1.14 специфікацію моделі порушника за можливістю подолання захисту. В табл. 1.15 Специфікація моделі порушника за часом дії. В табл. 1.16 специфікацію моделі порушника за місцем.В табл. 1.17 модель порушників.

Таблиця 1.11 Категорії порушників

Позначення	Визначення категорії	Рівень загроз
Внутрішні по відношенню до ІТС		
ПІ1	Технічний персонал (водії, слюсарі, електрики тощо)	1
ПІ2	Обліковці	2
ПІ3	Системний адміністратор, спеціалісти служби безпеки, група користувачів 2	3
ПІ4	Директор, керівники різних підрозділів	4
Зовнішні по відношенню до ІТС		
ПА1	Відвідувачі	1
ПА2	Співробітники комунальних служб	2
ПА3	Хакери	3
ПА4	Агенти конкурентів «під прикриттям»	4

Таблиця 1.12 – Мотив порушення

Позначення	Мотив порушення	Рівень загрози
М1	Необачність	1
М2	Отримання необхідної інформації	2
М3	Мати можливість вносити зміни в інформаційні потоки	3
М4	Знищення матеріалів та інформаційних цінностей	4

Таблиця 1.13 – Специфікація порушника за за рівнем кваліфікації та обізнаності в роботі з ІТС

Позначення	Основні кваліфікаційні ознаки порушника	Рівень загрози
К1	Низький рівень знань, але є вміння працювати з ІТС	1
К2	Середній рівень знань, досвід роботи у роботі з ІТС	2
К3	Високий рівень знань, великий досвід у програмуванні, вміння у галузі експлуатації ІТС	3

Таблиця 1.14 – Специфікація моделі порушника за можливістю подолання захисту

Позначення	Можливості порушника	Рівень загрози
З1	Підслуховувати розмови, підглядати в документи, які знаходяться на столі,	1
З2	Несанкціоновано користуватись технічними засобами співробітника з більшим рівнем доступу	2
З3	Отримувати доступ за допомогою сторонніх ресурсів	3

Таблиця 1.15 Специфікація моделі порушника за часом дії

Позначення	Можливості порушника	Рівень загрози
Ч1	Під час бездіяльності компонентів ІТС	1
Ч2	Під час функціювання ІТС	2
Ч3	Під час перерв на ремонт компонентів ІТС	3

Таблиця 1.16 – Специфікація моделі порушника за місцем

Позначення	Можливості порушника	Рівень загрози
Л1	Знаходячись в середині приміщення, але не маючи доступу до технічних засобів ІТС	1
Л2	З робочих місць користувачів	2
Л3	Маючи доступ до зони зберігання баз данних	3

Таблиця 1.17 – Модель порушників

Порушник	Категорія порушника	Мотив порушника	Рівень обізнаності щодо ІСТ	Подолання захисту	Час дії	Місце	Сума загроз
Директор	ПІ4	М3	К2	З3	Ч2	Л3	17
	4	3	2	3	2	3	
Зас. Директора з виробн.	ПІ4	М3	К2	З2	Ч2	Л2	15
	4	3	2	2	2	2	
Зас. Директора з тварин.	ПІ4	М3	К2	З1	Ч2	Л2	14
	4	3	2	1	2	2	

Продовження таблиці 1.17

Порушник	Категорія порушника	Мотив порушника	Рівень обізнаності щодо ІСТ	Подолання захисту	Час дії	Місце	Сума загроз
Бухгалтер	ПІ3	М3	К2	З1	Ч2	Л2	13
	3	3	2	1	2	2	
Головний бухгалтер	ПІ4	М3	К2	З2	Ч2	Л2	15
	4	3	2	2	2	2	
Обліковець	ПІ2	М3	К2	З1	Ч2	Л2	12
	2	3	2	1	2	2	
Керівник СБ	ПІ4	М3	К2	З1	Ч2	Л2	14
	4	3	2	1	2	2	
Зас. Керівника СБ	ПІ3	М3	К2	З1	Ч2	Л2	13
	3	3	2	1	2	2	
Юрист – консультант	ПІ3	М3	К2	З2	Ч2	Л2	14
	3	3	2	2	2	2	
Системний адміністратор	ПІ3	М3	К3	З2	Ч3	Л3	17
	3	3	3	2	3	3	
Відвідувачі	ПА1	М1	К1	З1	Ч1	Л1	6
	1	1	1	1	1	1	
Комунальні служби	ПА2	М1	К1	З1	Ч1	Л1	7
	2	1	1	1	1	1	
Хакери	ПА3	М4	К3	З3	Ч2	Л1	16

	3	4	3	3	2	1	

Продовження таблиці 1.17

Порушник	Категорія порушника	Мотив порушника	Рівень обізнаності щодо ІСТ	Подолання захисту	Час дії	Місце	Сума загроз
Агенти конкурентів «під прикриттям»	ПА4	М2	К2	З1	Ч1	Л3	13
	4	2	2	1	1	3	

Розглянувши табл. 1.17 можемо зробити висновки, що найбільшу загрозу серед внутрішніх працівників несуть директор та системний адміністратор.

З боку зовнішніх порушників набільш небезпечними є хакери і агенти під прикриттям.

1.4.2 Аналіз актуальних загроз

В загальному випадку загрози можна розділити на:

- Природні (стан природи, довкілля)
- Техногенні (залежать від якості обладнання)
- Антропогенні (людський фактор)

Ці загрози ми розглянемо в табл. 1.17.

Так як антропогенні джерела загроз не будуть використовувати технічні засоби розвідки, то технічні канали витоку інформації є неактуальними

Таблиця 1.18 – Модель загроз ІТС

№	Загроза	Ймовірність	Вразливість	Джерело загрози	Порушення властивостей інформації
Природні					
1.1	Стихійні лиха (землетрус,	Низька	Стара будівля.	Зовнішнє	ЦД

	повінь і тд.)				
Продовження таблиці 1.18					
№	Загроза	Ймовірність	Вразливість	Джерело загрози	Порушення властивостей інформації
1.2	Епідемія	Середня	Активний розвиток нових штамів вірусів.	Зовнішнє	ЦД
1.3	Бойові дії (війна)	Середня	Підприємство знаходиться в області, яка межує з зоною ведення бойових дій.	Зовнішнє	ЦД
Техногенні					
2.1	Збій системи електроживлення	Висока	Зумовлюється застарілою ТП.	Зовіншнє	ЦД
2.2	Збій в роботі серверу	Висока	Збої в системі електроживлення	Внутрішнє	ЦД
2.3	Збій системи опалювання	Низька	Залежить від рівня навантаженості і працездатності котельні	Зовнішнє	ЦД
2.4	Відмова каналів зв’язку	Середня	Канали зв’язку арендовані	Внутрішнє	ЦД
Антропогенні					
3.1	Несанкціонова	Середня	Відсутність	Зовнішнє/	КЦД

	ний доступ в систему		контролю режиму доступу до кабінетів. Відсутність контролю за блокуванням робочого комп’ютера.	Внутрішнє	

Продовження таблиці 1.18

№	Загроза	Ймовірність	Вразливість	Джерело загрози	Порушення властивостей інформації
3.2	Зловживання правами в системі задля власних цілей	Висока	Неправильне розмежування доступу до інформації. Немає контролю за журналом подій	Внутрішнє	КЦД
3.3	Порушення режиму експлуатації технічних засобів	Низька	Відсутність контролю за режимом експлуатації	Внутрішнє	ЦД
3.4	Зараження системи вірусами комп’ютера	Висока	Необізнаність працівників Отримання фішингових листів поштою.	Внутрішнє	КЦД

			Відсутність контролю підключення сторонніх носіїв		

Згідно з табл. 1.18, можна зробити висновки, актуальними загрозами є:

- Збій електроживлення. Вразливість: Зумовлюється застарілою ТП. Наслідки: Поломка обладнання, зупинка роботи.
- Збій в роботі серверу. Вразливість: Збої в системі електроживлення. Наслідки: втрата важливої інформації
- Зловживання правами в системі задля власних цілей. Вразливість: Неправильне розмежування доступу до інформації. Наслідки: Втрата або спотворення конфіденційної інформації.
- Зараження системи вірусами комп'ютера. Вразливість: Необізнаність працівників, отримання фішингових листів поштою, відсутність контролю підключення сторонніх носіїв. Наслідки: Порушення безпеки інформації

1.5 Обгрунтування профілю захищенності

На основі проаналізованих загроз, вразливостей і визначених актуальних загроз і можливих порушників ІТС за основу беремо страндартні функцііональні профілі захищеності в КС, що входять до складу АС класу 3, з підвищеними вимогами до забезпечення конфіденційності, цілісності і доступності оброблювальної інформації які вказані в НД ТЗІ 2.5-005 -99 [4]

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

Рівень гарантій: Г-2

Але для повного захисту підприємства цього недостатньо, тому додаємо послугу КА-2, та підвищуємо послугу ЦО-1 до рівня ЦО-2, з цього виходить:

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

Введемо позначення однакових множин КС, до яких можуть відноситись різні послуги:

Множина об’єктів КС 1: інформація на дисковому просторі серверу.

Множина об'єктів КС 2: ПЗ(прикладне, спеціальне і системне), технологічна інформація, інформація, яка міститься в файлах і базах даних, що зберігаються на жорсткому диску сервера .

Множина об'єктів КС 3: інформація про співробітників, копії персональних данних працівників, інформація про контракти, бухгалтерські звіт, інформація про прибуток, інформація про урожайність , інформація про удій створюється, організаційно-розпорядчі документи, вартість основного обладнання, технологія годування тварин, інформація про рівень безпеки підприємства, технологічна інформація.

Обгрунтування послуг:

КД-2 Базова довірча конфіденційність – Множина об’єктів до яких відноситься ця послуга це множина об’єктів 3. КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта КЗЗ, Користувачі, які мають доступ до інформації що належить до множини об’єктів 3, які мають право одержувати інформацію від об'єкта КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити конкретних користувачів, які мають право ініціювати процес. Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації. Як частина політики довірчої конфіденційності повинні бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту

КА-2 Базова адміністративна конфіденційність - Множина об’єктів до яких відноситься ця послуга це множина 1. КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта. Запити

на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністратора КЗЗ, якому надані відповідні повноваження. КЗЗ повинен надавати можливість адміністратору КЗЗ, що має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретних користувачів, які мають право одержувати інформацію від об'єкта. КЗЗ, повинен надавати можливість адміністратору КЗЗ, що має відповідні повноваження, для кожного процесу через керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів, які мають право ініціювати процес. Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної конфіденційності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту

КО-1. Повторне використання об'єктів - Політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною.

КВ-1. Базова конфіденційність при обміні – Інформація до якої відноситься ця послуга це бухгалтерські звіти та інформація про удій. 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.

ЦД-1. Мінімальна довірча цілісність – Множина об’єктів до яких відноситься ця послуга множина 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. Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту

ЦО-2. Повний відкат - Політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів КС (множина 1), до яких вона відноситься Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити всі операції, виконані над захищеним об'єктом за певний проміжок часу.

ЦВ-2: Базова цілісність при обміні - Інформація до якої відноситься ця послуга це бухгалтерські звіти та інформація про удій і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовуваними механізмами, і спроможність користувачів і/або процесів керувати рівнем захищеності. КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається а також фактів його видалення або дублювання.

ДР-1. Квоти - Політика використання ресурсів, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься (множина: системний простір жорстких дисків). 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.

ДВ-1. Ручне відновлення - Політика відновлення, забезпечує повернення КС у захищений стан після відмови, або переривання обслуговування. Послуга

відноситься до операційної системи. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція КС. Після відмови КС або переривання обслуговування КЗЗ повинен перевести КС до стану, із якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження. Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути КС до нормального функціонуванн

НР-2. Захищений журнал - Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються. КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки:

-автентифікація користувача в системі (з урахуванням результату автентифікації)

-зміна групи користувачів;

-використання сторонніх зовнішніх носіїв (флешносії, жорскі диски)

-зміна атрибутів доступу;

- встановлення, оновлення та запуск ПЗ,

-зміна компонентів захисту КС;

-збої активації корпоративної ліцензії;

-збої перевірки сертифікату сайту;

-перегляд журналу безпеки;

-виведення документів на друк.

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. Переглядати може системний адміністратор, редагувати адміністратор безпеки, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації

НИ-2. Одиночна ідентифікація і автентифікація - Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ. Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен. автентифікувати цього користувача з використанням захищеного механізму. КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування. Реалізується однозначного введення ідентифікатора користувача та паролю у відповідності з вимогами складності, яка встановлюється політикою безпеки.

НК-2. Двонаправлений достовірний канал - Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного каналу. Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації та у випадках, коли необхідний прямий зв'язок користувач/КЗЗ або КЗЗ/користувач. Зв'язок з використанням даного каналу повинен ініціюватися користувачем або КЗЗ. Обмін з використанням достовірного каналу, що ініціює КЗЗ, повинен бути однозначно ідентифікований як такий і має відбутися тільки після позитивного підтвердження готовності до обміну з боку користувача. Повинна бути забезпечена або організаційними, або іншими мірами реалізація двостороннього достовірного двонаправленого каналу.

НО-2. Розподіл обов'язків адміністраторів - Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції. Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі. Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі. Повинна бути окремо користувачі і адміністратори з наступними ролями:

- Адміністратор системний – займається контролем працеспроможності системи ІТС
- Адміністратор безпеки – контролює журнал подій, передбачає підключення сторонніх носіїв.
- Адміністратор КЗЗ – забезпечує керування розподілом доступу
- Користувачі – працюють відповідно розподілу доступу який їм надали.

НЦ-2. КЗЗ з гарантованою цілісністю –Необхідно забезпечити перевірку цілісності системних файлів, файлів КЗЗ які забезпечують безпеку. КЗЗ повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування. Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

НТ-2. Самотестування при старті - Політика самотестування, що реалізується КЗЗ повинна тестуватися на технічні елементи, накопичувачі, пам’ять, 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.

НВ-1: Автентифікація вузла - Політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму. Використовуватиметься при віддаленому підключенні системного адміністратора, при оновлені системи. Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації

1.6 Висновок

В першому розділі розглянули загальні відомості про сільськогосподарське підприємство «Чумаки», обгрунтували необхідності створення КСЗІ, було виконане обстеження середовища функціювання ІТС, на базі цього був проведений аналіз актуальних загроз, та обгрунтування профілю захищеності. Потрібно проаналізувати рівень реалізації профілю захищеності, запропонувати апаратні рішення щодо реалізації послуг, які нереалізовані, або реалізовані частково

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Визначення рівня реалізації послуг безпеки

Для визначення рівня реалізації послуг безпеки потрібно провести аналіз вже реалізованих послуг, реалізованих частково або нереалізованих.

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

На підприємстві встановлений Microsoft Windows 10 Professional.який має затверджений профіль захищеності: КД-2, КВ-1, КО-1, ЦД-1, ЦА-1, ЦВ-1, ЦО-1, ДР-1, ДЗ-2, ДВ-2, НР-1, НР-2, НИ-1, НИ-2, НК-1, НО-3, НЦ-2, НТ-2, НВ-1 з рівнем гарантій Г-2 оцінки коректності їх реалізації згідно з НД ТЗІ 2.5-004-99

Згідно цього деякі послуги захищеності вже реалізовані в системі:

Реалізовані: КД-2, КО-1, ЦД-1, ДР-1, НР-2, НИ-2, НК-1 ,НР-1 , НЦ-2, НТ-2, НВ-1,

Частково реалізовані КВ-1, НВ-1

Нереалізовані: КА-2, ЦО-2, НО-2

2.2 Проектні рішення щодо реалізації вимог безпеки

2.2.1 Розмеження повноважень адміністраторів

Після аналізу загроз було прийнято рішення про стоворення служби безпеки інформації [7].

Задачі служби безпеки:

- Захист законних прав безпеки інформації підприємства під час інформаційної діяльності;
- Виявлення загроз, каналів витоку інформації, а також визначення заходів спрямованих на реалізацію політики безпеки іфнормації;
- Організація та координація впливу, пов'язана з захистом інформації;
- Розроблення проектів розпорядчих і нормативних документів орієнтованих на захист інформації;
- Контроль виконання користувачами і персоналом вимог нормативних і розпорядчих документів стосовно захисту інформації.

Для впровадження цієї служби необхідно розробити документи в відповідності з НД ТЗІ 1.4-001.

До складу служби безпеки інформації будуть входити: Керівник СБ, заступник керівника СБ, системний адміністратор.

Вони будуть наділені окремими ролями:

Адміністратор безпеки – керівник СБ

Обов'язки: повинен буде контролювати журнал подій

Адміністратор КЗЗ – заступник керівника СБ

Обов'язки: повинен надавати права в системі користувачам

2.2.2 Розмеження доступу

Також було прийнято рішення переглянути матрицю розмежування доступу і зменшити можливість доступу до деякої інформації співробітникам. Оновлену матрицю розмежування доступу вказано в табл. 2.1

Інформацію 12 Технологічна інформація (облікові записи, журнал подій, реєстр тощо) Розділимо на декілька підпунктів 12.1 інформація про облікові записи, 12.2 журнал подій, 12.3 доступ до реєстру

Таблиця 2.1- Оновлена матриця розмежування доступу

Об’єкт	Інформація*														Повноваження	Доступ до ресурсів
Користувач	1	2	3	4	5	6	7	8	9	10	11	12.1	12.2	12.3		
Директор	Ч	Ч	Ч	Ч	Ч	Ч	ЧС РВ ЕД	Ч	Ч	Ч	Ч	-	-	-	Ні	П К1 - 15
Зас. Директора з виробн.	Ч	ЧС РВ ЕД	-	Ч	ЧС РВ ЕД	-	ЧС РВ ЕД	-	ЧС РВ ЕД	-	Ч	-	-	-	Ні	П К 13
Зас. Директора з тварин.	Ч	ЧС РВ ЕД	-	Ч	ЧЕД	ЧС РВ ЕД	ЧС РВ ЕД	-	-	ЧС РВ ЕД	Ч	-	-	-	Ні	П К14
Бухгалтер	-	Ч	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	-	-	-	-	-	-	-	Ні	П К1 -4
Головний бухгалтер	ЧС РВ ЕД	Ч	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	Ч	-	-	Ч	-	-	-	Ні	П К5
Обліковець	-	Ч	Ч	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	-	-	-	-	Ні	П К9 - 12
Керівник СБ	ЧС РВ ЕД	ЧС РВ ЕД	-	Ч	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	Ч	Ч	ЧС РВ ЕД	-	-	-	Ні	П К6
Зас. Керівника	Ч	Ч	-	Ч	ЧС РВ	ЧС РВ	ЧС РВ	ЧС РВ	Ч	Ч	ЧС РВ	-	-	-	Ні	П

СБ					ЕД	ЕД	ЕД	ЕД			ЕД					К7

Продовження таблиці 2.1

Користувач	1	2	3	4	5	6	7	8	9	10	11	12.1	12.2	12.3		
Юрист – консультант	ЧСРВЕД	ЧРВЕД	-	-	-	-	ЧСРВЕД	-	-	-	Ч	-	-	-	Ні	ПК8
Системний адміністратор	-	-	-	-	-	-	-	-	-	-	-	Ч	Ч	ЧСРВЕД	Так	ПК1-15С.
Адміністратор безпеки	-	-	-	-	-	-	-	-	-	-	-	-	ЧСРВЕД	-	Ні	ПК1-15С.
Адміністратор КЗЗ	-	-	-	-	-	-	-	-	-	-	-	ЧСРВЕД	-	-	Ні	ПК1-15С.

*Номера інформації наведено згідно з табл. 1.8.

Умовні позначення доступу до інформації.

Ч- читання.

С-створення нових файлів.

Р-редагування.

В-видалення.

Е-імпорт або експорт.

Д-друк.

2.2.3Заходи протидії надслідкам збоїв системи живлення

Для забезпечення захисту ПК і серверу від збоїв системи електроживлення необхідно:

-для серверу встановити генератор

-для пк встановити блоки безперебійного живлення

Для забезпечння робити серверу у разі збою буде достатньо однофазного генератора, з номінальною потужністю 2.5 кВт

Серед представлених варіантів генераторів, було вирішено обрати генератор Konner&Sohnen BASIC KS 2800C, так як його буде повністю достатньо для живлення серверу у разі збою системи електро живлення, також 2 розетки на 220 В, вольтметр, захист від перевантаження, захист по рівню мастила. Варіанти генераторів вказані в табл 2.2

Таблиця 2.2

Марка	Модель	Номінальна потужність	Гарантія	Ціна в грн
MEDIA LINE	MLG 3500/1	2,5 кВт	12	16500
Konner&Sohnen	KS 2900G	2,5 кВт	12	19470
Zipper	ZI-STE2800	2,5 кВт	12	18500
Konner&Sohnen	BASIC KS 2800C	2,5 кВт	12	13510
Alimar	ALM-B-2500M	2,5 кВт	24	17500

Для коректного завершення роботи ПК, щоб коректно були завершені транзакції, необхідно забезпечити не довгострокове але підтримку напруги для обладнання, для цього використовуються блоки безперебійного живлення.

Серед представлених варіантів блоків безперебійного живлення, було вирішено обрати FSP FP650 (PPF3601406), так як його потужності вистачить для корректного завершення роботи, так як принтери не будуть підключатись до

блоків безперебійного живлення, Орієнтовно беремо потужність комп'ютера 350 ВТ. Варіанти блоків безперебійного живлення вказані в табл. 2.3

Таблиця 2.3

Марка	Модель	Потужність	Ємність батареї	Гарантія	Ціна в грн
EAST	EA650U.SH	650 ВА; 390Вт	7Аг	24	1838
EATON	5E650IUSB	650 ВА; 360Вт	7Аг	Без гарантії	1836
FSP	PPF3601406	650 ВА; 360Вт	7Аг	24	1575
FSP	PPF3602800	650 ВА; 360Вт	7Аг	24	1720

2.2.4 Заходи щодо реалізації політики адміністративної конфіденційності

Для реалізації послуг безпеки, яких недостатньо в системі необхідно встановити на сервер додаткове КЗЗ. Будемо розглядати ті, які вказані на сайті державної служби спеціального зв'яку та захисту інформації України[8].

Серед наведених на сайті підходять Система «ЛОЗА™-1» або КЗЗ комплекс «Гриф» версії 4. Порівняємо їх:

Ціна одного комплекту ЛОЗА™-1 – 7200 грн без ПДВ, в той час як «Гриф» версії 4 з різних джерел коштує приблизно 8000 грн

Рівень захисту ЛОЗА™-1 має рівень гарантій Г-4, «Гриф» версії 4 також має рівень гарантії Г-4

Профіль системи ЛОЗА™-1:КД-2, КА-2, КО-1, ЦД-1, ЦА-1, ДС-1, ДЗ-1, ДВ-1, НР-4, НИ-2/НИ-3, НК-1, НО-2, НЦ-2, НТ-2.

«Гриф» версії 4: КА-2, КО-1, ЦА-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-3, НИ-3, НК1, НО-2, НЦ-2, НТ-2.

Отож згідно цих данних, можна визначити, що для нашої системи більше підходить система «ЛОЗА™-1» так як вона має усі необхідні нам послуги, та є нижчою у вартості, а також має експертне заключення № 1095, яке видано

державною службою спеціального зв'яку та захисту інформації України , яке діє до 2 квітня 2023 року.

2.2.5 Заходи щодо реалізації резервного копіювання

Враховуючи важливість інформації, яка зберігається на сервері, було прийняте рішення встановити RAID масив, контролер вже є в сервері(PERC H710), який підтримує рівні рейд масивів RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, RAID 50, RAID 60 залишилось підібрати рівень RAID масиву серед доступних варіантів.

Розглянемо варінати рівнів масивів, які ми можемо підібрати, та серед них оберемо потрібний рівень. Варіанти вказані в табл. 2.4

Таблиця 2.4

Рівень	Кількість дисків	Надійність	Швидкість читання	Швидкість запису
RAID 0	>2	Низька	Висока	Висока
RAID 1	>2	Висока	Висока	Середня
RAID 5	>3	Середня	Висока	Середня
RAID 6	>4	Висока	Висока	Низька
RAID 10	>4, парна	Середня	Висока	Висока
RAID 50	>6 парна	Середня	Висока	Висока
RAID 60	>8 парна	Середня	Висока	Середня

Серед усіх наведених рівнів зупинимось на рівні RAID 1. Хоча масиви рівня RAID 1 мають недолік, при використанні цього масиву данні просто відзеркалюються на два диски, але у разі поломки одного з дисків другий буде працювати в штатному режимі і інформація буде збережена. Також, при його високій надійності, має мінімальні затрати- лише два жорсктих диски.

Для реалізації рівня RAID 1, потрібно придбати 2 жорстких диски. Обирати будемо за показниками ціни, та об'ємом

Серед усіх варіантив зупинимось на жорстких дисках Seagate IronWolf ST4000VN008 4 ТБ, так як в нього достатній об'єм і не висока ціна

Всі варіанти вказані в табл 2.5

Таблиця 2.5

№	Марка	Модель	Об’єм	Вартість в грн за 2 шт.
1	Seagate	IronWolf ST4000VN008	4 ТБ	6240
2	Western Digital	Gold Enterprise Class WD4003FRYZ	4 ТБ	13542
3	Seagate	Exos ST16000NM001	16 ТБ	23418
4	Western Digital	Purple WD20PURZ	2 ТБ	5038

2.2.6 Заходи щодо реалізації захищеного підключення

Так як системним адміністратором для віддаленого доступу використовується програма Teamviewer 15.30.3, яка не має достатнього рівня захисту облікового запису, тоді було прийняте рішення використання VPN. Так як ця послуга вже реалізована в системі Windows.

Рекомендую переходити організації на іншу версію додатку бухгалтерського обліку, так як одразу перейти це буде не можливо, а ліцензія закінчується, рекомендую підприємству переходити на інший продукт, який можливо навіть має деякі функції безпеки вже реалізовані

Також було прийняте рішення про встановлення нового антивірусу, так як антивірус, який встановлено на данний момент, не має експертного висновку.

Серед запропонованих в списку було обрано програмний продукт антивірусного захисту ESET Endpoint Antivirus для Windows виробництва ESET, spol. s r.o. (Словаччина) вартістю 2205 грн.

Данний антивірус має експертний висновок №1257 Дійсний з 17.06.2021 до 17.06.2024

Висновок

В другому розділі визначили рівень реалізації послуг, порівняли його з тим рівнем, що вже є, після чого визначили які послуги потрібно ще реалізувати.

В ході проектних рішень, було запропоновано варіанти розмежування повноважень адміністратора, розмежування доступу, було запропоновано вжити заходи, протидії наслідкам збоїв системи електроживлення, заходи щодо реалізації політики адіміністративної конфіденційності, заходи щодо реалізації резервного копіювання, заходи щодо реалізації захищеного підключення.

Якщо інтегрувати всі запропоновані заходи буде реалізована основна мета моєї роботи, а саме забезпечення необхідного рівня безпеки інформації яка обробляється в ІТС.

3 ЕКОНОМІЧНА ЧАСТИНА

3.1Розрахунок капітальних (фіксованих) витрат.

Основною метою економічного розділу є підтвердження економічної доцільності впровадження комплексної системи захисту інформації інформаційно-телекомунікаційної системи. До розрахунків входить:

1) розрахунок капітальних витрат на придбання та налагодження складових системи інформаційної безпеки або витрат, що пов'язані з виготовленням апаратури, приладів, програмного забезпечення;

2) розрахунок річних експлуатаційних витрат на утримання і обслуговування об'єкта проектування;

3) визначення річного економічного ефекту від впровадження об'єкта проектування;

4) визначення та аналіз показників економічної ефективності запропонованого проектного рішення;

5) підведення висновків щодо доцільності проектного рішення.

3.1.1 Визначення трудомісткості розробки політики безпеки інформації

$t = t_{тз} + t_в + t_а + t_{вз} + t_{озб} + t_{овр} + t_д$, годин (3.1.1)

де $t_{тз}$ – тривалість складання ТЗ на розробку політики;

$t_{тз} = 15$ годин;

$t_в$ – тривалість розробки концепції безпеки інформації в організації;

$t_в$ = 13 годин;

$t_а$ – тривалість процесу аналізу ризиків

$t_а$ = 17 годин;

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

$t_{вз}$ = 10 годин;

$t_{озб}$ – тривалість виробу основних рішень з забезепечення безпеки інформації;

$t_{озб}$ = 18 годин;

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

$t_{овр}$ = 19 годин;

$t_д$ – тривалість документального оформлення політики безпеки;

$t_д$ = 6 годин.

t=15+13+17+10+18+19= 98годин.

3.1.2 Розрахунок витрат на створення політики безпеки інформації.

$К_{рп} = З_{зп} + З_{мч}$, (3.1.2.1)

Де $К_{рп}$ – витрати на розробку політики безпеки інформації;

$З_{зп}$ – витрати на заробітну плату спеціалісту з інформаційної безпеки;

$З_{мч}$ – вартость витрат машинного часу, що необхідний для розробки політики.

$К_{рп}$ = 16874 + 468= 17342 грн.

Заробітна плата виконавця враховує основну і додаткову ЗП, відрахування на соціальні потреби.

$З_{зп} = t*З_{іб}$, грн, (3.1.2.2)

де t – загальна тривалість розробки політики безпеки, годин;

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

$З_{зп}$ = 98*103 = 10116 грн.

$З_{мч} = t*С_{мч}$, грн, (3.1.2.3)

де t – трудомісткість розробки політики на ПК, годин;

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

$З_{мч}$ = 98*8,3 = 813,4 грн.

$$Смч = P \cdot t_{нал} \cdot C_e + \frac{Ф_{зал} \cdot Н_a}{F_p} + \frac{К_{лпз} \cdot Н_{апз}}{F_p}, \text{ грн,} \quad (3.1.2.3)$$

Де Р – встановлена потужність ПК, кВт;

$t_{нал}$ – кількість задіяних робочих станцій при написанні політики;

$С_е$ – тариф на електроенергію, грн./кВт*година;(1,68 гривні за 1кВт·год.

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

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

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

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

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

$С_{мч}$ = 0,7*1*1,68 + ((9200*0,3)/1920) + ((2205*0,1)/1920) = 13,31 грн.

На підприємстві СПП «Чумаки» планується додатково використовувати програмні засоби наведені в таблиці 3.1

Програмний засіб	Вартість, грн
RAID 1 QNAP TR-002	6240
ЛОЗА™-1	7200
FSP PPF3601406 (x15)	23625
Konner&Sohnen BASIC KS 2800C	13510
ESET Internet Security	2205
Всього	52780

Капітальні (фіксовані) витрати на створення політики безпеки інформації:

$К = К_{пр} + К_{зпз} + К_{рп} + К_{аз} + К_{навч} + К_{н}$, (3.1.2.4)

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

$К_{пр} = 0$.

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

$К_{зпз} = 9405$ грн.

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

$К_{рп} = 17342$ грн.

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

$К_{аз} = 43375$ грн.

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн;

$К_{навч} = 2500$ грн.

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

$К_{н} = 0$.

$К = 0 + 9405 + 17342 + 43375 + 2500 + 0 = 68622$ грн.

3.2 Розрахунок поточних (експлуатаційних) витрат

Експлуатаційні витрати – поточні витрати на обслуговування об’єкта проектування за визначений період.

Річні поточні витрати на функціонування системи інформаційної безпеки:

$С = С_{в} + С_{к} + С_{ак}$, грн, (3.2.1)

де $С_{в}$ – вартість відновлення й модернізації системи;

$С_{в} = 6240$ грн.

$С_{к}$ – витрати на керування системою в цілому;

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

$С_{ак} = 0$.

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

$$С_к = С_н + С_а + С_з + С_{єв} + С_{ел} + С_о + С_{тос}, \text{ грн,} \quad (3.2.2)$$

де $С_н$ – це витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються за даними організації з проведення тренінгів персоналу, курсів підвищення кваліфікації;

$С_н = 2500$ грн.

$С_а$ – це річний фонд амортизаційних відрахувань визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів ($П_з$);

Вартість ПК, яка складає 138000 грн., ділимо на термін корисного використання, який складає 10 років, і отримаємо 13800 грн.

$С_а = 13800$ грн.

$С_З$ – це річний фонд заробітної плати інженерно–технічного персоналу, що обслуговує систему інформаційної безпеки;

$$С_з = З_{осн} + З_{дод}, \text{ грн.,} \quad (3.2.3)$$

Де основна заробітна плата ($З_{осн}$) визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата ($З_{дод}$) – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата спеціаліста з інформаційної безпеки – 19110 грн./місяць.

Виконання робіт вимагає залучення спеціаліста з інформаційної безпеки на 0,25 ставки.

$С_з = (10116 * 12 + 10116 * 12 * 0,1) * 0,25 = 33382,8$ грн.

З 01.12.2021 р. ставка ЄСВ (єдиний соціальний внесок) складає 22%.

$С_{єв} = 68622 * 0,22 = 1596,84$ грн.

$С_{ел}$ – вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року;

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.,} \quad (3.2.4)$$

де Р – встановлена потужність апаратури інформаційної безпеки;

$Р = 0,7$ кВт.

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

$F_р$ = 1920 год.

$Ц_е$ – тариф на електроенергію;

$Ц_е$ = 1,68 грн./кВт за годину.

$С_{ел}$ = 0,7*1920*1,68 = 2258 грн.

$С_{тос}$ – витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат - 1%.

$С_о$ – витрати на залучення сторонніх організацій для виконання деяких видів обслуговування та сертифікацію обслуговуючого персоналу;

$С_о$ = 0.

$С_{тос}$ = 68622 *0,01 = 686,22 грн.

$С_к$ = 2500 + 13800 + 33382,8 + 1596,84 + 2258 + 686,22 = 54223,68 грн.

Річні поточні витрати на функціонування системи інформаційної безпеки складають 54223,68 грн.

3.3 Оцінка можливого збитку від атаки (взлому) на вузол або сегмент корпоративної мережі

3.3.1 Оцінка величини збитку

Вихідні дані для розрахунку:

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

$t_п$ = 2 години;

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

$t_в$ = 3 години;

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

$t_{ви}$ = 1.5 години;

$З_о$ – заробітна плата системного адмістратора;

$З_о$ = 10116 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі;

$З_с$ = 20000 грн./міс.;

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

$Ч_о$ = 1 особа;

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

$Ч_с$ = 103 особи;

О – обсяг збитку атакованого вузла або сегмента корпоративної мережі;

О = 6000000;

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

I – число атакованих сегментів корпоративної мережі;

I = 1;

N – середнє число атак на рік,

N = 7.

Упущена вигода від простою атакованого сегмента корпоративної мережі:

$$U = П_п + П_в + V, \qquad (3.3.1.1)$$

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

$$П_п = \frac{\sum Зс}{F} \cdot t_п, \qquad (3.3.1.2)$$

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

$П_п$ = ((20000 * 104)/176)*2 = 23636,36 грн,

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

$$П_в = П_{ви} + П_{пв} + П_{зч}, \qquad (3.3.1.3)$$

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

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

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

$$П_{ви} = \frac{\sum Зс}{F} \cdot t_{ви}, \quad (3.3.1.4)$$

$П_{ви}$ = ((20000 *104)/176) *1,5 = 17727,27 грн.

$$П_{пв} = \frac{\sum Зо}{F} \cdot t_{в}, \quad (3.3.1.5)$$

$П_{пв}$ = ((10116 *1)/176) *3 = 172,43 грн.

$П_{в}$ = 17727,27 +172,43= 17899,7 грн.

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

$$V = \frac{O}{Fг} \cdot (t_{П} + t_{В} + t_{ВИ}), \quad (3.3.1.6)$$

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

V = (6000000/2080) * (2+3+1,5) = 18750 грн.

U = 23636,36 + 17899,7 + 18750 = 60286,06 грн.

Загальний збиток від атаки на сегмент корпоративної мережі організації:

$$B = \sum_i \sum_n U, \quad (3.3.1.7)$$

B = 1 * 7 * 60286,06 = 422002,42 грн.

3.3.2 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B \cdot R - C, \text{ грн.}, \quad (3.3.2.1)$$

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

B = 422002,42 грн.;

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

R = 60 %;

C – щорічні витрати на експлуатацію системи інформаційної безпеки;

C = 54223,68 грн.

E = 422002,42 * 0,6 – 54223,68 = 198977,77 грн.

3.4 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

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

$$ROSI = \frac{E}{K}, \text{ частки одиниці,} \qquad (3.4.1)$$

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

Е = 54223,68грн.

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

К = 198977,77 грн.

ROSI = 54223,68/198977,77 = 0,27

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

$$ROSI > (N_{деп} - N_{інф})/100), \qquad (3.4.2)$$

де $N_{деп}$ – річна депозитна ставка;

$N_{деп}$ = 8 %.

$N_{інф}$ – річний рівень інфляції;

$N_{інф}$ = 5 %.

Розрахункове значення коефіцієнта повернення інвестицій:

0,27> (8 – 5)/100 = 0,03

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

Т = 1/0,27 = 3,7 місяців.

В цьому розділі проведено розрахунки капітальних (фіксованих) витрат на створення політики безпеки інформації, які складають 68622 грн.; розрахунки поточних (експлуатаційних) витрат на функціонування системи інформаційної безпеки, які складають 54223,68 грн. Провели оцінювання можливого збитку від

атаки (взлому) на вузол або сегмент корпоративної мережі, де визначили, що загальний збиток від атаки на сегмент корпоративної мережі організації складає 422002,42 грн.. Розрахували загальний ефект від впровадження системи інформаційної безпеки, який складає 198977,77 грн.. Згідно з коефіцієнтом повернення інвестицій ROSI, який показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки, який складає 0,27 на 1 грн., а також з терміном окупності капітальних інвестицій, який складає 3,7 місяців, можемо зробити висновок, що проектне рішення, яке прийняте на підприємстві СПП «Чумаки» економічно доцільне.

ВИСНОВКИ

В першому розділі кваліфікаційної роботи розглянули загальні відомості про сільськогосподарське підприємство «Чумаки», обгрунтували необхідності створення КСЗІ, було виконане обстеження середовища функціювання ІТС, на базі цього був проведений аналіз актуальних загроз, та обгрунтування профілю захищеності. Потрібно проаналізувати рівень реалізації профілю захищеності, запропонувати апаратні рішення щодо реалізації послуг, які нереалізовані, або реалізовані частково

В другому розділі визначили рівень реалізації послуг, порівняли його з тим рівнем, що вже є, після чого визначили які послуги потрібно ще реалізувати.

В ході проектних рішень, було запропоновано варіанти розмежування повноважень адміністратора, розмежування доступу, було запропоновано вжити заходи, протидії наслідкам збоїв системи електроживлення, заходи щодо реалізації політики адіміністративної конфіденційності, заходи щодо реалізації резервного копіювання, заходи щодо реалізації захищеного підключення.

Якщо інтегрувати всі запропоновані заходи буде реалізована основна мета моєї роботи, а саме забезпечення необхідного рівня безпеки інформації яка обробляється в ІТС.

У третьому розділі кваліфікаційної роботи було підтверджено доцільність впровадження розроблених елементів політики безпеки через отримані дані.

ПЕРЕЛІК ПОСИЛАНЬ

1. Пункт 2 статті 21 Закону України «Про інформацію» https://zakon.rada.gov.ua/laws/show/2657-12#Text
2. Стаття 9 Закону України «Про захист інформації в інформаційно-комунікаційних системах» https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
3. Стаття 5 Закону України «Про захист персональних даних» https://zakon.rada.gov.ua/laws/show/2297-17#Text
4. НД ТЗІ 2.5-005 -99 https://do.nmu.org.ua/pluginfile.php/274497/mod_folder/content/0/%D0%9D%D0%94%20%D0%A2%D0%97%D0%86%202.5-005-99.pdf?forcedownload=1
    a. https://zakon.rada.gov.ua/laws/show/2657-12#Text
5. Стаття 1 Закону України «Про інформацію» https://do.nmu.org.ua/mod/resource/view.php?id=28521
6. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» https://tzi.com.ua/downloads/1.4-001-2000.pdf
7. Державна служба спец.зв'язку https://cip.gov.ua/ua/statics/pro-derszhpeczv-yazku
8. Методичні рекомендації до виконання кваліфікаційних робіт бакалаврів спеціальності 124 Кібербезпека/ Упоряд.: О.В. Герасіна, Д.С. Тимофєєв, О.В. Кручінін, Ю.А. Мілінчук – Дніпро: НТУ «ДП», 2020. – 47 с.
9. 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 Таблиця - Основні технічні засоби

Таблиця - Основні технічні засоби

№	Назва	Марка	Модель	Серійний номер	Розміщення	Відстань ОІД в м.	№ Каб
1	PC монітор (ПК1)	LG	22m38a-B	703NTCZBG419	На столі	1,6	1
2	PC монітор (ПК2)	LG	22m38a-B	0mo0IdB28Epv	На столі	3,4	1
3	PC монітор (ПК3)	LG	22m38a-B	WO6S3Bae94Zn	На столі	5,0	1
4	PC монітор (ПК4)	LG	22m38a-B	n9nBkGJG503g	На столі	2,1	1
5	PC монітор (ПК5)	LG	22m38a-B	pPBb9mU337ra	На столі	4,0	1
6	PC монітор (ПК6)	LG	22m38a-B	LPZ607okpe2C	На столі	1,9	2
7	PC монітор (ПК7)	LG	22m38a-B	rJ4A36Dtus5h	На столі	1,6	2
8	PC монітор (ПК8)	LG	22m38a-B	hI3497UronzQ	На столі	2,3	2
9	PC монітор (ПК9)	LG	22m38a-B	v9jG93o8rORD	На столі	2,1	2
10	PC монітор (ПК10)	LG	22m38a-B	1i70YqzE8PnD	На столі	1,1	2
11	PC монітор (ПК11)	LG	22m38a-B	G19kKB8F0Duc	На столі	0,8	2
12	PC монітор (ПК12)	LG	22m38a-B	Lv90rYpS07jK	На столі	2,0	2
13	PC монітор (ПК13)	LG	22m38a-B	kx4q6H8ZWF6Y	На столі	1,3	9
14	PC монітор (ПК14)	LG	22m38a-B	31SGHte0WZ1K	На столі	4,0	7
15	PC монітор (ПК15)	LG	22m38a-B	kT8CanQg3J01	На столі	3,3	8
16	PC блок (ПК1)	DELL	OptiPlex 3010 SFF	7B7hw7fQCN3e	На столі	1,6	1
17	PC блок (ПК2)	DELL	OptiPlex 3010 SFF	2nOtVi0Q5tJ1	На столі	3,5	1
18	PC блок (ПК3)	DELL	OptiPlex 3010	n3oWQ9j95QES	На столі	4,9	1

			SFF				
19	PC блок (ПК4)	DELL	OptiPlex 3010 SFF	xfwi4A99p4VN	На столі	2,1	1
20	PC блок (ПК5)	DELL	OptiPlex 3010 SFF	WJ9YS0V0qU4A	На столі	3,9	1
21	PC блок (ПК6)	DELL	OptiPlex 3010 SFF	pz164ap1uJeY	На столі	1,9	2
22	PC блок (ПК7)	DELL	OptiPlex 3010 SFF	4RvXDygf64u4	На столі	1,7	2
23	PC блок (ПК8)	DELL	OptiPlex 3010 SFF	1gX7kJ5jcY9m	На столі	2,4	2
24	PC блок (ПК9)	DELL	OptiPlex 3010 SFF	tUD8lR3A3k5b	На столі	2,0	2
25	PC блок (ПК10)	DELL	OptiPlex 3010 SFF	W4qJlNp6w1j9	На столі	1,1	2
26	PC блок (ПК11)	DELL	OptiPlex 3010 SFF	Dl56TdjLiW99	На столі	0,9	2
27	PC блок (ПК12)	DELL	OptiPlex 3010 SFF	mTGJAx44r2l6	На столі	1,9	2
28	PC блок (ПК13)	DELL	OptiPlex 3010 SFF	a0i1NLUxS3W2	На столі	1,3	9
29	PC блок (ПК14)	DELL	OptiPlex x3010SFF	jeGAC28Q5i5m	На столі	4,1	7
30	PC блок (ПК15)	DELL	OptiPlex 3010 SFF	A0KE6nNNiD15	На столі	3,3	8
31	Комутатор	D-Link	DGS-1210-28XS/ME	D8Istd7DZ24M	На стіні	3,1	8
33	Маршрутизатор	TP-LINK	DVB4231GL	D8Istd7DZ24M	На стіні	2,7	1

35	Принтер	Canon	PIXMA G1520	e3KkuT3 M1X0x	На столі	4,0	1
36	Принтер	Canon	PIXMA G1520	e3KkuT3 M1X0x	На столі	5,2	1
37	Принтер	Canon	PIXMA G1520	e3KkuT3 M1X0x	На столі	1,5	9
38	Принтер	Canon	PIXMA G1520	e3KkuT3 M1X0x	На столі	2,0	6
39	Принтер	Canon	PIXMA G1520	e3KkuT3 M1X0x	На столі	1,2	4
40	Сервер	Dell	R730xd	gj4Xxq6 EqaNQ	На столі	5,0	11
41	Клавіатура (15)	Logitech	MK120	Va5inB8 Ho5u0	На столі	1,5	

ДОДАТОК Б - Допоміжні технічні засоби

Таблиця - Допоміжні технічні засоби

№	**Назва**	**Марка**	**Модель**	**Серійний номер**	**Розміщення**	**Відстань ОІД в м.**
1	Кондиціонер	Hyundai	ARN12HSSUAWF1	W1Q3H2uY2DmF	На стіні	0,1
2	Холодильник	Atlant	X 1602-500	cwRD0Y975Dfb	На полу	2,1
3	Електро-чайник	Delfa	3401 X	qZ7wd87tZ6kp	На столі	3,0
4	Бойлер	Bosch	TR 1000T ES 80	S4hGu5rt7qL3	На стіні	5,0
5	Настільна лампа	Splendid Rey	N203B WT	91Ud1MwC6JZs	На столі	3,1
6	Комп'ютерна миша	Logitech	910-001794	MWG1om028ogi	На столі	1,5
7	Енергозберігаюча лампа (45)	Brille	E27 PL-SP 24W/864 techno Br	6AM9Xh	На стелі	2

ДОДАТОК В. Відгук керівника економічного розділу

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г Відгук керівника кваліфікаційної роботи

В І Д Г У К
на кваліфікаційну роботу студента групи 125-18-1
Біжка Івана Сергійовича
на тему: «Комплексна система захисту інформації інформаційно-телекомунікаційної системи СПП «Чумаки»»

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

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

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

Запропоновано оновлену матрицю розмежування доступу. Розроблені проектні рішення: з впровадження додаткового КЗЗ та підсистеми резервного копіювання; із заміни системи антивірусного захисту та забезпечення резервного електроживлення.

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

До недоліків відноситься недостатньо обґрунтована модель загроз та профіль захищеності та деякі проектні рішення.

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

За час дипломування Біжко І.С. 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 «добре».

Керівник кваліфікаційної роботи, професор Корнієнко В.І.

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