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 магістра

студента *Біжка Івана Сергійовича*

академічної групи *125м-22-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Система управління інформаційною безпекою сільськогосподарського підприємства «Чумаки»*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	проф. Корченко А.О.			
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
2023

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня магістра

Студенту ***Біжку Івану Сергійовичу*** **академічної групи** ***125м-22-1***
(прізвище та ініціали) (шифр)

спеціальності ***125 Кібербезпека***

спеціалізації

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

на тему ***Система управління інформаційною безпекою сільськогосподарського підприємства «Чумаки.***

Затверджену наказом ректора НТУ «Дніпровська політехніка» від 09.10.23 № 1227-с

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз системи управління інформаційною безпекою для сільськогосподарського підприємства	20.10.2023
Розділ 2	Розробка комплексу заходів та рекомендацій щодо створення системи управління інформаційною безпекою сільськогосподарського підприємства	28.11.2023
Розділ 3	Обгрунтування економічної доцільності використання наведеної в роботі створеної та впровадженої СУІБ на сільськогосподарському підприємстві	17.12.2023

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

Дата видачі завдання: 01.09.2023

Дата подання до екзаменаційної комісії: 06.12.2023

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

РЕФЕРАТ

Пояснювальна записка: 83 с., 8 рис., 18 табл., 6 додатків, 15 джерел.

Об’єкт розробки: інформаційно-комунікаційна система сільськогосподарського підприємства «Чумаки»

Предмет розробки: система управління інформаційною безпекою.

Мета роботи: забезпечення необхідного рівня захисту відповідно з міжнародними стандартами безпеки.

У першому розділі проаналізовано типове сільськогосподарське підприємство, з урахуванням цього розглянуто загальні відомості про сільськогосподарське підприємство «Чумаки», розглянуто інформаційні потоки на сільськогосподарському підприємстві «Чумаки». Проведено інвентаризацію активів, а також їхнє категоріювання. Також було проаналізовано та обрано метод експертної оцінки ризиків. Проведено оцінку захищеності. Проведено аналіз ризиків інформаційної безпеки на сільськогосподарському підприємстві «Чумаки», та вирахувано загрози з найбільшим рівнем ризику.

У другому розділі обрано заходи для захисту цінних активів, надано рекомендації щодо впровадження цих заходів, та визначено їх ефективність. Призначено відповідальних осіб за функціонування СУІБ , а також визначено роль керівництва в СУІБ.

В економічному розділі обґрунтована економічна доцільність використання, наведеної в роботі, створеної та впровадженої, СУІБ на сільськогосподарському підприємстві «Чумаки». Також було проведено визначення та аналіз показників економічної ефективності.

Новизна дослідження полягає в тому, що розроблені рекомендації зі створення системи управління інформаційною безпекою сільськогосподарських підприємств.

ПОЛІТИКА БЕЗПЕКИ ІНФОРМАЦІЇ, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, ІНФОРМАЦІЙНА БЕЗПЕКА, СІЛЬСЬКОГОСПОДАРСЬКЕ ПІДПРИЄМСТВО, ЗАХИСТ ІНФОРМАЦІЇ.

ABSTRACT

Explanatory note: 83 p., 8 pictures, 18 tables, 6 applications, 15 sources.

Object of development: information and communication system of the agricultural enterprise "Chumaki"

Subject of development: information security management system.

The purpose of the work: to ensure the necessary level of protection in accordance with international safety standards.

In the first section, a typical agricultural enterprise is analyzed, with this in mind, general information about the Chumaki agricultural enterprise is considered, information flows at the Chumaki agricultural enterprise are considered. An inventory of assets was carried out, as well as their categorization. An analysis was also carried out and a method of expert risk assessment was chosen, thanks to which a security assessment was carried out and an analysis of information security risks at the Chumaki agricultural enterprise was carried out, and threats with the highest risk level were calculated

In the second section, measures for the protection of valuable assets are selected, recommendations are provided for the implementation of these measures, and their effectiveness is determined. Persons responsible for the operation of the ISMS have been appointed, and the role of management in the ISMS has also been determined.

In the economic section, the economic expediency of using the ISMS created and implemented at the agricultural enterprise "Chumaki" given in the work is substantiated. Determination and analysis of economic efficiency indicators were also carried out.

The novelty of the research lies in the recommendations developed for creating information security management systems for agricultural enterprises.

INFORMATION SECURITY POLICY, INFORMATION SECURITY MANAGEMENT SYSTEM, INFORMATION SECURITY, AGRICULTURAL ENTERPRISE, INFORMATION PROTECTION

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ІБ – інформаційна безпека;

ІТ – інформаційні технології;

ТЗ – технічні засоби обробки інформації;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

СУІБ – система управління інформаційною безпекою;

СПП – сільськогосподарське підприємство;

ЗМІСТ

ВСТУП

В сучасному суспільстві інформаційний простір стає невід'ємною частиною стрімкого розвитку галузей наукової діяльності, пов'язаних із забезпеченням інформаційної безпеки. Зараз з цим розвитком виникають нові загрози, такі як використання неперевіреного програмного забезпечення, хакерські атаки, спам, або халатність співробітників, що часто стає причиною втрат даних.

Ці загрози можуть призвести до серйозних втрат для компаній. Тому на сьогодні кожне підприємство в різному обсязі використовує систему управління інформаційною безпекою (СУІБ) для захисту своєї інформації та носіїв. Ця система включає комплекс заходів і технічних засобів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації в організації чи підприємстві.

Важливо враховувати особливості конкретного підприємства під час розробки СУІБ. Кожне підприємство має свої унікальні особливості, які можуть впливати на вибір технічних рішень і стратегій інформаційної безпеки. Ретельний аналіз бізнес-процесів, інфраструктури та внутрішнього середовища дозволить розробити ефективну СУІБ, яка відповідає потребам та конкретним викликам підприємства.

Головною метою системи управління інформаційною безпекою є ефективний контроль і захист інформації від небажаних втручань, кіберзагроз, витоків даних, втрати важливої інформації та інших потенційних ризиків для інформаційної безпеки.

РОЗДІЛ 1.СТАН ПИТАННЯ.ПОСТАНОВКА ЗАДАЧІ

1.1 Обґрунтування необхідності створення СУІБ з урахуванням специфіки сільськогосподарського підприємства

В сучасних умовах розвитку сільського господарства, виробництво та управління даними стають ключовими елементами ефективності та конкурентоспроможності сільськогосподарських підприємств. З урахуванням стрімкого технологічного прогресу та росту обсягів інформації, яка обробляється в сфері агробізнесу, виникає необхідність впровадження сучасних систем управління інформаційною безпекою. Особливо актуальним стає це питання для сільськогосподарських підприємств

Створення та впровадження СУІБ на сільськогосподарських підприємствах відкриває нові можливості для оптимізації управління, підвищення рівня безпеки даних та забезпечення стійкості бізнес-процесів у сучасному інформаційному середовищі. Це стає стратегічним кроком для забезпечення конкурентоспроможності на ринку та виробництві продукції в умовах постійних змін та викликів.

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. [1]

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. [2]

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. [3]

Згідно пункту 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.[4]

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 основного обладнання, зарплата, особисті данні співробітників. [5]

1.2 Етапи розроблення СУІБ

СУІБ розробляється в ряді етапів, щоб забезпечити ефективний та комплексний захист інформації в організації. В табл. 1.1 наведені етапи розроблення СУІБ. Ці етапи утворюють цикл управління інформаційною безпекою, який дозволяє системі адаптуватися до змін у середовищі, виявляти та виправляти вразливості, а також підвищувати рівень безпеки в організації.

Таблиця 1.1– Етапи розроблення СУІБ

Етап	Детальний розбір етапу
1. Аналіз стану ІБ	Аналіз особливостей типового підприємства
1. Аналіз стану ІБ	Збір інформації про структуру бізнеса та процеси підприємства.
2. Заходи з організації ІБ	Обов'язки керівництва з управління ІБ Призначення відповідальних осіб за функціонування СУІБ
3. Інвентаризація активів	Опис активів підприємства Категоріювання активів підприємства
4. Оцінка ризиків	Визначення найбільш відповідного методу оцінки ризиків Визначення загроз та ризиків Оцінка рівня інформаційних ризиків Оцінка можливостей загроз Вибір засобів захисту для зниження ризиків
5. Введення заходів щодо моніторингу ефективності СУІБ	Розробка документації для перевірки проведення внутрішнього аудиту СУІБ

Розробку СУІБ необхідно виконувати з урахуванням специфіки сільськогосподарського підприємства.

1.2.1 Аналіз типового сільськогосподарського підприємства

На сьогоднішній день, з високими темпами розвитку економічної сфери, а також з різким погіршенням екології, головним етапом економічного перетворення, який відбувається в сфері сільського господарства, є пошук та створення тих умов, які зможуть дати можливість підприємству працювати ефективніше, але при цьому не завдавати шкоди екології. Ефективне сільське

господарство, яке може продуктивно працювати, при цьому зберігаючи екологію для майбутніх поколінь, називають - сталим сільським господарством.

Технології сталого сільського господарства сприяють стабільному та безперервному виробництву, що в свою чергу дозволить забезпечити достатню кількість ресурсів у майбутньому. Згідно з Продовольчою та сільськогосподарською організацією Об'єднаних Націй така практика включає п'ять принципів:

- покращення харчового ланцюга;
- захист та економію природних ресурсів;
- поліпшення добробуту та економічного стану людей;
- стимулювання стійкості екосистем та угруповань;
- підтримку державних ініціатив та нормативних актів.[6]

Ефективне сільське господарство не можливо уявити без використання нових інформаційних технологій для оптимізації процесу виробництва. Сільськогосподарські підприємства, як і підприємства в інших галузях, стикаються з викликами і вимогами щодо забезпечення інформаційної безпеки. Особливості цієї галузі визначаються специфікою діяльності та умовами, в яких працюють сільськогосподарські підприємства. Розглянемо основні особливості інформації в цій галузі:

- Автоматизовані системи управління фермою:

Багато ферм використовують автоматизовані системи для контролю над різними процесами, такими як полив, годівля тварин, контроль за температурою тощо. Ці системи пов'язані з інтернетом, що може зробити їх вразливими до кібератак.

- Дані про виробництво:

Сільськогосподарські підприємства збирають великі обсяги даних про виробництво, такі як інформація про площі посівів, урожайність, розподіл добрив, погодні умови і т.д. Ця інформація може бути цінною для конкурентів чи зловмисників, тому її захист є важливим завданням.

- Залежність від мереж:

Велика частина сільськогосподарських підприємств знаходиться в віддалених районах, де можуть бути обмежені можливості доступу до стабільних і швидких мереж. Це може створювати виклики для впровадження заходів з інформаційної безпеки.

- Зберігання особистих даних:

Сільськогосподарські підприємства також можуть зберігати особисті дані своїх співробітників, клієнтів та інших сторін, що вимагає відповідної уваги до приватності та захисту цих даних.

- Освіта та навчання персоналу:

Забезпечення інформаційної безпеки також передбачає навчання персоналу, щодо відповідних практик безпеки, усвідомлення ризиків та заходів, що слід вживати для їх зменшення.

Далі в роботі розглядається конкретний випадок сільськогосподарського підприємства "Чумаки" та вивчатимуться заходи з покращення інформаційної безпеки для забезпечення сталого розвитку у сільському господарстві.

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

Сільськогосподарське підприємство «Чумаки» засноване в 2001 р., в с. Чумаки, 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 племінного молодняка загальна кількість 1211 голів.

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

Штат підприємства включає в себе 103 особи.

Організаційна структура підприємства зображена на рис. 1.1.

Директор підприємства орган управління підприємством виконує наступні функції:

- управління виробництвом;
- контроль, розподілення фінансових потоків;
- самостійно обирає план реалізації продукції;
- затвердження плану закупівлі;
- затвердження кадрових рішень;

Заступник директора з тваринництва на своїй посаді 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 слюсаря-ремонтника. А також виконує такі обов'язки :

- виробництво продукції тваринництва;
- годівля стада;
- утримання стада;
- відтворення стада;
- кормозаготівля;
- додержання технологічного процесу продукції тваринництва;

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 слюсаря.

Інженер з охорони праці:

- контроль за дотримуванням умов праці відповідно до чинного законодавства;
- закупівля спеціального одягу;

- закупівля спеціальних засобів;
- навчання працівників з техніки безпеки;

Головний бухгалтер:

- контроль ведення бухгалтерського обліку;
- нарахування заробітної плати;
- нарахування орендної плати за використання земельного паю;
- сплати податків і зборів до держбюджету;

Має в підпорядкуванні: чотирьох бухгалтерів, сім обліковців та спеціаліста в роботі з пайовиками.

Керівник служба безпеки:

- охорона території;
- збереження майна і цілісності підприємства;
- перевірка належного проведення закупівлі і продажу товарів;

Має в підпорядкуванні: замісника керівника служби безпеки та двадцять два спеціаліста служби безпеки.

Юрист-консультант:

- контроль оформлення юридичних договорів;
- представлення інтересів підприємства в судах;
- дотримання всіх мір і вимог законодавства при веденні господарчої діяльності підприємства;

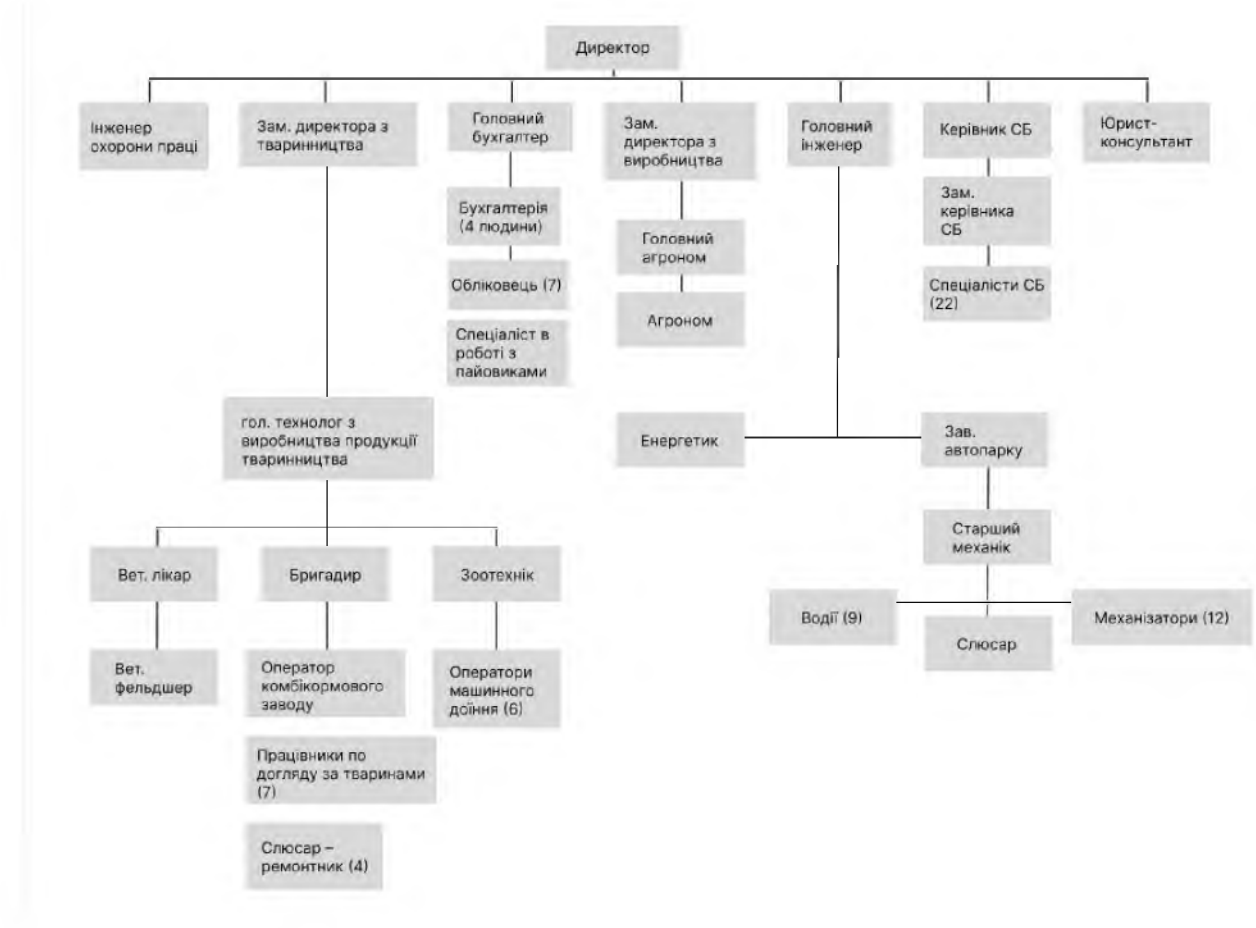

Рисунок 1.1 – Організаційна структура підприємства

1.2.3 Інформаційні потоки на сільськогосподарському підприємстві “Чумаки”

Інформаційні потоки стають невід'ємною частиною процесу розвитку підприємств сільського господарства, забезпечуючи обмін даними між обладнанням, робочими процесами, управлінським персоналом та іншими елементами сільськогосподарської інфраструктури. В сільськогосподарському підприємстві “Чумаки” схема інформаційних потоків виглядає так, як вказано на рис.2

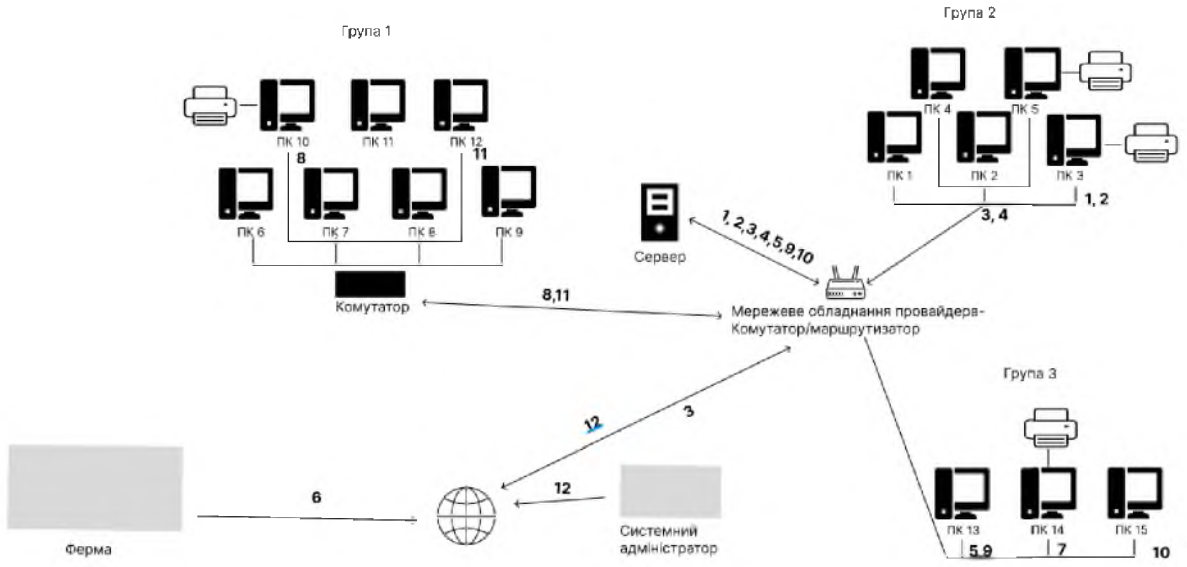

Рисунок 1.2 – Інформаційні потоки

В табл. 1.2 вказано класифікацію інформації.

Таблиця 1.2– Класифікація інформації

№	Інформація	Вид представлення інформації
1	Інформація про співробітників, копії персональних даних працівників.	Паперовий, електронний
2	Інформація про контракти.	Паперовий, електронний
3	Бухгалтерські звіти.	Паперовий, електронний
4	Інформація про прибуток.	Паперовий, електронний
5	Інформація про урожайність.	Паперовий, електронний
6	Інформація про удій.	Паперовий, електронний
7	Організаційно-розпорядчі документи.	Паперовий, електронний

Продовження таблиці 1.2

№	Інформація	Вид представлення інформації
8	Вартість основного обладнання.	Паперовий, електронний
9	Технологія вирощування зернових культур.	Електронний
10	Технологія годування тварин.	Електронний
11	Інформація про рівень безпеки підприємства.	Електронний
12	Технологічна інформація (облікові записи, журнал подій, реєстр тощо)	Електронний

Номер інформації в табл. 1.2 відповідає номеру інформації на рис. 1.2

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.

Матрицю розмежування доступу вказано в табл. 1.3

Таблиця 1.3 – 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	П К1 - 15

Продовження таблиці 1.3

Об’єкт	Інформація*												Повноваження Інсталювання ПЗ	Доступ до ресурсів
Користувач	1	2	3	4	5	6	7	8	9	10	11	12		
Зас. Директора з виробн.	Ч	ЧС РВ ЕД	-	Ч	ЧС РВ ЕД	-	ЧС РВ ЕД	-	ЧС РВ ЕД	-	Ч	-	Так	П К 13
Зас. Директора з тварин.	Ч	ЧС РВ ЕД	-	Ч	ЧЕ Д	ЧС РВ ЕД	ЧС РВ ЕД	-	-	ЧС РВ ЕД	Ч	-	Так	ПК14
Бухгалтер	-	Ч	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	-	-	-	-	-	Так	ПК1-4
Головний бухгалтер	ЧС РВ ЕД	Ч	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	Ч	-	-	Ч	-	Так	ПК5
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	ПК9-12
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	ПК6
Зас. Керівника СБ	Ч	Ч	-	Ч	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	Ч	Ч	ЧС РВ ЕД	-	Так	ПК7
Юрист – консультант	ЧС РВ ЕД	Ч РВ ЕД	-	-	-	-	ЧС РВ ЕД	-	-	-	Ч	-	Так	ПК8

Продовження таблиці 1.3

Об'єкт	Інформація*												Повноваження Інсталювання ПЗ	Доступ до ресурсів
Користувач	1	2	3	4	5	6	7	8	9	10	11	12		
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	ПК1-15

*Номера інформації наведено згідно з табл. 1.2

Умовні позначення доступу до інформації.

Ч- читання.

С-створення нових файлів.

Р-редагування.

В-видалення.

Е-імпорт або експорт.

Д-друк.

1.2.4 Інвентаризація активів на сільськогосподарському підприємстві "Чумаки"

Інвентаризацію активів на сільському господарстві «Чумаки» наведено в Додатку А. Програмне забезпечення яке використовується на підприємстві вказане в табл. 1.4

Таблиця 1.4 – Програмне забезпечення

№	Назва програмного забезпечення	Ліцензія	Тип програмного забеспечення
1	AnyDesk 6.2.6	Безкоштовна	Прикладне
2	Teamviewer 15.30.3	Безкоштовна	Прикладне
3	1с бухгалтерія 8.3	Комерційна до (13.10.2024)	Прикладне

Продовження таблиці 1.4

№	Назва програмного забезпечення	Ліцензія	Тип програмного забеспечення
4	Кліент-банк	Безкоштовна	Прикладне
5	Opera 75.0.3969.171	Безкоштовна	Прикладне
6	Google Chrome 102.0.5005.61/63	Безкоштовна	Прикладне
7	WinRAR 6.11	Безкоштовна	Прикладне
8	Avast 21.6.2474	Комерційна до (20.09.2024)	Спеціалізоване
9	Uniform Agri 5.4	Комераційна	Прикладне
10	Dairy Plan 5.2	Комерційна	Прикладне
11	Windows 10 Pro	Комерційна	Системне
12	Пакет програм Microsoft Office 2019 Home & Business	Комерційна	Прикладне
13	MS SQL Server 15.0.2000.5	Комерційна	Системне
14	Студия управления MS SQL Server	Комерційна	Системне
15	Windows 10 Server 2019	Комерційна	Системне

1.2.5 Категоріювання активів на сільськогосподарському підприємстві “Чумаки”

На цьому етапі створення СУІБ потрібно розділити активи компанії на категорії. Типи категорій та їх залежність один від одного вказана на рис. 1.3

Рисунок 1.3 – Типи категорій та їх залежність

Розділення починається з категорії бізнес активи, до бізнес активів відносяться клієнт-банк, e-mail. Бізнес активи сільськогосподарського підприємства «Чумаки» вказані в табл. 1.5

Таблиця 1.5 Бізнес активи сільськогосподарського підприємства «Чумаки»

№	Назва	Ціна в грн
1.	Пл. молочний комплекс Лугова ,1	1892 215,01
2	Будівлі та споруди польово стану номер 2 заг площею 1260 м2	95709,38
3	Будівлі та споруди польово стану номер 2 заг площею 934,2 м2	70957,58
4	Вагова Центральна 38А	60001,00
5	Вагова Відділення номер 2	94625,00
6	Комплекс зерно-склад	160425,00
7	Контора	782927,59
8	Котельня	149456,43
9	Машинний двір номер 1	198527,72
10	Машинний двір номер 2	131869,00

В таблиці1.6 вказані ІТ сервіси які використовуються на сільськогосподарському підприємстві «Чумаки»

Таблиця 1.6 ІТ сервіси сільськогосподарського підприємства «Чумаки»

№	Назва	Ліцензія
1	AnyDesk 6.2.6	Безкоштовна
2	Teamviewer 15.30.3	
3	1с бухгалтерія 8.3	Комерційна до (13.10.2024)
4	Кліент-банк	Безкоштовна
5	Opera 75.0.3969.171	Безкоштовна

Продовження таблиці 1.6

№	Назва	Ліцензія
6	Google Chrome 102.0.5005.61/63	Безкоштовна
7	WinRAR 6.11	Безкоштовна
8	Avast 21.6.2474	Комерційна до (20.09.2024)

В табл. 1.7 вказані програмні забезпечення та бази даних якими користується підприємство

Таблиця 1.7 Програмні забезпечення та бази даних сільськогосподарського підприємства «Чумаки»

№	Назва	Ліцензія
1	Windows 10 Pro	Комерційна
2	Пакет програм Microsoft Office 2019 Home & Business	Комерційна
3	MS SQL Server 15.0.2000.5	Комерційна
4	Студия управления MS SQL Server	Комерційна
5	Windows 10 Server 2019	Комерційна
6	Uniform Agri 5.4	Комерційна
7	Dairy Plan 5.2	Комерційна

В додатку Б вказане обладнання яке використовується на сільськогосподарському підприємстві «Чумаки»

В табл 1.8 вказана інженерна інфраструктура яка служить для функціонування підприємства

Таблиця 1.8 Інженерна інфраструктура сільськогосподарського підприємства «Чумаки»

№	Назва	Ціна
1	Блок безперебійного живлення (СПП Чумаки)	9807,50
2	Генератор GENERATOR Fe Power 220 kva	729 000,00
3	Джерело безперебійного живлення (СПП Чумаки)	7547,00
4	Фільтр живлення мережевий (СПП Чумаки)	57,80
5	Фільтр мережевий (СПП Чумаки)	83,13

1.2.6 Аналіз методів експертних оцінок

Один із ключових аспектів управління кібербезпекою полягає в адекватному визначенні та оцінці ризиків, пов'язаних з інформаційною безпекою підприємств. Для досягнення цієї мети, використання методів експертних оцінок стає невід'ємною складовою. На цьому етапі більш детальніше розглядається та проводиться аналіз деяких методів оцінки ризиків і визначається, який підходить найбільше.

Метод оцінки ризиків — один з основних класів методів науково-технічного прогнозування, який ґрунтується на припущенні, що на основі думок експертів можна збудувати адекватну модель майбутнього розвитку об'єкта прогнозування.

Ризик кібербезпеки – це комплексна величина, яка визначається, як функція ряду факторів: загроза, потенційно можлива шкода, вразливість інформаційної системи. Фактори загрози та потенційно можливої шкоди в поєднанні визначають ймовірність настання негативного впливу (події).

Методи для вирішення задачі оцінки можна розділити на кількісні та якісні.

Кількісні методи використовують числові дані для оцінки ризиків та вимагають більше обчислювальних ресурсів. Вони дозволяють чисельно оцінити параметри ризику, а також проводити аналіз витрат та прибутку при виборі заходів безпеки. Однак вони можуть бути складні у використанні та вимагати точних даних.

Якісні методи, навпаки, не використовують числові дані і надають загальні, якісні оцінки. Вони можуть бути швидкими та дешевими в реалізації. Однак вони не дозволяють визначити точні ймовірності та результати в числовому виразі.

Кожна група методів має свої переваги та недоліки, які наведено в табл. 1.8

Для того, щоб мінімізувати недоліки цих методів, можна просто поєднати кількісні та якісні методи.

Таблиця 1.9 - Методи оцінки

Методи оцінки	Недоліки	Переваги
Кількісні методи	1) Кількісні міри залежать від об'єму та точності шкали виміру. 2) Результати оцінки можуть бути неточними. 3) Повинні доповнюватись якісними характеристиками. 4) Оцінка з застосуванням цих методів зазвичай потребує більше досвіду та сучасного інструментарію	1) Дозволяють чисельно оцінити необхідні параметри. 2) Реалізовують аналіз витрат та прибутку при виборі захисту. 3) Надають більш точне відображення шуканих значень.
Якісні методи	1) Не дозволяють визначити ймовірності та результати з використанням числових коефіцієнтів. 2) Аналіз витрат та користі при виборі захисту важчий. 3) Отримані результати мають загальний, наближений характер.	1) Дозволяють визначити області критичних рівнів в короткий проміжок часу без значних витрат. 2) Дозволяють оцінювати відносно легко та дешево.

Кількісні методи:

Імітаційне моделювання та ймовірність виконання: Цей метод використовує математичні моделі для емуляції складних систем та розрахунку ймовірності виконання певних подій. Це кількісний метод, оскільки основний акцент робиться на числових оцінках та імітації процесів.

Якісні методи:

Метод Дельфі: Цей метод включає в себе консультації експертів для досягнення консенсусу, щодо певного питання або оцінки ризиків. Це, зазвичай, якісний метод, оскільки основний акцент робиться на якості думок та оцінках, а не на числових даних.

Метод CORAS: CORAS (Computer-aided Risk Analysis for Secure Systems) - це якісний метод аналізу ризиків, спрямований на оцінку інформаційної безпеки систем, а не на кількісний розрахунок.

Метод ситуаційного аналізу: Цей метод використовується для розгляду ситуацій, в яких ризики можуть виникнути, та аналізу можливих наслідків цих ситуацій. Це також якісний метод, оскільки акцент робиться на аналізі ситуацій.

Логіко-ймовірнісний підхід: Цей підхід поєднує логічні та ймовірнісні методи для аналізу ризиків інформаційної безпеки, і може включати якісні аспекти.

Імовірнісний аналіз безпеки: Цей метод визначає ймовірність виникнення ризиків інформаційної безпеки та оцінює їх потенційні наслідки, і може включати як якісні, так і кількісні аспекти.

У табл. 1.10 міститься матриця, де відображені критерії вибору зазначених вище методів. Ці критерії важливі при застосуванні цих методів для оцінки ризиків в області кібербезпеки критичної інформаційної інфраструктури.

Таблиця 1.10 - Матриця критеріїв вибору зазначених методів

Критерії	Методи					
	Метод Дельфі	Імітаційне моделювання та ймовірність виконання	Метод CORAS	Метод ситуаційного аналізу кібербезпеки	Логіко-ймовірнісний підхід	Імовірнісний аналіз безпеки
Аналіз потоків даних в інформаційній системі	-	-	+	+	-	-
Побудова функціональної моделі системи	-	+	+	+	+	+
Кількісна оцінка ризиків	-	+	+	+	+	+
Якісна оцінка ризиків	+	-	+	-	-	-
Оцінка існуючих заходів безпеки	+	+	+	+	+	+
Збір/використання статистичних даних	+	+	+	+	-	+
Проведення експериментів/тестування	-	+	-	-	-	-
Врахування зовнішніх впливів (людський фактор)	+	-	+	-	+	+
Оцінка надійності технічних систем	-	+	-	-	+	+
Прогнозування стану кібербезпеки	-	+	-	+	-	+
Реалізація управління ризиками	-	-	+	+	+	+
Економічна оцінка захисту інформації	+	+	+	-	+	-
Застосовність для оцінки ризиків кібербезпеки	+	+	+	+	+	-
Застосовність у сфері ядерної енергетики	+	+	+	+	+	+

Використовуючи табл. 1.10 можна визначити, що найбільше для сільськогосподарського підприємства «Чумаки» підходить метод експертної оцінки CORAS, так як він дає можливість кількісно та якісно оцінити ризики.

1.2.7 Оцінка захищеності інформаційної безпеки на сільськогосподарському підприємстві “Чумаки”

Для належної оцінки захищеності інформаційної безпеки, для початку потрібно зазначити, що не вся інформація на підприємстві повинна підлягати максимальному рівню захищеності, тому інформація в організації поділяється на критичну та чутливу[7]

Критична інформація, надзвичайно важлива інформація, яка забезпечує життєдіяльність підприємства, доступ до якої повинен бути лише тоді, коли є

необхідність в цій інформації. Поділення інформації за ступенем критичності вказано на схемі на рис 1.4

Рисунок 1.4 – Поділення інформації за ступенем критичності

Поділення інформації за ступенем чутливості ї вказано на схемі на рис 1.5

Рисунок 1.5 – Поділення інформації за ступенем чутливості

В свою чергу за ступенем критичності щодо доступності інформація поділяється так як вказано на рис 1.6

Рисунок 1.6 – Поділення інформації за ступенем критичності щодо доступності інформації

За рівнем критичності щодо цілісності поділення вказано на рис 1.7

Рисунок 1.7 – Поділення інформації за ступенем критичності щодо цілісності

Щодо конфіденційності інформація поділяється так як вказано на рис 1.8

Рисунок 1.8 – Поділення інформації за ступенем критичності щодо конфіденційності

Одна і та ж інформація може одночасно поділятися за різними класифікаціями, тому в табл. 1.11 була розглянута вся класифікація. Об'єктом захисту є конфіденційна інформація

Таблиця 1.11 Оцінка інформації

Вид інформації	Класифікація оцінювання				
	За ступенем критичності	За ступенем чутливості	За ступенем критичності щодо доступності	За ступенем критичності щодо цілісності	За ступенем критичності щодо конфіденційності

Продовження таблиці 1.11

Вид інформації	Класифікація оцінювання				
	За ступенем критичності	За ступенем чутливості	За ступенем критичності щодо доступності	За ступенем критичності щодо цілісності	За ступенем критичності щодо конфіденційності
Інформація про співробітників, копії персональних данних працівників.	Важлива	Чутлива	Важлива	Важлива	Критична
Інформація про контракти.	Суттєва	Високо чутлива	Дуже важлива	Критична	Дуже важлива
Бухгалтерські звіти	Суттєва	Чутлива	Важлива	Критична	Дуже важлива
Інформація про прибуток.	Суттєва	Чутлива	Важлива	Критична	Критична
Інформація про урожайність.	Суттєва	Чутлива	Важлива	Критична	Критична
Інформація про удій.	Суттєва	Чутлива	Важлива	Критична	Критична
Організаційно-розпорядчі документи.	Нормальна	Внутрішня	Корисна	Незначна	Незначна

Продовження таблиці 1.11

Вид інформації	Класифікація оцінювання				
	За ступенем критичності	За ступенем чутливості	За ступенем критичності щодо доступності	За ступенем критичності щодо цілісності	За ступенем критичності щодо конфіденційності
Технологія вирощування зернових культур.	Суттєва	Високо чутлива	Критична	Критична	Критична
Технологія годування тварин.	Суттєва	Високо чутлива	Критична	Критична	Критична
Інформація про рівень безпеки підприємства.	Суттєва	Високо чутлива	Критична	Критична	Критична
Технологічна інформація (облікові записи, журнал подій, реєстр тощо)	Суттєва	Високо чутлива	Критична	Критична	Критична

1.2.8 Оцінка ризиків інформаційної безпеки на сільськогосподарському підприємстві "Чумаки"

Використовуючи метод експертної оцінки CORAS можна прорахувати рівень ризику для загроз інформаційної безпеки.

Для цього в першу чергу потрібно зібрати групу експертів, які візьмуть на себе виявлення найбільш актуальних загроз інформаційної безпеки даного підприємства.

До групи експертів були запрошені:

- директор;
- керівник служби безпеки;
- головний інженер;

Після опитування були виявлені такі ризики інформаційної системи:

- пошкодження будівлі через стихійні лиха
- ризик втрати виробничих активів внаслідок воєнних дій.
- збій системи електроживлення
- відмова каналів зв'язку
- порушення режиму експлуатації технічних засобів
- несанкціоноване підключення до ТЗ за допомогою фішингових листів
- втрата або розголошення паролів доступу до системи
- ризик несанкціонованого доступу, через велику кількість прав в системі у системного адміністратора

Рівень ризику розраховується за формулою 1.1

$$R = I * P * 100\% \quad (1.1)$$

де R – рівень ризику;

P – ймовірність;

I – вплив;

Інтерпретація Результату:

Рівень ризику зазвичай інтерпретується наступним чином:

- 0% - 10% дуже низький
- 11% - 20% низький ризик
- 21% -40% нижче середнього
- 41% - 50% середній ризик

- 51% - 70% вище середнього
- 71% - 80% високий ризик
- 81% - 100% дуже високий ризик

Розрахуємо рівень ризику кожної події за формулою 1.1

- пошкодження будівлі через стихійні лиха

Ймовірність низька оскільки будівлі не знаходяться в зоні потенційного стихійного лиха P = 0.2.

Вплив середній оскільки серйозне пошкодження будівлі може зупинити роботу підприємства на деякий час I = 0.5.

$$R = 0.5 * 0.2 * 100\%$$

- ризик втрати виробничих активів внаслідок воєнних дій.

Ймовірність середня, оскільки підприємство знаходиться в області яка межує з зоною бойових дій P = 0.5

Вплив великий оскільки у разі втрати виробничих активів є можливість того що подальша робота підприємства буде неможлива I = 0.8

$$R = 0.3 * 0.8 * 100\%$$

- збій системи електроживлення

Ймовірність з огляду на воєнні дії та можливу атаку на енергетичні системи, ймовірність оцінюється дуже високо P = 0.9

Вплив нижче середнього так як у разі вимкнення світла на невеликі проміжки часу у підприємства є можливість використовувати генератори для стабільної роботи P =0.3

$$R = 0.9 * 0.3 * 100\%$$

- відмова каналів зв’язку

Ймовірність дуже низька так як усі домовленості за контрактом з постачальником виконуються в термін P = 0.1

Вплив середній так як у разі відмови каналів зв'язку частково паралізується робота підприємства I = 0.5

$$R = 0.1 * 0.5 * 100\%$$

- порушення режиму експлуатації технічних засобів

Ймовірність оцінюється як висока через низьку обізнаність персоналу P =0.8

Вплив визначено як високий, оскільки у разі поломки можлива втрата даних та часткова паралізація підприємства I = 0.8

$$R = 0.8 * 0.8 * 100\%$$

- несанкціоноване підключення до ТЗ за допомогою фішингових листів

Ймовірність оцінюється як вище середнього через високу активність шахраїв P =0.6

Вплив визначено як високий, оскільки у разі несанкціонованого підключення до ТЗ можлива втрата даних та часткова паралізація підприємства I = 0.8

$$R = 0.6 * 0.8 * 100\%$$

- втрата або розголошення паролів доступу до системи

Ймовірність оцінюється як середня через низьку обізнаність персоналу P = 0.6

Вплив визначено як середній, так як у разі страти паролю це частково паралізує роботу підприємства на невеликий термін, у разі отримання паролів зловмисником підключення повинно відбуватись лише в середині системи I = 0.5

$$R = 0.6 * 0.3 * 100\%$$

- втрата або збій зовнішніх носіїв інформації

Ймовірність оцінюється як вище середнього середня через низьку обізнаність персоналу P = 0.6

Вплив визначено як високий, оскільки у разі втрати або збою зовнішніх носіїв інформації є можливість втрати даних які на них зберігались, або потрапляння цих даних до третіх осіб I = 0.8

$$R = 0.6 * 0.8 * 100\%$$

- ризик несанкціонованого доступу, через велику кількість прав в системі у системного адміністратора

Ймовірність оцінюється як вище середньої так як системним адмініструванням займається інша компанія яка займається адмініструванням віддалено, або у разі потреби приїжджає на місце, P = 0.6

Вплив визначено як дуже високий, оскільки у разі несанкціонованого підключення до системи, можливе розголошення інформації , або втрата даних, з цього виходить I = 0.9

$$R = 0.6 * 0.9 * 100\%$$

Зазначені в табл. 1.12 ризики інформаційної безпеки сільськогосподарського підприємства «Чумаки» визначають потенційні ризики та їхній рівень, які можуть виникнути в результаті різноманітних природних, техногенних та антропогенних факторів.

Таблиця 1.12 Ризики інформаційної безпеки

№	Ризики інформаційної безпеки	Ймовірність	Вплив	Рівень ризику	Порушення властивостей інформації
Природні					
1.1	Пошкодження будівлі через стихійні лиха	0.2	0.5	10%	ЦД
Техногенні					
2.1	Ризик втрати виробничих активів внаслідок воєнних дій.	0.5	0.8	40%	ЦД
2.2	Збій в системі електроживлення	0.9	0.3	27%	ЦД
2.3	Відмова каналів зв’язку	0.1	0.5	5%	ЦД
Антропогенні					
3.1	Порушення режиму експлуатації технічних засобів	0.8	0.8	64%	КЦД
3.2	Несанкціоноване підключення до ТЗ за допомогою фішингових листів	0.6	0.8	48%	КЦД
3.3	Втрата або розголошення паролів доступу до системи	0.6	0.3	18%	КЦД
3.4	Втрата або збій зовнішніх носіїв інформації	0.6	0.8	48%	КЦД

Продовження таблиці 1.12

№	Ризики інформаційної безпеки	Ймовірність	Вплив	Рівень ризику	Порушення властивостей інформації
Антропогенні					
3.5	Ризик несанкціонованого доступу, через велику кількість прав в системі у системного адміністратора	0.6	0.9	54%	КЦД

Виходячи з інформації, наданої в табл. 1.12, можна зробити висновок, що найбільшими загрозами для підприємства на даний момент є порушення режиму експлуатації технічних засобів, ризик несанкціонованого доступу, через велику кількість прав в системі у системного адміністратора, несанкціоноване підключення до ТЗ за допомогою фішингових листів, а також втрата або збій зовнішніх носіїв інформації.

1.3 Висновок

На основі етапів розроблення СУІБ, а саме проаналізувавши типове сільськогосподарське підприємство, розглянувши загальні відомості про СПП «Чумаки», розглянувши інформаційні потоки на сільськогосподарському підприємстві «Чумаки», провівши інвентаризацію та категоріювання активів підприємства, обравши метод для оцінки ризиків і завдяки цьому методу розрахувавши ризики, в процесі подальшого створення СУІБ, необхідно розробити заходи, щодо реалізації пом’якшення впливу даних ризиків на інформаційну безпеку підприємства.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Обґрунтування заходів для захисту цінних активів

В даному розділі розглянуто заходи для захисту цінних активів сільськогосподарського підприємства «Чумаки» від різноманітних загроз, які впливають на інформаційну безпеку. Кожен захід має на меті підвищити рівень безпеки інформаційних систем, прискорити виявлення потенційних загроз та мінімізувати вплив можливих інцидентів на нормальний хід бізнес-процесів. З метою мінімізації цих ризиків та забезпечення стабільності та безпеки ведення господарської діяльності важливо вжити ефективні заходи захисту.

Для того щоб забезпечити безпеку цінних активів було розроблено ряд заходів на кожну загрозу для підприємства:

- пошкодження будівлі через стихійні лиха;

Рівень ризику низький, були запропоновані такі заходи:

1) проведення аудиту стійкості будівлі до стихійних лих;
2) встановлення сигналізаційних систем та систем аварійного оповіщення.

- ризик втрати виробничих активів внаслідок воєнних дій;

Рівень ризику нижче середнього, тому були запропоновані такі заходи:

1) розробка та впровадження плану надійності та безпеки;
2) резервне копіювання важливих даних та інформації;
3) розробка плану у випадку евакуації підприємства.

- збій в системі електроживлення;

Рівень ризику нижче середнього, тому були запропоновані такі заходи:

1) перевірка справності генераторів;
2) у разі необхідності ремонт генераторів;
3) захисні заходи для попередження перенапруги та інших проблем електропостачання.

- відмова каналів зв’язку;

Рівень ризику дуже низький, тому були запропоновані такі заходи:

1) використання множинних та резервних каналів зв'язку.

- порушення режиму експлуатації технічних засобів;

Рівень ризику високий, тому були запропоновані такі заходи:

1) технічне навчання та підвищення кваліфікації персоналу;
2) встановлення правил та процедур експлуатації.

- несанкціоноване підключення до ТЗ за допомогою фішингових листів;

Рівень ризику середній, тому були запропоновані такі заходи:

1) навчання персоналу щодо розпізнавання фішингових атак;
2) використання систем виявлення і запобігання інцидентам безпеки;
3) надання персоналу інструкцій по роботі з поштою для запобігання фішиговим атакам.

- втрата або розголошення паролів доступу до системи;

Рівень ризику низький, тому були запропоновані такі заходи:

1) впровадження строгих правил управління паролями;
2) двофакторна аутентифікація для усіх доступів до систем.

- втрата або збій зовнішніх носіїв інформації;

Рівень ризику середній, тому були запропоновані такі заходи:

1) встановлення інструкцій поводження та зберігання зовнішніх носіїв інформації;
2) резервне копіювання даних.

- ризик несанкціонованого доступу, через велику кількість прав в системі у системного адміністратора.

Рівень ризику вище середнього, тому були запропоновані такі заходи:

1) розмежування доступу;
2) надання відповідальному за СУІБ права адміністратора безпеки.

2.2 Рекомендації щодо впровадження обраних заходів обробки ризиків

Після ідентифікації та оцінки ризиків інформаційної безпеки на сільськогосподарському підприємстві та розгляду конкретних заходів для захисту цінних активів, настав час переходити до етапу впровадження цих заходів. В цьому розділі розглядаються конкретні кроки та стратегії, спрямовані на успішне впровадження обраних заходів обробки ризиків для забезпечення стійкості та безпеки інформаційного середовища підприємства.

Впровадження зазначених заходів є критичним етапом у зміцненні інформаційної безпеки підприємства та має на меті забезпечити оптимальний баланс між доступністю, конфіденційністю та цілісністю інформації. Процес впровадження включає в себе розробку плану дій, організаційні зміни, технічні модифікації та ефективний моніторинг для постійного вдосконалення системи інформаційної безпеки.

У розділі буде проведений детальний аналіз та обговорення обраних заходів обробки ризиків, спрямованих на зменшення середнього та високого рівнів ризиків. Однією з ключових стратегій управління ризиками є усвідомлення та ефективна обробка тільки тих загроз, які можуть значно вплинути на стабільність та продуктивність підприємства.

2.2.1 Заходи протидії ризику порушення режиму експлуатації технічних засобів

Так як ризик порушення режиму експлуатації має найбільший рівень ризику, далі розглядається реалізація протидії загрозам на основі засобів захисту, які були розроблені.

Ризик порушення режиму експлуатації технічних засобів може бути реалізований наступним чином:

- Крок 1. Співробітник може випадково використовувати технічні засоби неправильно або виконувати дії, які можуть призвести до виникнення несправностей або втрати даних.

Для зниження рівня ризику пропонуються наступні кроки:

- технічне навчання та підвищення кваліфікації персоналу.

Недостатня обізнаність співробітників та непорозуміння відповідальності за порушення вимог режиму експлуатації можуть призвести до фінансових збитків та негативних наслідків для компанії. Тому поширення інформації серед співробітників підприємства, щодо правил та положень, пов'язаних з порушенням режиму експлуатації, є важливим кроком.

Для навчання персоналу і підвищення їхньої кваліфікації, щоб ефективно протидіяти ризику порушення режиму експлуатації, на підприємстві

впроваджується технічне навчання, орієнтоване на конкретні вимоги та процедури, пов'язані із забезпеченням безпеки технічних засобів.

Важливо надати співробітникам повну картину щодо відповідальності та ролі кожного у забезпеченні безпеки технічних засобів. Це включає в себе визначення конкретних вимог експлуатації, освоєння процедур взаємодії з технічним обладнанням та реагування на можливі неполадки чи витоки інформації.

Використовуючи різноманітні методи технічного навчання, включаючи внутрішні семінари, віддалені тренінги та електронні навчальні платформи. Це дозволяє не лише забезпечити практичні навички, а й акцентувати на важливості кожного працівника у забезпеченні стійкості технічних засобів.

Серед віддалених курсів були запропоновані так курси які вказано в табл. 2.1

Таблиця 2.1 Запропоновані програми для підвищення кваліфікації та обізнаності персоналу

Назва компанії	Назва курсу	Термін проходження курсу	Ціна в грн/міс
danco	Комп'ютерні курси для офісу	2 місяці	3630
education.ua	Курс з ефективної експлуатації технічних засобів	2 місяців	2550

Серед даних курсів за ціною найбільше підходять курси компанії «education.ua» їхні плюси які виділяють їх від конкурентів :

- Гнучкий графік який компанія може обрати сама;
- Курси забезпечують інтерактивними елементами завдяки яким працівники можуть застосовувати отримані навички на практиці;
- Данні курси є актуальні та підлаштовуються під кожну компанію індивідуально виходячи з особливостей сфери діяльності компанії.

Ці курси повинні підняти рівень кваліфікації співробітників і зменшити ризик порушення експлуатації через низьку кваліфікацію співробітників.

- встановлення правил та процедур експлуатації.

Встановлення чітких правил та процедур експлуатації є важливою складовою стратегії. Ці правила та процедури створюють основу для ефективного управління технічними засобами та максимізації продуктивності підприємства.

По-перше необхідно встановити чіткий план дій у разі аварій, збоїв у системі, та інших екстрених ситуацій.

По-друге встановити план регулярних перевірок та технічного обслуговування.

По-третє встановити обмеження доступу до технічних засобів, особливо до системного адміністрування.

Після виконання цього плану рівень ризику через порушення режиму експлуатації повинен знизитись.

2.2.2 Заходи протидії ризику несанкціонованого доступу, через велику кількість прав в системі у системного адміністратора

Для ефективного управління цим ризиком та забезпечення надійності інформаційної безпеки системи, необхідно вжити конкретні заходи протидії.

Ризик несанкціонованого доступу, через велику кількість прав в системі у системного адміністратора може бути реалізований наступним чином:

- крок 1. На початковому етапі адміністратор системи отримує доступ до більшої кількості ресурсів, ніж йому дійсно потрібно для виконання своїх обов'язків, для забезпечення ефективного управління технічними засобами, мережами та іншими ресурсами сільськогосподарського підприємства;
- крок 2. Відсутність адекватних інструментів аудиту та моніторингу привілеїв може призводити до того, що несанкціонований доступ адміністратора залишається непоміченим. Невідомо, які конкретні операції відбуваються та на які ресурси здійснюється доступ;
- крок 3. З огляду на велику кількість привілеїв, адміністратор може

використовувати свій статус для виконання несанкціонованих дій, таких як перегляд конфіденційної інформації, зміна налаштувань системи, блокування інших користувачів і т.д.

Для зниження рівня ризику пропонується змінити матрицю розмежування доступу і зменшити доступ системного адміністратора до інформації на підприємстві, а також встановити контроль за журналом подій та контроль за правами в системі.

- розмежування доступу

Так як було виявлено в системного адміністратора доступ до важливої інформації, для збереження конфіденційності цієї інформації було прийняте рішення про зменшення прав доступу системного адміністратора. Оновлену матрицю розмежування доступу було вказано в табл. 2.2

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 2.2- 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	ЧСРВЕД	Ч	Ч	Ч	Ч	-	-	-	Ні	ПК1-15
Зас. Директора з виробн.	Ч	ЧСРВЕД	-	Ч	ЧСРВЕД	-	ЧСРВЕД	-	ЧСРВЕД	-	Ч	-	-	-	Ні	ПК13

Продовження таблиці 2.2

Об’єкт	Інформація*														Повноваження	Доступ до
Користувач	1	2	3	4	5	6	7	8	9	10	11	12.1	12.2	12.3		
Зас. Директора з тварин.	Ч	ЧС РВ ЕД	-	Ч	ЧЕД	ЧС РВ ЕД	ЧС РВ ЕД	-	-	ЧС РВ ЕД	Ч	-	-	-	Ні	ПК14
Бухгалтер	-	Ч	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	-	-	-	-	-	-	-	Ні	ПК1-4
Головний бухгалтер	ЧС РВ ЕД	Ч	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	Ч	-	-	Ч	-	-	-	Ні	ПК5
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	ПК9-12
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	ПК6
Зас. Керівника СБ	Ч	Ч	-	Ч	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	ЧС РВ ЕД	Ч	Ч	ЧС РВ ЕД	-	-	-	Ні	ПК7
Користувач	1	2	3	4	5	6	7	8	9	10	11	12.1	12.2	12.3		
Юрист – консультант	ЧС РВ ЕД	Ч РВ ЕД	-	-	-	-	ЧС РВ ЕД	-	-	-	Ч	-	-	-	Ні	ПК8

Продовження таблиці 2.2

Об’єкт	Інформація*														Повноваження	Доступ до
Користувач	1	2	3	4	5	6	7	8	9	10	11	12.1	12.2	12.3		
Системний адміністратор	-	-	-	-	-	-	-	-	-	-	-	Ч	Ч	ЧСРВЕД	Так	ПК1-15С.
Адміністратор безпеки	-	-	-	-	-	-	-	-	-	-	-	ЧСРВЕД	ЧСРВЕД	-	Ні	ПК1-15С.

*Номери інформації наведено згідно з табл. 1.2.

Умовні позначення доступу до інформації.

Ч- читання.

С-створення нових файлів.

Р-редагування.

В-видалення.

Е-імпорт або експорт.

Д-друк.

Після даного розмежування доступу ризик несанкціонованого доступу, через велику кількість прав в системі у системного адміністратора, повинен знизитись.

- надання відповідальному за СУІБ права адміністратора безпеки

З метою вдосконалення системи управління інформаційною безпекою та надання відповідальності за забезпечення безпеки інформації, вводиться посада

адміністратора безпеки. Виконувати обв’язки адміністратора безпеки буде співробітник який відповідальний за СУІБ. До обов’язків адміністратора безпеки відносяться:

- повинен контролювати журнал подій;
- повинен надавати права в системі користувачам;

2.2.3 Заходи протидії ризику несанкціонованого підключення до ТЗ за допомогою фішингових листів

Одним з найбільш небезпечних ризиків є ризик несанкціонованого підключення до ТЗ за допомогою фішингових листів, небезпека полягає в тому, що атаки фішингу можуть призвести до використання конфіденційної інформації та порушення цілісності даних.

Фішинг — це форма атаки з використанням соціальної інженерії, в ході якої зловмисник, маскуючись під надійний суб'єкт, виманює конфіденційну інформацію жертв[8].

Ризик несанкціонованого підключення до ТЗ за допомогою фішингових листів може бути реалізований наступним чином:

- крок 1. Відкриття фішингового листа: співробітник отримує електронний лист, який може виглядати як легітимний. Лист може містити текст, який закликає до термінової дії, наприклад, оновлення облікових даних, перевірка активності або завантаження важливого документа.
- крок 2. Перехід за посиланням або відкриття вкладення: під час відкриття листа співробітник може натискати на посилання або відкривати вкладення, що може викликати виконання шкідливого коду або перенаправлення на фішинговий веб-сайт.
- крок 3. Завантаження шкідливого програмного забезпечення: фішинговий лист може також містити вкладення, що містить шкідливе програмне забезпечення. Якщо співробітник завантажить і виконає це вкладення, це може призвести до інсталяції шкідливого коду на його комп'ютері.
- крок 4. Використання компрометованого облікового запису: якщо атака

успішна, атакуючий може використовувати скомпрометовані облікові записи для несанкціонованого доступу до систем і ресурсів сільськогосподарського підприємства.

- крок 5. Розповсюдження атаки: здобуті атакуючим облікові дані можуть використовуватися для розповсюдження атаки всередині мережі підприємства, отримання доступу до конфіденційної інформації та виконання інших атак.

Для зниження рівня ризику пропонуються наступні кроки:

- навчання персоналу щодо розпізнавання фішингових атак.

Так як фішинг, як інструмент соціальної інженерії, стає все більш вдосконаленим та складним для розпізнавання. Необізнаність персоналу із сучасними методами атак може стати слабким місцем в загальній системі безпеки підприємства.

Завданням сучасних організацій у сфері інформаційної безпеки є не лише захист власних ресурсів від зовнішніх загроз, але й підготовка персоналу до ефективного реагування на внутрішні загрози, зокрема фішингові атаки.

Для кваліфікованого навчання персоналу було прийняте рішення про купівлю онлайн курсів з виявлення та протидії фішинговим атакам. В табл. 2.3 вказані курси, які розглядались.

Таблиця 2.3 Курси для навчання протидії фішингових атак

Назва компанії	Назва курсу	Термін проходження курсу	Ціна в грн/міс
knowbe4	Виявлення та протидія фішинговим атакам	2 місяці	3140
cofense.	Курс базової кібербезпеки	4 місяців	4550
cybeready	Базовий курс протидії кібератакам	3 місяці	4740

Серед всіх запропонованих курсів було обрано курси від компанії «knowbe4», так як вони мають свій ряд переваг над їхніми конкурентами

- онлайн курси які працюють як в Україні, так і багатьох країнах Європи;
- компанія постійно оновлює базу знань, що допомагає при захисті від новостворених форм фішингових атак.

Після проходження даного курсу персонал буде більш інформований та кваліфікований для виявлення або протидії фішинговим атакам, через що рівень ризику через ці атаки знизиться.

- використання систем виявлення і запобігання інцидентам безпеки.

Для більшої захищеності від фішингових атак, окрім навчання персоналу, рекомендується використовувати системи виявлення і запобігання фішингових атак. На даному етапі розвитку антивірусів, вони досягають максимального рівня захищеності, використовуючи мінімальні ресурси.

Так як на підприємстві вже є встановлений антивірус Avast, було прийняте рішення замінити його на інший, який має більший рівень захисту саме від фішингових атак. Сільськогосподарському підприємству «Чумаки» було запропоновано декілька варіантів антивірусів які вказані в табл. 2.4

Таблиця 2.4 Антивіруси для підвищення безпеки від фішингових атак

Назва	Експертний висновок	Ціна в грн на місяць
ESET Endpoint Antivirus	№1257 Дійсний з 17.06.2021 до 17.06.2024	2205,00
Dr.Web Security Space	№ 610 Дійсний з 30.12.2015 до 30.12.2018 (дія експертного висновку зупинена).	1420,00
McAfee Web Security	№ 1151Дійсний з 27.08.2020 до 27.08.2023	2341,00

Серед даних антивірусів було обрано антивірус ESET Endpoint Antivirus для Windows виробництва ESET, spol. s r.o. (Словаччина) вартістю 2205 грн.

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

- надання персоналу інструкцій по роботі з поштою для запобігання

фішиговим атакам

Ще одним важливим аспектом в обізнаності та захисті персоналу від фішингових атак є створення інструкцій по роботі з поштою.

Пункти, які, обов'язково, повинні міститись в інструкції по роботі з поштою для запобігання фішинговим атакам на сільськогосподарському підприємстві «Чумаки».:

1) Обов'язково перевіряти адресу відправника: необхідно обов'язково перевіряти адресу відправника, так як фішери часто використовують подібні адреси, але з легкими змінами.

2) Одразу повідомити керівництво: у разі, якщо було помічено сумнівний лист і є підозра, що даний лист несе загрозу інформаційній безпеці підприємства, необхідно одразу повідомити про даний лист керівника підприємства, а також відповідального за СУІБ. Відкривати даного листа заборонено.

3) Не можна відкривати сумнівні посилання: Не потрібно клікати на посилання, якщо ви не впевнені в їхній надійності.

4) Потрібно завжди бути обережним з вкладеннями: Не відкривати файли від невідомих відправників. Вони можуть містити шкідливі програми.

5) Подавати скаргу: У разі, якщо ви отримаєте сумнівний лист, який видається фішинговим, необхідно повідомити про це вашого поштового провайдера чи компанію, яку фішери намагаються підробити.

6) Оперативно видаляти сумнівні листи: Якщо лист виглядає підозріло, оперативно видаляйте його. Не відкривайте вкладення чи не виконуйте дії, якщо ви не впевнені в легітимності листа.

Дотримання даної інструкції мінімізує ризик загрози від фішингофих атак.

2.2.4 Заходи для протидії ризику втрати або збою зовнішніх носіїв інформації

Одним із найбільш поширених видів загроз, пов'язаних із використанням зовнішніх носіїв інформації з професійною метою, є можливість їх втрати чи викрадення, зважаючи на невеликі розміри. Існує загроза, що випадкова знахідка

може опинитись у руках зловмисників, які із легкістю зможуть отримати доступ до всієї інформації та файлів, які містяться на ній.[9]

Ризик втрати або збою зовнішніх носіїв інформації може бути реалізований наступним чином:

- крок 1. Співробітник може випадково втратити зовнішній носій, наприклад, залишивши його у громадському транспорті, в кафе, вдома або в іншому доступному місці.
- крок 2. Треті особи можуть отримати фізичний доступ до зовнішнього носія та скопіювати, видалити або змінити інформацію на ньому.
- крок 3. Зовнішні носії можуть заражатися вірусами або іншим шкідливим програмним забезпеченням, яке може призвести до втрати даних або навіть до поширення інфекції через мережу підприємства.

Для зниження рівня ризику пропонуються наступні кроки:

- встановлення інструкцій поводження та зберігання зовнішніх носіїв інформації

Для зниження рівня ризику пов’язаного з втратою зовнішніх носіїв інформації, потрібно навчити співробітників підприємства поводженню з носіями інформації та надати їм інструкції зі зберігання та користування даними пристроями.

Пункти які, обов’язково, повинні міститись в інструкції поводження та зберігання зовнішніх носіїв інформації на сільськогосподарському підприємстві «Чумаки».:

1) Завжди безпечно відключати флешку: Потрібно переконатися, що після закінчення роботи з флешкою вибрали опцію "Безпечне відключення апаратного забезпечення" перед видаленням флешки з комп'ютера. Це допомагає уникнути втрати даних або пошкодження файлової системи.

2) Використовувати утримання на робочому місці: Зберігати флешку у відповідному кейсі чи на робочому столі, де вона може бути легко знайдена. Уникати залишання її випадково в різних місцях.

3) Постійно перевіряти місце зберігання: Перед виходом з робочого місця

потрібно перевірити і переконатися, що всі зовнішні носії інформації знаходяться на своєму місці.

4) Уникати фізичних пошкоджень: зовнішні носії інформації досить вразливі до механічних впливів. Потрібно уникати впливу високих температур, вологості та ударів.

5) Не використовувати зовнішні носії інформації на невідомих комп'ютерах: Підключати зовнішні носії інформації до сторонніх комп'ютерів строго заборонено.

6) Не наповнювати зовнішні носії інформації повністю: Потрібно залишати трохи вільного місця, оскільки це може допомогти уникнути проблем з втратою даних чи зменшенням швидкості роботи.

- резервне копіювання даних

Для мінімізації рівня ризику пов'язаного з втратою даних які зберігалися на зовнішніх носіях інформації, потрібно створити резервні копії всієї інформації, яка зберігається на зовнішніх носіях.

Резервне копіювання — процес створення копії даних з носія, призначений для відновлення цих даних у разі їх пошкодження або видалення[10].

Для створення резервних копій необхідно мати сховище, куди ці копії можна буде додавати. Як приклад, для зменшення загальної вартості процесу резервного копіювання, сільськогосподарському підприємству «Чумаки» було запропоновано взяти жорсткий диск для зберігання резервних копій файлів, які знаходяться на зовнішніх носіях інформації.

Було обрано для вибору декілька варіантів жорстких дисків які вказані в табл. 2.5

Таблиця 2.5 Варіанти жорстких дисків для резервного копіювання

№	Марка	Модель	Об'єм	Вартість в грн
1	Seagate	STKP18000400	18 ТБ	15240,00
2	Western Digital	Ultrastar DC HC550	18 ТБ	15542,00

Продовження таблиці 2.5

№	Марка	Модель	Об’єм	Вартість в грн
3	Seagate	Ironwolf Pro ST16000NT001	18 ТБ	15799,00
4	Western Digital	Purple WD20PURZ	16 ТБ	12038,00

Серед представлених в табл.2.5 жорстких дисків було обрано жорсткий диск «Seagate STKP18000400 18 ТБ» вартістю 16240,00 грн., так як даний жорсткий диск має ряд переваг перед своїми конкурентами:

- серед представлених варіантів даний жорсткий диск єдиний з зовнішнім підключенням;
- компанія має гарну репутацію у сфері зовнішніх накопичувачів інформації;
- ціна, яка нижча в порівнянні з іншими представниками того ж об’єму.

Після впровадження даних порад рівень ризику від втрати або збою зовнішніх носіїв інформації повинен знизитись.

2.3 Контроль виконання та ефективність обраних заходів

На даному етапі розробки СУІБ ми можемо визначити рівень впливу засобів захисту загроз які були проведені

- порушення режиму експлуатації технічних засобів

Ймовірність знизилась через підвищення обізнаності співробітників за допомогою курсів, а також через створення правил та процедур експлуатації технічних засобів, тепер ймовірність оцінюється як низька P =0.2

Вплив не змінився, він залишається таким як попередній I = 0.8

$$R = 0.\ 2 * 0.8 * 100\%$$

- несанкціоноване підключення до ТЗ за допомогою фішингових листів

Ймовірність знизилась через підвищення обізнаності співробітників за допомогою курсів та інструкцій, які були надані співробітникам, а також через

використання нових систем виявлення і запобігання інцидентам безпеки, тепер ймовірність оцінюється як низька P =0.2

Вплив не змінився, він залишається таким як попередній I = 0.8

$$R = 0.\ 2 * 0.8 * 100\%$$

- втрата або збій зовнішніх носіїв інформації

Ймовірність знизилась через встановлення інструкцій поводження та зберігання зовнішніх носіїв інформації. Тепер ймовірність оцінюється як низька P = 0.2

Вплив знизився, завдяки створенню резервного копіювання і тепер вплив оцінюється як нижче середнього I = 0.4

$$R = 0.\ 2 * 0.4 * 100\%$$

- ризик несанкціонованого доступу, через велику кількість прав в системі у системного адміністратора

Ймовірність знизилась через розмежування доступу і тепер системний адміністратор не має доступу до конфіденційної інформації , тому ймовірність стала низькою P = 0.2

Вплив визначено як дуже високий, оскільки у разі несанкціонованого підключення до системи, можливе розголошення інформації, або втрата даних, з цього виходить I = 0.9

$$R = 0.2 * 0.9 * 100\%$$

Після впровадження всіх засобів захисту від загроз, які були на сільськогосподарському підприємстві «Чумаки» оновлена оцінка ризиків інформаційної безпеки на сільськогосподарському підприємстві "Чумаки" виглядає так, як вказано в табл. 2.6

Таблиця 2.6 Оновлена таблиця ризиків інформаційної безпеки

№	Ризики інформаційної безпеки	Ймовірність	Вплив	Рівень ризику	Порушення властивостей інформації
Природні					
1.1	Пошкодження будівлі через стихійні лиха	0.2	0.5	10%	ЦД
Техногенні					
2.1	Ризик втрати виробничих активів внаслідок воєнних дій.	0.5	0.8	40%	ЦД
2.2	Збій в системі електроживлення	0.9	0.3	27%	ЦД
2.3	Відмова каналів зв’язку	0.1	0.5	5%	ЦД
Антропогенні					
3.1	Порушення режиму експлуатації технічних засобів	0.2	0.8	16%	КЦД
3.2	Несанкціоноване підключення до ТЗ за допомогою фішингових листів	0.2	0.8	16%	КЦД
3.3	Втрата або розголошення паролів доступу до системи	0.6	0.3	18%	КЦД
3.4	Втрата або збій зовнішніх носіїв інформації	0.2	0.4	8%	КЦД

Продовження таблиці 2.6

№	Ризики інформаційної безпеки	Ймовірність	Вплив	Рівень ризику	Порушення властивостей інформації
3.5	Ризик несанкціонованого доступу, через велику кількість прав в системі у системного адміністратора	0.2	0.9	18%	КЦД

Виходячи з інформації наданої в табл. 2.6 можна визначити, що на сільськогосподарському підприємстві «Чумаки» на даному етапі, після впровадження всіх засобів захисту, рівень захисту підвисився, у зв'язку з цим, рівень ризику зменшився і загроз високого, вище середнього, або навіть середнього рівня ризику не залишилось.

2.4 Призначення відповідальних осіб за функціонування СУІБ

Призначення відповідальних осіб за функціонування СУІБ є ключовим елементом забезпечення ефективного та безпечного ведення бізнес-процесів у сучасному цифровому середовищі. В умовах постійно зростаючих загроз та вимог до конфіденційності, цілісності та доступності інформації, визначення відповідальних осіб в області інформаційної безпеки стає критичною у впровадженні ефективних стратегій та політик безпеки.

На сільськогосподарському підприємстві «Чумаки» було прийнято рішення по призначення керівника СБ відповідальним за організацію та функціонування СУІБ. Так як його повноваження суміжні з функціоналом, який потрібно виконувати для забезпечення функціонування СУІБ.

Зміни до СУІБ вносяться виключно зі згоди керівника сільськогосподарського підприємства «Чумаки».

2.5 Роль керівництва підприємства в СУІБ

Керівництво підприємства відіграє ключову роль в реалізації та ефективному функціонуванні СУІБ. Ця роль визначається кількома важливими аспектами:

1) Загальна відповідальність за СУІБ залишається за керівником сільськогосподарського підприємства «Чумаки».

2) Заміна відповідальних осіб за СУІБ. Керівник має призначити відповідальних осіб, які будуть керувати реалізацією СУІБ та забезпечувати відповідність інформаційної безпеки.

3) Фінансова підтримка. Забезпечення фінансових ресурсів для впровадження інфраструктури інформаційної безпеки та навчання персоналу.

4) Затвердження політики інформаційної безпеки може бути реалізоване лише керівником.

У разі виконання керівництвом даних аспектів, система управління інформаційною безпекою зможе функціонувати та перешкоджати ризикам інформаційної безпеки.

2.6 Висновок

На основі проведеного аналізу ризиків, в першій частині було визначено конкретні заходи для захисту цінних активів, а також впроваджено обрані заходи обробки ризиків для тих загроз, які мали середній рівень ризику, та високий, а саме було надано рекомендації щодо впровадження заходів протидії ризику порушення режиму експлуатації, протидії ризику несанкціонованого доступу, через велику кількість прав в системі у системного адміністратора, заходів протидії ризику несанкціонованого підключення до ТЗ, за допомогою фішингових листів, заходів протидії ризику втрати або збою зовнішніх носіїв інформації. Також було призначено відповідальну особу за функціонування СУІБ, та визначено роль керівника підприємства в СУІБ.

Таким чином, на основі аналізу ризиків після впровадження, можна стверджувати, що запропоновані заходи безпеки є ефективними і забезпечують необхідний рівень безпеки інформації на сільськогосподарському підприємстві «Чумаки».

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

У роботі створена система управління інформаційною безпекою для сільськогосподарського підприємства «Чумаки».

Загальна площа сільськогосподарського підприємства «Чумаки» складає 50000650 м^2, яка є власністю підприємства. Дохід складає 38000000 грн на рік. Загальна чисельність співробітників 103 чоловік.

Метою економічного розділу є визначення :

- капітальних витрат на створення та впровадження СУІБ;
- експлуатаційних витрат на підтримку функціонування СУІБ;
- визначення річного економічного ефекту від впровадження СУІБ;

3.1 Визначення капітальних витрат

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

Капітальні (фіксовані) витрати на проектування та впровадження СУІБ складають:

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} \quad (3.1)$$

$К_{пр}$ – вартість розробки проекту інформаційною безпеки та залучення до нього зовнішніх консультантів, тис.грн;

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

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

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

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

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

Для розробки СУІБ немає потреби в залученні зовнішніх спеціалістів, а буде використовуватись власний персонал. Тому потрібно визначити лише вартість розробки проекту, наприклад, витрати на закупівлю ліцензійоного програмного забезпечення для впровадження СУІБ будуть складати 22500 грн.

Для використання впровадженої СУІБ потрібне придбання ліцензії антивірусу ESET Endpoint Antivirus для Windows.

Програма ESET Endpoint Antivirus для Windows – ключ з терміном дії 1 рік коштує 22500 грн.

Отже:

$К_{зпз} = 22500$ грн.

Витрати на навчання $К_{навч}$ співробітників складають 11380 грн.

Для використання впровадженої СУІБ потрібне придбання навчальних курсів:

1) Education.ua
2) Knowbe4

Покупка курсів Education.ua коштує 5100 грн. за 2 місяці навчання.

Покупка курсів Knowbe4 коштує 6280 грн. за 2 місяці навчання.

Отже:

$$К_{навч} = 5100 + 6280 = 11380 \text{ грн.}$$

Витрати на впровадження та налагодження СУІБ $К_н$, складаються з заробітньої платні спіробітників, які займалися створенням СУІБ , та кількості часу витраченого на це. Впровадженням СУІБ займались два співробівтника, заробітня платня одного працівника складає 200 грн/год, на процес впровадження може бути витрачено 7 робочих днів, що дорівнює 56 робочих годин. Таким чином розрахуємо $К_н$:

$$К_н = 2*56*200 = 22400 \text{ грн.}$$

Для впровадження СУІБ на підприємстві необхідно було закупити жорсткий диск «Seagate STKP18000400 18 ТБ» вартістю 16240,00 грн.

Отже витрати на купівлю апаратного забезпечення та допоміжних матеріалів складають $К_{аз}$ =16240 грн.

Маючи всі ці дані, можна розрахувати капітальні витрати на проектування та впровадження СУІБ за формулою (3.1)

$$К = 11380 + 22400 + 16240 + 22500 = 72520 \text{ грн.}$$

3.2 Розрахунок поточних (експлуатаційних) витрат

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

Витрати на керування СУІБ (С) складають:

$$С = С_н + С_а + С_з + С_{єв} + С_{ел} + С_о + С_{тос}, \text{ грн,} \quad (3.2)$$

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

$С_н$ = 1896,60 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;

$$С_з = З_{осн} + З_{дод}, \text{ грн.}, \quad (3.3)$$

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 – 33600грн./місяць.

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

$$З_{осн} = 22*8*200*2*12 = 844800 \text{ грн.}$$
$$З_{дод} = 0,08* З_{осн} = 0,08 * 844800 = 67584 \text{ грн.}$$
$$С_з = З_{осн} + З_{дод} = 67584 + 844800 = 912384 \text{ грн.}$$

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

$$С_{єв} = 912384 * 0,22 = 200724,48 \text{ грн.}$$

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

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.}, \quad (3.4)$$

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.

$$С_{ел} = 0,7*1920*1,68 = 2257,92 \text{ грн.}$$

$С_{тос}$ – 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;

$$С_о = 0.$$

$$С_{тос} = 72520 *0,01 = 725,20 \text{грн.}$$

$$С = 1896,60 + 13800 + 912384 + 200724,48 + 2257,92 + 725,20 = 1131788,20 \text{ грн.}$$

Річні поточні витрати на функціонування СУІБ складають 1131788,20 грн.

3.3 Оцінка величини збитку

Кінцевим результатом впровадження й проведення заходів, щодо забезпечення інформаційної безпеки, є величина відвернених втрат, що розраховується, виходячи з ймовірності виникнення інциденту інформаційної безпеки й можливих економічних втрат від нього. По суті, ця величина відображає ту частину прибутку, що могла бути втрачена.

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

Необхідні вихідні данні 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;

$З_о$ = 33600грн./міс.;

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

$З_с$ = 33600грн./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 доходу підприємства грн за рік

О = 38000000;

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

I – число атакованих сегментів корпоративної мережі;

I = 4;

N – середнє число атак на рік,

N = 7.

Упущена вигода від простою атакованого сегмента корпоративної мережі:

$$U = П_п + П_в + V, \quad (3.5)$$

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

$$П_п = \frac{\sum Зс}{F} \cdot t_п, \quad (3.6)$$

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

$$П_п = ((33600 * 103)/176)*2 = 39327,27 \text{ грн},$$

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

$$П_в = П_{ви} + П_{пв} + П_{зч}, \quad (3.7)$$

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.

$$П_{ви} = \frac{\sum Зс}{F} \cdot t_{ви}, \quad (3.8)$$

$$П_{ви} = ((33600 *103)/176) *1,5 = 29495,45 \text{ грн.}$$

$$П_{пв} = \frac{\sum Зо}{F} \cdot t_в, \quad (3.9)$$

$$П_{пв} = ((33600 *1)/176) *3 = 572,73 \text{ грн.}$$

$$П_в = 29495,45 +572,73= 30068,18 \text{ грн.}$$

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

$$V = \frac{О}{Fг} \cdot (t_п + t_в + t_{ви}), \quad (3.10)$$

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.

$$V = (38000000/2080) * (2+3+1,5) = 118750 \text{ грн.}$$

$$U= П_п + П_в +V, \quad (3.11)$$

U = 39327,27 + 30068,18 + 118750 = 188145,45грн.

Загальний збиток від атаки на сегмент корпоративної мережі організації:

$$B = \sum_i \sum_n U, \quad (3.12)$$

B = 5 * 7 * 188145,45*I = 6585090,75грн.

3.4 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B \cdot R - C, \text{ грн.}, \quad (3.13)$$

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

B = 6585090,75грн.;

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

R = 20 %;

C – щорічні витрати на експлуатацію системи управління інформаційної безпеки;

C = 1131788,20 грн.

E = 6585090,75г* 0,2 – 1131788,20 =185229,95грн.

3.5 Визначення та аналіз показників економічної ефективності запропонованого в кваліфікаційній роботі проектного рішення

Оцінка економічної ефективності СУІБ, здійснюється на основі визначення та аналізу наступний показників:

1. Сукупна вартість володіння (TCO);

2. Коефіцієнт повернення інвестицій (ROSI);

3. Термін окупності капітальних інвестицій T_o.

Коефіцієнт повернення інвестицій (ROSI) показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи управління інформаційною безпекою.

$$\text{ROSI} = \frac{E}{K}\text{, частки одиниці} \qquad (3.14)$$

де Е - загальний ефект від впровадження системи управління інформаційною безпекою, грн;

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

$$\text{ROSI} = \frac{E}{K} = \frac{185229{,}95}{72520} = 2{,}55$$

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

$$T_o = \frac{К}{Е} = \frac{1}{ROSI}\text{, років} \qquad (3.15)$$

$$T_o = \frac{К}{Е} = \frac{72520}{185229{,}95} = 0.4 \text{ років (4, 5 місяці)}$$

3.6 Висновок до третього розділу

В результаті розрахованих витрат на розробку та впровадження системи управління інформаційною безпекою на сільськогосподарському підприємстві «Чумаки», було доведено економічну доцільність розробки системи управління інформаційною безпекою на сільськогосподарському підприємстві «Чумаки». Такі висновки зроблені, виходячи з коефіцієнту повернення інвестицій ROSI, який означає, що на 1 грн. капітальних витрат приходиться 2,55 грн. економічного ефекту. Період окупності при цьому складе 4, 5 місяці. Капітальні витрати складають 70520 грн, а експлуатаційні 185229,95 грн.

ВИСНОВКИ

У першому розділі, на основі етапів розроблення СУІБ, а саме проаналізувавши типове сільськогосподарське підприємство «Чумаки», розглянувши загальні відомості про СПП «Чумаки», розглянувши інформаційні потоки на сільськогосподарському підприємстві «Чумаки», провівши інвентаризацію та категоріювання активів підприємства, обравши метод для оцінки ризиків і завдяки цьому методу розрахувавши ризики, в процесі подальшого створення СУІБ, було виявлено необхідність розробки заходів щодо реалізації пом'якшення впливу даних ризиків на інформаційну безпеку.

У другому розділі, на основі проведеного аналізу ризиків в першому розділі, було визначено конкретні заходи для захисту цінних активів, а також впроваджено обрані заходи обробки ризиків для тих загроз, які мали середній рівень ризику, та високий, а саме було впроваджено заходи протидії ризику порушення режиму експлуатації, заходи протидії ризику несанкціонованого доступу, через велику кількість прав в системі у системного адміністратора, заходи протидії ризику несанкціонованого підключення до ТЗ за допомогою фішингових листів, заходи протидії ризику втрати або збою зовнішніх носіїв інформації. Також було призначено відповідальну особу за функціонування СУІБ, та визначено роль керівника підприємства в СУІБ.

В третьому розділі, в результаті розрахованих витрат на розробку та впровадження систему управління інформаційною безпекою на сільськогосподарському підприємстві «Чумаки», було доведено економічну доцільність розробки системи управління інформаційною безпекою на сільськогосподарському підприємстві «Чумаки». Такі висновки зроблені, виходячи з коефіцієнту повернення інвестицій ROSI, який означає, що на 1 грн. капітальних витрат приходиться 2,55 грн. економічного ефекту. Період окупності при цьому складе 4, 5 місяці. Капітальні витрати складають 70520 грн, а експлуатаційні 185229,95 грн.

Новизна даної роботи полягає в тому, що розроблені рекомендації зі створення системи управління інформаційною безпекою для

сільськогосподарського підприємства з урахуванням особливостей сільськогосподарського підприємства.

ПЕРЕЛІК ПОСИЛАНЬ

1. 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

2. Стаття 5 Закону України «Про захист персональних даних» https://zakon.rada.gov.ua/laws/show/2297-17#Text

3. Стаття 1 Закону України «Про інформацію» https://do.nmu.org.ua/mod/resource/view.php?id=28521

4. Пукт 2 статті 21 Закону України «Про інформацію» https://zakon.rada.gov.ua/laws/show/2657-12#Text

5. Кваліфікаційна робота на тему “ Комплексна система захисту інформації інформаційно-телекомунікаційної системи СПП «Чумаки»” Біжко Іван https://ir.nmu.org.ua/handle/123456789/161242

6. Стале Сільське Господарство: Методи Та Їх Переваги https://eos.com/uk/blog/stale-silske-hospodarstvo/

7. Домарев В. В. Безпека інформаційних технологій системний підхід. Київ 2004

8. Фішинг - що це таке і яка мета фішингу? Енциклопедія https://www.eset.com/ua/support/information/entsiklopediya-ugroz/fishing/

9. Секрети кібербезпеки: USB-флеш-накопичувач як складова арсеналу хакерів https://eba.com.ua/sekrety-kiberbezpeky-usb-flesh-nakopychuvach-yak-skladova-arsenalu-hakeriv/

10. Information technology. Security techniques. Information management. Measurement: ISO/IEC 27000:2022 [Електронний ресурс]., https://www.iso.org/ua/standard/iso-iec-27000-family

11. Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека / Упорядн.: Д.П. Пілова – Дніпро: Національний технічний університет «Дніпровська політехніка», 2017. – 17 с.

12. Кваліфікаційна робота магістра. Методичні рекомендації до виконання для студентів спеціальності 125 «Кібербезпека» (освітньо-професійна програма

«Кібербезпека») / Упоряд.: О.Ю.Гусєв, В.І.Корнієнко, В.І.Магро, Д.С. Тимофєєв; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Д.: НТУ «ДП», 2022. – 34 с.

13. Information technology. Security techniques. Information management. Measurement: ISO/IEC 27001:2016 [Електронний ресурс]. Режим доступу: https://www.iso.org/ua/standard/27001

14. Information technology. Security techniques. Information management. Measurement: ISO/IEC 27002:2022 [Електронний ресурс]. https://www.iso.org/ua/standard/75652.html

15. Засоби ТЗІ, які мають експертний висновок про відповідність до вимог технічного захисту інформації [Електронний ресурс]. Режим доступу: https://cip.gov.ua/ua/news/zasobi-tzi-yaki-mayut-ekspertnii-visnovok-pro-vidpovidnist-do-vimog-tekhnichnogo-zakhistu-informaciyi

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	1 Розділ	30	
5	А4	2 Розділ	19	
6	А4	3 Розділ	11	
7	А4	Висновки	2	
8	А4	Перелік посилань	2	
9	А4	Додаток А	1	
10	А4	Додаток Б	4	
11	А4	Додаток В	4	
12	А4	Додаток Г	1	
13	А4	Додаток Ґ	1	
14	А4	Додаток Д	1	

ДОДАТОК Б. Таблиця інвентаризації активів на сільськогосподарському підприємстві “Чумаки”

Назва	Сума в грн
1 GPS прилад для вимір площі ГеоМетр S7(СПП Чумаки)	9650,00
2 Maximum Acoustics Mobi.12 (СПП Чумаки)	6599,00
3 WiFi адаптер TP-LINK TL-WN722N (СПП Чумаки)	581,67
4 Акумул DJI для Mavic2 Part2 для квадрок(СПП Чумаки)	3824,17
5 Акумулятор CSB GP 1272 для UPS 12V (СПП Чумаки)	749,30
6 Багатофунк пристр Canon i-SENSYS MF237(СПП Чумаки)	11082,50
7 Багатофункційний пристрій лазерн HPLG (СПП Чумаки)	9364,17
8 Блок безперебійного живлення (СПП Чумаки)	9807,50
9 Блок внутрішній настінний MSZ-HR50VF	6 625,00
10 Блок зовнішній MUZ-HRVF	15 458,33
11 БФП лазерний HP Lazer Jet M1212nf	1 835,98
12 БФП лазерний HP Lazer Jet M1212nf	1 835,97
13 Вимірювач а/т механ Paramed comfort (СПП Чумаки)	768,44
14 Відеокамера DH-HAC-HDW1000RP-0360B(СПП Чумаки)	1080,00
15 Відеокамера DH-HAC-HDW1200MP-S3(СПП Чумаки)	8060,00
16 Відеокамера Hikvision DS-2CE56D0T-IRMF(СПП Чумаки)	665,00
17 Відеокамера HikvisionDS2CE16D0T-VFIR3F(СПП Чумаки)	1360,00
18 Відеокарта (СПП Чумаки)	3240,00
19 Відеопередавач NVL-210HD (СПП Чумаки)	4568,00
20 Відеореєстратор DHI (СПП Чумаки)	4620,00
21 Вогнетривка шафа сейфового типа ВМ-1993КІ	10 464,00
22 Генератор GENERATOR Fe Power 220 kva	729 000,00

Продовження таблиці Додатку Б

Назва	Сума в грн
23 Джерело безперебійного живлення (СПП Чумаки)	7547,00
24 Джерело безперебійного живлення (СПП Чумаки)	7547,00
25 Електрон прил для контр за роб насосу(СПП Чумаки)	683,33
26 Електрон прилад контролю за роб насосу(СПП Чумаки)	2425,00
27 Животноводческий комплекс Лугова ,1а	1 018 351,74
28 Жорсткий диск Western DigitaL 500 Gb (СПП Чумаки)	3998,00
29 Карта пам'яті (СПП Чумаки)	349,17
30 Карта пам'яті (СПП Чумаки)	349,17
31 КвадрокоптерDJI Mavic 2Pro	39 849,17
32 Коммутатор для мережі (СПП Чумаки)	5110,35
33 Комплект системи точного землеробства TrimbIe EZ-Guide 250 з антеною AG-15	32 226,25
34 Комплект системи точного землеробства TrimbIe EZ-Guide 250 з антеною AG-15	32 226,25
35 Комп'ютер персональний Extreme PC	11 405,63
36 Комп'ютер персональний Extrem PC(системний блок на базі І3-4170/4Gb/500Gb/	8 699,25
37 Контроллер Nav II Автопілот GPS навігації	44 391,67
38 Ксерокс КИА Тошиба №685	5 500,00
39 Лічильник палива VZO - 8 з захист.корпусом	12 300,00
40 Лічильник палива VZO -4 з захист.корпусом	24 000,00
41 Мікробіологічний інкубатор Binder BD 115	22 123,00
42 Модуль УММ 1-001	267 800,00
43 Монітор Samsung 23.5" (СПП Чумаки)	3366,75
44 Монітор 21.5 LG22M38A-B (СПП Чумаки)	4696,13
45 Монітор 22*LG EN 43S-B LED подсветка(СПП Чумаки)	1024,17

Продовження таблиці Додатку Б

Назва	Сума в грн
46 Монітор 23.6" Philips (СПП Чумаки)	3591,00
47 Монітор 28" SAMSUNG LU28R550 (СПП Чумаки)	5981,00
48 Моноблок HP 3420	7 634,52
49 Накопичувач USB 3.0 SANDISK 64 GB (СПП Чумаки)	859,17
50 Моноблок HP 3420	7 634,52
51 Накопичувач USB 3.0 SANDISK 64 GB (СПП Чумаки)	859,17
52 Накопичувач USB 3.1 SANDISK 32 GB(СПП Чумаки)	1544,16
53 Ноутбук HP250G7 (6HL16EA)	13 299,14
54 Обладнання боксу для корів	125 245,00
55 Обладнання для "каруселі"	1512 194,79
56 Пенетрометр грунту	3 674,00
57 Пл. молочний комплекс Лугова ,1	1892 215,01
58 Принтер CanonМФУ (СПП Чумаки)	6357,95
59 Принтер БФП HP M1212 A4	4 333,33
60 Принтер БФП HP M1212 A4	2 166,67
61 Принтер БФП HP M1212 A4	2 166,67
62 Пульт управління QET 300 (СПП Чумаки)	938,88
63 Реєстратор (СПП Чумаки)	2476,00
64 Розкидач мінеральних добрив Axis 30.2 K з бортом XL1800	210 807,53
65 Роутер TP-Link Archer C20 (СПП Чумаки)	665,83
66 Сейф ЛУКА ШО-085 (СПП Чумаки)	4255,00
67 Сейф ШМ-44-1М (СПП Чумаки)	2605,00
68 Системний телефон Panasonik KX-T7730	3 192,00
69 Танк "Де Лаваль"	157 880,00
70 Телевізор SAMSUNG 43NU7097	10 832,50
71 Телевізор SAMSUNG 43NU7097	10 632,50

Продовження таблиці Додатку А

	Назва	Назва
72	Трекер автомобільний GPS BCE FMS-500(СПП Чумаки)	1230,00
73	Фільтр живлення мережевий (СПП Чумаки)	57,80
74	Фільтр мережевий (СПП Чумаки)	83,13
75	Флеш -накопичувач 8Gb (СПП Чумаки)	333,90
76	Флеш -накопичувач 16Gb (СПП Чумаки)	433,70
77	Флешка (СПП Чумаки)	170,00

ДОДАТОК В. Таблиця обладнання сільськогосподарського підприємства «Чумаки»

№	Назва	Ціна
1	Монітор Samsung 23.5" (СПП Чумаки)	3366,75
2	Монітор 21.5 LG22M38A-B (СПП Чумаки)	4696,13
3	Монітор 22*LG EN 43S-B LED підсвітка(СПП Чумаки)	1024,17
4	Монітор 23.6" Philips (СПП Чумаки)	3591,00
5	Монітор 28" SAMSUNG LU28R550 (СПП Чумаки)	5981,00
6	Моноблок HP 3420	7 634,52
7	Накопичувач USB 3.0 SANDISK 64 GB (СПП Чумаки)	859,17
8	Накопичувач USB 3.1 SANDISK 32 GB(СПП Чумаки)	1544,16
9	Ноутбук Lenovo	19 165,00
10	Ноутбук HP250G7 (6HL16EA)	13 299,14
11	Відеореєстратор DHI (СПП Чумаки)	4620,00
12	Акумул DJI для Mavic2 Part2 для квадрок(СПП Чумаки)	3824,17
13	Акумулятор CSB GP 1272 для UPS 12V (СПП Чумаки)	749,30
14	Багатофунк пристр Canon i-SENSYS MF237(СПП Чумаки)	11082,50
15	Багатофункційний пристрій лазерн HPLG (СПП Чумаки)	9364,17
16	Блок внутрішній настінний MSZ-HR50VF	6 625,00
17	Блок зовнішній MUZ-HRVF	15 458,33
18	БФП лазерний HP Lazer Jet M1212nf	1 835,98

Продовження таблиці Додатку В

№	Назва	Ціна
19	БФП лазерний HP Lazer Jet M1212nf	1 835,97
20	Вимірювач а/т механ Paramed comfort (СПП Чумаки)	768,44
21	Відеокамера DH-HAC-HDW1000RP-0360B(СПП Чумаки)	1080,00
22	Відеокамера DH-HAC-HDW1200MP-S3(СПП Чумаки)	8060,00
23	Відеокамера Hikvision DS-2CE56D0T-IRMF(СПП Чумаки)	665,00
24	Відеокамера HikvisionDS2CE16D0T-VFIR3F(СПП Чумаки)	1360,00
25	Відеокарта (СПП Чумаки)	3240,00
26	Відеопередавач NVL-210HD (СПП Чумаки)	4568,00
27	Електрон прил для контр за роб насосу(СПП Чумаки)	683,33
28	Електрон прилад контролю за роб насосу(СПП Чумаки)	2425,00
29	Жорсткий диск Western DigitaL 500 Gb (СПП Чумаки)	3998,00
30	Карта пам’яті (СПП Чумаки)	349,17
31	КвадрокоптерDJI Mavic 2Pro	39 849,17
32	Коммутатор для мережі (СПП Чумаки)	5110,35
33	Комплект системи точного землеробства TrimbIe EZ-Guide 250 з антеною AG-15	32 226,25
34	Комплект системи точного землеробства TrimbIe EZ-Guide 250 з антеною AG-15	32 226,25
35	Комп'ютер персональний Extreme PC	11 405,63

Продовження таблиці Додатку В

№	Назва	Ціна
36	Комп'ютер персональний Extrem PC(системний блок на базі І3-4170/4Gb/500Gb/	8 699,25
37	Контроллер Nav II Автопілот GPS навігації	44 391,67
38	Ксерокс КИА Тошиба №685	5 500,00
39	Модуль УММ 1-001	267 800,00
40	Монітор Samsung 23.5" (СПП Чумаки)	3366,75
41	Монітор 21.5 LG22M38A-B (СПП Чумаки)	4696,13
42	Монітор 22*LG EN 43S-B LED подсветка(СПП Чумаки)	1024,17
43	Монітор 23.6" Philips (СПП Чумаки)	3591,00
44	Монітор 28" SAMSUNG LU28R550 (СПП Чумаки)	5981,00
45	Моноблок HP 3420	7 634,52
46	Накопичувач USB 3.0 SANDISK 64 GB (СПП Чумаки)	859,17
47	Накопичувач USB 3.1 SANDISK 32 GB(СПП Чумаки)	1544,16
48	Ноутбук Lenovo	19 165,00
49	Ноутбук HP250G7 (6HL16EA)	13 299,14
50	Принтер CanonМФУ (СПП Чумаки)	6357,95
51	Принтер БФП HP M1212 A4	4 333,33
52	Принтер БФП HP M1212 A4	2 166,67
53	Пульт управління QET 300 (СПП Чумаки)	938,88
54	Реєстратор (СПП Чумаки)	2476,00
55	Системний телефон Panasonik KX-T7730	3 192,00
56	WiFi адаптер TP-LINK TL-WN722N (СПП Чумаки)	581,67

Продовження таблиці Додатку В

№	Назва	Ціна
57	Флеш -накопичувач 8Gb (СПП Чумаки)	333,90
58	Флешка (СПП Чумаки)	170,00
59	Роутер TP-Link Archer C20 (СПП Чумаки)	665,83
29	Жорсткий диск Western DigitaL 500 Gb (СПП Чумаки)	3998,00
30	Карта пам’яті (СПП Чумаки)	349,17

ДОДАТОК Г. Перелік матеріалів на оптичному носії

Біжко_І.С._125м-22-1.docx

Біжко_І.С._125м-22-1.pptx

Біжко_І.С._125м-22-1.pdf

ДОДАТОК Ґ. Відгук керівника економічного розділу

Відгук керівника економічного розділу

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

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (ініціали, прізвище)

ДОДАТОК Д. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125м-22-1

Біжка Івана Сергійовича

на тему: «Система управління інформаційною безпекою сільськогосподарського підприємства «Чумаки»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 81 сторінці.

Метою кваліфікаційної роботи є забезпечення заданого рівня захисту інформації в інформаційно-телекомунікаційній системі сільськогосподарського підприємства «Чумаки».

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності магістра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: аналіз нормативно-правової бази із створення СУІБ; інвентаризація та категоріювання активів, оцінка ризиків інформаційної безпеки; обґрунтування заходів для захисту цінних активів; розробка рекомендації щодо впровадження цих заходів.

Практичне значення результатів кваліфікаційної роботи полягає у адаптації запропонованих рішень до умов функціонування сільськогосподарського підприємства.

До недоліків роботи відноситься:

- недостатньо структуровано викладення запропонованих рішень;
- недостатньо обґрунтовано перелік потенційних ризиків.

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 магістра 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 Корченко А.О.

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