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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Шворака Микити Сергійовича*

академічної групи *125-19-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка комплексної системи захисту інформації в інформаційно-комунікаційній системі підприємства «Vinson»*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	к.ф-м.н.,проф. Кагадій Т.С.			
розділів:				
спеціальний	асист. Мілінчук Ю.А.			
економічний	к.е.н., доц. Романюк Н.М.			
Рецензент				
Нормоконтролер				

Дніпро
2023

ЗАТВЕРДЖЕНО:

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студента *Шворака Микити Сергійовича* **академічної групи** *125-19-2*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка комплексної системи захисту інформації в інформаційно-комунікаційній системі підприємства «Vinson»*

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

Розділ	Зміст	Термін виконання
Розділ 1	Опис підприємства «Vinson», Аналіз поточного стану інформаційної безпеки ІКС, аналіз існуючих заходів з захисту інформації на попередньому етапу, визначення необхідності у створенні КСЗІ.	25.02.2023 – 31.03.2023
Розділ 2	Визначення складу захищуваної інформації, вибір методів та засобів захисту, розробка проекту КСЗІ.	01.04.2022 – 12.05.2023
Розділ 3	Розрахунки капітальних витрат, економічного ефекту та терміну окупності капітальних інвестицій застосування запропонованих рішень.	13.05.2022 – 09.06.2023

Завдання видано _____ Мілінчук. Ю.А.
(підпис керівника) (прізвище, ініціали)

Дата видачі: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Шворак М.С
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: с.88, 1 рис., 13 табл., 4 додатки, 17 джерел.

Об’єкт дослідження: інформаційно-комунікаційна система на підприємстві.

Предмет дослідження: аналіз комплексної системи захисту ІКС на досліджуваному підприємстві.

Мета кваліфікаційної роботи: виокремлення напрямів покращення комплексної системи захисту інформації в інформаційно-комунікаційній системі підприємства.

Наукова новизна результатів полягає у принципово новому підході до розробки комплексної системи захисту інформації в інформаційно-комунікаційній системі підприємства.

У першому розділі було виконано обстеження ІКС, а саме: загальні відомості про підприємство, співробітники та їх обов’язки, огляд програмного забезпечення підприємства, визначені актуальні загрози для інформації, яка обробляється в ІКС.

У спеціальній частині було визначено склад інформації, що захищається, а саме: комерційна інформація, технічна інформація, фінансова та персональні дані. Було обрано методи та засоби захисту в інформаційно-комунікаційній системі.

У економічному розділі було обґрунтовано економічну доцільність реалізації КСЗІ для підприємства, прораховано всі витрати на реалізацію та розробку КСЗІ в ІКС, та надано рекомендації щодо зниження витрат на розробку на обслуговування КСЗІ.

ІНФОРМАЦІЙНА БЕЗПЕКА, КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ЗАСОБИ ЗАХИСТУ

Abstract

Explanatory note: p. 76, fig. 18, tab. 1, 4 additions, 39 sources.

Object of research: information and communication system at the enterprise.

Subject of research: analysis of the integrated ICS protection system at the enterprise under study.

The purpose of the qualification work: to identify areas for improving the integrated information security system in the information and communication system of the enterprise.

The scientific novelty of the results lies in a fundamentally new approach to the development of an integrated information security system in the information and communication system of an enterprise.

In the first section, a survey of the ICS was carried out, namely: general information about the enterprise, employees and their responsibilities, an overview of the enterprise software, and current threats to the information processed in the ICS.

In a special part, the composition of the protected information was determined, namely: commercial information, technical information, financial and personal data. The methods and means of protection in the information and communication system were selected.

The economic section substantiates the economic feasibility of implementing an IPSS for an enterprise, calculates all the costs of implementing and developing an IPSS in an ICS, and provides recommendations for reducing the development costs for maintaining an IPSS.

INFORMATION SECURITY, INTEGRATED INFORMATION SECURITY SYSTEM, MEANS OF PROTECTION

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – Автоматизована система;

ІКС– Інформаційно-комунікаційна система;

ІТ – Інформаційні технології;

КСЗІ – Комплексна система захисту інформації;

МСФЗ- міжнародні стандарти фінансової звітності;

ОС- Операційна система;

ОТЗ- Організаційно технічні заходи;

ПЗ – Програмне забезпечення;

ПК- персональний комп'ютер;

СВА – Системи виявлення атак;

ШІ – Штучний інтелект;

GDPR- General Data Protection Regulation- Загальний регламент про захист даних;

USB- Universal Serial Bus- універсальна послідовна шина;

VPN -Virtual Private Network - Віртуальна приватна мережа;

ЗМІСТ

ВСТУП

Актуальність обраної теми полягає в тому, що в сучасному світі, де інформаційні технології відіграють дуже важливу роль у бізнес-операціях, інформаційна безпека є одним із найважливіших питань, які потребують негайного вирішення. Збільшення кількості зловмисних кібератак, розповсюдження вірусів та інших загроз інформаційній безпеці ставить перед нами завдання створення комплексної системи захисту інформації в інформаційно-комунікаційній системі підприємства «Vinson».

Підприємство «Vinson» займається перероблюванням та пакуванням рослинної сировини, здебільшого горіхів. У своїй діяльності підприємство оперує великим обсягом конфіденційної інформації, такої як технологічні розробки, клієнтські дані, фінансові звіти та інше. Враховуючи зростання кіберзагроз та зміни сучасних методів забезпечення кібербезпеки, необхідно створити проактивну систему захисту інформації, яка відповідає сучасним потребам і забезпечує надійність і безпеку даних у всіх сферах діяльності підприємства.

Метою даної кваліфікаційної роботи є розробка КСЗІ для підприємства «Vinson». Система захисту інформації буде здійснювати контроль діяльності компанії та використовувати новітні методи та технології комп'ютерної безпеки для забезпечення точності, конфіденційності та доступності інформації. Частиною дослідження є вивчення поточної ситуації інформаційної безпеки компанії, виявлення потенційних загроз, аналіз поточної системи безпеки та створення нової, комплексної та ефективної системи інформаційної безпеки.

Відповідно до поставленої мети визначено такі завдання дослідження:

– проаналізувати поточний стан інформаційної безпеки інформаційно-комунікаційної системи підприємства «Vinson»;

– визначити сильні та слабкі сторони чинних заходів безпеки на підприємстві;

– виокремити можливі загрози в інформаційній безпеці компанії;

– проаналізувати типи атак, які можуть призвести до порушень безпеки, зокрема зловмисне програмне забезпечення, соціальна інженерія, фішинг та інші загрози;

– розробити комплексну систему захисту інформації, яка відповідає загрозам і потенційним потребам підприємства;

– визначити необхідні технологічні рішення, зокрема, антивірусні системи, системи моніторингу тощо для забезпечення надійного захисту даних;

– реалізувати розроблену систему захисту інформації та провести її впровадження в інформаційно-комунікаційну систему підприємства;

Результатом цієї кваліфікаційної роботи стане комплексна система захисту даних, розроблена спеціально для досліджуваного підприємства «Vinson». Система буде враховувати інформацію про особливості діяльності компанії та забезпечувати надійний захист інформації від можливих загроз. Розроблена система має забезпечити підприємству високий рівень кібербезпеки, покращити надійність, конфіденційність і доступність даних.

РОЗДІЛ 1.
ОПИС ТА АНАЛІЗ ПІДПРИЄМСТВА «VINSON».
ВИЗНАЧЕННЯ НЕОБХІДНОСТІ СТВОРЕННЯ КСЗІ

1.1 Опис досліджуваного підприємства.

Підприємство «Vinson» - це інноваційна компанія, що спеціалізується у переробленні рослинної сировини, зокрема горіхів та виробництвом різноманітної продукції. У процесі перероблювання використовуються передові технології, що дозволяють зберегти корисні властивості сировини та отримати якісний фінальний продукт. Виробництво забезпечує високий рівень контролю якості на всіх етапах виробництва та дотримується всіх необхідних стандартів і вимог. Мета підприємства полягає в створенні високоякісних продуктів, які поєднують в собі природну смакову насиченість та корисні властивості. Завдяки використанню передових технологій та відповідності найвищим стандартам якості, вони здатні задовольнити потреби найвимогливіших клієнтів.

Організація виробляє широкий асортимент продукції на основі горіхів. Серед продукції можна виділити ядра горіхів, олію з горіхів, сухофрукти з додаванням горіхів, солодощі та десерти на основі горіхів, а також інші інноваційні продукти. Всі вироби фірми відповідають високим стандартам якості та безпеки харчових продуктів.

«Vinson» акцентує увагу на збереженні цінних харчових властивостей горіхів під час їх перероблення. Кожен етап виробництва, починаючи зі збору сировини, проходить зі строгим контролем якості, що дозволяє зберегти неповторний смак, аромат і корисні речовини горіхів. Підприємство використовує передові технології перероблювання, включаючи лущення, сушіння, подрібнення та наступну обробку, щоб гарантувати найкращі результати.

Підприємство має сучасну виробничу базу, оснащену передовими технологічними лініями та обладнанням для перероблення рослинної сировини. Виробничі приміщення обладнані необхідними системами безпеки та контролю якості. Крім того, фірма має власні складські приміщення для зберігання готової продукції та сировини.

Однією з переваг виробництва є постійний пошук нових інноваційних продуктів. Фірма постійно вдосконалює свої технології, вивчає нові тенденції та ринкові потреби, щоб задовольнити смаки своїх клієнтів і відповідати вимогам сучасного ринку. Крім того, «Vinson» активно співпрацює з фермерами та постачальниками сировини, що дозволяє отримувати високоякісну сировину безпосередньо з джерела. Виробництво прагне досягти міцної позиції на ринку, як лідера у сфері перероблення рослинної сировини.

Команда «Vinson» - це згуртована група професіоналів з глибоким розумінням процесів перероблювання рослинної сировини. Вони працюють разом, поєднуючи креативний підхід з науковими знаннями, щоб розробляти нові рецепти, виробляти інноваційні продукти та покращувати наявні. Спеціалісти знаходяться на передній лінії досліджень і розвитку, постійно вдосконалюючи процеси та шукаючи нові способи максимізувати якість та ефективність перероблювання. Підприємство «Vinson» має добре організовану систему управління. Управління підприємством здійснюється керівництвом, яке складається з директора та вищих керівників. До складу персоналу також входять спеціалісти з різних галузей, таких як виробництво, логістика та фінанси.

Підприємство має закритий доступ до свого офісу та цеху, тому ніхто, окрім співробітників, не має доступу до захищеної інформації. Підприємство на даному етапі не має КСЗІ, але через недавній витік інформації та через плани масштабування підприємства, виникла необхідність приділити належний контроль до безпеки внутрішніх даних.

Розглянемо структуру підприємства та хто має доступ до інформації (рис. 1.1.)

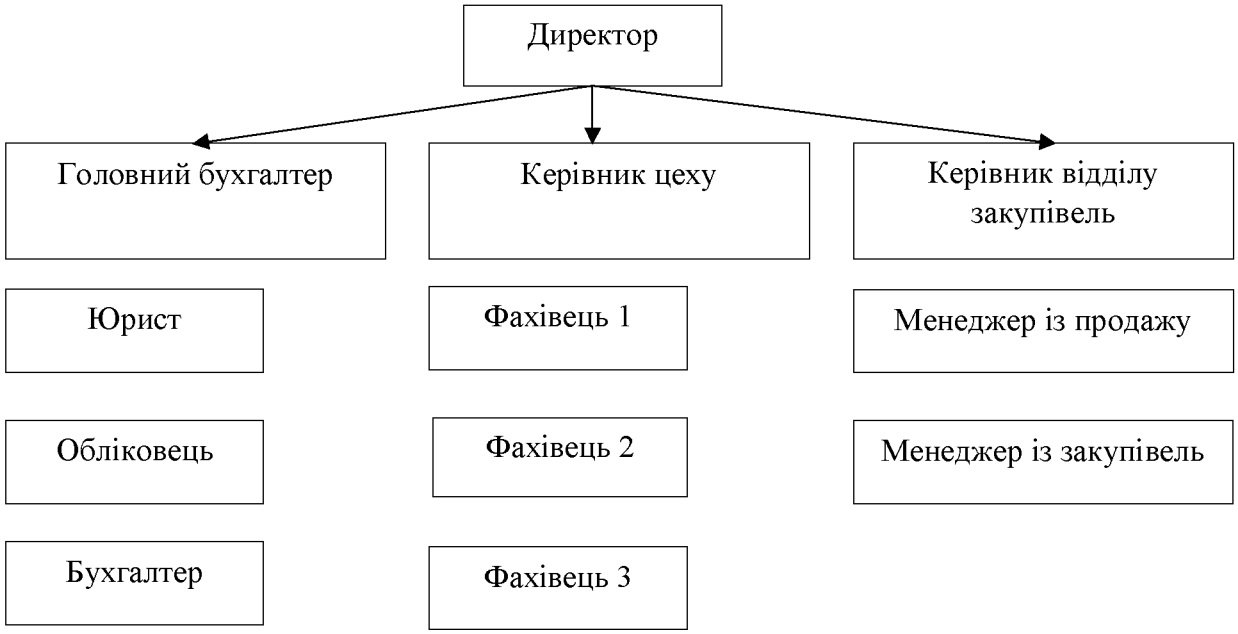

Рисунок 1.1. Організаційна структура підприємства

Директор - власник підприємства, має доступ до захищеної інформації. Його основні обов'язки – управління діяльністю підприємства, затвердження стратегій та річних планів. Йому підзвітні бухгалтерський,, виробничий та логістичний відділи.

У складі бухгалтерського відділу є головний бухгалтер- людина, яка виконує організаційно-розпорядчі та адміністративно-господарські функції, відповідає за організацію і ведення бухгалтерського та податкового обліку, достовірне складання звітності. Також бухгалтеру підпорядковані: юрист, економіст, бухгалтер. Вони мають повний доступ до ІКС.

Керівник виробничого відділу – відповідний за налагодження праці у цеху, відповідний за виконання плану виготовлення продукції, усіх можливих нюансів, які виникають у фахівців при виробництві. У нього в розпорядженні: фахівці з переробки рослинної сировини та фахівці з ремонту цехового обладнання. Має повний доступ до ІКС.

Керівник логістичного відділу відповідає за своєчасну доставку сирої сировини до виробничого відділу. Також відповідає за перші переговори з майбутніми партнерами підприємства. У його розпоряджені: менеджери з поставок та менеджери з закупівель. Вони мають повний доступ до ІКС.

Організаційний склад персоналу досить малий, проте Vinson намагається йти в ногу з часом. Так як деякі компоненти їх комп`ютерної безпеки застарілі – підприємство вирішило в першу чергу налагодити питання із безпекою, а вже потім масштабуватися. Саме з цією метою фірмі необхідне створення КСЗІ.

На підприємстві наявна інформації, яка підлягає автоматизованій обробці та потребує захисту і забезпечення конфіденційності, цілісності та доступності відповідно до вимог нормативно-правових актів України, що є підставою для необхідності створення КСЗІ. Власником інформації, прийняте рішення щодо створення КСЗІ та видано наказ «Про визначення відповідального за забезпечення технічного захисту інформації та створення КСЗІ на підприємстві ТОВ «Vinson».

Підприємство «Vinson» дбає про захист своїх інтелектуальних прав і має деякі патенти та ліцензії на свої розробки та технології, також укладає угоди щодо прав власності та користування з деякими постачальниками сировини та співробітниками, що забезпечує йому стабільність та конкурентоспроможність на ринку

Організація має успішні фінансові результати господарської діяльності. За останні роки підприємство зміцнило своє фінансове становище та збільшило обсяги виробництва і продажу своєї продукції. Завдяки високій якості продукції та інноваційному підходу до виробництва, підприємство зуміло завоювати довіру споживачів та отримати стійку позицію на ринку. Розширення асортименту продукції та впровадження нових технологій дозволяють підприємству залучати нових клієнтів та розширювати свої ринки збуту. Завдяки цьому, фінансові показники підприємства «Vinson» постійно зростають, що свідчить про його успішну та стабільну роботу.

1.2 Аналіз існуючих заходів із захисту інформації.

Заходи із захисту інформації - це комплекс заходів, стратегій і технологій, спрямованих на захист інформації від несанкціонованого доступу, втрати, руйнування або зміни. Оскільки інформація є цінним активом для багатьох організацій і осіб, важливо забезпечувати її конфіденційність, цілісність та доступність.

Захист інформації від несанкціонованого доступу дозволяє зберегти конфіденційні дані в безпеці. Це може бути особиста інформація про клієнта, фінансові дані, комерційна таємниця або будь-яка інша приватна інформація. Ці дані повинні бути захищені від несанкціонованого доступу, щоб запобігти витоку інформації, крадіжці або неправомірному використанню.

Система захисту інформації допомагає забезпечити цілісність даних, що означає, що дані залишаються недоторканими та незмінними. Це важливо для попередження незаконної модифікації, випадкових помилок чи зловмисних дій, які можуть призвести до пошкодження інформації та спотворення її змісту.

Система захисту інформації також гарантує доступність даних, коли користувачам це необхідно. Це означає, що інформація повинна бути доступною для авторизованих користувачів, коли вони цього вимагають, і вона не повинна бути недоступною через системні помилки, відмову обладнання або зловмисні атаки.

Політика інформаційної безпеки підприємства «Vinson» наведена у таблиці 1.1.

Таблиця 1.1.

Політика інформаційної безпеки підприємства

Розділ	Пункти
Загальні принципи	Інформаційна безпека є невід'ємною частиною діяльності підприємства «Vinson» і повинна бути дотримувана всіма співробітниками та сторонніми партнерами.
	Керівництво підприємства зобов'язується забезпечувати ресурси, необхідні для впровадження та збереження ефективної системи інформаційної безпеки.

	Інформаційна безпека повинна враховуватися на всіх етапах діяльності підприємства, включаючи планування, розробку, впровадження та експлуатацію інформаційних систем.
Класифікація інформації	Всю інформацію підприємства «Vinson» необхідно класифікувати залежно від її конфіденційності, цілісності та доступності.
	Класифікація інформації має бути проведена згідно з установленими процедурами та критеріями
	Визначені категорії інформації повинні мати відповідні рівні захисту та доступу
Фізична безпека	Підприємство «Vinson» зобов'язується забезпечувати фізичну безпеку своїх приміщень, де знаходиться обладнання та інформація
	Контроль доступу до приміщень повинен бути здійснюватися за допомогою системи ідентифікації та автентифікації, такої як картки доступу або біометричні системи
	Обладнання, що зберігає чутливу інформацію, повинно бути фізично захищене від несанкціонованого доступу, втрати або крадіжки
Керування доступом	Всі співробітники підприємства «Vinson» повинні мати визначені ролі та рівні доступу відповідно до їхніх обов'язків та потреб
	Керування доступом до інформаційних ресурсів повинно здійснюватися на основі принципу найменших привілеїв, тобто користувач повинен мати доступ лише до необхідного обсягу інформації для виконання своїх обов'язків
	Права доступу до інформаційних систем повинні періодично переглядатися та оновлюватися відповідно до змін у ролях та обов'язках співробітників.
Захист інформації	Усі інформаційні системи підприємства «Vinson» повинні бути забезпечені відповідними технічними заходами безпеки, такими як антивірусне програмне забезпечення, брандмауери, шифрування даних тощо
	Передача чутливої інформації повинна здійснюватися за допомогою захищених каналів зв'язку, наприклад, використанням протоколів шифрування та віртуальних приватних мереж (VPN).
	Всі співробітники підприємства «Vinson» повинні бути навчені засобам інформаційної безпеки та виконувати регулярні перевірки на предмет виявлення можливих загроз інформаційній безпеці
Реагування	Підприємство «Vinson» повинно мати визначені процедури

на інциденти	та плани дій для реагування на інциденти інформаційної безпеки, такі як вторгнення, витоги даних або вірусні атаки
	Повідомлення про інциденти повинні бути здійснені швидко і ефективно, включаючи встановлення контактів зі спеціалістами з безпеки та розробку планів відновлення.
	Проведення аналізу інцидентів та впровадження необхідних заходів для запобігання подібним ситуаціям у майбутньому

Ця політика інформаційної безпеки підприємства «Vinson» забезпечує основні принципи та заходи для захисту інформації від несанкціонованого доступу, витоків даних та інших загроз безпеці. Вона повинна оновлюватись та переглядатися періодично, відповідно до змін у загрозах та потребах підприємства.

На основі наданих положень політики інформаційної безпеки підприємство «Vinson» можна відзначити, що вона містить основні принципи та заходи для захисту інформації від несанкціонованого доступу, витоків даних та інших загроз безпеці.

Основні аспекти політики, які можна оцінити, включають:

1.Загальні принципи. Загальні принципи, які зобов'язують керівництво забезпечити ресурси та включають інформаційну безпеку на всіх етапах діяльності, є важливими і відповідають стандартам та регуляторним вимогам.

2.Класифікація інформації. Наявні положення про класифікацію інформації відповідають стандартам безпеки даних. Проте, без конкретизації процедур та критеріїв класифікації, оцінка їх відповідності стандартам стає складнішою.

3.Фізична безпека. Заходи щодо фізичної безпеки, зокрема контроль доступу та захист обладнання, відповідають загальним стандартам безпеки приміщень та фізичної безпеки.

4.Керування доступом. Загальні принципи керування доступом до інформаційних ресурсів, такі як принцип найменших привілеїв та періодичний перегляд прав доступу, є важливими аспектами стандартів безпеки даних.

5.Захист інформації. Заходи для захисту інформаційних систем, включаючи технічні засоби безпеки та навчання співробітників, відповідають загальним стандартам безпеки інформації.

6.Реагування на інциденти.Наявність процедур та планів реагування на інциденти відповідає вимогам стандартів безпеки даних.

Захист фізичної безпеки підприємство виконало на вищому рівні. У охоронців є електрона база даних робітників, за допомогою якої вони можуть перевіряти електроні перепустки співробітників, це допомагає уникати небажаних гостів на підприємстві. Також, слід додати, що компанія дуже сувора до того, щоб тільки працівники знаходились на підприємстві, наявна система штрафів та покарань.

В сучасному світі, де технології швидко розвиваються й інформація стає найціннішим ресурсом, належна мережева інфраструктура стає ключовим фактором успіху для багатьох підприємств. Підприємство «Vinson» не є винятком. Фірма розуміє, що добре організована та безперебійна мережа є фундаментом для ефективного функціонування та розвитку бізнесу.

Мережева інфраструктура відіграє вирішальну роль у сучасному бізнес-середовищі, особливо для компаній, як «Vinson», що займаються переробкою сировини. Відправляючись в невидимий світ передачі даних, ця інфраструктура створює основу для швидкого, ефективного та безперебійного обміну інформацією всередині організації. «Vinson» ще не розробив мережеву структуру для своєї компанії, тому розробимо в рамках створення КСЗІ.

Завдяки стрімкому розвитку технологій і інноваційному підходу до виробництва, підприємство «Vinson» трохи відстало від сучасного комп'ютерного та програмного технічного обладнання. Це надає конкурентам підприємства значну перевагу на ринку перероблення рослинної сировини.

Технічне цехове обладнання підприємства «Vinson» на даний момент складається з передових технологічних ліній, машин та устаткування, які забезпечують високу ефективність та якість перероблення. Виробництво планує використовувати сучасні механічні та автоматизовані системи для обробки та

сортування сировини, що дозволить забезпечити точність та швидкість виробничих процесів.

Фірма оснащена передовими технологіями, яке дозволить зберегти корисні властивості сировини та отримати продукцію високої якості. Використання контрольно-вимірювальних систем дозволить здійснювати постійний моніторинг якості продукції на кожному етапі виробництва, що гарантує клієнтам компанії бездоганний результат.

Крім того, технічне цехове обладнання відповідає вимогам безпеки та екологічних стандартів. Підприємство дбає про ефективне використання енергоресурсів і зменшення впливу на навколишнє середовище. «Vinson» прагне до сталого розвитку, і тому впроваджує енергоефективні технології та засоби автоматизації, що допомагають знизити споживання ресурсів і викиди в атмосферу.

Технічне цехове обладнання підприємства «Vinson» є однією складовою успіху виробництва, яка допомагає досягати високих стандартів якості, ефективності та інноваційності. Підприємство задоволено своїми технологіями та завжди готові надати своїм клієнтам найкращі рішення в галузі перероблювання рослинної сировини.

Розглянемо технічне комп' ютерне обладнання компанії: (див табл. 1.2)

Таблиця 1.2 – Перелік основних технічних засобів(ОТЗ)

№	Назва	Серійний номер	Де знаходиться
1	Ноутбук Lenovo Z570	8439204583920	Кабінет директора, на столі робочого місця директора
2	Ноутбук Lenovo Z570	9430259304930	Кабінет бухгалтерів, на столі робочого місця головного бухгалтера
3	Ноутбук Lenovo Z570	2394290852409	Кабінет бухгалтерів, на столі робочого місця бухгалтера
4	Ноутбук Lenovo Z570	3495234942045	Кабінет бухгалтерів, на столі робочого місця юриста
5	Ноутбук Lenovo	7429043280955	Кабінет бухгалтерів, на столі

	Z570		робочого місця обліковця
6	Ноутбук Lenovo Z570	6527892438042	Кабінет закупівель, на столі робочого місця керівника відділу закупівель
7	Ноутбук Lenovo Z570	8274389752934	Кабінет закупівель, на столі робочого місця менеджера за продажів
8	Ноутбук Lenovo Z570	9234572479432	Кабінет закупівель, на столі робочого місця менеджера з закупівель
9	Ноутбук Lenovo Z570	2004334903414	Кабінет керівника цеху, на столі робочого місця керівника цеху
10	Принтер Canon PIXMA TS3150	2349809234852	Кабінет директора, на столі робочого місця директора
11	Принтер Canon PIXMA TS3150	2903487452435	Кабінет бухгалтерів, на столі робочого місця головного бухгалтера
12	Бездротовий маршрутизатор Keenetic Ultra (KN-1810)	9028489723484	Кабінет директора на комоді з документами в ПН-ЗХ куту кімнати

Проаналізувавши ОТЗ можна зробити висновок:

– працівники фірми використовують комп'ютери та ноутбуки для виконання своїх робочих завдань, вони мають доволі слабке апаратне забезпечення, де невстановлені всі необхідні програми для вирішення завдань. Працівники використовують застарілі моделі ноутбуків Lenovo Z570 ,які було придбано у Вересні 2018 року, коли підприємство розпочинало свою роботу, що зменшують продуктивність робітників;

– у підприємства є принтери для друку та сканування документів, вони використовуються для створення паперової документації та її зберігання;

– підприємство використовує точки доступу Wi-Fi для забезпечення безперебійного з'єднання всіх пристроїв у мережі.

В рамках сучасного бізнесу, програмне забезпечення відіграє вирішальну роль у забезпеченні ефективності та успішності будь-якого підприємства. «Vinson» прекрасно розуміє ситуацію, що склалася у фірмі, розуміє, що програмне забезпечення застаріле, не відповідає вимогам безпеки підприємства, тому планує оновити або створити нові компоненти ПЗ, включаючи:

– антивірусне програмне забезпечення, яке є важливими інструментами для виявлення і блокування шкідливих програм, вірусів та інших загроз для безпеки. Вони надають регулярні оновлення вірусних баз, активний моніторинг та сканування системи для виявлення можливих загроз;

– фаєрволи, що допомагають контролювати доступ до мережі та блокувати небажані підключення, вони фільтрують мережевий трафік, забезпечуючи захист від несанкціонованого доступу до системи;

– антишпигунське програмне забезпечення, ці програми здатні виявляти і видаляти шпигунське програмне забезпечення та рекламний софт, допоможуть захистити особисту інформацію, запобігаючи витоку даних;

– віртуальна приватна мережа (VPN), що дозволить створювати зашифроване з'єднання між пристроєм та Інтернетом. Вони допомагають забезпечити конфіденційність та анонімність, шифруючи трафік і приховуючи вашу реальну IP-адресу;

– парольні менеджери дозволяють зберігати і керувати паролями. Вони генерують складні паролі, зберігають їх в зашифрованому вигляді та автоматично заповнюють поля входу на веб-сайтах, забезпечуючи безпеку паролів і запобігаючи повторному використанню паролів;

– програми для шифрування диска дозволяють захистити ваші дані шляхом шифрування всього вмісту вашого диска або окремих файлів та папок.

Оновлення операційної системи важливо з кількох причин:

1.Безпека: Оновлення операційної системи допомагає усунути вразливості та уразливі місця, що можуть бути використані зловмисниками для несанкціонованого доступу до системи та крадіжки даних. Патчі та виправлення, що входять до оновлень, зміцнюють безпеку вашої системи.

2.Виправлення помилок: Оновлення ОС містять виправлення для помилок, які виявлені в попередніх версіях. Це допомагає поліпшити стабільність та продуктивність системи, усуваючи збої та некоректну роботу програм.

3.Покращення функціональності: Оновлення можуть включати нові функції, покращення і оптимізацію, що поліпшують роботу та зручність використання системи. Це дозволяє отримати доступ до нових можливостей та підвищити продуктивність роботи.

Програмне забезпечення має бути розроблене з урахуванням специфіки виробництва та потреб клієнтів. Для успішної сучасної роботи фірма має використовувати інтегровані системи управління, що дозволять керувати всіма аспектами діяльності підприємства: від прийняття сировини до випуску готової продукції. Це забезпечить їм цілісну перспективу бізнесу та дозволить ефективно планувати, координувати та контролювати виробничі процеси.

Програмне забезпечення підприємства відповідає мінімальним стандартам безпеки та захисту інформації. Фірма намагається вживати заходів для забезпечення конфіденційності, цілісності та доступності своїх даних, а також захисту від потенційних кібератак і загроз.

Підприємству «Vinson» потрібно оновлювати своє програмне забезпечення, щоб воно допомагало фірмі досягати максимальної продуктивності, ефективності та якості у переробній діяльності. Компанія планує вдосконалювати своє програмне забезпечення, враховуючи нові технології та потреби своїх клієнтів, з метою забезпечення місця лідера на ринку та задоволення їх очікувань.

Розглянемо наявне програмне забезпечення:

1. Операційна система: На комп'ютерах та серверах «Vinson» встановлені застаріла операційна система Windows 7, вона забезпечує стабільну та не зовсім безпечну роботу пристроїв, бо підтримка цієї операційної системи завершилася 14 січня 2020 року, а це означає, що більше не буде оновлень безпеки, будуть відсутні нові функції та покращення, збільшений ризик атак, бо

зловмисники будуть використовувати вразливості, які більше не будуть виправлені. Доволі актуальною є проблема обмеженої сумісності. Нові програми можуть не підтримувати Windows 7, і це буде обмежувати можливість компанії роботи з новими технологіями, та знижувати продуктивність.

2. Програмне забезпечення: Підприємство використовує антивірусне програмне забезпечення . для забезпечення безпеки даних.

3. Системи зберігання даних: «Vinson» використовує системи зберігання даних, такі як CRM-система, файлові системи та хмарні системи зберігання даних, для ефективного зберігання та організації інформації про клієнтів, постачальників та виробництво

У сучасному цифровому світі, де інформація стала найціннішим активом, захист інформації та кібербезпека стають життєво важливими аспектами для будь-якого підприємства. Підприємство «Vinson» не робить винятку і починає приділяти велику увагу заходам забезпечення безпеки своїх даних та систем.

Компанія визнає, що в сучасному цифровому середовищі кіберзагрози стають все складнішими й винахідливими та планують вживати широкого спектра заходів забезпечення інформаційної безпеки, щоб зменшити ризики та забезпечити захист своїх даних.

Один із ключових аспектів стратегії захисту інформації - це впровадження передових технологій і систем безпеки. Підприємство використовує застаріле програмне забезпечення та апаратні засоби, що не може дозволити їм на належному рівні виявляти та запобігати потенційним загрозам, включаючи віруси, зламані паролі, шкідливі програми та інші види кібератак. Компанія доволі рідко проводить аудит безпеки, щоб оцінити ефективність наших заходів та виявити можливі уразливості.

Підприємство підтримує принцип безперервності бізнесу та резервне копіювання даних. Фірма має в планах регулярні оновлення своїх систем, з метою виявлення та усунення можливих слабких місць у захисті інформації.

Аналізуючи заходи з захисту інформації та кібербезпеки підприємства, можна сказати, що підприємство ніколи не задумувалось про забезпечення належного захисту інформації, але через недавній витік інформації, та через плани масштабування підприємства «Vinson» серйозно поставилися до питання захисту інформації підприємства

Нижче наведені основні заходи, які вживає підприємство «Vinson»:

1. Політика безпеки: Vinson розробив і впроваджує політику безпеки, яка встановлює правила та процедури для захисту інформації та забезпечення відповідності нормам безпеки.

2. Резервне копіювання та відновлення даних: Підприємство регулярно робить резервні копії важливих даних та має процедури відновлення даних в разі втрати або пошкодження.

3. Строгий контроль доступу: Підприємство використовує систему контролю доступу, що дозволяє обмежити фізичний і логічний доступ до приміщень та інформації.

Отже, підприємство «Vinson» займається перероблюванням рослинної сировини, зокрема горіхів, і привертає увагу до свого, технічного обладнання, програмного забезпечення насамперед тим, що вони дуже відстали від часу.

Технічне обладнання, що використовується в підприємстві «Vinson», включає застаріли сервери, робочі станції, мережеві пристрої та засоби зберігання даних. Це не дозволяє підприємству ефективно опрацьовувати великі обсяги даних і забезпечувати швидкий доступ до інформації для співробітників.

Програмне забезпечення, яке використовується в підприємстві «Vinson», включає антивірус та програми для обробки та аналізу даних, мережі. Ці програми допомагають підприємству керувати мережею, забезпечувати безпеку і цілісність даних, але самі програми є застарілими, що не допомогає компанії проводити належний аналіз своєї діяльності, а також захисту мережі.

Підприємство «Vinson» планує приділяти велику увагу заходам з захисту інформації та кібербезпеки. Всі ці заходи призначені для забезпечення конфіденційності, цілісності та доступності інформації підприємства.

За рахунок того, що в компанії не забезпечений належний рівень технічного обладнання, програмного забезпечення та заходів з захисту інформації та кібербезпеки, підприємство «Vinson» не може забезпечувати стійкість та надійність своєї інформаційно-комунікаційної системи, захищати важливі дані від несанкціонованого доступу та забезпечувати безперебійну роботу бізнес-процесів. Це не дозволяє підприємству на 100% зосередитися на своїх головних завданнях і досягати успіху у своїй галузі.

1.3 Аналіз поточного стану інформаційної безпеки ІКС підприємства Vinson

Аналіз поточного стану інформаційної безпеки інформаційно-комунікаційної системи підприємства включає оцінку потенційних загроз, ідентифікацію потенційних вразливостей та оцінку ефективності заходів забезпечення безпеки. Ось кілька кроків, які допоможуть зробити аналіз поточного стану інформаційної безпеки ІКС підприємства Vinson:

– Ідентифікація активів: Потрібно скласти перелік інформаційних активів, які належать підприємству. Це можуть бути грошові кошти, рахунки клієнти , запаси, нерухомість, обладнання, інтелектуальна власність, інвестиції, дебіторська заборгованість, тощо. (див табл. 1.3 та 1.4)

– Оцінка загроз: Потрібно визначити потенційні загрози, які можуть впливати на безпеку інформаційної системи. Це можуть бути хакерські атаки, зловживання співробітників, віруси, фішингові атаки тощо. Розглянути як зовнішні, так і внутрішні загрози.

– Визначення вразливостей: Необхідно виявити потенційні вразливості вашої інформаційно-комунікаційної системи. Це може включати

застарілі програмне забезпечення, слабкі паролі, недостатні заходи з контролю доступу тощо.

– Оцінка ризику: Слід оцінити ймовірність та вплив кожної загрози на активи підприємства. Для цього використовуємо шкалу від низького до високого ризику, щоб визначити найбільш значущі загрози.

– Аналіз типів атак: Аналіз атак, які можуть призвести до порушень безпеки, зокрема зловмисне програмне забезпечення, соціальна інженерія, фішинг та інші загрози

– Аналіз заходів безпеки: Оцінка ефективності поточних заходів забезпечення безпеки. Це включає перевірку наявності антивірусного програмного забезпечення, брандмауера, системи контролю доступу, резервного копіювання даних тощо.

– Розробка плану заходів: На основі виявлених загроз і вразливостей варто розробити план заходів забезпечення безпеки. Це можуть бути технічні заходи (оновлення програмного забезпечення, встановлення ефективних механізмів захисту) та організаційні заходи (навчання співробітників з питань безпеки, встановлення політик безпеки тощо).

– Впровадження та моніторинг: Потрібно реалізувати заплановані заходи та систематично контролювати їх ефективність. Потрібно забезпечити постійне оновлення системи безпеки, враховуючи нові загрози та вразливості

Важливо пам'ятати, що безпека інформаційної системи є постійним процесом і потребує систематичного оновлення та вдосконалення.

Таблиця 1.3. – Ідентифікація активів

Найменування	**Сума**
Грошові кошти	353 000грн
Рахунки-клієнти	72 000 грн
Запаси	97 000 грн
Нерухомість	0 грн

Обладнання	995 000 грн
Інтелектуальна власність	50 000 грн
Інвестиції	0 грн
Всього	1 567 000 грн

Таблиця 1.4. – Ідентифікація пасивів

Найменування	**Сума**
Кредиторська заборгованість	0 грн
Позичковий капітал	65 000 грн
Власний капітал	0 грн
Всього	65 000 грн

У сучасному світі, де інформаційні технології є невід'ємною частиною діяльності більшості підприємств, забезпечення інформаційної безпеки стає ключовим завданням. Підприємство Vinson, яке спеціалізується на переробці горіхів, також стикається з різноманітними загрозами в цифровому середовищі, що можуть негативно позначитися на його діяльності, репутації та фінансовому стані.

Для забезпечення ефективного управління інформаційною безпекою та запобігання можливим загрозам, підприємство Vinson може скористатися моделлю оцінки загроз. Ця модель дозволяє ідентифікувати потенційні загрози, оцінити їх імовірність виникнення та потенційний вплив на активи підприємства. На основі цих оцінок, можна призначити вагу або пріоритет кожній загрозі, що дозволяє фокусуватися на найважливіших аспектах інформаційної безпеки.

Активи підприємства Vinson потребують захисту від можливих загроз, що можуть вплинути на їх цілісність, конфіденційність та доступність. Оцінка загроз та призначення їм пріоритету дозволить підприємству Vinson розробити

ефективні стратегії захисту, які спрямовані на забезпечення надійності та безпеки його активів.

Модель оцінки загроз інформаційної безпеки підприємства Vinson:

1.Ідентифікація активів:

– інформаційні системи (CRM-системи, файлові системи, хмарні системи зберігання даниї)

– бази даних з інформацією про клієнтів, постачальників та фінансові дані

– електронна пошта та комунікаційна система(маршрутизатор)

– конфіденційна документація щодо рецептур, технологій та клієнтських контрактів

– клієнтські дані (замовлення, адреси, контактна інформація)

2.Виявлення загроз:

– хакерські атаки (DDoS атаки, вторгнення, фішинг)

– втрата або крадіжка пристроїв, що містять конфіденційну інформацію

– віруси, шкідливі програми та розповсюдження малварного коду

– несанкціонований доступ співробітників до конфіденційної інформації

– порушення даних через недостатні заходи безпеки

3.Аналіз загроз:

– оцінка імовірності виникнення загрози (низька, середня, висока)(див табл. 1.5)

– оцінка потенційного впливу загрози на активи (низький, середній, високий) (див табл.1.6)

– визначення рівня доступності та вразливості інформаційної інфраструктури (див табл. 1.7)

– врахування існуючих заходів забезпечення безпеки (файрволи, антивірусне програмне забезпечення, регулярні оновлення)

4.Ранжування загроз: Призначення кожній загрозі ваги або пріоритету на основі її імовірності та впливу(див табл.1.8). Використання шкали або системи оцінювання (наприклад, від 1 до 5, де 1 - найнижчий пріоритет, 5 - найвищий пріоритет)

5.Розробка стратегій захисту:

– встановлення технічних засобів безпеки (файрволи, антивірусне програмне забезпечення, системи виявлення вторгнень)

– впровадження політик доступу та ідентифікації (сильні паролі, двофакторна аутентифікація)

– навчання співробітників з питань безпеки (свідомість про фішингові атаки, правила використання паролів)

– резервне копіювання даних та проведення регулярних аудитів безпеки

Таблиця 1.5 Форма для оцінки імовірності виникнення загрози

	Низька	Середня	Висока
Хакерські атаки			+
Втрата або крадіжка пристроїв	+		
Віруси,шкідливі програми		+	
Несанкціонований доступ співробітників	+		
Порушення даних			+

Підприємство Vinson не має належного рівня технічної та програмної безпеки, операційна система Windows 7, яка не підтримується з 14 січня 2020 року не може забезпечити належного рівня захисту інформації. В першу чергу через те, що вразливості системи більше не будуть виправлені. Антивірусне програмне забезпечення Avast Free Antivirus не найкращий вибір для безпеки даних, бо не має багатьох важливих коштів. Безкоштовна версія дійсно непоганий варіант, але для розробки КСЗІ нам потрібен всебічний антивірус з

багатьма функціями, безкоштовна версія, встановлена на ноутбуках співробітників фірми має лише основні функції захисту Також додається те, що підприємство не має достатнього рівня забезпечення технічного обладнання. Lenovo Z570 має застаріли комплектуючі, що заважає, як мінімум, встановити новітні програми захисту інформації. Через це на підприємстві існує висока загроза хакерських атак, порушення даних, та середній рівень загрози потрапляння вірусів, шкідливих програм.

Втрата або крадіжка пристроїв та несанкціонований доступ співробітників мають низький рівень виникнення загрози, через те, що на підприємстві використовується новітня система охорони, та перепусток, про яку було написано раніше.

Таблиця 1.6 Форма для оцінки потенційного впливу загрози на активи

	Низька	Середня	Висока
Грошові кошти			+
Рахунки-клієнти		+	
Запаси	+		
Обладнання	+		
Інтелекуальна власність			+

Запаси та обладнання мають низький рівень безпеки через гарну систему охорони підприємства. Рахунки клієнти мають середній рівень загрози, бо у підприємства не має усіх даних про рахунок клієнта. Грошові кошти, та інтелектуальна власність мають високий рівень ризику через технічні та програмні проблеми підприємства, а також через низький рівень обізнаності співробітників про політику безпеки компанії, та про елементарні засоби безпеки у мережі інтернет.

Таблиця 1.7 – Форма для визначення рівня доступності та вразливості інформаційної інфраструктури

	Низька	Середня	Висока
Фізичний доступ	+		
Логічний доступ			+
Аутентифікація та авторизація			+
Захист даних			+
Вразливості програмного забезпечення			+
Управління інцидентами		+	
Культура безпеки		+	

Логічний доступ має високий рівень вразливості, тому що окрім антивірусу у підприємства немає заходів безпеки. Аутентифікація та авторизація у будь якій системі або додатку виконуються за допомогою ідентифікації та паролю. Інших методів захисту для фірми не існує, і це загрожує витоком інформації про паролі. Вразливості програмного забезпечення та захист даних мають високий рівень через проблеми з програмним забезпеченням, про які написано раніше. Управління інцидентами має середній рівень, бо фірма, як тільки дізналась про виток інформації, відразу почала робити кроки для того, щоб така ситуація не повторилась, почала роботу по розробці КСЗІ. Культура безпеки має середній рівень, бо працівники не обізнані достатньою інформацією про технічний рівень безпеки, але мають високий рівень безпеки на виробництві, та дотримуються політики безпеки підприємства. Фізичний доступ має низький рівень вразливості, бо компанія дотримується останніх вимог охорони підприємства.

Аналіз типів атак, які можуть призвести до порушень безпеки інформаційно-комунікаційної системи Vinson, включає наступні загрози:

1. Зловмисне програмне забезпечення :

– віруси – програми, які прикріплюються до інших файлів та поширюються без дозволу користувача, вони можуть пошкоджувати дані, викрадати конфіденційну інформацію або навіть призводити до втрати контролю над системою;

– троянські програми – шкідливі програми, які приховуються під корисною або легітимною програмою та намагаються отримати несанкціонований доступ до системи або виконати шкідливі дії;

– рекламне ПЗ (Adware) – програми, які відображають рекламу без згоди користувача. Вони можуть впливати на продуктивність системи та порушувати приватність користувача.

2. Соціальна інженерія:

Надання фальшивих електронних повідомлень, веб-сторінок або телефонних дзвінків з метою викликати обман користувачів і викликати їх до виконання певних дій, таких як розкриття конфіденційної інформації або виконання фінансових транзакцій.

3. Використання слабких місць у безпеці:

Використання вразливостей програмного забезпечення, зловмисники можуть використовувати вразливості в операційних системах, програмах або додатках для злому системи та отримання несанкціонованого доступу.

4. Деніал сервісу (DoS) і Розподілений деніал сервісу (DDoS)

Атаки, спрямовані на перевантаження ресурсів мережі або серверів, що призводить до відмови в обслуговуванні або недоступності послуг для законних користувачів.

5. Несанкціонований доступ:

Злам пароля: Зловмисники можуть використовувати різні методи для вгадування або підбору паролів з метою незаконного доступу до системи або аккаунтів користувачів.

6. Внутрішні загрози:

Неналежна поведінка або недбалість співробітників можуть призвести до витоку конфіденційної інформації або порушень безпеки.

Для забезпечення адекватного рівня безпеки інформаційно-комунікаційної системи Vinson рекомендується впровадження широкого спектру заходів безпеки, включаючи регулярне оновлення програмного забезпечення, навчання персоналу з питань безпеки, використання міцних паролів, використання мережевих фаерволів та антивірусного програмного забезпечення відповідного рівня та моніторинг активності мережі для виявлення підозрілих дій.

Аналіз заходів безпеки підприємства Vinson, що використовує лише антивірусне програмне забезпечення Avast Free Antivirus, зроблено наступним чином:

1. Захист від вірусів і шкідливих програм:

Avast Free Antivirus надає базовий рівень захисту від вірусів, шкідливих програм та інших загроз, шляхом сканування системи на наявність вірусів та блокування підозрілих файлів.

2. Захист електронної пошти:

Avast Free Antivirus може надавати базовий рівень захисту електронної пошти, перевіряючи вхідні та вихідні повідомлення на наявність вірусів або шкідливих вкладень.

3. Брандмауер:

Avast Free Antivirus може містити модуль брандмауера, який допомагає блокувати небажаний мережевий трафік та захищати систему від несанкціонованого доступу.

4. Оновлення визначень вірусів:

Однією з важливих функцій Avast Free Antivirus є постійне оновлення бази визначень вірусів для виявлення нових загроз.

Однак, варто зазначити, що Avast Free Antivirus є базовим рішенням забезпечення безпеки, і для повноцінного захисту підприємства рекомендується впровадження додаткових заходів безпеки, таких як:

1. Встановлення апаратного або програмного файрволу, який дозволяє контролювати мережевий трафік та блокувати несанкціонований доступ до системи.

2. Антивірусні рішення класу "Enterprise". Потрібно розглянути можливість використання комерційних антивірусних рішень, спеціально розроблених для підприємств, з більш широким функціоналом та підтримкою корпоративних мереж.

3. Резервне копіювання даних. Регулярне резервне копіювання важливих даних та забезпечення доступу до резервних копій для відновлення інформації у разі втрати або пошкодження.

4. Система управління патчами: Встановлення системи управління патчами, яка автоматично оновлює програмне забезпечення та операційні системи з офіційними виправленнями безпеки.

5. Освіта співробітників: Проведення навчання та тренінгів з питань безпеки інформації для співробітників, щоб підвищити свідомість та усвідомлення потенційних загроз.

Впровадження цих додаткових заходів безпеки сприятиме підвищенню рівня захисту інформаційної інфраструктури підприємства Vinson.

6. Розробка плану заходів.

Перш за все, потрібно звернути увагу на технічні заходи безпеки. Як було написано раніше, а ні програмне забезпечення, а ні антивірусне програмне забезпечення, а ні ноутбуки не відповідають вимогам для конкурентної боротьби з конкурентами у сфері інформаційної безпеки.

Перш за все нам потрібно оновити застарілий ноутбук. Ми бачимо рішенням- зібрати ПК, через такі причини як:

– Висока продуктивність: ПК зазвичай мають більш потужні процесори, відеокарти та більший обсяг оперативної пам'яті, що дозволяє виконувати важкі обчислювальні завдання та використовувати вимогливе програмне забезпечення без затримок чи проблем з продуктивністю.

– Більший розмір екрану: ПК зазвичай мають більші екрани порівняно з ноутбуками, що полегшує роботу з документами, таблицями, графіками та іншими бізнес-додатками. Більший розмір екрану також поліпшує комфорт при редагуванні відео, дизайну та інших творчих завданнях.

– Більше місця для зберігання даних: ПК зазвичай мають більші жорсткі диски або можливість підключення додаткових зовнішніх накопичувачів. Це дозволяє зберігати великі обсяги даних, такі як файлові бази даних, відеоархіви та інші ресурсомісткі файли.

– Більші можливості розширення: ПК зазвичай мають більше місця для розширення, таке як додаткові слоти для розширювальних карт або вільні роз'єми для підключення додаткових пристроїв. Це дозволяє легко розширювати функціональність ПК, наприклад, додавати додаткові порти USB, мережеві карти, звукові пристрої тощо.

– Більш надійна конструкція: ПК зазвичай мають більш просту конструкцію і легші відремонтовані компоненти, що полегшує технічне обслуговування та ремонт у разі необхідності. Крім того, компоненти ПК часто доступні на ринку, що спрощує їх заміну, підвищуючи тривалість експлуатації системи.

– Більша гнучкість при виборі компонентів: ПК надають можливість вибрати компоненти за своїми потребами і бюджетом. Ви можете вибрати бажану марку процесора, відеокарти, монітора та інших компонентів, що дозволяє створити систему з оптимальним співвідношенням ціна-якість для вашого підприємства.

–

Таблиця 1.8. – Збирання ПК для персоналу

Комплектуючі	**Ціна (грн)**
Процесор AMD Ryzen 3 PRO 4350G	3192 грн
Материнська плата GIGABYTE A520M K V2	2537 грн
Пам'ять для настільних комп'ютерів AMD 16 GB DDR4 3200 MHz Radeon R9 Gamer	2422 грн
Корпус GTL 1614+ Black	1090 грн
SSD Samsung PM9A1 512 GB	2442 грн

Повітряне охолодження Deepcool Gamma Archer	289 грн
Блок живлення Chieftec APB-500B8	1253 грн
Монітор Acer V226HQL	3644 грн
Комплект ASUS U2000 Keyboard + Mouse	646 грн
Усього до сплати	17 515 грн

Також ми повинні розробити план,який дозволить нам оновити антивірусне програмне забезпечення, та створити для інформаційно-комунікаційної системи фаєрвол , антишпигунське програмне забезпечення ,віртуальна приватна мережа (VPN),парольний менеджер,шифрування диска. Від цього залежить безпека інформації на підприємстві, фірма не хоче повторяти історії з витоком секретної інформації підприємства.

Необхідно організувати навчання співробітників з питань безпеки, не в останню чергу через необізнаність питань безпеки стався виток інформації. Існує кілька причин, чому це необхідно робити:

По-перше, навчання співробітників допомагає захистити компанію від кіберзагроз. В сучасному світі, де інтернет та цифрові технології стали неодмінною частиною робочого процесу, кібератаки є поширеним явищем. Навчання допомагає співробітникам бути свідомими про потенційні загрози та навчає їх розпізнавати та уникати небезпеки.

По-друге, навчання сприяє захисту конфіденційної інформації компанії. Багато організацій мають конфіденційні дані, такі як особисті відомості клієнтів, фінансові деталі або торгові секрети. Правильне навчання співробітників допомагає підвищити усвідомлення про значення захисту цих даних та використовувати належні заходи безпеки для їх збереження.

Навчання співробітників також покращує загальну культуру безпеки в організації. Воно спонукає співробітників бути більш уважними та відповідальними щодо своїх дій, які можуть вплинути на безпеку компанії. Збільшення свідомості та знань співробітників створює кращу обізнаність про загрози та допомагає запобігати можливим інцидентам.

Враховуючи ці причини, організація навчання співробітників з питань безпеки є критично важливою для забезпечення безпеки, захисту конфіденційної інформації та зменшення ризиків для компанії. Тому керівництвом було видано наказ «Про організацію навчання співробітників з питань безпеки та захисту конфіденційної інформації» (Додаток Б.)

1.4 Визначення необхідностей у створенні КСЗІ

Сучасний світ характеризується безпрецедентним розвитком інформаційних технологій і стрімким впровадженням електронних систем у всі сфери діяльності. Такий розвиток подій неминуче несе низку викликів і загроз у сфері інформаційної безпеки та кібербезпеки. З цією проблемою стикаються і такі компанії, як «Vinson».

«Vinson» відомий власним набором функцій і вимог, які впливають на безпеку даних. Одним із найбільших недоліків, який можна виявити, є відсутність належної системи захисту даних, яка максимально гарантує конфіденційність, цілісність і доступність даних. Бувають випадки, коли погано поінформовані співробітники здійснюють діяльність, пов’язану з обробкою та зберіганням даних, не відповідають стандартам безпеки та випадково чи навмисно порушують інформаційну безпеку.

Слід зазначити, що «Vinson» може бути вразливим до зовнішніх атак, таких як хакерство, фішингові атаки, витік даних та інші форми кіберзлочинності. Наразі компанія не має достатньо ефективних засобів протидії таким загрозам, що може призвести до серйозних наслідків, таких як втрата важливої інформації, порушення бізнес-процесів та шкода репутації.

Ці недоліки вказують на необхідність КСЗІ у «Vinson». Комплексна система захисту інформації може розв'язувати ці проблеми та покращити

безпеку компанії. Використання КСЗІ дає змогу проводити навчання та курси працівників у сфері кібербезпеки та покращувати їхні знання та навички у цій сфері. Крім того, впровадження систем моніторингу, аналізу та виявлення загроз дозволить швидко реагувати на можливі атаки та гарантувати інформаційну безпеку. Не менш важливим є регулярне оновлення обладнання та програмного забезпечення для захисту від вразливостей і зловмисних атак.

Метою створення КСЗІ у «Vinson» є забезпечення стабільності, безпеки та конфіденційності даних. Впровадження КСЗІ є важливим кроком КСЗІ дозволить вам ефективно протидіяти загрозам, захистити конфіденційність і забезпечити успішне ведення бізнесу в сучасному цифровому середовищі. Пристосування КСЗІ до потреб «Vinson» , включаючи проведення оцінки ризиків, вибір правильного програмного забезпечення та впровадження необхідних політик і процедур безпеки, є критично важливим кроком у забезпеченні успіху та стабільності компанії.

Тому розробка комплексної системи інформаційної безпеки (КСЗІ) у «Vinson» є важливим завданням для забезпечення безпеки та конфіденційності інформації. Аналіз недоліків у системі захисту інформації свідчить про необхідність впровадження КСЗІ для розв'язання виявлених проблем та підвищення рівня безпеки компанії. Впровадження КСЗІ сприятиме безперебійній роботі компанії на рівні кібербезпеки та збереженню її репутації на ринку.

Вивчаючи потребу підприємства «Vinson» у комплексній системі захисту інформації, варто звернути увагу на наступні моменти:

1. Аналіз чинної мережевої інфраструктури включає перевірку чинних систем, мережевих підключень, мережевої архітектури та інших компонентів для виявлення вразливостей, потенційних загроз, якими можуть скористатися зловмисники.

2. Визначення необхідних заходів безпеки, після аналізу мережевої інфраструктури необхідно визначити конкретні заходи, які гарантують належний рівень безпеки. Це можуть бути заходи, пов'язані з аутентифікацією

та авторизацією користувачів, шифруванням даних, блокуванням небезпечних дій та інші.

3. Після визначення необхідних заходів безпеки «Vinson» повинен розробити план впровадження комплексної системи безпеки. Цей план має включати такі кроки, як впровадження нових технологій, навчання персоналу, перегляд політики безпеки та проведення системних аудитів.

4. Системі інформаційної безпеки необхідно постійно оновлюватися для забезпечення поточного рівня безпеки. Варто визначити регулярний аудит системи, плани оновлення програмного та апаратного забезпечення та регулярні тренінги з кібербезпеки для персоналу.

Маючи вже сильну клієнтську базу та репутацію на ринку, потреба «Vinson» у розробці комплексної системи захисту інформації (КСЗІ) для забезпечення стабільності, безпеки та конфіденційності даних стає все більш важливою. Аналізуючи слабкі місця системи інформаційної безпеки «Vinson», можна виділити кілька важливих аспектів, які потребують уваги та вдосконалення.

Першим недоліком є відсутність знань та підготовки працівників щодо заходів кібербезпеки та захисту інформації. Багато інцидентів безпеки спричинені недбалістю персоналу або недостатньою обізнаністю про потенційні загрози. Використання КСЗІ може розв'язувати цю проблему, запровадивши освітню та навчальну програму, яка допоможе зрозуміти ризики та навчити персонал вживати необхідних запобіжних заходів.

Другим недоліком є відсутність комплексної системи моніторингу та виявлення загроз. Відсутність автоматизованих методів виявлення вразливостей і потенційних атак ускладнює швидке реагування та запобігання можливим інцидентам. КСЗІ допоможе розв'язувати цю проблему шляхом впровадження системи швидкого реагування на потенційні атаки, моніторингу, аналізу подій та виявлення загроз для забезпечення інформаційної безпеки.

Третій недолік – несистематичне оновлення технічного обладнання та програмного забезпечення. Застарілі версії програмного забезпечення та

незахищене апаратне забезпечення роблять їх легкою мішенню для зловмисників. КСЗІ допоможе розв'язувати цю проблему, запровадивши політику регулярного оновлення програмного забезпечення та забезпечивши безпеку технічного обладнання.

Всі ці недоліки вказують на необхідність створення підприємством «Vinson» КСЗІ. Досягти цього можна шляхом комплексного підходу, такого як впровадження системи навчання та навчання персоналу з кібербезпеки, впровадження системи моніторингу та виявлення загроз, систематичне оновлення технічного обладнання та програмного забезпечення.

Використання КСЗІ у «Vinson» має на меті забезпечити високий рівень безпеки, захистити інформацію та обмежити можливості зловмисників. Це дозволяє компанії ефективно протистояти загрозам, підтримувати конфіденційність даних і захищати IT-інфраструктуру. Важливо враховувати специфіку «Vinson» і адаптувати КСЗІ до його потреб, включаючи оцінку ризиків, вибір відповідного програмного забезпечення та впровадження необхідних політик і процедур безпеки.

Тому створення комплексної системи інформаційної безпеки у «Vinson» є важливим кроком у забезпеченні інформаційної безпеки та конфіденційності. В результаті аналізу недоліків чинної системи захисту інформації та використання КСЗІ вдасться розв'язувати проблеми, виявлені у «Vinson», і підвищити рівень безпеки IT-інфраструктури. Це забезпечить стабільність бізнесу в сучасному цифровому середовищі та підтримає довіру споживачів до репутації та безпеки даних.

Для IT-інфраструктури «Vinson» необхідна комплексна оцінка ризиків. Це включає визначення потенційних загроз, виявлення вразливостей та оцінку потенційного впливу на бізнес у разі успішної атаки. На основі цього аналізу були визначені пріоритети

Побудова комплексної системи інформаційної безпеки у «Vinson» має багато переваг, які допомагають посилити та підтримувати безпеку вашого бізнесу. Основними перевагами впровадження КСЗІ є:

1. Захист від зовнішніх загроз:

КСЗІ допомагає «Vinson» захистити свою інформацію від злому, шпигунства, фішингу та інших видів кіберзлочинності. КСЗІ забезпечує надійний захист корпоративних даних, надаючи ефективні механізми для виявлення, запобігання та відновлення після атак. КСЗІ дозволяє забезпечити надійний захист інформаційних ресурсів підприємства.

2. Конфіденційність і цілісність даних:

Впроваджуючи КСЗІ, «Vinson» може забезпечити конфіденційність і цілісність своїх даних. Механізми шифрування, контролю доступу та цілісності даних гарантують, що лише авторизовані користувачі мають доступ до даних і що їх вміст не змінюється без причини.

3. Забезпечення високої доступності:

КСЗІ допомагає «Vinson» забезпечити високу доступність своїх інформаційних ресурсів. Захист від вимогливих атак та впровадження розширеного захисту від атак, механізмів резервного копіювання, відновлення та усунення неполадок, дозволяє забезпечити безперервну роботу інформаційної системи підприємства.

4. Відповідність вимогам законодавства:

КСЗІ допомагає «Vinson» відповідати нормативним вимогам щодо інформаційної безпеки. КСЗІ допомагає дотримуватися необхідних стандартів і вимог у сфері захисту даних, враховуючи законодавчі вимоги, що застосовуються в окремих сферах діяльності компанії.

5. Для захисту репутації та довіри клієнтів:

Застосування КСЗІ допомагає підтримувати репутацію «Vinson» і зміцнювати довіру клієнтів. Забезпечення конфіденційності даних та ефективна боротьба зі зловмисниками свідчить про високу відповідальність та професіоналізм компанії.

Усі ці переваги свідчать про необхідність розробки комплексної системи захисту інформації у «Vinson». Впровадження КСЗІ допомагає посилити безпеку, забезпечити конфіденційність і цілісність даних, забезпечити високу

доступність ресурсів даних, відповідати нормативним вимогам і зберегти довіру клієнтів. Розуміючи переваги «Vinson» і аналізуючи недоліки чинних систем інформаційної безпеки, впровадження КСЗІ стане важливим кроком на шляху до забезпечення стійкості бізнесу та успіху в епоху цифрових технологій.

Ось чому комплексна система захисту інформації є такою важливою для «Vinson». Це допомагає зменшити недоліки поточних систем безпеки, підвищити обізнаність і навчання персоналу, визначити потенційні загрози, оновити апаратне та програмне забезпечення, а також забезпечити високий рівень безпеки та конфіденційності даних. Впровадження КСЗІ у «Vinson» допоможе компанії бути стійкою, безпечною та квітучою в сучасному цифровому середовищі.

Усі ці переваги свідчать про необхідність розробки комплексної системи захисту інформації у «Vinson». Прийняття КСЗІ допомагає посилити безпеку, забезпечити конфіденційність і цілісність даних, забезпечити високу доступність ресурсів даних, відповідати нормативним вимогам і зберегти довіру клієнтів. Розуміючи сильні сторони «Vinson» і аналізуючи слабкі сторони чинних систем інформаційної безпеки, впровадження КСЗІ є важливим кроком на шляху до забезпечення стійкості бізнесу та успіху в епоху цифрових технологій.

Загалом, «Vinson» має впровадити комплексну систему захисту інформації з урахуванням особливостей компанії, забезпечення конфіденційності, цілісності та доступності інформації. Це дозволяє компанії ефективно захищати інформацію від потенційних загроз і забезпечувати стабільність бізнес-процесів.

1.5 Висновок

У даному розділі було проведено детальний аналіз і опис досліджуваного підприємства Vinson. Було визначено основні характеристики підприємства,

зокрема його вид діяльності - переробка горіхів. Крім того, було наведено перелік активів підприємства, таких як грошові кошти, рахунки-клієнти, запаси, нерухомість, обладнання та інтелектуальна власність.

У рамках аналізу існуючих заходів з захисту інформації на попередньому етапу було визначено, що підприємство використовує лише антивірусне програмне забезпечення Avast Free Antivirus. Це свідчить про недостатність заходів безпеки на підприємстві, оскільки існують багато інших аспектів інформаційної безпеки, які не враховуються.

Проаналізувавши поточний стан інформаційної безпеки інформаційно-комунікаційної системи (ІКС) підприємства Vinson, було виявлено сильні та слабкі сторони чинних заходів безпеки. Серед сильних сторін можна відзначити наявність антивірусного програмного забезпечення, що допомагає виявляти і запобігати зараженню комп'ютерів шкідливими програмами. Однак, слабкими сторонами є відсутність комплексного підходу до захисту інформації, відсутність системи контролю доступу та автентифікації, а також недостатня усвідомленість персоналу щодо культури безпеки.

Визначення необхідностей у створенні комплексної системи захисту інформації (КСЗІ) є важливим кроком для покращення інформаційної безпеки підприємства. З урахуванням виявлених загроз та слабкостей існуючої інформаційної інфраструктури, важливо розробити та впровадити комплексний план заходів забезпечення безпеки, включаючи використання потужних систем аутентифікації та авторизації, впровадження механізмів виявлення та запобігання атакам, навчання персоналу щодо культури безпеки та створення політик і процедур безпеки.

Проаналізувавши типи атак, які можуть призвести до порушень безпеки, такі як зловмисне програмне забезпечення, соціальна інженерія, фішинг та інші загрози, виявлено потенційні ризики для інформаційно-комунікаційної системи підприємства Vinson. Враховуючи ці ризики, необхідно вжити відповідні заходи безпеки, зокрема регулярне оновлення програмного забезпечення, встановлення мережевих фаерволів та антивірусного програмного

забезпечення, навчання персоналу щодо виявлення фішингових атак та підвищення культури безпеки.

Загалом, на основі проведеного аналізу можна зробити висновок, що інформаційна безпека підприємства Vinson потребує значних поліпшень. Використання лише антивірусного програмного забезпечення не є достатнім для захисту від різноманітних загроз. Необхідно впровадити комплексну систему захисту інформації, яка включатиме не лише технічні заходи, але й освіту та навчання персоналу з питань безпеки. Такий підхід допоможе забезпечити ефективний рівень інформаційної безпеки і зменшити ризик порушень та витоку конфіденційної інформації.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Визначення складу інформації, що захищається.

Підприємство «Vinson» має значну кількість цінної інформації, яка включає комерційні дані, технічні розробки, фінансові документи, персональні дані клієнтів та іншу конфіденційну інформацію. Забезпечення безпеки цієї інформації стало надзвичайно важливим завданням для збереження довіри клієнтів, уникнення фінансових втрат і запобігання потенційним правовим наслідкам.

Склад захищуваної інформації включає різноманітні категорії даних, які потребують особливої уваги та захисту. Це включає конфіденційні бізнес-плани, маркетингові стратегії, даних про продукти і розробки, власницькі технології, договори та фінансові документи, а також особисту інформацію клієнтів та співробітників.

З метою захисту цієї інформації від ризиків витоку, несанкціонованого доступу та зловживання, необхідно розробити КСЗІ, яка включатиме комплекс заходів технічного, організаційного та фізичного захисту. Розробка КСЗІ

враховуватиме особливості підприємства «Vinson», його інформаційні потреби та ризики, що існують в його сфері діяльності.

Цей розділ присвячено визначенню складу захищуваної інформації підприємства «Vinson» та розробці ефективних заходів КСЗІ для її захисту. Результати цього дослідження допоможуть забезпечити високий рівень безпеки і конфіденційності інформації у «Vinson», а також зменшити ризики витоку та несанкціонованого доступу до даних.

З метою забезпечення безпеки та конфіденційності даних, підприємство «Vinson» захищає різноманітну інформацію, яка має важливе значення для його діяльності та конкурентоспроможності. Склад захищуваної інформації включає, але не обмежується наступним:

1.Комерційна інформація:

«Vinson» повинно забезпечувати захист комерційної інформації, яка включає такі дані, як стратегічні плани розвитку компанії, маркетингові стратегії, плани введення нових продуктів на ринок, цінову політику, інформацію про партнерів та клієнтів. Ці дані вважаються конфіденційними та необхідно забезпечувати їх захищеність від несанкціонованого доступу.

Комерційна інформація є одним із найважливіших видів захищуваної інформації для підприємства «Vinson». Вона включає в себе конфіденційні дані про бізнес-операції, стратегії, плани розвитку, цінову політику, конкурентні переваги та іншу важливу інформацію, яка може бути цінною для конкурентів або шкідливо використана в разі розкриття.

Комерційна інформація є головним ресурсом підприємства «Vinson». Розкриття цієї інформації може призвести до серйозних негативних наслідків, таких як втрата конкурентної переваги, витоки клієнтів, пошкодження репутації, втрата прибутку та інші небажані наслідки. Тому важливо забезпечувати належний рівень захисту комерційної інформації.

Комерційна інформація «Vinson» є конфіденційною і підлягає захисту від несанкціонованого доступу. Це означає, що доступ до неї повинні мати лише

уповноважені особи, які підписали необхідні угоди про нерозголошення та обмеження використання цієї інформації.

Підприємство планує приділяти особливу увагу заходам безпеки, щоб запобігти витоку комерційної інформації. Це включає впровадження технологій шифрування даних, контроль доступу до інформаційних систем, моніторинг мережі на виявлення незвичайної активності, застосування систем виявлення вторгнень та інші заходи для забезпечення цілісності та конфіденційності комерційної інформації.

«Vinson» розробляє та впроваджує політики та процедури управління ризиками, пов'язаними з комерційною інформацією. Це включає проведення оцінки ризиків, розробку планів відновлення бізнесу, встановлення контрольних точок та моніторинг виконання заходів безпеки.

«Vinson» буде проводити навчання та свідомість серед свого персоналу щодо значення та захисту комерційної інформації. Працівники отримуватимуть інструктаж щодо правил обробки, передачі та зберігання комерційної інформації, а також повинні дотримуватися політик і процедур, що регулюють доступ до цієї інформації. Це сприятиме свідомому підходу до захисту комерційної інформації та зменшує ризик витоку.

«Vinson» укладає угоди про нерозголошення та обмеження використання комерційної інформації зі своїми партнерами та постачальниками. Це дозволяє забезпечити захист інформації, що обмінюється між організаціями та підтримує довіру взаємовідносин.

«Vinson» проводить внутрішні аудити з метою перевірки дотримання політик та процедур захисту комерційної інформації. Аудит дозволяє виявляти можливі проблеми та слабкі місця в системі захисту і приймати відповідні заходи для усунення виявлених проблем.

«Vinson» дотримується відповідних законодавчих вимог щодо захисту комерційної інформації. Організація встановлює внутрішні правила, які відповідають діючим законам та регуляторним вимогам, що стосуються захисту конфіденційної інформації.

Загалом, комерційна інформація для підприємства «Vinson» є критично важливою та потребує належного захисту. Підприємство вживає широкий спектр заходів, включаючи контроль доступу, шифрування даних, навчання персоналу та співробітництво з партнерами, для забезпечення конфіденційності комерційної інформації. Крім того, внутрішні аудити та дотримання відповідних законодавчих вимог гарантують високий рівень захисту комерційної інформації та довіру партнерів та клієнтів підприємства.

2.Технічна інформація:

«Vinson» планує активно захищати технічну інформацію, яка включає інтелектуальну власність, патенти, розробки, технічні креслення, схеми, програмне забезпечення, алгоритми та інші технічні документації. Ця інформація є важливою для забезпечення конкурентоспроможності підприємства і потребує високого рівня захисту від втрати та незаконного використання.

Технічна інформація підприємства «Vinson» є цінним активом, який потребує надійного захисту. Вона включає всі дані, пов'язані з технічними аспектами діяльності підприємства, включаючи дизайн, розробку, виробництво, наукові дослідження, інтелектуальну власність, патенти, секрети виробництва та іншу конфіденційну інформацію.

Забезпечення безпеки технічної інформації важливе для успішного функціонування підприємства і його конкурентної переваги. Ось чому впровадження комплексної системи захисту інформації (КСЗІ) є критичним для підприємства «Vinson». Розглянемо деякі ключові аспекти, які демонструють значення КСЗІ для захисту технічної інформації:

– конфіденційність: технічна інформація може містити комерційні та конфіденційні дані, які необхідно захищати від несанкціонованого доступу. КСЗІ забезпечує механізми шифрування та контролю доступу, які гарантують, що лише авторизовані користувачі мають доступ до цієї інформації. Шифрування даних забезпечує їх захищеність навіть у разі проникнення зовнішніх загроз.

– інтелектуальна власність: технічна інформація може включати інтелектуальну власність, таку як нові розробки, патенти, дизайни тощо. Ці активи є важливими для конкурентної переваги підприємства і потребують особливого захисту. КСЗІ допомагає забезпечити конфіденційність цих інформаційних активів та запобігає їх незаконному використанню або крадіжці.

– цілісність: важливим аспектом технічної інформації є забезпечення цілісності даних. Це означає, що дані мають бути захищені від несанкціонованої модифікації або втрати. КСЗІ надає засоби контролю цілісності даних, які дозволяють виявляти будь-які недоречні зміни і вживати заходів для їх усунення.

– надійність: технічна інформація є критичною для функціонування підприємства, і будь-які порушення цієї інформації можуть мати серйозні наслідки для його діяльності. КСЗІ включає резервне копіювання, відновлення та інші механізми, які допомагають забезпечити надійність технічної інформації. В разі випадкової втрати даних або випадку форс-мажорних ситуацій, таких як катастрофи або кібератаки, КСЗІ дозволяє відновити важливу інформацію та продовжити роботу підприємства.

– відповідність вимогам: у багатьох галузях, зокрема в оборонному, медичному або фінансовому секторах, існують специфічні вимоги до захисту технічної інформації. КСЗІ допомагає підприємству відповідати цим вимогам і забезпечує документування та аудит заходів забезпечення безпеки.

Отже, для підприємства «Vinson» впровадження системи комплексного захисту інформації (КСЗІ) для технічної інформації є критично важливим. КСЗІ допомагає забезпечити конфіденційність, цілісність, надійність та відповідність вимогам для захисту технічної інформації, що є ключовим активом підприємства. Реалізація КСЗІ допоможе зменшити ризики витоку інформації, зберегти конкурентну перевагу та підтримати успішну діяльність підприємства «Vinson».

3.Фінансова інформація:

Для забезпечення фінансової стабільності та дотримання вимог законодавства, «Vinson» захищає фінансову інформацію, включаючи бухгалтерські записи, звіти, фінансові прогнози, договори, фінансові розрахунки та іншу фінансову документацію. Ці дані є конфіденційними і необхідно забезпечувати їх захищеність від несанкціонованого доступу, фальсифікації та втрати.

Фінансова інформація підприємства «Vinson» є однією з найбільш цінних та чутливих інформаційних активів. Розкриття цієї інформації може мати серйозні наслідки для підприємства, його клієнтів, партнерів та інших зацікавлених сторін. Тому важливо розглянути, чому необхідно робити комплексний захист інформації (КСЗІ) саме для фінансової інформації.

-Конфіденційність: Фінансова інформація, така як звіти про прибутки, збитки, баланси, плани розвитку та інші фінансові показники, містить конфіденційні дані, які не повинні бути доступними несанкціонованим особам. Розкриття такої інформації може призвести до фінансових втрат, зловживання ринковою конкуренцією або шахрайства. КСЗІ допомагає забезпечити конфіденційність фінансової інформації шляхом реалізації механізмів контролю доступу, шифрування та інших заходів безпеки.

-Цілісність: Фінансова інформація повинна бути надійно захищена від недоречної модифікації або випадкової втрати. Несанкціоновані зміни в фінансовій інформації можуть призвести до спотворення даних та втрати довіри інвесторів, клієнтів та партнерів. КСЗІ надає механізми контролю цілісності даних, які дозволяють виявляти будь-які зміни та забезпечувати їх правильність і цілісність.

-Надійність: Фінансова інформація має бути доступною та надійною для внутрішніх та зовнішніх користувачів. Потерпілий доступ до фінансових даних може спричинити втрату даних, перерви в роботі, порушення договорів та навіть правопорядку. КСЗІ допомагає забезпечити надійність фінансової інформації шляхом використання резервних копій, механізмів відновлення та інших методів забезпечення доступності даних.

-Відповідність вимогам: Фінансова інформація підприємства підпадає під деякі правові, регуляторні та стандартизаційні вимоги, які необхідно дотримуватися. Наприклад, підприємство може бути зобов'язане відповідати вимогам Податкового кодексу, Міжнародних стандартів фінансової звітності (МСФЗ), законодавства про захист персональних даних тощо. КСЗІ дозволяє підприємству виконувати ці вимоги та забезпечувати дотримання встановлених стандартів.

-Конкурентна перевага: Фінансова інформація може містити стратегічні дані, які є особливо цінними для конкурентного ринку. Розкриття такої інформації конкурентам може спричинити втрату конкурентної переваги та порушення бізнес-стратегій. КСЗІ допомагає захистити фінансову інформацію від несанкціонованого доступу та зберегти конкурентну перевагу підприємства.

Отже, комплексний захист інформації (КСЗІ) для фінансової інформації підприємства «Vinson» є критично важливим. Це дозволяє забезпечити конфіденційність, цілісність, надійність та відповідність вимогам фінансової інформації. КСЗІ також забезпечує збереження конкурентної переваги і запобігає можливим фінансовим втратам, репутаційним ризикам та правовим наслідкам. Розробка та впровадження ефективної системи КСЗІ стає пріоритетним завданням для підприємства «Vinson» у забезпеченні безпеки своїх фінансових даних і довіри своїх клієнтів і партнерів.

4.Персональні дані:

Зважаючи на значення конфіденційності та захисту особистої інформації, «Vinson» дотримується вимог законодавства щодо захисту персональних даних своїх співробітників, клієнтів, партнерів та інших зацікавлених осіб. Персональні дані включають інформацію, таку як імена, адреси, контактну інформацію, соціальні страхування, фінансові дані та іншу особисту ідентифікуючу інформацію. Забезпечення конфіденційності та цілісності цих даних є важливою складовою частиною політики безпеки «Vinson .

Персональні дані підприємства «Vinson» є важливою категорією інформації, яку необхідно захищати за допомогою Комплексної системи

захисту інформації (КСЗІ). Розкриття такої інформації може мати серйозні наслідки для підприємства та його клієнтів, включаючи порушення приватності, ризик ідентифікації, фінансові втрати та недовіру.

Основні причини робити КСЗІ для захисту персональних даних підприємства «Vinson» включають:

-Законодавчі вимоги: У багатьох країнах існують законодавчі норми, які регулюють збір, обробку та зберігання персональних даних. Наприклад, Загальний регламент про захист персональних даних (GDPR) в Європейському Союзі встановлює вимоги до захисту приватності та конфіденційності персональних даних. КСЗІ допомагає підприємству виконувати ці вимоги та запобігати можливим штрафам і санкціям.

-Збереження довіри клієнтів: Підприємство «Vinson» має обов'язок зберігати та обробляти персональні дані своїх клієнтів з великою обережністю. Недостатня захищеність цих даних може призвести до витоку інформації, порушення довіри клієнтів та втрати бізнесу. КСЗІ забезпечує відповідність та надійний захист персональних даних, що сприяє підтримці довіри від клієнтів.

-Ідентифікація та аутентифікація: Персональні дані, такі як імена, адреси, номери телефонів, електронні пошти і банківські реквізити, можуть бути використані для ідентифікації осіб та здійснення аутентифікації. КСЗІ допомагає захистити ці дані від несанкціонованого доступу, підробки та зловживання.

-Запобігання шахрайству: Персональні дані можуть стати об'єктом шахрайства, включаючи крадіжку ідентичності, фішинг, шпигунство та інші види шахрайських дій. КСЗІ допомагає виявляти та запобігати таким загрозам, забезпечуючи захищений обмін інформацією та шифрування даних.

-Конкурентна перевага: Захист персональних даних через КСЗІ може стати конкурентною перевагою для підприємства «Vinson». Клієнти та партнери надають перевагу підприємствам, які демонструють високий рівень захисту персональних даних. КСЗІ дозволяє підприємству використовувати цю перевагу, залучаючи більше клієнтів і зберігаючи існуючих.

Розробка та впровадження КСЗІ для захисту персональних даних підприємства «Vinson» стає необхідним завданням, оскільки це забезпечує високий рівень конфіденційності, захищеності та відповідності законодавству щодо персональних даних. Крім того, КСЗІ допомагає зберегти довіру клієнтів, запобігти фінансовим втратам, шахрайству та забезпечити конкурентну перевагу на ринку.

5.Класифікована інформація:

У разі якщо «Vinson» має класифіковану інформацію, таку як державні секрети або інформацію з обмеженим доступом, воно повинно дотримуватися вимог, встановлених відповідними правовими нормами та державними органами. Захищеність та обробка цієї інформації повинні відповідати вимогам забезпечення національної безпеки та нерозголошення державної таємниці.

Класифікована інформація підприємства «Vinson» є найбільш чутливою та важливою категорією інформації, яку необхідно захищати за допомогою Комплексної системи захисту інформації (КСЗІ). Розкриття такої інформації може мати серйозні наслідки для безпеки підприємства, національної безпеки та відносин з іншими державами. Дотримання високих стандартів безпеки і захисту класифікованої інформації є критично важливим для функціонування підприємства та його успіху.

Основні причини робити КСЗІ для захисту класифікованої інформації підприємства «Vinson» включають:

-Національна безпека: Класифікована інформація може містити державні та військові секрети, які становлять важливу складову національної безпеки. Розкриття такої інформації може загрожувати безпеці держави, національній обороні та геополітичним інтересам. КСЗІ допомагає забезпечити захист та конфіденційність класифікованої інформації, запобігаючи її неправомірному доступу та витоку.

-Комерційна конфіденційність: Класифікована інформація може включати комерційні та торговельні секрети підприємства, такі як інноваційні розробки, технології, патенти, процеси виробництва, маркетингові стратегії

тощо. Розкриття цієї інформації може призвести до втрати конкурентної переваги, порушення довіри клієнтів та фінансових втрат. КСЗІ допомагає забезпечити конфіденційність та інтегрітет класифікованої комерційної інформації.

-Законодавча вимога: У багатьох країнах існують закони та регуляції, що вимагають захисту класифікованої інформації. Порушення таких вимог може призвести до правових наслідків, штрафів та інших санкцій. КСЗІ допомагає підприємству виконувати законодавчі вимоги щодо захисту класифікованої інформації та демонструвати відповідність нормативним вимогам.

-Міжнародні відносини: В разі співпраці з іншими країнами або міжнародними організаціями, захист класифікованої інформації є ключовим для збереження довіри та забезпечення безпеки спільних проектів, обміну інформацією та технологіями. КСЗІ допомагає забезпечити високий рівень захисту і конфіденційності класифікованої інформації в рамках міжнародних співтовариств.

-Збереження репутації: Класифікована інформація може містити чутливі дані про клієнтів, партнерів або співробітників. Розкриття такої інформації може пошкодити репутацію підприємства та спричинити втрату довіри з боку зацікавлених сторін. КСЗІ допомагає зберегти репутацію підприємства, захищаючи класифіковану інформацію від несанкціонованого доступу та витоку.

Розробка та впровадження КСЗІ для захисту класифікованої інформації підприємства «Vinson» є важливим завданням для забезпечення безпеки, конфіденційності та інтегрітету цієї інформації. Вона включає в себе використання шифрування, контролю доступу, ідентифікації та автентифікації, моніторингу та аудиту, фізичного захисту та інших заходів безпеки. КСЗІ дозволяє підприємству ефективно управляти ризиками та захищати свою класифіковану інформацію від потенційних загроз та нападів.

Отже, розкриття класифікованої інформації підприємства «Vinson» може мати серйозні наслідки для безпеки, конкурентоспроможності та репутації

підприємства. Комплексна система захисту інформації є необхідною для забезпечення конфіденційності, цілісності та доступності класифікованої інформації. Розробка та впровадження КСЗІ є стратегічним кроком для підприємства «Vinson» у забезпеченні безпеки та успіху в динамічному інформаційному середовищі.

6.Доступ до систем та інформації:

«Vinson» забезпечує захищений доступ до своїх інформаційних систем та додатків. Це включає керування доступом, автентифікацію, авторизацію, захист мережі, моніторинг активності та інші технічні заходи для запобігання несанкціонованому доступу, втраті даних та зловживанню.

Доступ до систем та інформації підприємства «Vinson» є ключовим аспектом безпеки та ефективного функціонування підприємства. Розкриття такої інформації може мати серйозні наслідки, включаючи виток конфіденційної інформації, порушення цілісності даних, несанкціонований доступ до систем та можливість зловживання цим доступом. Розробка та впровадження комплексної системи захисту інформації (КСЗІ) є необхідним для забезпечення безпеки доступу до систем та інформації підприємства «Vinson» .

Основні аспекти, які варто врахувати при розкритті інформації про доступ до систем та інформації підприємства «Vinson» , включають:

-Аутентифікація та авторизація: Для забезпечення безпеки доступу до систем та інформації, підприємство «Vinson» використовує механізми аутентифікації, що перевіряють ідентифікацію користувачів та їх права доступу. Це можуть бути паролі, біометричні дані, токени або інші методи ідентифікації. Крім того, авторизація визначає, які ресурси та функції доступні окремим користувачам або групам користувачів.

-Керування привілеями: Щоб обмежити доступ до конфіденційної інформації та системних ресурсів, підприємство «Vinson» використовує привілеї та рівні доступу. Це дозволяє встановлювати права доступу залежно від ролей та відповідальностей користувачів, обмежувати можливості

редагування, видалення або копіювання інформації, а також контролювати доступ до критичних системних ресурсів.

-Шифрування даних: Для забезпечення конфіденційності та захисту інформації, передаваної по мережі або зберіганої на носіях, підприємство «Vinson» використовує методи шифрування даних. Шифрування забезпечує захищене перетинання даних, що робить їх незрозумілими для несанкціонованих осіб, які не мають необхідних ключів або паролів.

-Моніторинг та аудит: Для виявлення несанкціонованої діяльності та виявлення можливих загроз безпеці, підприємство «Vinson» використовує системи моніторингу та аудиту. Ці системи відстежують активність користувачів, реєструють спроби несанкціонованого доступу та зберігають журнали подій для подальшого аналізу та розслідування.

-Фізичний захист: Крім захисту доступу до систем та інформації, підприємство «Vinson» також забезпечує фізичний захист своїх приміщень, серверних кімнат та інших інфраструктурних компонентів. Це можуть бути системи контролю доступу, відеоспостереження, захищені зони з обмеженим доступом та інші заходи безпеки.

Розробка та впровадження КСЗІ для доступу до систем та інформації підприємства «Vinson» має на меті забезпечити захист конфіденційності, цілісності та доступності даних. Це дозволяє підприємству ефективно управляти ризиками, запобігати несанкціонованому доступу, витоку даних та іншим загрозам безпеці, а також дотримуватися законодавства та вимог щодо захисту персональних даних.

7.Фізична безпека:

«Vinson» забезпечує фізичну безпеку своїх приміщень, серверних залів, дата-центрів та інших місць зберігання інформації. Це включає контроль доступу, відеоспостереження, захист від несанкціонованого доступу та інші заходи для запобігання фізичному вторгненню та втраті даних.

Фізична безпека підприємства «Vinson» відіграє критичну роль у забезпеченні безперебійної роботи, захисту активів та запобіганні

несанкціонованому доступу до приміщень та інфраструктурних компонентів. Розкриття цієї інформації допоможе вам краще зрозуміти, на що спрямована реалізація комплексної системи захисту інформації (КСЗІ) для фізичної безпеки підприємства «Vinson».

Основні аспекти фізичної безпеки, які варто розглянути, включають:

-Контроль доступу: Це включає в себе застосування систем контролю доступу, таких як електронні картки, біометричні системи (відбитки пальців, розпізнавання обличчя) або підключення до централізованих систем контролю доступу. Це дозволяє обмежувати доступ до приміщень тільки авторизованим особам, зменшує ризик несанкціонованого доступу та витоку конфіденційної інформації.

-Відеоспостереження: Установлення систем відеоспостереження дозволяє в режимі реального часу спостерігати за діяльністю на підприємстві. Відеокамери можуть бути розташовані у важливих зонах, таких як входи, коридори, складські приміщення тощо. Це забезпечує виявлення та реагування на підозрілу або небезпечну діяльність, зменшує ризик крадіжок, вандалізму та інших небажаних подій.

-Фізична безпека приміщень: Забезпечення фізичної безпеки приміщень включає в себе застосування системи запобігання та виявлення пожеж, контроль температури та вологості, захист від стихійних лих та інших фізичних небезпек. Використання системи виявлення вторгнень, датчиків руху та систем автоматичної сигналізації також може допомогти вчасно виявляти та реагувати на несанкціонований доступ або підозрілу діяльність.

-Запобігання збоїв та відновлення роботи: Крім захисту від зовнішніх загроз, КСЗІ також забезпечує запобігання та відновлення роботи в разі технічних збоїв, аварій або катастроф. Це можуть бути системи резервного живлення, резервне копіювання даних, відновлення після відмови та інші заходи, що допомагають підтримувати безперебійну роботу підприємства.

-Обізнаність персоналу: Здійснення навчання та свідомості персоналу щодо важливості фізичної безпеки, правил поводження, процедур евакуації та

інших аспектів безпеки допомагає зменшити ризик інцидентів та забезпечити вчасну реакцію на небезпеку.

Розробка та впровадження КСЗІ для фізичної безпеки підприємства «Vinson» є необхідним для забезпечення захисту активів, протидії злочинності, запобігання фізичним ризикам та забезпечення неперервності роботи підприємства. КСЗІ допомагає зменшити загрози безпеки, підвищити ефективність діяльності та зберегти репутацію підприємства. Загалом, склад захищуваної інформації підприємства «Vinson» включає комерційну, технічну, фінансову, персональну та класифіковану інформацію.

«Vinson» прагне забезпечувати високий рівень безпеки та конфіденційності цих даних шляхом використання різноманітних технічних, організаційних та фізичних заходів. Дотримання політики безпеки, навчання персоналу та використання сучасних технологій є основою для успішного захисту захищуваної інформації підприємства «Vinson» від витоку, несанкціонованого доступу та зловживань.

Зазначений склад захищуваної інформації відображає важливість безпеки та конфіденційності для підприємства «Vinson». Захист цих видів інформації є необхідним для забезпечення стабільності, конкурентоспроможності та довіри клієнтів і партнерів. «Vinson» приділяє належну увагу розробці та впровадженню ефективних заходів безпеки для забезпечення інтегритету, конфіденційності та належного використання захищуваної інформації.

У цьому розділі був розглянутий склад захищуваної інформації підприємства «Vinson» з метою забезпечення безпеки та конфіденційності даних. Захищувана інформація включає комерційну інформацію, технічну інформацію, фінансову інформацію, персональні дані, класифіковану інформацію та вимоги до доступу до систем та інформації.

Підприємство «Vinson» виконує різноманітні заходи забезпечення безпеки, включаючи технічні, організаційні та фізичні заходи. Це включає керування доступом, шифрування, мережевий захист, моніторинг активності, контроль доступу до приміщень, відеоспостереження та інші заходи, які

сприяють запобіганню несанкціонованому доступу, втраті даних та зловживанню.

Захист інформації є важливою складовою частиною стратегії підприємства «Vinson», оскільки вона забезпечує конфіденційність, цілісність та доступність даних. Застосування ефективної системи захисту інформації дозволяє підприємству зберігати довіру клієнтів, уникнути фінансових втрат, запобігти порушенням законодавства та зберегти свою конкурентоспроможність на ринку.

Загалом, ретельний аналіз та визначення складу захищуваної інформації підприємства «Vinson», а також розробка відповідних заходів КСЗІ, допоможуть забезпечити надійний рівень безпеки та захисту інформації, що є критичним для успішної діяльності підприємства.

2.2 Вибір методів та засобів захисту.

Вибір методів і засобів захисту в інформаційно-комунікаційній системі (ІКС) підприємства "Vinson" є важливим етапом забезпечення інформаційної безпеки. При виборі методів і засобів необхідно враховувати конкретні потреби та вимоги підприємства, а також типи загроз, з якими воно стикається. Основні методи захисту, які можуть бути застосовані в ІКС підприємства "Vinson", включають:

1.Аутентифікація і авторизація:

-Встановлення міцних паролів і політики паролів для забезпечення безпечного доступу до системи.

-Використання багатофакторної аутентифікації, яка включає використання двох або більше методів перевірки особи (наприклад, пароль та відбиток пальця).

-Реєстрація та управління користувачами з обмеженням прав доступу до конфіденційної інформації.

-Моніторинг активності користувачів для виявлення потенційно підозрілих дій та несанкціонованого доступу.

-Застосування заходів для захисту від несанкціонованого доступу, таких як використання брандмауерів, віртуальних приватних мереж (VPN) та інших технологій.

2.Шифрування даних:

-Застосування шифрування даних в покої компанії для захисту інформації від несанкціонованого доступу фізичної особи.

-Шифрування даних на серверах та в хмарних сервісах для забезпечення конфіденційності при зберіганні та передачі даних.

-Шифрування передачі даних по мережі з використанням протоколів, таких як SSL / TLS, для запобігання перехопленню інформації.

3.Захист від шкідливих програм:

-Встановлення та регулярне оновлення актуального антивірусного програмного забезпечення для виявлення та блокування шкідливих програм.

-Проведення регулярного оновлення вірусних баз та програмного забезпечення для забезпечення захисту від нових загроз.

-Використання механізмів виявлення та блокування підозрілих активностей, таких як системи IDS (системи виявлення інтравідвізій) та IPS (системи запобігання інтравідвізій), для реагування на шкідливі програми.

4.Забезпечення резервного копіювання:

-Регулярне створення резервних копій важливих даних та інформації.

-Зберігання резервних копій в безпечних і надійних місцях, таких як віддалені сервери або хмарні сховища.

5.Оновлення програмного забезпечення:

-Проведення регулярного оновлення програмного забезпечення, операційних систем та інших компонентів ІКС з метою усунення вразливостей та встановлення останніх захисних патчів.

6.Навчання та свідомість персоналу:

-Забезпечення навчання персоналу щодо основних принципів безпеки інформації, виявлення соціальної інженерії, фішингу та інших загроз.

-Спонукання персоналу до створення сильних паролів та свідомого використання комп'ютерів та інших пристроїв.

Для вибору заходів захисту в інформаційно-комунікаційній системі (ІКС) підприємства "Vinson", рекомендується враховувати такі аспекти:

1.Оцінка загроз і ризиків: Було проведено оцінку ризиків и загроз у розділі 1.3, та виявлено потенційні загроз для ІКС підприємства "Vinson", також було визначено рівень ризику для кожної загрози. Це допоможе нам зосередитися на найважливіших аспектах захисту і вибрати відповідні заходи.

2.Фізична безпека: "Vinson" забезпечило безпеку приміщень, де розташована інформаційно-комунікаційна інфраструктура на належному рівні. Це включає встановленні систем відеоспостереження, захист серверів від пожежі та інші фізичні заходи.

3.Аутентифікація і авторизація: Для якомога надійнішого захисту інформації потрібно використовувати міцну аутентифікацію та авторизацію для забезпечення лише авторизованого доступу до системи. Розглянемо використання багатофакторної аутентифікації, біометричних технологій та контролю доступу до ресурсів. Для того, щоб підвищити інформаційну грамотність співробітників у цьому аспекті було видано наказ «Про організацію навчання співробітників з питань безпеки та захисту конфіденційної інформації» (Додаток Б)

4.Шифрування даних: Застосуйте шифрування для захисту конфіденційності даних під час їх зберігання та передачі. Розгляньте

використання шифрування на рівні файлів, дискових просторів, мережевих з'єднань та інших важливих компонентів ІКС. Розглянемо кілька способів, якими ми покращимо безпеку ІКС:

-Шифрування даних під час передачі: Використовуйте шифрування з'єднання за допомогою VPN CyberGhost, щоб захистити дані під час їх передачі по мережі. Це перешкоджає можливості несанкціонованого доступу до інформації під час її трансляції через мережеві канали.

- Криптографічні програмні бібліотеки: Для реалізації симетричного шифрування (AES, DES) та асиметричного шифрування (RSA) можна використовувати популярні криптографічні бібліотеки. Однією з популярних криптографічних бібліотек, яку можна впровадити для Vinson, є OpenSSL. OpenSSL є відкритим інструментом з високим рівнем підтримки криптографічних алгоритмів і протоколів, включаючи симетричне та асиметричне шифрування, хеш-функції, цифрові підписи та багато іншого.

Нижче наведена форма з порівнянням криптографічних бібліотек, включаючи OpenSSL, Bouncy Castle та Cryptography API: Next Generation (CNG).(табл. 2.1)

Кріптографічна бібліотека	**Переваги**	**Недоліки**
OpenSSL	Відкрите програмне забезпечення	Складніше використання для початківців
	Високий рівень підтримки криптографічних алгоритмів і протоколів	Деякі питання безпеки у минулому
	Підтримує різні мови програмування та платформи	Менше документації порівняно з іншими бібліотеками
Bouncy Castle	Відкрите програмне забезпечення	Менша популярність в порівнянні з OpenSSL
	Підтримка широкого спектру криптографічних	Менша кількість ресурсів

	алгоритмів та протоколів	та документації
Cryptography API: Next Generation (CNG)	Вбудована підтримка в операційні системи Windows	Обмежена підтримка на інших платформах
	- Простий інтерфейс програмування	- Менша гнучкість порівняно з OpenSSL

Таблиця 2.1- Порівняння криптографічних бібліотекъ

Захист від шкідливого програмного забезпечення: Встановимо надійне антивірусне програмне забезпечення Avast Ultimate. Використовуємо таку систему виявлення і запобігання вторгнення як Маршрутизатор Cisco 871-SEC-K9 ,який має інтегроване IDS/IPS, фаєрвол та інші заходи для виявлення та блокування загроз.

Резервне копіювання та відновлення даних: Буде забезпечена наявна резервних копій в хмарному сховищі pCloud для захисту від втрати даних внаслідок випадкового видалення, технічних збоїв або кібератак. pCloud пропонує своїм партнерам криптографічне шифрування, безпеку даних, гнучкість доступу до файлів, спільну роботу та широкі можливості планування

Хмарне сховище	Безкоштовний простір	Плани та ціни	Додаткові функції
Google Drive	15 ГБ	Платні плани: від $1.99/місяць за 100 ГБ	Спільна робота над документами, гнучкість
Dropbox	2 ГБ	Платні плани: від $11.99/місяць за 2 ТБ	Офлайн-доступ до файлів, спільна робота
Microsoft OneDrive	5 ГБ	Платні плани: від $1.99/місяць за	Інтеграція зі службами

		100 ГБ	Microsoft, спільна робота
pCloud	10 ГБ	Платні плани: від $3.99/місяць за 500 ГБ	Криптографічне шифрування, безпека даних
Mega	15 ГБ	Платні плани: від €4.99/місяць за 400 ГБ	Криптографічне шифрування, спільна робота

Таблиця 2.2- Порівняння бюджетних хмарових сховищ

Навчання персоналу: Фірма почала приділяти увагу навчанню персоналу, і тому організувала навчальні програми з питань безпеки інформації для всього персоналу (Додаток Б). Підвищує свідомість персоналу щодо потенційних загроз, соціальної інженерії, фішингу та важливості дотримання політик безпеки.

Система моніторингу та виявлення вторгнень: Планується придбання та використання маршрутизатору Cisco 871-SEC-K9 ,який має інтегроване IDS/IPS

Постійне вдосконалення: Безпека ІКС - це постійний процес. Відстежуйте нові загрози та технології, оцінюйте ефективність заходів безпеки та впроваджуйте вдосконалення для забезпечення високого рівня захисту.

2.3 Розробка проекту комплексної системи захисту інформації.

Проект комплексної системи захисту інформації для підприємства Vinson міститиме різні складові, які допоможуть забезпечити цілісність, конфіденційність та доступність інформації. Ось загальний огляд компонентів, які будуть включені до проекту:

1.Аналіз загроз і ризиків: Підприємство Vinson не має належного рівня технічної та програмної безпеки, а операційна система Windows 7, яка більше не підтримується після 14 січня 2020 року, та не може забезпечити належний

рівень захисту інформації. Це головним чином пов'язано з вразливостями системи, які більше не можна виправити. Безкоштовне антивірусне програмне забезпечення Avast не є найкращим вибором для захисту даних, оскільки йому бракує багатьох важливих функцій. Безкоштовна версія, безумовно, є хорошим варіантом, але для розробки КСЗІ потрібен комплексний антивірус з багатьма функціями. Безкоштовна версія, встановлена на ноутбуках співробітників компанії, забезпечує лише базовий захист: Lenovo Z570 має застарілі компоненти і не може встановити найновіше програмне забезпечення для захисту інформації. Як наслідок, компанія стикається з високим ризиком хакерських атак і витоку даних, а також із середнім рівнем загрози від вірусів і шкідливих програм.

Ризик втрати або крадіжки пристроїв і несанкціонованого доступу співробітників є низьким завдяки використанню сучасних систем і засобів захисту, як зазначалося раніше.

На заміну застарілому обладнанню, за наказом директора підприємства (див додаток) було повністю оновлене апаратне та технічне обладнання підприємства. Lenovo Z570 були замінені на ПК (див. табл 1.8) Операційна система на нових ПК- Windows 10. Безкоштовна версія антивірсного ПЗ Avast була замінена на Avast Ultimate, котрий має більше можливостей, та функцій. Маршрутизатор Cisco 871-SEC-K9 , який має системи виявлення та запобігання вторгненню IDS/IPS зменшує ризики хакерських атак до низького

2.Політики безпеки:

a.Політика паролів:

-Вимога до складності паролів, включаючи комбінацію великих і малих літер, цифр та спеціальних символів.

-Регулярна зміна паролів.

-Заборона використання одного пароля для різних систем або облікових записів.

b.Політика контролю доступу:

-Принцип найменших привілеїв: Надання користувачам лише необхідного рівня доступу до ресурсів інформаційної системи.

-Установка індивідуальних облікових записів для кожного користувача.

-Використання механізмів аутентифікації та авторизації для контролю доступу до ресурсів.

c. Політика резервного копіювання даних:

-Регулярне створення резервних копій інформації.

-Перевірка та тестування процедур відновлення даних.

-Зберігання резервних копій в безпечному та віддаленому місці.

d.Політика антивірусних заходів:

-Встановлення та оновлення антивірусного програмного забезпечення на всіх комп'ютерах та серверах.

-Регулярне сканування системи на наявність вірусів та шкідливого програмного забезпечення.

-Налагодження механізмів оновлення вірусних баз та виявлення нових загроз.

e.Політика захисту периметра:

-Встановлення мережевих брандмауерів для контролю трафіку і фільтрації небезпечних з'єднань..

3.Фізична безпека: Забезпечення фізичної безпеки включає контроль доступу до приміщень, захист серверних кімнат, використання систем відеоспостереження та інших засобів для захисту фізичного обладнання. Для забезпечення фізичної безпеки будуть розглянуті такі заходи безпеки:

a. Контроль доступу до приміщень:

-Встановлення системи контролю доступу, яка обмежує фізичний доступ до приміщень з обладнанням або інформацією.

-Використання електронних карток, біометричних систем або інших методів ідентифікації для авторизації доступу.

b. Використання систем відеоспостереження:

-Встановлення камер відеоспостереження для контролю фізичного доступу до об'єктів та приміщень.

-Моніторинг та запис відеозаписів для забезпечення доказів в разі виникнення інцидентів.

-Розташування камер в стратегічних місцях, щоб охоплювати важливі зони та точки входу/виходу.

с. Захист фізичного обладнання:

-Забезпечення фізичної безпеки серверів, комутаторів, маршрутизаторів та іншого обладнання шляхом їх установки у відповідних захищених шафах або кімнатах.

-Обмеження фізичного доступу до обладнання тільки авторизованим особам.

4.Захист мережі: VPN CyberGhost у порівнянні з аналогами був трохи краще у кожному компоненті, тому використовуємо його для захисту. Маршрутизатор Cisco 871-SEC-K9 , який має системи виявлення та запобігання вторгненню IDS/IPS відіграє ключову роль у захисті мережі.

5.Кріптографічний захист: Шифрування даних під час передачі CyberGhost VPN шифрує з'єднання та захищає дані під час їхнього переміщення мережею. Це запобігає несанкціонованому доступу до інформації під час її передачі мережевим каналом.

-Криптографічні програмні бібліотеки: симетричне (AES, DES) та асиметричне (RSA) шифрування можна реалізувати за допомогою поширених криптографічних бібліотек Однією з поширених криптографічних бібліотек, яка може бути реалізована у Vinson, є OpenSSL, OpenSSL - це інструмент з відкритим вихідним кодом з розширеною підтримкою криптографічних алгоритмів і протоколів, таких як симетричне і асиметричне шифрування, хеш-функції і цифрові підписи.

6.Безпека даних: Резервне копіювання до хмарного сховища pCloud забезпечує захист від втрати даних через випадкове видалення, технічні збої та

кібератаки. pCloud пропонує шифрування, захист даних, гнучкий доступ до файлів, спільну роботу та широкі можливості планування для партнерів.

7.Навчання та свідомість: Компанія приділяє більше уваги навчанню персоналу та організувала навчальну програму з інформаційної безпеки для всіх співробітників.Підвищити обізнаність персоналу про потенційні загрози, соціальну інженерію, фішинг та важливість дотримання політики безпеки.

8.Аудит безпеки: Vinson ознайомлені з необхідністю проведення аудитів безпеки з метою забезпечення надійності та захищеності їхньої інформаційно-комунікаційної системи. Аудит безпеки є важливим етапом в управлінні безпекою, оскільки дозволяє оцінити поточний стан заходів безпеки, виявити потенційні загрози та слабкі місця і розробити стратегію покращення. Vinson розуміють, що аудит безпеки є процесом, що вимагає регулярного проведення для виявлення нових загроз та аналізу ефективності наявних заходів захисту. Це дозволяє забезпечити високий рівень безпеки, захистити конфіденційну інформацію, запобігти несанкціонованому доступу та мінімізувати можливі втрати чи пошкодження даних. Vinson готові активно співпрацювати з професіоналами в галузі безпеки для проведення аудиту та розробки оптимальних стратегій захисту своїх інформаційних активів.

9. Vinson повністю усвідомлює важливість оновлення програмного забезпечення (ПЗ) та встановлення патчів безпеки. Вони розуміють, що такі заходи є необхідними для забезпечення надійності та захищеності їхньої інформаційно-комунікаційної системи. Періодичне оновлення ПЗ дозволяє виправити виявлені помилки, вразливості та слабкі місця, що можуть бути використані зловмисниками для несанкціонованого доступу. Встановлення патчів безпеки є важливим кроком для заповнення потенційних прогалин у системі, забезпечуючи високий рівень захисту від відомих загроз. Vinson регулярно перевіряє наявність оновлень та патчів, а також встановлює їх негайно, щоб забезпечити стійку та безпечну роботу своєї інформаційно-комунікаційної системи.

2.4 Висновки до Розділу 2.

У другому розділі кваліфікаційної роботи були проведені важливі кроки у напрямку забезпечення безпеки інформації в підприємстві Vinson. Спочатку був визначений склад захищуваної інформації, що дозволило чітко визначити обсяг та характер даних, які потребують захисту.

Після цього були вибрані методи та засоби захисту, з урахуванням потенційних загроз та потреб підприємства. Було розроблено комплексну систему захисту інформації, включаючи антивірусні системи, системи моніторингу та інші технологічні рішення. Ці заходи були вибрані з метою надійного захисту даних та запобігання можливим загрозам.

Завершальним етапом була реалізація розробленої системи захисту інформації та її впровадження в інформаційно-комунікаційну систему підприємства. Це забезпечило практичне втілення розроблених заходів безпеки та їх інтеграцію у робочий процес підприємства Vinson.

В результаті реалізації проекту комплексної системи захисту інформації, підприємство Vinson змогло підвищити рівень безпеки своїх даних та інформаційно-комунікаційної системи. Розроблені методи та засоби захисту дозволили ефективно протидіяти потенційним загрозам і забезпечити стабільну та безпечну роботу підприємства. Впровадження цієї системи є важливим кроком у забезпеченні надійності та захищеності інформації в організації.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

За результатами передпроектного обстеження виявлено слабкі місця, які необхідно усунути. Ці проблеми можна усунути шляхом створення КСЗІ. Для цього необхідний розрахунок економічної ефективності проекту, який дасть відповідь на питання про доцільність впровадження заходів зі створення комплексної системи захисту інформації.

Задачу щодо обчислення витрат господарства на розробку КСЗІ умовно можливо розділити на такі етапи:

– Розрахунок витрат на придбання та налаштування елементів системи інформаційної безпеки;

– розрахунок капітальних витрат на придбання, та налагодження елементів системи інформаційної безпеки, або витрат, які пов'язані з впровадженням апаратури, приладів, програмного забезпечення;

– розрахунок річних експлуатаційних витратна утримання та обслуговування КСЗІ;

– визначення річних економічної результатів від впровадження КСЗІ;

– визначення та аналіз показників економічної ефективності запропонованого проєктного рішення;

– висновки.

3.1 Розрахунок витрат на обладнання та програмне забезпечення

Розрахуємо витрати на розробку заходів для забезпечення безпеки інформації та витрати на придбання необхідних засобів. Вартість ліцензійного програмного забезпечення наведено в табл. 3.1. та вартість нового ПК у табл. 3.2.

Таблиця 3.1. – Вартість ліцензійного ПЗ на рік

		Кількість	Вартість за од	Сума (грн)
1	Windows 10 Pro	9	2 800	25 200
2	WPS-Office 365 For Business 2021			
3	Avast Ultimate			

4	winRAR			
5	VPN CyberGhost	2	1301	2602
6	хмарне сховище Pcloud	1	4200	4200
7	Маршрутизатор Cisco 871-SEC-K9	1	17 226	17 226
	Разом			**49 228**

Таблиця 3.2 – Розрахунок вартості нового ПК

Комплектуючі	**Ціна (грн)**
Процесор AMD Ryzen 3 PRO 4350G	3 192
Материнська плата GIGABYTE A520M K V2	2 537
Пам'ять для настільних комп'ютерів AMD 16 GB DDR4 3200 MHz Radeon R9 Gamer	2 422
Корпус GTL 1614+ Black	1 090
SSD Samsung PM9A1 512 GB	2 442
Повітряне охолодження Deepcool Gamma Archer	289
Блок живлення Chieftec APB-500B8	1 253
Монітор Acer V226HQL	3 644
Комплект ASUS U2000 Keyboard + Mouse	646
Разом	**17 515 грн**

Щоб розрахувати трудомісткість розробки КСЗІ, спочатку необхідно визначити тривалість кожної операції за формулою (3.1):

$$t = t_з + t_в + t_а + t_{вз} + t_{озб}, \text{годин} \qquad (3.1)$$

де $t_з$ – час для оформлення технічного завдання.

$t_в$ – час на розробку моделі безпеки інформації господарства.

$t_а$ – час на аналіз ризиків.

$t_{вз}$ - час на визначення вимог, які пов’язані з забезпеченням засобів та заходів захисту.

$t_{озб}$ – час на вибір основних рішень для забезпечення безпеки інформації.

Тож, сумарно витрачений час:

$$t = 18 + 10 + 27 + 25 + 14 = 94 \text{ год.}$$

З огляду на те, що політика інформаційної безпеки все ще є необхідністю для суспільства, можна зрозуміти, що вирішальним фактором для початку створення та впровадження політики інформаційної безпеки та КСЗІ є, насамперед, економічна доцільність цієї політики загалом.

Необхідно порахувати, скільки грошей компанія витратить на розробку політики інформаційної безпеки. Зробимо це за допомогою формули 3.2:

$$К_{рп} = З_{зп} + З_{мч} \qquad (3.2)$$

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

$З_{зп}$ – заробітна плата співробітника;

$З_{мч}$ – час, який витрачено на розробку політики безпеки.

Для обґрунтованого розрахунку, потрібно розглянути погодинну заробітну плату співробітників, яка зазначена в таблиці 3.3

Таблиця 3.3 – Погодинна та місячна заробітна плата співробітників

№	Посада	Погодинна заробітна плата (грн.)	Місячна заробітна плата (грн.)
1	Бухгалтер	150	15 000
2	Головний бухгалтер	205	20 500
3	Юрист	170	14 000
4	Обліковець	120	12 000

Середня погодинна заробітна платня фахівця з інформаційної безпеки (ІБ) складає 150 грн.

Питаннями щодо забезпечення ІБ буде займатись бухгалтер та юрист, томі слід розрахувати додаткові витрати на премії співробітників:

Премія для бухгалтера:

$$0.05 \times 150 \text{ грн} \times 288 \text{ робочих днів на рік} = 2\,160 \text{ грн}$$

Премія для юриста:

$$0.05 \times 170 \times 288 \text{ робочих днів на рік} = 2\,448 \text{ грн}$$

Щоб розрахувати машинний час, використаємо формулу 3.3:

$$С_{мч} = Р \times t_{нал} \times С_е + \frac{Ф_{зал} \times Н_а}{F_p} + \frac{К_{лпз} \times Н_{апз}}{F_p}, \text{грн} \qquad (3.3)$$

Р – потужність ноутбуку;

$С_е$ – тариф на електроенергію;

$Ф_{зал}$ – залишкова вартість ноутбуків на поточний рік;

$Н_а$ – річна норма амортизації;

$Н_{апз}$ – річна норма амортизації на ліцензійне ПЗ;

$К_{лпз}$ – вартість ліцензійного ПЗ на рік;

F_p – річний фонд робочого часу.

Сумарна вартість ліцензійного програмного забезпечення для комп'ютерів на рік становить 49 228 грн.

Вартість одного комп'ютера 17 515 грн, строк корисної служби – 66 місяців (5,5 років)

Накопичена амортизація = (17 515 * 66)/(9*12) = 10 704 грн.

Залишкова вартість = 17 515 - 10 704= 6 811 грн.

Відповідно до цього, можемо сказати, що головним ресурсом для реалізації КСЗІ є фінансовий ресурс, та для того, щоб впроваджувати КСЗІ – необхідно проаналізувати економічний рівень безпеки господарства, для того, щоб визначити можливість реалізації КСЗІ.

$$С_{мч} = 0.25 \times 9 + \frac{6\,811 \times 0.4}{1920} + \frac{49\,228 \times 0.1}{1920} = 6{,}23 \text{ грн.}$$

Відштовхуючись від розрахунків вище, можемо знайти зарплатню виконавця та витрати машинного часу:

$$З_{зп} = 94 \times 150 = 14100 \text{ грн.}$$
$$З_{мч} = 94 \times 6{,}23 = 585{,}9 \text{ грн.}$$

Отже, прорахувавши всі показники, можемо визначити витрати на розробку КСЗІ. Так як$З_{мч}$ – час, який витрачено на розробку КСЗІ, можемо зробити розрахунки за формулою 3.2:

$$К_{рп} = 14100 + 585{,}9 = 14\,658{,}9 \text{ грн.}$$

Повну вартість капітальних витрат будемо розраховувати за формулою 3.4:

$$К = К_{рп} + К_{аз}, \text{грн} \qquad (3.4)$$

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

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

Для впровадження КСЗІ в господарстві, необхідно придбати програмне забезпечення, що наведене у табл. 3.1.

Тому розрахуємо повну вартість капітальних витрат за формулою 3.4:

$$К = 14\,658{,}9 + (49\,228) = 63\,886{,}9 \text{ грн.}$$

3.2 Розрахунок витрат на підтримку обладнання та програмного забезпечення.

На цьому етапі слід розрахувати витрати підприємства на підтримку роботи КСЗІ. Так як в організації забезпечувати БІ будуть 2 особи (бухгалтер та юрист), і їх заробітна платня фіксована (без урахування премій), то можемо розрахувати витрати на підтримку КСЗІ за формулою 3.5:

$$С = С_а + С_з + С_{ел} + С_е + С_{єв} + С_{ліц}, грн \quad (3.5)$$

де $С_а$ – річний фонд амортизаційних відрахувань;

$С_з$ – річний фонд заробітної плати технічного персоналу;

$С_{ел}$ – вартість електроенергії, що споживає апаратура;

$С_{єв}$ – розмір єдиного внеску на загальнообов'язкове соціальне страхування;

$С_{ліц}$ – річні витрати на продовження ліцензій програмного забезпечення.

Для розрахунку річного фонду амортизаційних відрахувань використаємо формулу 3.6.:

$$С_а = Ф_п \div Т, грн \quad (3.6)$$

Де $Ф_п$ - первісна вартість придбаного обладнання;

Т – мінімальний термін корисного використання (2 роки для програмного забезпечення).

$$С_а = 49\,228 \div 2 = 24\,614 \text{ грн}$$

Річний фонд заробітної плати розраховується за формулою 3.7:

$$С_з = (З_{осн1} + З_{осн2} + \ldots З_{оснn}) \times 12, грн. \quad (3.7)$$

Де $З_{осн}$ – заробітна плата співробітника технічного персоналу (премія для співробітників які займаються питаннями ІБ додатково) .

$$С_з = (2\ 160 + 2\ 448) \times 12 = 55\ 296 \text{ грн.}$$

Тепер розрахуємо вартість електроенергії за формулою 3.8:

$$С_{ел} = Р \times F_р \times Ц_е, \text{грн} \qquad (3.8)$$

Де Р – встановлена потужність апаратури (кВт);

$F_р$ – річний фонд робочого часу системи ІБ;

$Ц_е$ – тариф на електроенергію (грн/кВт * год).

$$Ц_е = 2.64 \text{ грн}\backslash\text{кВт} * \text{год}$$

За розрахунками господарства за цей рік, встановлена потужність апаратури ІБ = 1.5 кВт. Режим роботи = 1950 годин на рік.

Отже:

$$С_{ел} = 1.5 \times 1950 \times 2.64 = 7\ 722 \text{ грн.}$$

Витрати на технічне та адміністративне керування ІБ визначаються у відсотках від розміру капітальних витрат.

$$С_{ліц} = 49\ 228 \text{ грн.}$$

Також, до суми річного фонду заробітної плати додається Єдиний Внесок ($С_{єв}$) на загальнообов'язкове загальне державне соціальне страхування – консолідований страховий внесок.

Розмір єдиного внеску на загальнообов'язкове загальне державне соціальне страхування визначається на підставі встановленого чиним законодавством відсотка від суми заробітної плати та становить – 22%:

$$С_{єв} = 0.22 \times С_з, \qquad (3.9)$$

$$C_{єв} = 0.22 \times 55\,296 = 12\,165{,}12 \text{ грн.}$$

Повна вартість річних експлуатаційних витрат:

$$C = 24\,614 + 55\,296 + 7\,722 + 12\,165{,}12 + 49\,228 = 149025{,}1 \text{ грн.}$$

Отже, поточні витрати на рік складають 149 025,1 грн враховуючи витрати на підтримку КСЗІ, ЄСВ та премії співробітникам, які займаються ІБ додатково.

3.3. Оцінка величини збитку у разі реалізації загрози

Оцінка величини збитку у разі реалізації загрози є важливою для розуміння потенційних наслідків інциденту та прийняття обґрунтованих рішень з питань безпеки і захисту інформації. Знання очікуваних втрат, якщо загроза матеріалізується, допомагає приймати обґрунтовані рішення щодо інвестицій у заходи безпеки. На підставі оцінки збитку можна визначити, чи цілком розумні витрати на запобігання загроз або ліквідацію інцидентів.

Прорахуємо можливі збитки, для початку врахуємо погодинну заробітну платню співробітників ІКС. Умовно візьмемо 8 годин простою системи. Відповідно до цього можемо прорахувати $П_п$ за формулою 3.10:

$$П_п = \frac{\sum З_с}{F} \times t_п, \qquad (3.10)$$

$$П_п = (150 + 170) \times 8 = 2\,560 \text{ грн.}$$

Витрати на відновлення сегменту ІКС будуть залежати від витрат на технічний персонал. В нашому випадку, питаннями відновлення сегменту ІКС займаються бухгалтер та юрист які також виконують ролі адміністраторів системи, тому ми можемо знайти дані витрати:

$$П_з = 2\,560 \times 2 = 5\,120 \text{ грн.}$$

Розрахуємо загальний збиток від атаки за формулою 3.11:

$$B = \sum i \times \sum n \times U, \qquad (3.11)$$

де і – кілька атакованих сегментів;

n – середнє число атак на рік.

За нещодавніми показниками, в ІКС за попередні 5 років загалом було атаковано 12 сегментів ІКС. Можна зробити припущення, що за рік було атаковано 6 сегментів. В середньому за рік було проведено 18 спроб атакувати сегменти ІКС.

Отже, можемо прорахувати загальні збитки від атаки:

$$B = 6 \times 12 \times 5\,120 = 368\,640 \text{ грн.}$$

Ймовірність реалізації загрози умовно взято як 50%. Тоді можемо прорахувати ефект від впровадження КСЗІ.

$$E = 368\,640 \times 0.5 - 149025{,}1 = 35\,294{,}9 \text{ грн}$$

Дивлячись на дані розрахунки, можемо зробити висновок, що ефект реалізованого КСЗІ достатньо добре знизить можливі збитки від реалізації атак на сегменти ІКС. Спочатку треба визначити коефіцієнт повернення інвестицій за формулою 3.12:

$$ROSI = \frac{E}{K}, \qquad (3.12)$$

де Е – загальний ефект від впровадження ІБ;

K – капітальні інвестиції, які забезпечили даний ефект. Отже:

$$ROSI = \frac{35\ 294{,}9\ \text{грн}}{63\ 658{,}9\ \text{грн}} = 0.55$$

В розрахуванні витрат на реалізацію КСЗІ, підсумковим пунктом буде розрахунок терміну окупності, що представляє собою час, за який окупляться встановлені системи ІБ та впроваджені політики.

Доцільним вважається проєкт системи ІБ, який має розрахункове значення коефіцієнта повернення інвестицій більший ніж величина річної депозитної ставки з урахуванням інфляції:

$$ROSI > \frac{(N_{\text{деп}} - N_{\text{інф}})}{100}, \qquad (3.13)$$

де $N_{деп}$ – річна депозитна ставка (20%);

$N_{інф}$ – річний рівень інфляції (5%).

Так як 0,55 > 0.15, то проєкт можна вважати економічно доцільним.

Термін окупності капітальних інвестицій (T_O) показує, скільки потрібно років, щоб окупити капітальні інвестиції за рахунок загального ефекту від впровадження системи ІБ, та розраховується за формулою 3.14:

$$T_O = \frac{K}{E}, \qquad (3.14)$$

Розрахуємо:

$$T_O = \frac{63\ 658{,}9\ \text{грн}}{35\ 294{,}9\text{грн}} = 1.81\ \approx 1\ \text{рік та 8 місяців.}$$

В розділі було проведено розрахунки:

– капітальних витрат на придбання та налагодження складових системи ІБ та витрат, що пов’язані з закупкою апаратури та програмного забезпечення (63 886,9.);

– річних експлуатаційних витрат на підтримку та обслуговування об’єкту проєктування (149025,1.);

– терміну окупності капітальних інвестицій (1 рік та 8 місяців).

3.4. Висновок

Результатом виконаної роботи є проект створення комплексної системи захисту інформації в організації ТОВ «Vinson». Метою створення КСЗІ є: запобігання розголошенню, копіюванню, викраденню, знищенню, модифікації, спотворенню інформації з обмеженим доступом; захист відомостей, що становлять комерційну таємницю відповідно до закону.

Розроблено необхідні програмно-технічні та інженерні заходи. Прораховуються ризики реалізації проекту. Виконувана робота була розподілена та організована впорядковано.

Результатом реалізації проекту є реалізація розроблених заходів щодо комплексного захисту інформації. За результатами розрахунку витрат на створення КСЗІ на ТОВ «Vinsos» та її обслуговування проведено оцінку ефективності. Згідно з оцінкою, загальна вартість проекту становить 200018 грн.

З точки зору економічної доцільності проект визнано ефективним, про що свідчать результати розрахунку.

Реалізуючи цей проект, організація заощадить гроші, усуне загрози, а отже, компанія отримає додаткові вигоди.

ВИСНОВКИ

У даній кваліфікаційній роботі було проведено детальний аналіз інформаційно-комунікаційної системи (ІКС) підприємства "Vinson" з метою визначення поточного стану безпеки та необхідності створення комплексної системи захисту інформації (КСЗІ). У розділі 1 було розглянуто опис підприємства "Vinson", аналіз існуючих заходів з захисту інформації та визначено поточний стан інформаційної безпеки ІКС. На основі цього аналізу була встановлена необхідність у створенні КСЗІ для забезпечення надійного захисту інформації.

У розділі 2 було розроблено комплексну систему захисту інформації в ІКС підприємства "Vinson". Було визначено склад захищуваної інформації та проведений вибір методів та засобів захисту, що відповідають потребам підприємства. Також був розроблений проект комплексної системи захисту інформації, який включає контроль доступу користувачів, шифрування даних, мережевий захист та інші заходи безпеки.

У розділі 3 було визначено вартість розроблення КСЗІ та проведений аналіз економічних переваг та недоліків впровадження КСЗІ для підприємства "Vinson". Встановлено, що впровадження КСЗІ є вигідним з точки зору забезпечення надійності та захищеності інформації, а також може запобігти потенційним втратам чи пошкодженню даних.

Завдання дослідження, поставлені у роботі, були успішно виконані. В рамках дослідження був проведений аналіз поточного стану інформаційної безпеки інформаційно-комунікаційної системи підприємства "Vinson". Були ідентифіковані сильні та слабкі сторони чинних заходів безпеки на підприємстві та визначені можливі загрози в інформаційній безпеці компанії.

Також були проаналізовані типи атак, які можуть призвести до порушень безпеки, зокрема зловмисне програмне забезпечення, соціальна інженерія, фішинг та інші загрози. На основі отриманих результатів була розроблена комплексна система захисту інформації, яка враховує виявлені загрози та потреби підприємства.

Також були визначені необхідні технологічні рішення, зокрема антивірусні системи, системи моніторингу та інші, для забезпечення надійного захисту даних. Розроблена система захисту інформації була реалізована та успішно впроваджена в інформаційно-комунікаційну систему підприємства "Vinson".

Таким чином, завдяки проведенню цього дослідження та виконанню поставлених завдань, підприємство "Vinson" змогло покращити безпеку своєї інформаційно-комунікаційної системи, забезпечивши надійний захист даних та запобігши можливим загрозам та атакам.

ПЕРЕЛІК ПОСИЛАНЬ

1. Дудатьєв А. В. Захист комп'ютерних мереж. Теорія та практика. Навчальний посібник / Дудатьєв А. В., Войтович О. П., Каплун В. А. – Вінниця ВНТУ - 219 с.

2. Комплексные системы защиты информации предприятия: учебное пособие / В.Т. Еременко, М.Ю. Рытов, О.М. Голембиовская, П.Н. Рязанцев. – Орел: ФГБОУ ВО «Орловский государственный университет имени И.С. Тургенева», 2016. – 116 с.

3. Поради (рекомендації) щодо створення КСЗІ в ІТС, які використовуються для надання послуг доступу до мережі Інтернет [Електроннийресурс]- Режим доступу:https://cip.gov.ua/ua/news/poradi-rekomendaciyi-shodo-stvorennya-kszi-v-its-yaki-vikoristovuyutsya-dlya-nadannya-poslug-dostupu-do-merezhi-internet?fbclid=IwAR3RcWOpnttuJROqWpz0bwL1u-0OsySollvFJqw2vLCFk6X_EA79Se3_1ZY

4. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. [Електроннийресурс]- Режим доступу: https://tzi.com.ua/downloads/3.7-0032005.pdf?fbclid=IwAR078jEedTuTzkNMfZIybcuywbBxCJr1znhTvkKEpYywIPP3FRBZGqAr3AI

5. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. [Електроннийресурс]- Режим доступу: https://tzi.ua/assets/files/НД-ТЗІ-2.5-005--99.pdf.

6. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу НД ТЗІ 2.5-004-99. [Електроннийресурс]- Режим доступу: https://tzi.ua/assets/files/НД-ТЗІ-2.5-004-99.pdf?fbclid=IwAR16Qka92G63wtjvFfHcK5rALmf2z0iKjdO0rN6f005_fxovlJX3-RtIpqk

7. Манжай О. В. Правові засади захисту інформації: навчальнийпосібник. Харків : Ніка Нова, 2014. 104 с.

8. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу;

9. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу;

10. НД ТЗІ 1.1-004-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу;

11. 16. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації.

12. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі;

13. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу;

14. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу;

15. Degtyareva L., Miroshnykova M. The problems of the security of information transport and logistics systems/ // Theses of international scientific and practical conference "Globalization of scientific and educational space. Innovations of transport. Problems, experience, prospects", May 2018, Italy. – C. 32-34.

16. Porkodi V., Sivaram M., Mohammed A.S., Manikandan V. Survey on White-Box Attacks and Solutions. Asian Journal of Computer Science and Technology. Vol. 7, Is. 3. pp. 28–32.

17. Manikandan V, Porkodi V, Mohammed AS, Sivaram M, "Privacy Preserving Data Mining Using Threshold Based Fuzzy cmeans Clustering", ICTACT Journal on Soft Computing, Volume 9, Issue 1, 2018, pp.1813-1816. DOI: 10.21917/ijsc.2018.0252

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	**Формат**	**Найменування**	**Кількість листів**	**Примітки**
Документація				
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	Стан питання. Постановка задачі	33	
6	А4	Спеціальна частина	24	
7	А4	Економічний розділ	9	
8	А4	Висновки	2	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	2	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	
13	А4	Додаток Ґ	1	
13	А4	Додаток Д	1	

ДОДАТОК Б. Наказ «Про організацію навчання співробітників з питань безпеки та захисту конфіденційної інформації»

Приватне підприємство«Vinson»

Наказ

№ 28 01.06.23 р.

Про організацію навчання співробітників з питань безпеки та захисту конфіденційної.інформації

На виконання вимог щодо забезпечення безпеки і захисту конфіденційної інформації, а також з метою підвищення рівня обізнаності та компетентності співробітників на підприємстві ТОВ "Vinson" у цих питаннях, НАКАЗУЮ:

1. Організувати навчання співробітників підприємства з питань безпеки та захисту конфіденційної інформації.

2. Визначити відповідальну особу, яка буде координувати процес навчання та забезпечувати його ефективність.

3. Розробити навчальну програму, яка буде включати наступні питання:

-Основні принципи безпеки і захисту інформації.

-Розпізнавання потенційних загроз та ризиків для інформаційно-комунікаційної системи.

-Використання паролів та інших методів аутентифікації.

-Використання шифрування для захисту конфіденційної інформації.

-Заходи безпеки під час роботи з електронною поштою та використання Інтернету.

-Процедури забезпечення фізичної безпеки приміщень та обладнання.

4. Планування та проведення навчання повинні бути здійснені з урахуванням графіку роботи співробітників. Забезпечити належну організацію та проведення занять.

5. Після завершення навчання здійснити оцінку засвоєння матеріалу співробітниками та видачу відповідних сертифікатів або довідок.

6. Забезпечити документування проведеного навчання та зберігання відповідних записів.

7. Контроль за виконанням даного наказу покласти на Пратта Кирила Анатолійовича

Цей наказ набирає чинності з моменту його підписання.

Додатки на 5 аркушах.

Директор (підпис) С. І. Дрозд

ДОДАТОК В. Наказ «Про заміну застарілого обладнання на нове»

Приватне підприємство«Vinson»

Наказ

№ 29 03.06.23 р.

Про заміну застарілого обладнання на нове

На виконання рішення директора підприємства щодо оновлення апаратного та технічного обладнання, а з метою покращення ефективності роботи та забезпечення надійності інформаційно-комунікаційної системи підприємства «Vinson» , НАКАЗУЮ:

1. Здійснити повну заміну застарілого обладнання на нове згідно зі списком:

-ПК: Процесор AMD Ryzen 3 PRO 4350G, Материнська плата GIGABYTE A520M K V2, Пам'ять для настільних комп'ютерів AMD 16 GB DDR4 3200 MHz Radeon R9 Gamer, Корпус GTL 1614+ Black, SSD Samsung PM9A1 512 GB, Повітряне охолодження Deepcool Gamma Archer, Блок живлення Chieftec APB-500B8, Монітор Acer V226HQL, Комплект ASUS U2000 Keyboard + Mouse.

-Операційна система на нових ПК - Windows 10.

-Антивірусне ПЗ: заміна безкоштовної версії Avast на Avast Ultimate.

2. Забезпечити встановлення та належну конфігурацію нового обладнання згідно з вимогами безпеки та потребами підприємства.

3. Провести перенесення даних зі старого обладнання на нове з урахуванням збереження конфіденційності та цілісності інформації.

4. Здійснити впровадження нового обладнання в інформаційно-комунікаційну систему підприємства з мінімальними перервами у роботі.

5. Визначити відповідальних осіб, які будуть забезпечувати належну експлуатацію та обслуговування нового обладнання.

Цей наказ набирає чинності з моменту його підписання.

Додатки на 5 аркушах. Директор (підпис) С. І. Дрозд

ДОДАТОК Г. Перелік документів на оптичному носії

1 Презентація Шрамова.ppt

2 Диплом Шрамова.doc

ДОДАТОК Ґ. Відгук керівника економічного розділу

Керівник розділу _____ _____

(підпис) (прізвище, ініціали)

ДОДАТОК Д. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125-19-2 Шворака М.С.

на тему: «Розробка комплексної системи захисту інформації в інформаційно-комунікаційній системі підприємства «Vinson»

Керівник роботи,

Ю.А. Мілінчук