**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**КЕМЕРОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

**Институт цифры**

**ОТЧЕТ**

Расчетно-графическая работа

по дисциплине «Специальные вопросы защиты информации»

Направление 02.03.02 – «Фундаментальная информатика и информационные технологии»

Студенты:

Копытов А.В

Рябов В.А

Мордвинов С.Е

Работа защищена

«\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_»

“\_\_\_\_” \_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_г.

Кемерово 2024

Оглавление

[1. Описание объекта защиты 3](#_Toc180581096)

[2. Анализ объекта защиты 3](#_Toc180581097)

[3. Схема подчиненности 5](#_Toc180581098)

[4. Денежные обороты 5](#_Toc180581099)

[4.1. ГИС 7](#_Toc180581100)

[4.2. АСУ ТП 7](#_Toc180581101)

[4.3. ИСПДн 8](#_Toc180581102)

[4.4. КИИ 8](#_Toc180581103)

[АКТ № 1 10](#_Toc180581104)

[АКТ № 2 12](#_Toc180581105)

[5. Модель угроз безопасности информации 14](#_Toc180581106)

[5.1. Возможные негативные последствия от реализации угроз ИБ 14](#_Toc180581107)

[5.2. Возможные объекты воздействия угроз ИБ 15](#_Toc180581108)

[5.3. Источники угроз безопасности информации 17](#_Toc180581109)

[5.4. Способы реализации угроз безопасности информации 20](#_Toc180581110)

[5.5. Возможные угрозы безопасности информации 21](#_Toc180581111)

[5.6. Актуальные угрозы безопасности информации 22](#_Toc180581112)

# Описание объекта защиты

Проект «Инновационная мебельная логистика» (ИМЛ) предполагает организацию автоматизированного производства и доставки мебели с использованием современных технологий. Для управления проектом будет создана компания-оператор ИМЛ при участии государства, институтов развития и частных инвесторов.

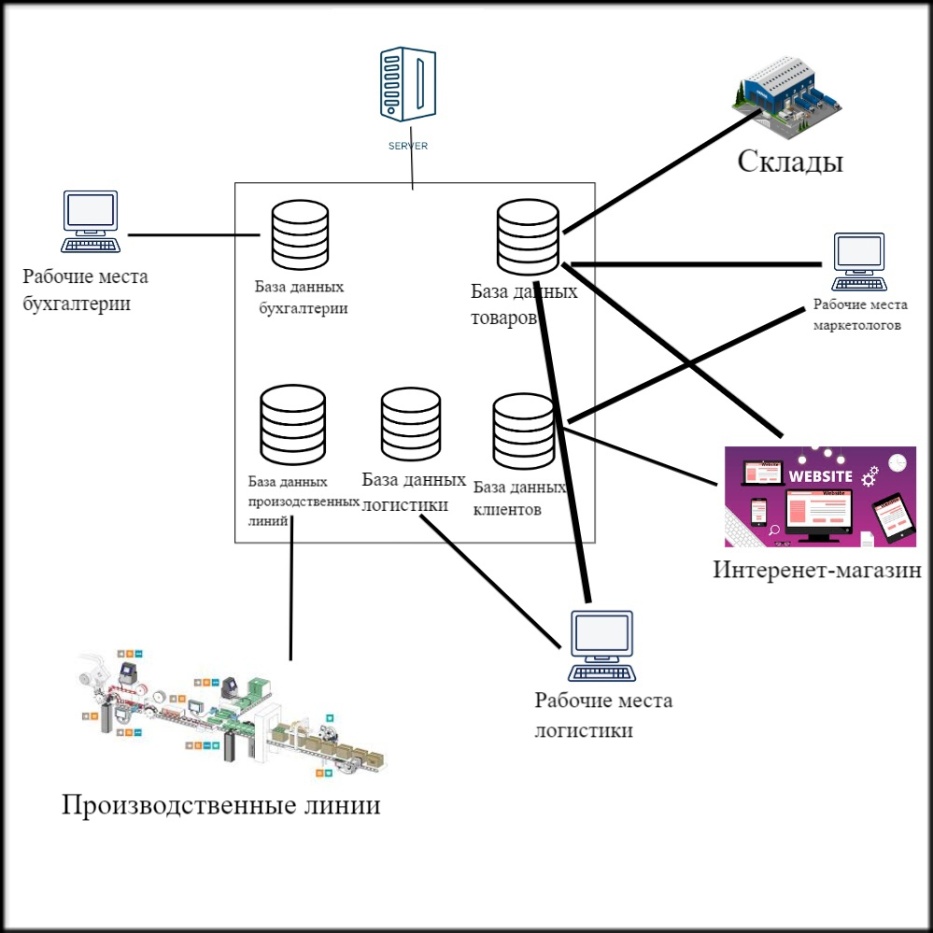
Нормативные акты:

1. Федеральный закон №152-ФЗ "О персональных данных" Регулирует сбор, обработку, хранение и защиту персональных данных граждан. Для мебельной компании это может включать личную информацию клиентов, такую как имя, адрес, контактные данные и историю покупок. Нарушение правил сбора или обработки может привести к ответственности.

2. Федеральный закон №149-ФЗ "Об информации, информационных технологиях и о защите информации" Устанавливает общие требования к защите информации, включая меры по предотвращению несанкционированного доступа и утечек информации. Для мебельной компании это может касаться защиты коммерческой информации, технологий производства и бизнес-планов.   
Проект направлен на создание «вытягивающего» эффекта для следующих технологий:  
- Производство мебели;  
- Сборка и доставка мебели;  
- Управление складами и логистикой;  
- Беспроводные коммуникации для мониторинга и управления процессами;  
- Технология управления цепочками поставок;  
- Кибербезопасность для защиты данных и систем.

# Анализ объекта защиты





# 3. Схема подчиненности

Генеральный директор

Директор по производству

Генеральный директор

Менеджер по доставке

Менеджер по складам

Менеджер по автоматизации

Менеджер по качеству

Специалист по транспортировке

Специалист по логике

Специалисты по ИТ

Специалисты по качеству

Генеральный директор: Возглавляет всю компанию и отвечает за стратегическое руководство проектом.

Директор по производству: Отвечает за организацию и контроль процессов производства мебели, управления качеством и внедрения инновационных технологий.

Директор по логистике: Несет ответственность за логистические операции, включая управление складами и процессами доставки.

Менеджеры: Каждый из них управляет определенной областью и подчиняется соответствующему директору. Они курируют работу своих отделов, контролируют выполнение задач и взаимодействуют с другими подразделениями.

Специалисты: Работают в своих областях, занимаются конкретными задачами и обеспечивают выполнение повседневных функций.

# 4. Денежные обороты

Доходы

*- Продажа мебели:*

- Ожидаемые годовые продажи: 100 000 000 рублей

*- Доставка и установка:*

- Дополнительные услуги: 10% от продаж

- Общий доход от услуг: 10 000 000 рублей

*- Партнёрские программы:*

- Ожидаемый доход: 5 000 000 рублей

*- Лицензирование технологий:*

- Ожидаемый доход: 3 000 000 рублей

*- Государственное финансирование:*

- Поддержка в рамках проекта: 2 000 000 рублей

*Общие доходы:*

- 100 000 000 + 10 000 000 + 5 000 000 + 3 000 000 + 2 000 000 = 120 000 000 рублей

Расходы

*- Производственные расходы:*

- Сырьё и материалы: 40 000 000 рублей

- Оборудование: 25 000 000 рублей

*- Заработная плата:*

- ЗАТРАТЫ на оплату труда сотрудников: 15 000 000 рублей

*- Логистические расходы:*

- Доставка: 5 000 000 рублей

- Складирование: 4 000 000 рублей

*- Маркетинг и реклама:*

- Расходы на продвижение: 3 000 000 рублей

*- Налоги и сборы:*

- Обязательные платежи: 6 000 000 рублей

*- Исследования и разработки:*

- Инвестиции в новые технологии: 2 000 000 рублей

*Общие расходы:*

- 40 000 000 + 25 000 000 + 15 000 000 + 5 000 000 + 4 000 000 + 3 000 000 + 2 000 000 = 94 000 000 рублей

Итог

Чистая прибыль:

- Общие доходы - Общие расходы = 120 000 000 - 94 000 000 = 26 000 000 рублей

# 4.1. ГИС

Исходя из Федерального закона от 27.07.2006 N 149-ФЗ (ред. от 31.07.2023) "Об информации, информационных технологиях и о защите информации", организация «Эвонекс» не является Государственной Информационной Системой(ГИС), так как информационная система создана на основании нужд производства.

# 4.2. АСУ ТП

Согласно приказу ФСТЭК №31 «Об утверждении требований к обеспечению защиты информации в АСУ ТП на КВО, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» (далее – приказ ФСТЭК №31) класс защищенности автоматизированной системы управления определяется в зависимости от уровня значимости (УЗ) обрабатываемой в ней информации.

УЗ определяется степенью возможного ущерба от нарушения ее целостности, доступности или конфиденциальности, в результате которого возможно нарушение штатного режима функционирования автоматизированной системы управления или незаконное вмешательство в процессы ее функционирования.

В связи с особенностями работы системы отсутствие КДЦ обрабатываемой в системе информации не приведет к негативным последствиям.

Для определения уровня защищённости необходимо определить степень ущерба по КДЦ для АСУ ТП.

При нарушении конфиденциальности возможна низкая степень ущерба, потому что потеря конфиденциальность производства мебели не нанесёт большого ущерба ввиду доступности знаний и отсутствия секретной рецептуры и номенклатуры производства.

При нарушении конфиденциальности возможна низкая степень ущерба, потому что потеря доступности не имеет большого значения ущерба при остановке производства и не произведёт ЧС площадью больше локальногоуровня.

При нарушении целостности также не произойдёт ЧС выше локального уровня, исходя из чего ущерб не будет выше низкого уровня.

Информация, обрабатываемая в автоматизированной системе управления, имеет низкий уровень значимости (УЗ 3), если для всех свойств безопасности информацииопределены низкие степени ущерба. Таким образом, класс защищенности автоматизированной системы управления – третий (К3).

# 4.3. ИСПДн

Согласно Федеральному закону от 27.07.2006 №152-ФЗ(ред. от 06.02.2023) "О персональных данных" информационная система «ИМЛ» располагает ИСПДн с хранящимися в ней ПДн вида «Иные».

Исходя из Постановления Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" актуальность угрозы безопасности ПДн оценивается как угрозы 3-го типа, то есть актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Постановление Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" позволяет сделать вывод о 3-ем уровне защищенностиИСПДн на основе категоризации ПДн и субъектов. Присвоение третьего типа УЗ рассматриваемой ИСПДн основывается на нескольких условиях: категория ПДн - «Иные», категория субъектов – «не сотрудников оператор», количество которых предположительно превышает 100 000 человек, тип угрозы ПДн – актуальны угрозы 3 типа.

# 4.4. КИИ

Исходя из определений КИИ и объекта КИИ статьи №187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" рассматриваемое предприятие по изготовлению и сбыту мебели «ИМЛ» не относится к объектам КИИ, поскольку возможные нарушения в работе фирмы не повлекут за собой негативные социальные, политические, экономические или экологические последствия.

Наша организация не относится к субъектам КИИ, так как она относится к производству товаров потребления и не является ни объектом, ни субъектом КИИ

ООО «Госкомнадзор»

# АКТ № 1

ОПРЕДЕЛЕНИЯ УРОВНЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ УПРАВЛЕНИЯ ПРОИЗВОДСТВОМ «ИМЛ»

от 25 сентября 2024

**Комиссия по приведению в соответствие с требованиями**

**законодательства Российской Федерации в области персональных данных:**

Зам. директора по ФЭР Иванова О.В.

Зам. директора по ФЭР Игорева О.В.

Зам. директора по УВР Сергеева Е.А.

Секретарь Антонова Н.Н.

электроник Гайзенбергова Д.Н

рассмотрела исходные данные ИСПДн «ИМЛ»:

**Тип актуальных угроз** 3 тип. Угрозы, не связанные с наличием недокументированных

(недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе

**Категория обрабатываемых ПДн** Иные данные

**Состав обрабатываемых ПДн** В информационной системе

обрабатываются персональные данные субъектов персональных данных, не являющихся сотрудниками оператора

**Количество субъектов ПДн** Обрабатываются персональные данные более чем 100000 субъектов персональных данных

В соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119, Регламентом по определению уровня защищенности ПДн, а так же в результате анализа исходных данных, проведенной оценки возможного вреда и проведенного анализа и оценки угроз безопасности персональных данных с учетом особенностей данной информационной системы, комиссия

РЕШИЛА:

Установить 3 уровень защищенности персональных данных при их обработке в ИСПДн «ИМЛ»

ООО «Госкомнадзор»

# АКТ № 2

ОПРЕДЕЛЕНИЯ ПРОГРАММНЫХ И ТЕХНИЧЕСКИХ СРЕДСТВ ДЛЯ АВТОМАТИЗАЦИИ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ОБОРУДОВАНИЕМ В ИНФОРМАЦИОННОЙ СИСТЕМЕ УПРАВЛЕНИЯ ПРОИЗВОДСТВОМ «ИМЛ»

от 25 сентября 2024

**Комиссия по приведению в соответствие с требованиями**

**законодательства Российской Федерации в области персональных данных:**

Зам. директора по ФЭР Иванова О.В.

Зам. директора по ФЭР Игорева О.В.

Зам. директора по УВР Сергеева Е.А.

Секретарь Антонова Н.Н.

электроник Гайзенбергова Д.Н

рассмотрела особенности работы АСУ ТП «ИМЛ»:

**Уровень защищенности** имеет низкий уровень значимости (УЗ 3), если для всех свойств безопасности информации определены низкие степени ущерба

**При нарушении целостности** Не произойдёт ЧС выше локального уровня, исходя из чего ущерб не будет выше низкого уровня.

**При нарушении конфиденциальности** Низкая степень ущерба, не нанесёт большого ущерба ввиду доступности знаний и отсутствия секретной номенклатуры производства.

**При нарушении доступности** Низкая степень ущерба, потому что потеря доступности не имеет большого значения ущерба при остановке производства

**Уровень значимости** Имеет уровень значимости 3, если для всех свойств безопасности информации определены низкие степени ущерба.

В соответствии с Приказом ФСТЭК России от 14.03.2014 N 31 (ред. от 15.03.2021) "Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды", комиссия

РЕШИЛА:

Установить 3 класс автоматизированной системы управления «ИМЛ».

# 5. Модель угроз безопасности информации

Модель угроз безопасности информации составлена согласно методическому документу ФСТЭК от 5 февраля 2021 г. «Методика оценки угроз безопасности информации».

Согласно приложению 3 к Методике, рекомендуемая структура модели угроз безопасности информации состоит из следующих разделов:

1. Общие положения
2. Описание систем и их характеристика как объектов защиты
3. Возможные негативные последствия от реализации (возникновения) угроз безопасности информации
4. Возможные объекты воздействия угроз безопасности информации
5. Источники угроз безопасности информации
6. Способы реализации угроз безопасности информации
7. Актуальные угрозы безопасности информации.

Содержимое разделов «Общие положения» и «Описание систем» были приведены в работе ранее.

# 5.1. Возможные негативные последствия от реализации угроз ИБ

Исходя из Приложения 4 к Методике оценки угроз безопасности информации и особенностей объекта защиты, существую следующие виды рисков (ущерба) и негативных последствий от реализации угроз безопасности информации:

Таблица 1. Возможные негативные последствия от реализации угроз ИБ.

|  |  |
| --- | --- |
| Виды риска (ущерба) | Возможные типовые негативные  последствия |
| Ущерб физическому лицу | * Угроза жизни или здоровью. * Финансовый, иной материальный ущерб физическому лицу. |
| Риски юридическому лицу, связанные с хозяйственной деятельностью | * Потеря денежных средств. * Недополучение ожидаемой прибыли. * Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций. * Необходимость дополнительных затрат на восстановление деятельности. * Нарушение штатного режима функционирования АСУ и управляемого объекта и/или процесса. * Срыв запланированной сделки с партнером. * Утрата доверия. * Причинение имущественного ущерба. |
| Ущерб государству в  социальной, экономической,  политической, экологической  сферах деятельности | * Причинение ущерба жизни и здоровью людей. * Прекращение или нарушение функционирования объектов транспортной инфраструктуры. * Снижение уровня дохода организации с государственным участием. * Доступ к системам и сетям с целью незаконного использования вычислительных мощностей. |

# 5.2. Возможные объекты воздействия угроз ИБ

Основные компоненты системы, на которые можно произвести воздействие, приведены в таблице 2.

Таблица 2. Возможные объекты воздействия угроз ИБ.

|  |  |
| --- | --- |
| **Группы информационных ресурсов** | **Объекты воздействия** |
| Информация (данные), содержащаяся в системах и сетях | * Данные о маршрутах грузового автотранспорта * Данные о клиентах * Данные о производимых товарах |
| Программно-аппаратные средства сбора, обработки и хранения информации | * Серверное оборудование (обработки данных с датчиков, центра управления трафиком, хабов) * Система управления базами данных, базы данных * Датчики * Оборудование |
| Программные средства | * Системное ПО * Прикладное ПО |
| Средства защиты информации | * Средства защиты информации |
| Привилегированные и непривилегированные пользователи систем и сетей, а также интерфейсы взаимодействия с ними | * Системные администраторы * Сетевые инженеры * Сотрудники Центра * Сотрудники, работающие в хабах * Другие сотрудники |
| Обеспечивающие системы | * Проводные и беспроводные каналы передачи данных |

# 5.3. Источники угроз безопасности информации

В рамках данного раздела определены актуальные антропогенные источники угроз безопасности информации, то есть модель нарушителя.

Нарушители имеют разные уровни компетентности, оснащенности ресурсами и мотивации для реализации угроз безопасности информации. Совокупность данных характеристик определяет уровень возможностей нарушителей по реализации угроз безопасности информации. В зависимости от уровня возможностей нарушители подразделяются на нарушителей, обладающих:

* базовыми возможностями по реализации угроз безопасности информации (Н1) – имеют возможность реализовывать только известные угрозы, направленные на известные (документированные) уязвимости, с использованием общедоступных инструментов, а также имеют возможность совершать физическое воздействие;
* базовыми повышенными возможностями по реализации угроз безопасности информации (Н2) - имеют возможность реализовывать угрозы, в том числе направленные на неизвестные (недокументированные) уязвимости, с использованием специально созданных для этого инструментов, свободно распространяемых в сети «Интернет». Не имеют возможностей реализации угроз на физически  
  изолированные сегменты систем и сетей;
* средними возможностями по реализации угроз безопасности информации (Н3) – в основном к ним относятся террористические и экстремистские группировки, а также разработчики программных, программно-аппаратных средств;
* высокими возможностями по реализации угроз безопасности информации (Н4) – в основном к ним относятся специальные службы иностранных государств.

При этом нарушители подразделяются на две категории:

* внешние нарушители – нарушители, не имеющие прав доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочий по доступу к информационным ресурсам и компонентам систем и сетей, требующим авторизации;
* внутренние нарушители – нарушители, имеющие права доступа в  
  контролируемую (охраняемую) зону (территорию) и (или) полномочия по автоматизированному доступу к информационным ресурсам и компонентам систем и сетей.

Актуальные нарушители определены в таблице 3. Вид ущерба (У-1, У-2, У-3) определен согласно таблице 1.

Таблица 3. Источники угроз безопасности информации.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Вид нарушителя | Категория | Уровень  возмож-ностей | Цели реализации угроз | Вид ущерба |
| Отдельные физические лица (хакеры) | Внешний | Н2 | Получение финансовой или материальной выгоды (по найму конкурирующих организаций). | У-1, У-2 |
| Любопытство или желание самореализации. | У-1, У-2, У-3 |
| Конкурирующие организации | Внешний | Н2 | Получение конкурентных преимуществ. | У-2 |
| Получение финансовой или иной  материальной выгоды | У-2 |
| Поставщики  вычислительных услуг и услуг связи | Внутренний | Н1 | Непреднамеренные, неосторожные или  неквалифицированные действия. | У-2 |
| Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ | Внутренний | Н1 | Непреднамеренные, неосторожные или  неквалифицированные действия. | У-2 |
| Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.) | Внутренний | Н1 | Непреднамеренные, неосторожные или  неквалифицированные действия. | У-2 |
| Авторизованные  пользователи систем и сетей | Внутренний | H1 | Получение финансовой или иной материальной выгоды. | У-2 |
| Месть за ранее совершенные действия. | У-1, У-2 |
| Непреднамеренные, неосторожные или неквалифицированные действия | У-1, У-2 |
| Системные администраторы и администраторы  безопасности | Внутренний | H2 | Получение финансовой или иной материальной выгоды. | У-2 |
| Любопытство или желание самореализации. | У-2 |
| Месть за ранее совершенные действия. | У-2 |
| Неосторожные или неквалифицированные действия | У-2 |
| Бывшие работники (пользователи) | Внешний | H1 | Получение финансовой или иной материальной выгоды. | У-2 |
| Месть за ранее совершенные действия | У-2 |

# 5.4. Способы реализации угроз безопасности информации

В ходе оценки угроз безопасности информации должны быть определены актуальные способы реализации (возникновения) угроз безопасности информации, за счет использования которых актуальными нарушителями могут быть реализованы угрозы безопасности информации в системах и сетях.

Способы являются актуальными, когда возможности нарушителя позволяют их использовать для реализации угроз безопасности и имеются или созданы условия, при которых такая возможность может быть реализована в отношении объектов воздействия.

На актуальность были проанализированы способы реализации, представленные в Методике, а также в Перечне способов реализации угроз с сайта ФСТЭК (bdu.fstec.ru).

Актуальными были признаны следующие способы реализации угроз:

• Эксплуатация известных уязвимостей

• Использование недостатков конфигурации

• Использование недостатков архитектуры (эксплуатация недостатков незащищенных протоколов передачи данных и др.)

• Внедрение вредоносного программного обеспечения

• Сканирование сетевой инфраструктуры

• Изучение информации о системе

• Считывание вводимой и выводимой информации

• Реализация социальной инженерии

• Атака типа "отказ в обслуживании"

• Подбор (восстановление) аутентификационной информации

• Модификация (подмена) прошивки (микропрограммы)

• Физическое воздействие.

# 5.5. Возможные угрозы безопасности информации

В данном разделе были определены возможные угрозы безопасности информации (УБИ) для ранее определенных систем и сетей.

Для оценки актуальности угроз безопасности информации использовались такие исходные данные, как общий перечень угроз безопасности информации, содержащийся в банке данных угроз безопасности информации ФСТЭК России, негативные последствия от реализации УБИ, виды и категории актуальных нарушителей, которые могут реализовывать УБИ, в том числе непреднамеренные угрозы, а также актуальные способы реализации (возникновения) угроз безопасности информации.

|  |  |
| --- | --- |
| Идентификатор УБИ | Наименование УБИ |
| УБИ.006 | Угроза внедрения кода или данных |
| УБИ.008 | Угроза восстановления и/или повторного использования аутентификационной информации |
| УБИ.012 | Угроза деструктивного изменения конфигурации/среды окружения программ |
| УБИ.014 | Угроза длительного удержания вычислительных ресурсов пользователями |
| УБИ.022 | Угроза избыточного выделения оперативной памяти |
| УБИ.023 | Угроза изменения компонентов информационной (автоматизированной) системы |

# 5.6. Актуальные угрозы безопасности информации

Актуальность возможных угроз безопасности информации определяется наличием сценариев их реализации. Определение сценариев предусматривает установление последовательности возможных тактик и соответствующих им техник, применение которых возможно актуальным нарушителем с соответствующим уровнем возможностей, а также доступности интерфейсов для использования соответствующих способов реализации угроз безопасности информации.

Исходя из Приложения 11 к Методике оценки угроз безопасности информации: Перечень основных тактик и соответствующих им типовых техник, используемых для построения сценариев реализации угроз безопасности информации, нами была составлена таблица актуальных угроз безопасности информации, их тактик и техник.

Таблица 5

|  |  |  |
| --- | --- | --- |
| **УБИ №006. Угроза внедрения кода или данных** | | |
| **Т1** | Сбор информации о системах и сетях | Т1.1. Направленное сканирование при помощи специализированного программного обеспечения подключенных к сети устройств с целью идентификации сетевых сервисов, типов и версий программного обеспечения этих сервисов, а также с целью получения конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений.  Пример: сканирование при помощи сканера nmap |
|  | Тактическая задача: нарушитель стремится получить любую техническую информацию, которая может оказаться полезной в ходе реализации угроз безопасности информации | Т1.2. Сбор информации о пользователях, устройствах, приложениях, а также сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений путем поиска и эксплуатации уязвимостей подключенных к сети устройств.  Пример: эксплуатация уязвимости типа directory traversal публично доступного веб-сервера |
|  |  | Т1.3. Сбор информации о пользователях, устройствах, приложениях, авторизуемых сервисами вычислительной сети, путем перебора.  Пример: сбор информации о почтовых адресах при помощи directoryharvestattack на почтовые сервера |
|  |  | Т1.4. Сбор информации, предоставляемой DNS сервисами, включая DNS Hijacking |
|  |  | Т1.5. Сбор информации о пользователе при посещении им веб-сайта, в том числе с использованием уязвимостей программы браузера и надстраиваемых модулей браузера |
|  |  | Т1.6. Сбор информации через получение контроля над личными устройствами сотрудников (смартфонами, планшетами, ноутбуками) для скрытой прослушки и видеофиксации |
|  |  | Т1.7. Поиск и покупка баз данных идентификационной информации, скомпрометированых паролей и ключей на специализированных нелегальных площадках |
|  |  | Т1.8. Техники конкурентной разведки и промышленного шпионажа для сбора информации о технологическом процессе, технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах |
|  |  | Примечание 1: Сбор информации может выполняться с использованием одной или более из перечисленных выше техник, пока нарушитель не получит достаточно информации для реализации другой тактики в продолжении атаки |
| **Т2** | Получение первоначального доступа к компонентам систем и сетей | Т2.1. Использование внешних сервисов организации в сетях публичного доступа (Интернет)  Примеры: 1) доступ к веб-серверу, расположенному в сети организации; 2) доступ к интерфейсу электронной почты OutlookWebAccess (OWA) почтового сервера организации |
|  | Тактическая задача: нарушитель, находясь вне инфраструктуры сети или системы, стремится получить доступ к | Т2.2. Эксплуатация уязвимостей сетевого оборудования и средств защиты вычислительных сетей для получения доступа к компонентам систем и сетей при удаленной атаке.  Пример: обход межсетевого экрана путем эксплуатации уязвимостей реализации правил фильтрации |
|  | любому узлу в инфраструктуре и использовать его как плацдарм для дальнейших действий | Т2.3. Использование ошибок конфигурации сетевого оборудования и средств защиты, в том числе слабых паролей и паролей по умолчанию, для получения доступа к компонентам систем и сетей при удаленной атаке |
|  |  | Т2.4. Эксплуатация уязвимостей компонентов систем и сетей при удаленной или локальной атаке.  Примеры: 1) эксплуатация уязвимостей веб-сервера с целью выполнения произвольного кода в контексте этого сервера; 2) эксплуатация уязвимостей операционной системы устройства человеко-машинного интерфейса автоматизированной системы управления с целью внедрения средств получения вводимых на этом устройстве паролей доступа; 3) эксплуатация уязвимостей браузера вредоносными скриптами при посещении пользователем вредоносного или скомпрометированного веб-сайта |
|  |  | Т2.5. Использование недокументированных возможностей программного обеспечения сервисов, приложений, оборудования, включая использование отладочных интерфейсов, программных, программно-аппаратных закладок |
|  |  | Т2.6. Использование методов социальной инженерии, в том числе фишинга, для получения прав доступа к компонентам системы |
| **Т3** | Внедрение и исполнение вредоносного программного обеспечения в системах и сетях | Т3.1. Автоматический запуск скриптов и исполняемых файлов в системе с использованием пользовательских или системных учетных данных, в том числе с использованием методов социальной инженерии |
|  | Тактическая задача: получив доступ к узлу сети или системы, нарушитель стремится внедрить в его | Т3.2. Активация и выполнение вредоносного кода, внедренного в виде закладок в легитимное программное и программное-аппаратное обеспечение систем и сетей |
|  | программную среду инструментальные средства, необходимые ему для дальнейших действий | Т3.3. Автоматическая загрузка вредоносного кода с удаленного сайта или ресурса с последующим запуском на выполнение |
|  |  | Т3.4. Копирование и запуск скриптов и исполняемых файлов через средства удаленного управления операционной системой и сервисами |
|  |  | Т3.5. Эксплуатация уязвимостей типа удаленное исполнение программного кода (RCE, Remotecodeexecution) |
|  |  | Т3.6. Автоматическое создание вредоносных скриптов при помощи доступного инструментария от имени пользователя в системе с использованием его учетных данных |
|  |  | Т3.7. Подмена файлов легитимных программ и библиотек непосредственно в системе. Примечание 3: В том числе может сочетаться с техникой компрометации сертификата, используемого для цифровой подписи образа ПО |

Таблица 6

|  |  |  |
| --- | --- | --- |
| **УБИ №008. Угроза восстановления и/или повторного использования аутентификационной информации** | | |
| **Т1** | Сбор информации о системах и сетях | Т1.1. Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций |
|  | Тактическая задача: нарушитель стремится получить любую техническую информацию, которая может оказаться полезной в ходе реализации угроз безопасности информации | Т1.2. Сбор информации о пользователях, устройствах, приложениях, авторизуемых сервисами вычислительной сети, путем перебора.  Пример: сбор информации о почтовых адресах при помощи directoryharvestattack на почтовые сервера |
|  |  | Т1.3. Сбор информации о пользователе при посещении им веб-сайта, в том числе с использованием уязвимостей программы браузера и надстраиваемых модулей браузера |
|  |  | Т1.4. Сбор информации о пользователях, устройствах, приложениях путем поиска информации в памяти, файлах, каталогах, базах данных, прошивках устройств, репозиториях исходных кодов ПО, включая поиск паролей в исходном и хэшированном виде, криптографических ключей.  Пример: получение хэшей паролей из /etc/passwd или получение паролей по умолчанию путем обратного инжиниринга прошивки устройства |
|  |  | Т1.5. Сбор личной идентификационной информации (идентификаторы пользователей, устройств, информация об идентификации пользователей сервисами, приложениями, средствами удаленного доступа), в том числе сбор украденных личных данных сотрудников и подрядчиков на случай, если сотрудники/подрядчики используют одни и те же пароли на работе и за ее пределами |
|  |  | Т1.6. Сбор информации через получение контроля над личными устройствами сотрудников (смартфонами, планшетами, ноутбуками) для скрытой прослушки и видеофиксации |
|  |  | Т1.7. Поиск и покупка баз данных идентификационной информации, скомпрометированых паролей и ключей на специализированных нелегальных площадках |
|  |  | Т1.8. Техники конкурентной разведки и промышленного шпионажа для сбора информации о технологическом процессе, технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах |
|  |  | Примечание 1: Сбор информации может выполняться с использованием одной или более из перечисленных выше техник, пока нарушитель не получит достаточно информации для реализации другой тактики в продолжении атаки |

Таблица 7

|  |  |  |
| --- | --- | --- |
| **УБИ №012. Угроза деструктивного изменения конфигурации/среды окружения программ** | | |
| **Т1** | Сбор информации о системах и сетях | Т1.1. Направленное сканирование при помощи специализированного программного обеспечения подключенных к сети устройств с целью идентификации сетевых сервисов, типов и версий программного обеспечения этих сервисов, а также с целью получения конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений.  Пример: сканирование при помощи сканера nmap |
|  | Тактическая задача: нарушитель стремится получить любую техническую информацию, которая может оказаться полезной в ходе реализации угроз безопасности информации | Т1.2. Сбор информации о пользователях, устройствах, приложениях, а также сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений путем поиска и эксплуатации уязвимостей подключенных к сети устройств.  Пример: эксплуатация уязвимости типа directory traversal публично доступного веб-сервера |
|  |  | Т1.6. Сбор информации о пользователях, устройствах, приложениях, авторизуемых сервисами вычислительной сети, путем перебора.  Пример: сбор информации о почтовых адресах при помощи directoryharvestattack на почтовые сервера |
|  |  | Т1.7. Сбор информации, предоставляемой DNS сервисами, включая DNS Hijacking |
|  |  | Т1.3. Сбор информации о пользователе при посещении им веб-сайта, в том числе с использованием уязвимостей программы браузера и надстраиваемых модулей браузера |
|  |  | Т1.4. Сбор информации через получение контроля над личными устройствами сотрудников (смартфонами, планшетами, ноутбуками) для скрытой прослушки и видеофиксации |
|  |  | Т1.5. Поиск и покупка баз данных идентификационной информации, скомпрометированых паролей и ключей на специализированных нелегальных площадках |
|  |  | Т1.20. Техники конкурентной разведки и промышленного шпионажа для сбора информации о технологическом процессе, технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах |
|  |  | Примечание 1: Сбор информации может выполняться с использованием одной или более из перечисленных выше техник, пока нарушитель не получит достаточно информации для реализации другой тактики в продолжении атаки |
| **Т2** | Получение первоначального доступа к компонентам систем и сетей | Т2.1. Использование внешних сервисов организации в сетях публичного доступа (Интернет)  Примеры: 1) доступ к веб-серверу, расположенному в сети организации; 2) доступ к интерфейсу электронной почты OutlookWebAccess (OWA) почтового сервера организации |
|  | Тактическая задача: нарушитель, находясь вне инфраструктуры сети или системы, стремится получить доступ к | Т2.2. Эксплуатация уязвимостей сетевого оборудования и средств защиты вычислительных сетей для получения доступа к компонентам систем и сетей при удаленной атаке.  Пример: обход межсетевого экрана путем эксплуатации уязвимостей реализации правил фильтрации |
|  | любому узлу в инфраструктуре и использовать его как плацдарм для дальнейших действий | Т2.3. Использование ошибок конфигурации сетевого оборудования и средств защиты, в том числе слабых паролей и паролей по умолчанию, для получения доступа к компонентам систем и сетей при удаленной атаке |
|  |  | Т2.4. Эксплуатация уязвимостей компонентов систем и сетей при удаленной или локальной атаке.  Примеры: 1) эксплуатация уязвимостей веб-сервера с целью выполнения произвольного кода в контексте этого сервера; 2) эксплуатация уязвимостей операционной системы устройства человеко-машинного интерфейса автоматизированной системы управления с целью внедрения средств получения вводимых на этом устройстве паролей доступа; 3) эксплуатация уязвимостей браузера вредоносными скриптами при посещении пользователем вредоносного или скомпрометированного веб-сайта |
|  |  | Т2.5. Использование недокументированных возможностей программного обеспечения сервисов, приложений, оборудования, включая использование отладочных интерфейсов, программных, программно-аппаратных закладок |
|  |  | Т2.6. Использование методов социальной инженерии, в том числе фишинга, для получения прав доступа к компонентам системы |
| **Т3** | Внедрение и исполнение вредоносного программного обеспечения в системах и сетях | Т3.1. Автоматический запуск скриптов и исполняемых файлов в системе с использованием пользовательских или системных учетных данных, в том числе с использованием методов социальной инженерии |
|  | Тактическая задача: получив доступ к узлу сети или системы, нарушитель стремится внедрить в его | Т3.2. Активация и выполнение вредоносного кода, внедренного в виде закладок в легитимное программное и программное-аппаратное обеспечение систем и сетей |
|  | программную среду инструментальные средства, необходимые ему для деструктивного изменения конфигурации/среды окружения программ | Т3.3. Автоматическая загрузка вредоносного кода с удаленного сайта или ресурса с последующим запуском на выполнение |
|  |  | Т3.4. Копирование и запуск скриптов и исполняемых файлов через средства удаленного управления операционной системой и сервисами |
|  |  | Т3.5. Эксплуатация уязвимостей типа удаленное исполнение программного кода (RCE, Remotecodeexecution) |
|  |  | Т3.6. Автоматическое создание вредоносных скриптов при помощи доступного инструментария от имени пользователя в системе с использованием его учетных данных |
|  |  | Т3.7. Подмена файлов легитимных программ и библиотек непосредственно в системе. Примечание 3: В том числе может сочетаться с техникой компрометации сертификата, используемого для цифровой подписи образа ПО |

**Методика оценки рисков нарушения информационной безопасности**

Исходные данные

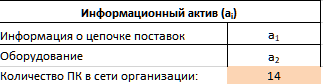


Рисунок 1 – Исходные данные

Исходные данные включают в себя следующую информацию

* Информация о цепочке поставок
* Оборудование(все программы, циклы, цепочки производства)
* Количество компьютеров

Средства защиты



Рисунок 2 – Средства защиты

Таблица описывает средства защиты, используемые компанией.

Экономические показатели

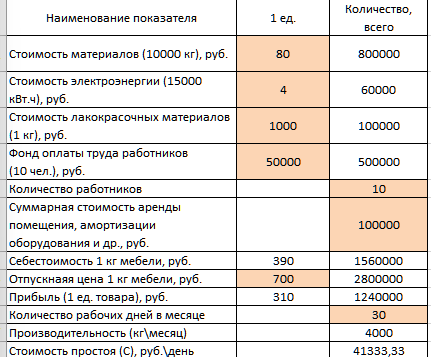


Рисунок 3 – Экономические показатели

В таблице представлена стоимость компонентов продукта, себестоимость и отпускная цена продукта, а также информация о количестве рабочих дней и производительности предприятия.

Вероятность реализации угрозы

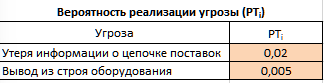


Рисунок 4 – Вероятность реализации угрозы

Данная таблица содержит информацию и возможных угрозах и вероятность их реализации.

Время восстановления актива

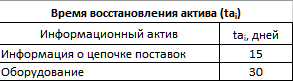


Рисунок 5 – Время восстановления актива

Время восстановления актива – t(a) – показывает, как долго процесс будет простаивать до возобновления (пока не восстановят вторичный актив, который его (процесс) обеспечивает). Если повредятся или потеряются программы и само оборудование, то восстановление может занять до 30 дней. Из-за потери информации о цепочке поставок(кража/удаление) можно застопорить работу до 15 дней.

Стоимость восстановления актива

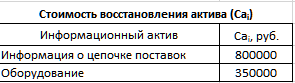


Рисунок 6 – Стоимость восстановления актива

Стоимость восстановления — C(a) – показывает, сколько потребуется денег, чтобы восстановить актив.

В данной таблице представлен коэффициент, фонд оплаты и число программистов. Эти данные используются для вычисления суммы, которая будет затрачена на восстановление технической документации и коммерческой информации.

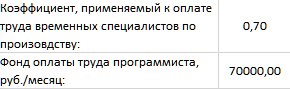


Рисунок 7 – Информация о средствах восстановления

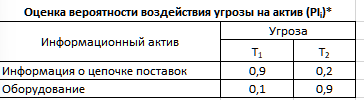


Рисунок 8 – Оценка вероятности воздействия угрозы на актив

Значения PI при угрозе T1 означают, что если T1 (Передача инсайдером информации конкурентам) произойдет, то в одном случае из 10 будет создана угроза для оборудования.

Стоимость последствий

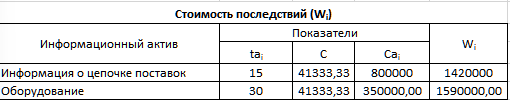


Рисунок 9 – Стоимость последствий

Стоимость последствий – W – вычисляется как время восстановления актива умножить на стоимость простоя плюс стоимость восстановления актива.

Значения рисков

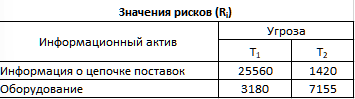


Рисунок 10 – Значения рисков

Значения рисков вычисляются следующим образом: вероятность реализации угрозы умножить на вероятность воздействия угрозы и умножить на стоимость последствий.

Расчет вероятности воздействия угрозы хотя бы на 1 из активов

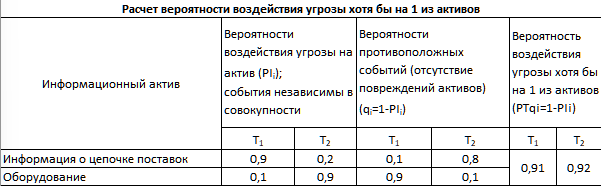


Рисунок 11 – Расчет вероятности воздействия угрозы хотя бы на 1 из активов

В данной таблице происходит расчёт вероятности воздействия угрозы на хотя бы один из активов. Вероятность воздействия оказалась не менее 0.919.

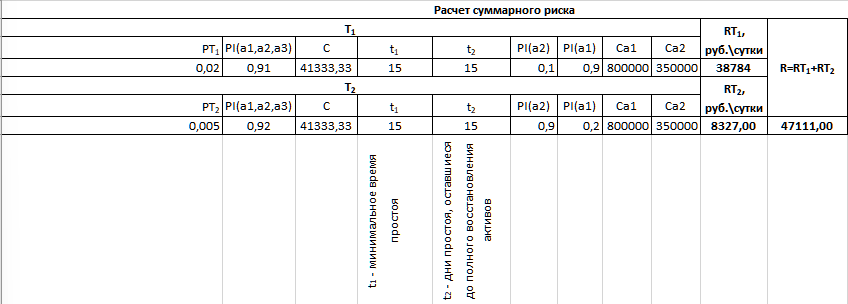


Рисунок 12 – Средства защиты

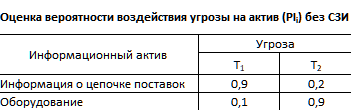


Рисунок 13 – Оценка вероятности воздействия угрозы на актив без СЗИ

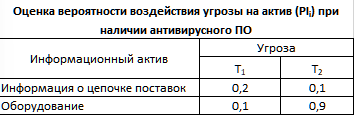


Рисунок 14 – Оценка вероятности воздействия угрозы на актив при наличии антивирусного ПО

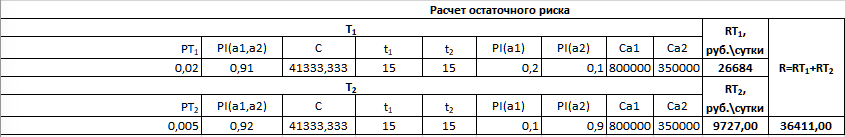


Рисунок 15 – Расчёт остаточного риска

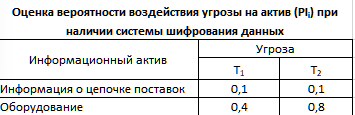


Рисунок 16 – Оценка вероятности воздействия угрозы на актив при наличии системы шифрования данных

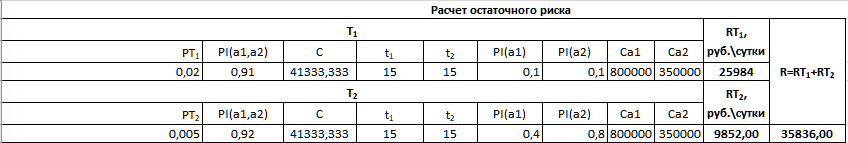


Рисунок 17 – Расчёт остаточного риска

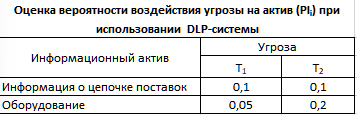


Рисунок 18 – Оценка вероятности воздействия угрозы на актив при использовании DLP-системы



Рисунок 19 – Расчёт остаточного риска

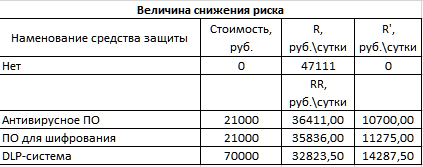


Рисунок 20 – Величина снижения риска

**R'=R–RR** – величина, на которую снизился риск (разность между риском до внедрения средства защиты и остаточным риском). Кроме того, приобретенное средство защиты, станет вторичным активом, обеспечивающим процесс защиты активов. Стоимость простоя данного процесса равна R'.

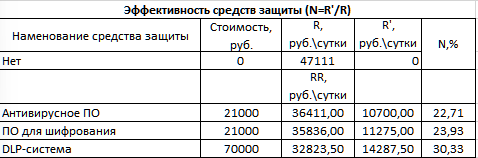


Рисунок 21 – Эффективность средств защиты

**N=R'/R** – эффективность средств защиты. Показатель позволяет определить, какое из средств защиты будет наиболее эффективным для защиты активов.

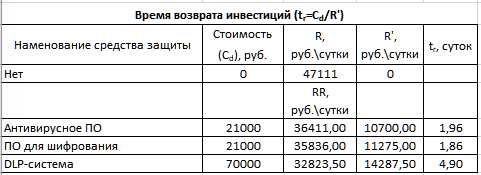


Рисунок 22 – Время возврата инвестиций

Приведенные цифры показывают через какое время (в данном случае в сутках) средство защиты окупится и начнет приносить прибыль.

Заключение: Проанализировав получившиеся стоимость, эффективность и время возврата инвестиций за каждое средство защиты, был сделан вывод, что рациональнее всего выбрать антивирусное ПО и DLP-систему, потому что у них более высокая эффективность и меньшее время возврата инвестиций, нежели чем у ПО для шифрования.

**Защита информации**

Компания Оператор связи Кузбасса

Уровень защищенности ИСПДн – 3.

Класс защищенности автоматизированной системы управления – 3.

Приказы ФСТЭК - №21, №239 и №31

Таблица 1 – Меры защиты информации

|  |  |  |
| --- | --- | --- |
| Условное обозначение и номер меры | Меры защиты информации | Способ реализации меры, наименование |
| ИАФ.0 | Разработка политики идентификации и аутентификации | Разработка политики идентификации и аутентификации через создание регламента, определение процедур учета, выдачи и контроля доступа, инструктаж сотрудников. |
| ИАФ.1 | Регламентация правил и процедур идентификации и аутентификации пользователей | Secret Net Studio |
| ИАФ.2 | Идентификация и аутентификация устройств |
| ИАФ.3 | Управление идентификаторами |
| ИАФ.4 | Управление средствами аутентификации |
| ИАФ.5 | Идентификация и аутентификация внешних пользователей | Континент  TLS |
| ИАФ.7 | Защита аутентификационной информации при передаче | Secret Net Studio |
| УПД.0 | Регламентация правил и процедур управления доступом | Регламентация управления доступом через разработку документации, физическое разграничение, учет доступа и обучение сотрудников. |
| УПД.1 | Управление учетными записями пользователей | Secret Net Studio |
| УПД.2 | Реализация модели управления доступом |
| УПД.3 | Доверенная загрузка |
| УПД.4 | Разделение полномочий (ролей) пользователей |
| УПД.5 | Назначение минимально необходимых прав и привилегий |
| УПД.6 | Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему |
| УПД.10 | Блокирование сеанса доступа пользователя при неактивности |
| УПД.11 | Управление действиями пользователей до идентификации и аутентификации |
| УПД.13 | Реализация защищенного удаленного доступа | Континент 4 |
| УПД.14 | Контроль доступа из внешних информационных (автоматизированных) систем | CL DATAPK,  Определение порядка предоставления доступа авторизованными (уполномоченным) пользователями из внешних информационных систем |
| ОПС.0 | Регламентация правил и процедур ограничения программной среды | Разработка инструкций по ограничению доступа, регламентация использования ресурсов, обучение сотрудников, аудит и контроль соблюдения политики безопасности. |
| ОПС.2 | Управление установкой (инсталляцией) компонентов программного обеспечения | CL DATAPK |
| ЗНИ.0 | Регламентация правил и процедур защиты машинных носителей информации | Разработка инструкций по хранению, транспортировке и утилизации носителей, обучение сотрудников, регулярный аудит, контроль доступа и защиты информации. |
| ЗНИ.1 | Учет машинных носителей информации | Secret Net Studio |
| ЗНИ.2 | Управление физическим доступом к машинным носителям информации | InfoWatch Endpoint Security |
| ЗНИ.5 | Контроль использования интерфейсов ввода (вывода) информации на съемные машинные носители информации | Secret Net Studio |
| ЗНИ.7 | Контроль подключения съемных машинных носителей информации |
| ЗНИ.8 | Уничтожение (стирание) информации на машинных носителях информации |
| АУД.0 | Регламентация правил и процедур аудита безопасности | Разработка и внедрение процедур регулярного аудита, назначение ответственных за безопасность, проведение проверок, анализ уязвимостей, документирование результатов и принятие мер по устранению нарушений безопасности. |
| АУД.1 | Инвентаризация информационных ресурсов | CL DATAPK |
| АУД.2 | Анализ уязвимостей и их устранение |
| АУД.3 | Генерирование временных меток и (или) синхронизация системного времени | Континент 4 |
| АУД.4 | Регистрация событий безопасности | Secret Net Studio |
| АУД.6 | Защита информации о событиях безопасности |
| АУД.7 | Мониторинг безопасности |
| АУД.8 | Реагирование на сбои при регистрации событий безопасности |
| АУД.10 | Проведение внутренних аудитов |
| АВЗ.0 | Регламентация правил и процедур антивирусной защиты | Разработка инструкций по установке и обновлению антивирусного ПО, регулярное сканирование систем, обучение сотрудников, мониторинг угроз, контроль соблюдения стандартов безопасности и регулярные отчеты о состоянии защиты. |
| АВЗ.1 | Реализация антивирусной защиты | Secret Net Studio |
| АВЗ.2 | Антивирусная защита электронной почты и иных сервисов | InfoWatch ARMA |
| АВЗ.4 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) | Secret Net Studio |
| СОВ.0 | Регламентация правил и процедур предотвращения вторжений (компьютерных атак) | Разработка процедур мониторинга и анализа сетевого трафика, установка систем предотвращения атак, регулярное обновление ПО, обучение сотрудников, проведение тестов на проникновение и анализ инцидентов безопасности. |
| СОВ.1 | Обнаружение и предотвращение компьютерных атак | Secret Net Studio |
| СОВ.2 | Обновление базы решающих правил |
| ОЦЛ.0 | Регламентация правил и процедур обеспечения целостности | Разработка процедур контроля целостности данных, регулярная проверка и верификация файлов, использование систем контроля версий, обучение сотрудников и аудит изменений для предотвращения несанкционированных модификаций. |
| ОЦЛ.1 | Контроль целостности программного обеспечения | Secret Net Studio |
| ОЦЛ.4 | Контроль данных, вводимых в информационную (автоматизированную) систему | InfoWatch Person Monitor |
| ОЦЛ.5 | Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях |
| ОДТ.1 | Использование отказоустойчивых технических средств | Континент 4 |
| ОДТ.2 | Резервирование средств и систем |
| **ОДТ.3** | Контроль безотказного функционирования средств и систем |
| **ОДТ.4** | Резервное копирование информации | Astra Linux Special Edition РУСБ.10015-01  Резервное копирование осуществляется с использованием специальных программ и утилит, позволяющих восстанавливать информацию и объекты файловой системы с сохранением их атрибутов безопасности и аудита |
| **ОДТ.5** | Обеспечение возможности восстановления информации |
| **ОДТ.6** | Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях |
| **ЗТС.0** | Регламентация правил и процедур защиты технических средств и систем | Разработка и внедрение внутренних регламентов и политик безопасности. |
| **ЗТС.1** | Защита информации от утечки по техническим каналам | Разработка политик безопасности для контроля передачи данных, ограничение использования съемных носителей, мониторинг сетевого трафика, обучение сотрудников, внедрение систем защиты от утечек и регулярный аудит. |
| **ЗТС.2** | Организация контролируемой зоны | Физическая защита помещений с использованием систем контроля доступа (СКУД). |
| **ЗТС.3** | Управление физическим доступом | Физическая защита помещений с использованием систем контроля доступа (СКУД). |
| **ЗТС.5** | Защита от внешних воздействий | Разработка процедур защиты от внешних угроз, физическая охрана, контроль доступа, мониторинг инфраструктуры, регулярные проверки на уязвимости, обучение сотрудников и подготовка к чрезвычайным ситуациям. |
| **ЗИС.0** | Регламентация правил и процедур защиты информационной системы и ее компонентов | Разработка и утверждение политик информационной безопасности. |
| **ЗИС.2** | Защита периметра информационной системы | Организационные: Разработка и внедрение системы контроля доступа (СКУД), ограничение физического доступа, установка видеонаблюдения, мониторинг доступа, регулярный аудит и обучение персонала по безопасности периметра.  Технические: Secret Net Studio |
| **ЗИС.3** | Эшелонированная защита информационной системы | Организационные:  Разработка многослойных мер безопасности, включая контроль доступа, антивирусную защиту, шифрование данных, мониторинг трафика, регулярные проверки и обучение сотрудников для предотвращения угроз на всех уровнях.  Технические: InfoWatch ARMA |
| **ЗИС.4** | Сегментирование информационной системы | Континент 4 |
| **ЗИС.6** | Управление сетевыми потоками |
| **ЗИС.19** | Защита информации при ее передаче по каналам связи |
| **ЗИС.20** | Обеспечение доверенных канала, маршрута |
| **ИНЦ.0** | Регламентация правил и процедур реагирования на компьютерные инциденты | Разработка и внедрение процедур реагирования на инциденты. |
| **ИНЦ.1** | Выявление компьютерных инцидентов | Secret Net Studio |
| **ИНЦ.3** | Анализ компьютерных инцидентов |
| **ИНЦ.4** | Устранение последствий компьютерных инцидентов | Организационные:  Разработка планов реагирования на инциденты, создание команды по ликвидации последствий, регулярные тренировки, анализ инцидентов, восстановление данных, обновление систем и улучшение мер безопасности.  Технические:  InfoWatch ARMA |
| **УКФ.0** | Регламентация правил и процедур управления конфигурацией | Разработка политики управления конфигурацией информационной (автоматизированной) системы. |
| **УКФ.1** | Идентификация объектов управления конфигурацией | CL DATAPK |
| **УКФ.2** | Управление изменениями |
| **ОПО.0** | Регламентация правил и процедур управления обновлениями ПО | Разработка и утверждение политики обновления ПО. |
| **ОПО.1** | Поиск, получение обновлений ПО от доверенного источника | Континент 4 |
| **ОПО.3** | Тестирование обновлений ПО | Создание тестовой среды для проверки обновлений. Соболь 4 |
| **ОПО.4** | Установка обновлений ПО | Континент 4 |
| **ПЛН.0** | Регламентация правил и процедур планирования мероприятий по обеспечению защиты информации | Разработка и утверждение плана мероприятий по безопасности. |
| **ПЛН.1** | Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации | Регулярный пересмотр и обновление плана безопасности. |
| **ДНС.0** | Регламентация правил и процедур обеспечения действий в нештатных ситуациях | Разработка и внедрение плана действий в нештатных ситуациях. |
| **ДНС.1** | Разработка плана действий в нештатных ситуациях | Создание и утверждение плана аварийного восстановления. |
| **ДНС.2** | Обучение и отработка действий персонала в нештатных ситуациях | Проведение регулярных тренировок и учений. |
| **ИПО.0** | Регламентация правил и процедур информирования и обучения персонала | Разработка и внедрение программы обучения по безопасности. |
| **ИПО.1** | Информирование персонала об угрозах безопасности информации и о правилах безопасной работы | Проведение регулярных семинаров и рассылка информационных бюллетеней. |
| **ИПО.2** | Обучение персонала правилам безопасной работы | Организация курсов и тренингов по информационной безопасности. |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации | Secret Net Studio |
| АНЗ.4 | Контроль состава технических средств, программного обеспечения и средств защиты информации |
| АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе |

Используемые программы, зарегистрированные в реестре ФСТЭК России:

* Secret Net Studio;
* Континент TLS;
* Континент 4;
* CL DATAPK;
* InfoWatch ARMA;
* InfoWatch Person Monitor;
* Astra Linux Special Edition;
* Соболь 4.

Используемые программы, отсутствующие в реестре ФСТЭК России:

* InfoWatch Endpoint Security.

Заключение:

В ходе выполнения данной работы были рассмотрены ключевые меры защиты информации, основанные на требованиях Приказов ФСТЭК №239, №31 , №21, а также предложены конкретные способы их реализации. Основное внимание уделялось важности системного подхода к обеспечению безопасности информационных систем, который включает в себя не только технические, но и организационные меры.

Эффективная реализация предложенных мер позволит значительно повысить уровень защищенности информации, минимизировать риски утечек и инцидентов, а также обеспечить соответствие современным требованиям безопасности.