МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«МИРЭА – Российский технологический университет»

РТУ МИРЭА

Колледж программирования и кибербезопасности

Отчет о выполнении практического задания
по дисциплине «МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении»
на тему «Разработка концепции защиты автоматизированной (информационной) системы»
Практическое задание № 6
Специальность – 10.05.02 Информационная безопасность автоматизированных систем

Выполнил студент:
_____ Маркаров М. О.
Группа: ИБ-32
Руководитель:
_____ Герасин В. Ю.
Работа защищена с оценкой _____
Дата защиты _____

Москва
2024

Практическая работа № 6

Цель: составление основополагающего документа в системе информационной безопасности организации.

Введение: Для создания в информационных системах концепцию защиты необходимо иметь полноценный документ, имеющий определённую степень секретности.

Ход работы: Проведение анализа угроз модели в информационной системе.

1. Этап введение в концепции защиты автоматизированной (информационной) системы.

В результате многократных посещений различных помещений организации.

1) Первым шагом в разработке концепции является анализ существующей организационно-распорядительной документации, а также неформальных требований, отражающих текущую или желаемую политику безопасности. Это поможет выявить сильные и слабые стороны текущей системы “склада” мы выявили что требуется установить не только аппаратные средства защиты, но и программные средства защиты информации.

Защита конфиденциальности информации обеспечит то, чтобы доступ к конфиденциальным данным имели только авторизованные пользователи.

Обеспечение целостности данных гарантия того, что информация не была изменена, уничтожена или искажена несанкционированным образом.

Обеспечение доступности информации гарантия того, что информация доступна для авторизованных пользователей в любое время, когда это необходимо.

Соблюдение законодательных и нормативных требований обеспечение соответствия действующему законодательству и внутренним регламентам.

2) Основные задачи включают в себя. Оценка рисков проведение регулярных оценок рисков для выявления уязвимостей и угроз. Разработка и

внедрение политик безопасности создание и внедрение документов, регламентирующих порядок работы с информацией и действия в случае инцидентов. Обучение и повышение осведомленности сотрудников проведение тренингов и семинаров для повышения уровня осведомленности персонала о вопросах ИБ. Мониторинг системы безопасности регулярный контроль за состоянием системы ИБ и проведение аудитов для выявления недостатков и их устранения. Реагирование на инциденты разработка и реализация процедур по реагированию на инциденты безопасности, включая их расследование и устранение последствий.

3) Разработка моделей угроз в нашей информационной системе главной угрозой считаются внешние угрозы и внутренние угрозы, физические угрозы.

Внутренние угрозы это неправомерные действия сотрудников или неумышленное раскрытие конфиденциальной информации.

Внешние угрозы это кибератаки такие как взломы вирусы (DoS-атаки) социальная инженерия манипуляция людьми.

Физические угрозы это потеря или кража оборудования уничтожение или несанкционированный доступ к устройствам. К физическим угрозам также относится и природные катастрофы которые способны нанести вред инфраструктуре

4) Для определение нормативно-технической базы информационной безопасности существуют законодательные акты, например ФЗ-152 "О персональных данных", ФЗ-149 «Об информации, информационных технологиях и о защите информации», 187-ФЗ «О безопасности критической информационной инфраструктуры», ФЗ-161 «О национальной платёжной системы», ФЗ-395-1 «О банках и банковской деятельности».

5) Разработка основных положений системы управления информационной безопасностью включает в себя структура управления ИБ пределение ответственных лиц и их полномочий в области информационной безопасности, процессы управления ИБ установление процессов для оценки

рисков, мониторинга и реагирования на инциденты, обучение и осведомленность.

6) Чтобы реализовать определение требований к комплексу мер и средств обеспечения информационной безопасности.

Технические меры обеспечивают использование средств антивирусной защиты и межсетевых экранов. Шифрование данных для защиты конфиденциальной информации.

Организационные меры позволяют разрабатывать и внедрять регламенты по обработке и хранению информации. Наличие процедур по реагированию на инциденты и их расследованию.

Мониторинг и аудит необходим мониторинг системы безопасности и проведение аудитов для оценки ее эффективности применятся для обнаружения и предотвращения вторжений.

1.2 Подготовительный этап составление основополагающего документа в системе информационной безопасности организации.

Для разработки карты информационной системы организации и обеспечения информационной безопасности с использованием матричных графов, необходимо следовать нескольким этапам. Ниже приведен подробный план действий, который включает в себя описание сетевой инфраструктуры, функциональных обязанностей пользователей, маршрутов доступа к электронным документам и применение математических алгоритмов.

Составление карты информационной системы

Сетевые устройства применяемые в самой организации.

Маршрутизаторы обеспечивают связь между различными сетями и маршрутизацию трафика.

Коммутаторы соединяют устройства в локальной сети и управляют трафиком на уровне канального уровня.

Брандмауэры защищают сеть от внешних угроз, фильтруя входящий и исходящий трафик.

ПЭВМ и их подключения.

ПЭВМ A1 (Рабочая станция отдела продаж).

IP-адрес: 192.168.1.10

Подключение порт 1 на коммутаторе Switch1.

Функции работа с CRM-системой, обработка заказов.

Круг лиц сотрудники отдела продаж.

ПЭВМ B2 (Сервер базы данных).

IP-адрес: 192.168.1.20

Подключение порт 2 на коммутаторе Switch1.

Функции такие как хранение и управление данными клиентов.

Круг лиц являются администраторы базы данных.

ПЭВМ C3 (Рабочая станция отдела бухгалтерии)

IP-адрес: 192.168.1.30

Подключение порт 3 на коммутаторе Switch2.

Функции ведение бухгалтерского учета, работа с финансовыми документами.

Круг лиц это сотрудники бухгалтерии.

Функциональные обязанности пользователей.

Отдел продаж обработка заказов, работа с клиентами, обновление базы клиентов.

Отдел бухгалтерии ведение учета, подготовка отчетности, работа с финансовыми документами.

Администраторы базы данных управление данными, обеспечение их целостности и доступности.

Описание маршрутов доступа и прав.

Маршрут движения и права доступа к электронным документам.

Доступ к базе данных.

Отдел продаж имеет доступ только к информации о клиентах и заказах.

Отдел бухгалтерии имеет доступ к финансовым документам и отчетам.

Администраторы базы данных полный доступ ко всем данным, включая конфиденциальную информацию.

Маршрут доступа.

Сотрудник отдела продаж запрашивает доступ к CRM через ПЭВМ А1.

Запрос передается через маршрутизатор к серверу базы данных (ПЭВМ В2).

Сервер проверяет права доступа и возвращает необходимую информацию.

Анализ состояния системы и разработка математических алгоритмов

Алгоритм проверки доступа.

Для проверки, имеет ли пользователь доступ к ресурсу, можно использовать умножение матриц. Если результат произведения матрицы доступа на вектор прав доступа (где 1 — доступен, 0 — недоступен) дает 1, то доступ разрешен.

Анализ угроз и динамическая модель

Типы угроз внешние (кибератаки) и внутренние (ошибки сотрудников).

Объект угрозы сервер базы данных (ПЭВМ В2) как основной объект хранения конфиденциальной информации.

Методы устранения угроз.

Внедрение системы мониторинга и обнаружения вторжений.

Регулярное обновление программного обеспечения и патчей.

Применение теории графов для анализа потоков информации

Графы и потоки информации использование ориентированных графов для представления потоков информации между пользователями и ресурсами.

Контроль состояния системы матричная форма полномочий позволяет отслеживать изменения в доступе и реагировать на инциденты.

1.3 Примерная математическая модель

Основные математические концепции ИБ включают:

Обеспечение защиты информации хащита конфиденциальных данных от несанкционированного доступа и утечек.

Оптимизация затрат на ИБ выбор наиучшего сочетания средств защиты при ограничнных ресурсах.

Повышение доверия клиентов Создание надежной системы защиты информации, что способствует увеличению клиентской базы и доходов компании.

Увеличение продуктивности сотрудников Ограничение доступа к неслужебной информации, что позволяет сосредоточиться на выполнении рабочих задач.

Математическая модель

Для достижения поставленных целей необходимо использовать методы математического моделирования. Основные компоненты модели включают:

Множество информационных угроз (ИУ) определение всех возможных угроз, которые могут возникнуть в автоматизированной информационной системе (АИС) организации.

Множество средств защиты (СЗ) перечень аппаратных и программных средств, которые могут быть использованы для нейтрализации угроз.

Эффективность нейтрализации для каждого сочетания ИУ и СЗ определяется коэффициент эффективности r(i,j), отражающий, насколько эффективно средство защиты может нейтрализовать угрозу.

Оптимизация задача оптимизации заключается в выборе такого набора средств защиты, который максимизирует эффективность нейтрализации угроз при ограничениях на объем затрат (Q) и минимизации затрат при заданном уровне эффективности (P). Для этого используется двудольный граф, где одна группа вершин соответствует средствам защиты, а другая — информационным угрозам. Каждой вершине присваивается вес, равный стоимости средства защиты, что позволяет формализовать задачу выбора оптимальной СИБ.

Вероятность причинения ущерба важным аспектом концепции является оценка вероятности причинения вреда АИС при НСД. Это достигается путем моделирования последовательности защитных преград, которые злоумышленник должен преодолеть. Вероятность успешного преодоления всех преград зависит от времени между изменениями параметров системы защиты и времени, необходимого для их преодоления. Рассматриваются различные варианты распределения времени, что позволяет более точно оценить риски.

2 Введение в концепцию системы управление складом.

В процессе развития информационных технологий организация по системы управления складом представляет собой комплексное решение, предназначенное для оптимизации процессов хранения, обработки и распределения товаров на складе. В условиях современного бизнеса, где скорость и эффективность логистики играют ключевую роль, внедрение эффективной системы управления складом становится необходимостью для достижения конкурентных преимуществ. Но в большинстве случаев в таких информационных системах существуют нарушители который несут характер либо навредить с целью нарушения работы либо с целью кражи данных.

Система управления складом представляет собой набор процессов и технологий, направленных на оптимизацию хранения, обработки и распределения товаров. Основные функции СУС включают управление запасами, обработка заказов, отслеживание товаров, аналитика и отчетность.

В условиях современного бизнеса, где конкуренция и требования клиентов постоянно растут, эффективное управление складом и безопасность информационных ресурсов становятся критически важными аспектами успешной деятельности компании. Система управления складом обеспечивает оптимизацию логистических процессов, в то время как система безопасности информационных ресурсов защищает данные и инфраструктуру от киберугроз. Взаимодействие этих систем позволяет повысить общую эффективность и безопасность бизнеса.

3. Общие положения.

Настоящая 'Концепция обеспечения безопасности информации в автоматизированной системе управлении складом

Настоящая концепция для организации управления складом основывается на следующих нормативных актах:

1. ФЗ-152 "О персональных данных".

2. ФЗ-149 «Об информации, информационных технологиях и о защите информации».

3. 187-ФЗ «О безопасности критической информационной инфраструктуры».

Организация управления складом должна учитывать современное состояние информационных систем и технологий. Она должна распространяться на все объекты, связанные со складом, такие как товары, поставщики, клиенты и процессы обработки заказов. Концепция будет являться методологической основой для разработки и внедрения автоматизированных систем управления складом, которые позволят повысить эффективность работы склада, оптимизировать использование складских площадей и улучшить обслуживание клиентов.

Организация управление складом обеспечивает распределение перевозку и хранение различных инструментов или оборудований. Ключенвая опора на защиту лежит между обеспечением противостоянию несанкционированных доступов и обеспечение противодействие от физического несанкционированного доступа.

4. Объекты защиты.

Основными объектами информационной безопасности в организации управлении складом.

Основными объектами информационной безопасности в организации управления складом являются:

1. Информационные ресурсы:

- Данные о запасах и складских операциях.

- Информация о клиентах и поставщиках.

- Данные о логистике и транспортировке.

- Финансовая информация и отчетность.

- Другие виды информации, важные для функционирования склада.

2. Процессы обработки информации в АС:

- Ввод, хранение и обработка данных о запасах.

- Автоматизированные процессы управления складом.

- Обмен данными между различными системами и подразделениями.

- Программное обеспечение, используемое для управления складом.

- Другие процессы, связанные с обработкой информации в АС.

3. Информационная инфраструктура:

- Серверы и рабочие станции.

- Сетевые устройства и коммуникационные каналы.

- Системы хранения данных и архивирования.

- Программное обеспечение, обеспечивающее функционирование АС.

-Другие компоненты информационной инфраструктуры, обеспечивающие безопасность и надежность АС.

Эти объекты информационной безопасности являются активами организации, и их защита имеет решающее значение для обеспечения бесперебойной работы склада и сохранения конфиденциальности данных.

I. Назначение, цели создания и эксплуатация АС как объекта информатизации.

Эта автоматизирована система нужна для моделирования процессов в организации, а также способы многопоточного определения угроз у организации управлении складом.

II. Структура, состав и размещение основных элементов АИС, информационные связи с другими объектами.

Демонстрация планирования АИС в виде блок схемы показана на (Рис. 1).

Рисунок 1 Планирования АИС

Демонстрация аппаратной реализации АИС показана на (Рис. 2).

Рисунок 2 Аппаратная реализации АИС

Описание связи

Пользователи взаимодействуют с АИС через Интерфейс пользователя.

Интерфейс пользователя получает и отображает данные из Базы данных.

Модули обработки, анализа и отчетности работают с данными из базы данных, обмениваясь информацией между собой.

АИС может взаимодействовать с внешними системами для обмена данными (получение информации или отправка отчетов).

ПО которое используется в системе управления складом (WMS), обеспечивающая учет и контроль товарных запасов.

Базы данных для хранения информации о товарах, поставщиках и клиентах.

Локальная сеть (LAN) для соединения всех элементов системы.

Маршрутизаторы и коммутаторы для обеспечения связи между различными компонентами.

III. Категории информационных ресурсов, подлежащих защите.

Уровни конфиденциальности информационные ресурсы в автоматизированной системе (АС) управления складом могут иметь различные уровни конфиденциальности, которые определяются в зависимости от характера информации и ее важности для организации. Основные уровни конфиденциальности включают:

Открытая информация доступна для всех сотрудников и может быть распространена без ограничений. Например, информация о наличии товаров на складе.

Внутренняя информация доступна только для сотрудников организации и не подлежит раскрытию третьим лицам. Это может включать внутренние отчеты, планы по управлению запасами.

Конфиденциальная информация доступ к которой ограничен определенной группой сотрудников. Это может быть информация о поставщиках, контрактах, ценах и других коммерческих данных.

Секретная информация: Наиболее чувствительная информация, доступ к которой имеют только уполномоченные лица. Например, данные о финансовых показателях, стратегические планы и персональные данные сотрудников.

Типы документов, циркулирующих в документообороте АИС в документообороте АС управления складом могут циркулировать различные

типы документов, среди которых Приемные документов акты приемки товаров, накладные, товарные чеки. Отгрузочные документы: Накладные на отгрузку, документы, подтверждающие доставку. Учетные документы инвентаризационные ведомости, отчеты о движении товаров. Договорные документы контракты с поставщиками и клиентами, соглашения о сотрудничестве. Финансовые документы счета-фактуры, акты выполненных работ, платежные поручения. Внутренние отчеты отчеты по эффективности работы склада, анализ запасов.

Информация, подлежащая защите: Информация, подлежащая защите в АС управления складом, включает:

Персональные данные сотрудников ФИО, адреса, контактные данные, данные о заработной плате.

Коммерческая информация цены на товары, условия поставок, данные о клиентах и контрагентах.

Финансовая информация бухгалтерская отчетность, данные о доходах и расходах.

Техническая информация данные о программном обеспечении, конфигурации системы, пароли и ключи доступа.

Стратегическая информация: Планы по развитию бизнеса, результаты маркетинговых исследований, конкурентные стратегии.

Нормативные документы, регулирующие защиту информации: Защита информации в АС управления складом осуществляется на основании ряда нормативных документов, включая:

Федеральный закон "О персональных данных" от 27 июля 2006 г. № 152-ФЗ: Регулирует обработку и защиту персональных данных, устанавливает требования к их защите и права субъектов данных.

Приказы и постановления Минкомсвязи России: Нормативные акты, устанавливающие требования к защите информации в информационных системах.

Уровни конфиденциальности

Конфиденциальность информации может быть разделена на несколько уровней:

Общедоступная информация не требует специальных мер защиты. Может быть свободно распространена и доступна любому желающему. Примеры: законодательные акты, общие сведения о компании.

Внутренняя информация информация, предназначенная для использования исключительно внутренними пользователями. Доступ к ней ограничивается, и она не должна быть доступна третьим лицам. Примеры: внутренние инструкции, отчеты.

Конфиденциальная информация данные, доступ к которым ограничен и которые могут нанести ущерб, если будут раскрыты. Данный уровень требует установления строгих мер безопасности. Примеры: финансовые отчеты, документы с персональными данными сотрудников.

Секретная информация информация, раскрытие которой может вызвать серьезные последствия для безопасности государства или организации. Необходим строгий контроль доступа и специальная защита. Примеры: государственные тайны, уникальные разработки.

Уровни конфиденциальности

Конфиденциальность информации может быть разделена на несколько уровней:

Общедоступная информация не требует специальных мер защиты. Может быть свободно распространена и доступна любому желающему. Примеры: законодательные акты, общие сведения о компании.

Внутренняя информация информация, предназначенная для использования исключительно внутренними пользователями. Доступ к ней ограничивается и она не должна быть доступна третьим лицам. Примеры: внутренние инструкции, отчеты.

Конфиденциальная информация данные, доступ к которым ограничен и которые могут нанести ущерб, если будут раскрыты. Данный уровень требует установления строгих мер безопасности.

Примеры финансовые отчеты, документы с персональными данными сотрудников.

Секретная информация информация, раскрытие которой может вызвать серьезные последствия для безопасности государства или организации. Необходим строгий контроль доступа и специальная защита. Примеры государственные тайны, уникальные разработки.

Категорирование критичности информационного ресурса http://portal.gersen.ru Авиасейлс (Aviasales) Репетиционный ущерб критический ресурс:трата ресурса приводит к серьезному репутационному ущербу, который может привести к потере доверия клиентов, партнеров и инвесторов. Критический ресурс в случае потери или утраты ресурса может привести к частичному прекращению деятельности компании. Финансовые потери могут привести к утрате критических ресурсов что приводит к значительным финансовым истощениям, которые могут поставить под угрозу компанию. Правовые последствия критический ресурс утрата ресурса может привести к серьезным правовым последствиям, штрафам, уголовной ответственности. Важный ресурс утрата ресурса может привести к незначительным правовым последствиям, например, административным штрафам В итоге информационные ресурс категорируется по экономической значимости исходя из правовых последствий

IV. Категории пользователей АС, режимы использования и уровни доступа к информации.

Пользователи АС, режимы использования и уровни доступа к информации

I. Пользователи автоматизированной системы (АС)

1. Администраторы серверов
2. Файловые серверы
3. Серверы приложений
4. Серверы баз данных
5. Администраторы локальной вычислительно

6. Режимы использования
7. Оперативный режим

Основные функции обработка заказов, управление запасами, выполнение инвентаризации.

Аналитический режим

Основные функции анализ данных, составление отчетов, планирование.

Административный режим

Основные функции настройка системы, управление пользователями, обеспечение безопасности.

Уровни доступа к информации

Полный доступ

Пользователи администраторы серверов, администраторы информационной безопасности, руководство.

Возможности полный контроль над системами, настройка прав доступа, управление данными.

Ограниченный доступ

Пользователи операторы складов, менеджеры по логистике, финансовые аналитики.

Возможности доступ к необходимым данным для выполнения своих функций, создание и редактирование записей, но без возможности изменения системных настроек.

Только чтение Пользователи Финансовые аналитики (в некоторых случаях), руководство.

Возможности доступ к отчетам и аналитическим данным, но без возможности редактирования.

V. Уязвимость основных компонентов АС.

Каналы несанкционированного получения информации.

У организации так же есть канал несанкционированного получения информации такой как параметрические (троянские программы и шпионское ПО). Виброакустические — сигналы, возникающие посредством

преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации защищаемых помещений. В организации имеются электрически технический канал утечки информации при её передаче по каналам связи могут использоваться sql-иньекции, xss-атаки. Электромагнитные — копирование полей путём снятия индуктивных наводок. Информационные электромагнитные излучения, а именно размещение ОТСС.

Социальная инженерия может быть применена злоумышленн иком, который будет воздействоват ь на сотрудника после окончания рабочего дня на эмоции с целью получения необходимой информации.

Фишинг с помощью спама или таргетированной рекламы злоумышленники рассылают свои поддельные сообщения большому числу людей. Они могут использовать базы данных с контактами.

Администраторы ошибки в настройках системы или недостаточная проверка прав доступа могут привести к серьезным уязвимостям. отсутствие регулярного мониторинга и аудита систем безопасности может оставить уязвимости незамеченными.

5. Цели и задачи.

I. Интересы затрагиваемых при эксплуатации АС субъектов информационных отношений.

Субъектами правоотношений при использовании АИС организации и обеспечении безопасности информации являются Организация как собственник информационных ресурсов подразделения и отделы, должностные лица и сотрудники, юридические лица, физические лица

Организация как собственник информационных ресурсов конфиденциальность заинтересована в защите своих коммерческих тайн, интеллектуальной собственности и личных данных клиентов от несанкционированного доступа Достоверность необходим контроль за точностью и актуальностью информации для принятия обоснованных управленческих решений. Своевременный доступ организация стремится

обеспечить оперативный доступ к информации для сотрудников, что способствует эффективному выполнению задач и повышению производительности. Разграничение ответственности важно четко определить роли и обязанности сотрудников в отношении обработки и защиты информации, чтобы избежать путаницы и ошибок. Контроль необходимость мониторинга доступа и использования информации для выявления потенциальных угроз безопасности и обеспечения соблюдения внутренних норм и правил.

Подразделения и отделы конфиденциальность заинтересованы в защите информации, относящейся к их специфическим задачам и проектам, от внешних и внутренних угроз. Достоверность необходимость получения точной информации для выполнения своих функций и достижения целей подразделения. Своевременный доступ подразделения нуждаются в быстром доступе к данным для оперативного выполнения задач и принятия решений. Разграничение ответственности важно, чтобы каждый сотрудник понимал свою роль и ответственность в обработке информации, что помогает минимизировать риски.

Должностные лица и сотрудники достоверность необходимость работы с актуальной и точной информацией для выполнения своих обязанностей. Своевременный доступ сотрудники должны иметь доступ к нужной информации в нужный момент, чтобы эффективно выполнять свои задачи. Разграничение ответственности четкое понимание обязанностей помогает избежать конфликтов и повышает эффективность работы.

Юридические лица своевременный доступ юридические лица нуждаются в оперативном доступе к информации для своевременного реагирования на изменения в законодательстве и рыночной среде. Разграничение ответственности четкое распределение обязанностей между юридическими лицами и их представителями для минимизации правовых рисков. Контроль наличие механизмов контроля за соблюдением правовых норм и внутренней политики в области безопасности информации.

Физические лица конфиденциальность защита личных данных и информации о себе от несанкционированного доступа. Своевременный доступ: необходимость получения информации в удобное время для принятия обоснованных решений. Разграничение ответственности понимание своих прав и обязанностей в отношении предоставления информации организации. Контроль заинтересованы в наличии механизмов контроля за использованием их личных данных организацией.

II. Цели защиты.

Основной целью защиты в контексте автоматизированных информационных систем управлением склада (АИС) является обеспечение безопасности субъектов информационных отношений, чьи интересы могут быть затронуты в процессе создания и функционирования этих систем. Эта защита направлена на предотвращение возможного ущерба, который может быть причинён как случайным, так и преднамеренным несанкционированным вмешательством в работу АИС или доступом к информации, циркулирующей в системе, с её последующим незаконным использованием.

Для достижения данной цели необходимо обеспечить и поддерживать следующие ключевые свойства информации и автоматизированной системы её обработки:

Доступность информация должна быть доступна уполномоченным пользователям в любое время, когда это необходимо для выполнения их задач. Это включает в себя защиту от сбоев системы, атак и других факторов, которые могут ограничить доступ к информации.

Сохранность информация должна быть защищена от потери или повреждения. Это включает в себя механизмы резервного копирования, восстановление данных и защиту от физического ущерба, а также защиту от угроз, таких как вирусы и вредоносные программы.

Целостность информация должна оставаться неизменной и точной в процессе её хранения и передачи. Это включает в себя защиту от

несанкционированных изменений, а также механизмов проверки целостности данных, чтобы гарантировать их достоверность.

Аутентичность необходимо удостовериться, что информация и её источники являются подлинными. Это включает в себя механизмы аутентификации пользователей и проверку подлинности данных, чтобы предотвратить мошенничество и подделку информации.

III. Основные задачи системы обеспечения безопасности информации.

Чтобы достичь основной цели защиты субъектов информационных отношений и обеспечения безопасности автоматизированных информационных систем (АИС) необходимо решить ряд ключевых задач. Вот примерный список задач, которые должна решать система обеспечения безопасности информации:

Защита от вмешательства в процесс функционирования АС обеспечение устойчивости системы к внешним и внутренним угрозам, включая кибератаки, физическое вмешательство и другие виды воздействия, которые могут нарушить нормальное функционирование АС.

Разграничение прав доступа к информации, ПЭВМ и средствам защиты установка четких правил и политик доступа, позволяющих ограничить доступ к информации и ресурсам только для авторизованных пользователей, что минимизирует риск несанкционированного доступа.

Регистрация (иницианирование происходящих событий в АИС). Ведение журналов событий, которые фиксируют действия пользователей и системные события. Это позволяет отслеживать и анализировать действия в системе для выявления потенциальных угроз и инцидентов.

Процедуры обеспечения целостности (мониторинг) и достоверности информации внедрение механизмов проверки целостности данных, таких как контрольные суммы и хеширование, а также процедуры для подтверждения подлинности и актуальности информации.

Методы восстановления информации (бэкапы) разработка и внедрение планов и процедур восстановления данных после инцидентов, включая резервное копирование и восстановление системы после сбоя или атаки.

Защита от несанкционированных действий реализация мер по предотвращению несанкционированного доступа и действий, включая использование межсетевых экранов, систем предотвращения вторжений и других средств защиты.

Авторизация и аутентификация пользователей обеспечение надежных механизмов аутентификации для проверки идентичности пользователей и авторизации их действий в системе, что помогает предотвратить доступ неавторизованных лиц.

Мониторинг возможных угроз и информационной защищенности постоянный мониторинг состояния системы безопасности, выявление и анализ потенциальных угроз, а также оценка уровня защищенности информации.

Действия для минимизации и локализации ущерба от неправомерных действий разработка и внедрение мер по быстрому реагированию на инциденты, включая локализацию ущерба, восстановление нормального функционирования системы и минимизацию последствий для организации и её пользователей.

IV. Основные пути достижения целей защиты (решения задач системы защиты).

Чтобы достичь желаемой безопасности в организации управлении складом и способов защиты необходимо установить межсетевые экраны, Linux Astra, использовать DLP систему обеспечить постоянное обновление межсетевых экранов от обнаружения уязвимостей, передачи данных и создать серверную инфраструктуру мониторинга процессов далее стоит обеспечить конфиденциальность, а именно программную защиту которая обеспечит конкретную защиту от программных средств кражи информации.

6. Основные угрозы.

В данном разделе угрозы безопасности информации, которые могут возникнуть в процессе управления складом. Это касается как защиты информации, так и обеспечения бесперебойной работы всех процессов, связанных с хранением и обработкой товаров.

Виды угроз информационной безопасности в организации управлении складом

Нарушение конфиденциальности это утечка информации, которая может произойти в результате умышленных или случайных действий. Она может быть связана с разглашением коммерческой тайны или личных данных клиентов.

Нарушение работоспособности это дезорганизация работы системы, что может произойти в результате саботажа, вирусных атак или ошибок в программном обеспечении. Среди последствий замедление работы системы, невозможность выполнения операций и т.д.

Основные угрозы

Непреднамеренные источники ошибки и случайные действия сотрудников, например, при вводе данных или использовании программного обеспечения.

Умышленные действия третьих лиц, направленные на получение выгоды или нанесение ущерба организации.

Внешние воздействия атаки из других логических и физических сегментов автоматизированной системы.

Ошибки проектирования

Проблемы возникшие на этапе разработки и внедрения автоматизированной системы, которые могут привести к сбоям в работе.

Стихийные бедствия а именно аварии и другие непредвиденные ситуации, которые могут повлечь за собой повреждение инфраструктуры или информацию.

Непреднамеренные угрозы и меры по их нейтрализации

Изучим, как минимизировать риски, возникающие из-за случайных ошибок или халатности сотрудников.

Обучение и повышение осведомленности сотрудников о правилах обращения с данными, требованиях безопасности.

Внедрение контрольных механик, позволяющих отслеживать действия пользователей и реагировать на несанкционированные попытки доступа или ошибочные операции.

Преднамеренные угрозы и пути их реализации

Важно рассмотреть, как потенциальные злоумышленники могут осуществить свои цели.

Выработка стратегий предотвращения доступа к критическим системам и информациям для неавторизованных сотрудников.

Установление строгих протоколов по доступу и использованию информации, а также регулярные аудиты и мониторинг действий сотрудников.

Утечка информации через технические каналы

Обсудим возможные векторы утечки информации через технические системы:

Использование оборудования, которое может быть подвержено электромагнитным излучениям, представляющим угрозу для информации.

Защита от перехвата информации через акустические или визуальные сигналы.

Неформальная модель нарушителя

Различные группы нарушителей могут угрожать безопасности информации.

Неправомерные действия могут исходить как от текущих, так и от бывших сотрудников, а также от внешних лиц.

7. Основные положения технической политики в обеспечении безопасности информации в организации управлении складом.

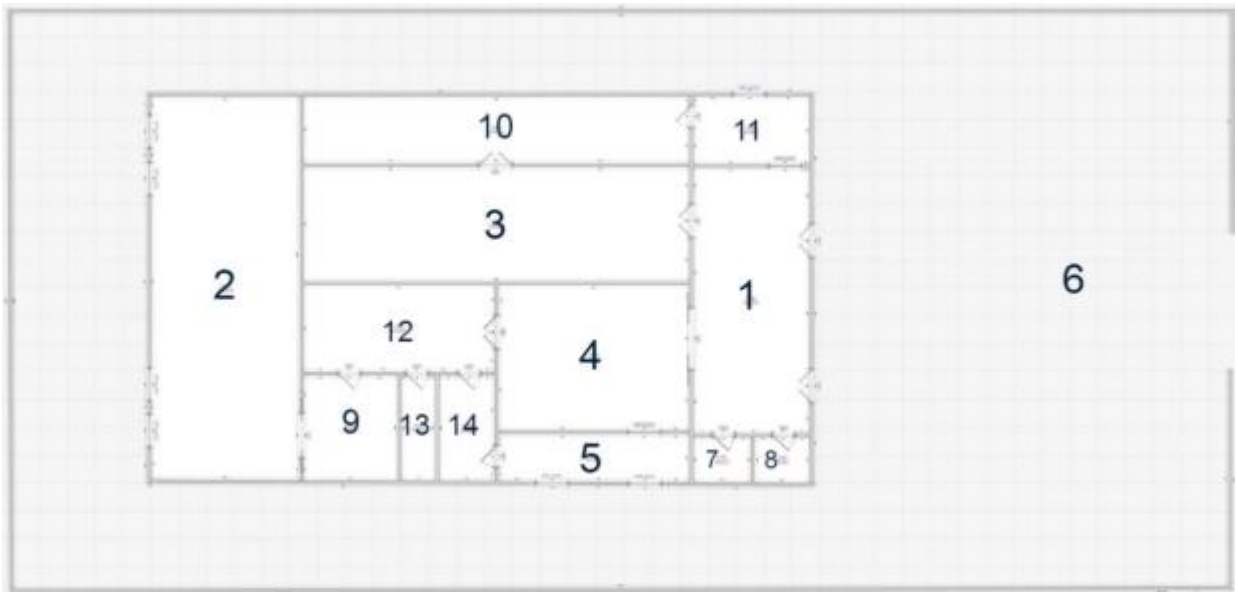

Рисунок 3 Схема здания организации управлением склада

Таблица 1 Наименование помещений здания организации управлением склада

Номер помещения	Название и уровень контроля помещения
1	Входное помещение в здание организации имеет средний уровень контроля содержит камеры мо

Таблица 1 (продолжение) Наименование помещений здания организации управлением склада

Номер помещения	Название и уровень контроля помещения
2	Склад по периметру помещения расставлены камеры и ведётся активное проверка систем пожаротушения, охрана и связи
3	Коридор отдыха персонала имеет камеры для контроля безопасности сотрудников
4	Помещение с пожарной сигнализации камерами видео наблюдениями а так же с турникетами.
5	Кабинка охраны для индикации сотрудников перед входом в организацию на
6	Склад ограждён забором по периметру здания расположены камеры. Также имеется на самой задней части склада охрана от скрытого проникновения
7	Мужской туалет не имеет никаких средств мониторинга
8	Женский туалет не имеет никаких средств мониторинга
9	Помещение для индикации сотрудников для доступа к складу может содержать доступ только через ключ карты

Таблица 1 (продолжение) Наименование помещений здания организации управлением склада

Номер помещения	Название и уровень контроля помещения
10	Столовая имеет средний контроль доступа так как содержит камеры.
11	Гардеробная имеет камеры от проникновения либо от кражи имущества сотрудников
12	Комната разработчиков имеет сетевые оборудования коммутаторы, маршрутизаторы (роутеры) имеет высокий уровень контроля от утечки материально вещественной информации
13	Комната с серверами могут получить доступ те сотрудники который имеют уникальные цифровые ключи для доступа
14	База данных имеет аналогичный метод защиты от НСД как в 13-ом помещеннии оно отличается лишь только тем что постоянно мониторится активные процессы от утечки по электромагнитному каналу утечки.

Цели технической политики.

Определять принципы и подходы к принятию решения о затратах на ремонты и замену оборудования.

Обеспечить достижение рентабельности бизнеса техническими мероприятиями.

Определять показатели эффективности в области загрузки, отгрузки и замене хранения оборудования, а также целевые значения показателей. Обозначить ответственность за достижение значений показателей;

Разработать набор мероприятий, направленных на реализацию принципов и подходов технологической эффективности производства.

Расчет показателей наработки на отказ, последствий отказа.

1) рамках указанных направлений она будет осуществляться

Основные направления технической политики в организации управления складом могут включать следующие аспекты:

Автоматизация процессов:

Внедрение систем управления складом (WMS) использование специализированного программного обеспечения для автоматизации учета товаров, управления запасами, обработки заказов и оптимизации процессов.

Использование сканеров и мобильных устройств: Для отслеживания перемещений товаров на складе, получения информации о наличии и состоянии запасов в режиме реального времени.

Оптимизация пространства:

Рациональное размещение товаров анализ и переоснащение складских площадок для более эффективного использования пространства с учетом частоты обращения товаров.

Управление запасами

Система прогнозирования спроса применение аналитических инструментов для определения оптимального уровня запасов и избежания перенасыщения или дефицита.

Мониторинг сроков годности: Для товаров с ограниченным сроком хранения необходимо вести учет и управлять изменениями в запасах.

Технологии отслеживания и идентификации:

RFID и штрих-коды: Использование технологий для упрощения и ускорения учета товаров, повышения точности данных и минимизации ошибок.

Интеграция с ERP-системами объединение данных о складе с другими бизнес-процессами для обеспечения единой информационной среды что демонстрируется в таблице 2 (продожение) в помещении номер 14.

Обучение персонала

Программы повышения квалификации: Регулярные тренинги и курсы для сотрудников, чтобы повысить их компетенции в работе с новыми технологиями и процессами.

Мотивация к улучшениям: Создание системы поощрений за инициативу и внедрение эффективных решений.

2) Для того чтобы разграничить доступ пользователей к информационным ресурсам мы будим использовать DLP систему которая позволит обмениваться данными между компьютерами безопасно, быстро и мониторить что подгружается в логере загрузок после завершения процесса запуска инсталерра.

3) Все средства для обработки хранились бы на сервере а база данных которая бы могла хранить большое количество информации должна быть в сервере и быть всегда включена для того чтобы база данных могла внести нового о пользователе в базу данных.

Регистрация действий пользователей

4**)** Регистрация действий пользователей логирование действий пользователей включают защиту от Dos, DDoS атак от злоумышленников необходимо вести журналы (логи) всех действий пользователей в системе имеется помещение где осуществляется это таблица 1 (продолжение) номер помещения 12. Это включает в себя входы и выходы, доступ к файлам, изменения настроек и другие взаимодействия. Логи помогают отслеживать активность и выявлять подозрительные действия э.

Аутентификация и авторизация использование многофакторной аутентификации повышает уровень безопасности доступа к ресурсам. Необходимо также правильно настраивать права доступа, чтобы пользователи

имели доступ только к тем ресурсам, которые им действительно нужны за несанкционированным доступом и действиями пользователей

Определение инцидентов безопасности необходимо разработать процедуры для определения и реагирования на инциденты безопасности. Это включает в себя анализ и документирование инцидентов, чтобы улучшить защиту в будущем.

5) Надежное хранение традиционных и машинных носителей информации.

Традиционные носители информации

Хранение на бумаге используется архивные материалы для хранения документов используйте специальную архивную бумагу и папки, которые защищают от света и влаги.

Условия хранения храните документы в темном, сухом и холодном месте, вдали от источников света и влаги.

Флэш-накопители и внешние диски регулярное резервное копирование создавайте резервные копии на нескольких устройствах и в облачных сервисах.

Защита от перегрева из таблицы 1 (продолжение) помещение 13 предназначена для хранения носителей в местах с высоким температурным режимом.

Машинные носители информации жесткие диски и SSD защита от сбоев: используйте RAID-массивы для повышения надежности хранения. Регулярные проверки проводятся тестирование разработчиками о состояния дисков и заменяйте их при необходимости. Облачные технологии шифрование данных используется шифрование для защиты информации при хранении и передаче в облаке. Выбор надежного провайдера облачные сервисы с хорошей репутацией по безопасности данных.

6) Криптографическое преобразование информации, обрабатываемой и передаваемой средствами вычислительной техники и связи.

Весь ассортимент склада храниться и проверяется что он в наличии в базе данных, а для постоянного хранения и мониторинга используется сервер где выходящие данные для просмотра шифруется от несанкционированного доступа к базе данных и к складу управления.

7) необходимое резервирование технических средств и информационных ресурсов.

Постоянное резервное копирования базы данных, отчётах документов инвентаризационных описей, журналы учета прихода и расхода, технические инструкции и руководства пользователя.

8) Электрическая развязка цепей питания.

Основная цель обеспечить защиту оборудования и пользователей от потенциально опасных условий, таких как короткие замыкания, перегрузки и электромагнитные помехи.

Разделение цепей питания помогает предотвратить электрические удары и повреждения оборудования. Это особенно важно в местах с высокой концентрацией людей и оборудования.

Надежность работы: Разделение цепей позволяет избежать влияния помех от одного устройства на работу другого. Например, если одно устройство выходит из строя, это не должно влиять на работу других устройств в системе.

Снижение риска повреждений электрическая развязка может защитить чувствительное оборудование (например, системы автоматизации склада) от перенапряжений и других электрических аномалий.

Методы электрической развязки.

В зависимости от требований и условий эксплуатации, можно использовать различные методы электрической развязки:

Трансформаторы используются для разделения низковольтных и высоковольтных цепей, а также для снижения уровня помех.

Оптоизоляторы позволяют передавать сигналы между цепями при полной электрической изоляции, что особенно полезно в системах управления и мониторинга.

Реле и контакторы: Применяются для управления цепями питания и могут обеспечить физическую изоляцию между различными цепями.

Фильтры используются для снижения уровня электромагнитных помех и обеспечения чистоты сигналов.

Применение на складе.

На складе электрическая развязка может быть реализована в следующих аспектах:

Системы освещения разделение цепей освещения от цепей питания для оборудования, чтобы избежать влияния помех.

Системы управления использование оптоизоляторов в системах автоматизации для защиты контроллеров от высоковольтных сигналов.

Электропитание оборудования разделение цепей питания для различных типов оборудования (например, погрузчиков, конвейеров, систем учета) для повышения надежности и безопасности.

8. Принципы построения комплексной системы защиты.

a) Законность в организации управления складом.

Организация, занимающиеся управлением складом, обязаны соблюдать ряд законодательных актов, касающихся защиты информации и технологиях, а также саму информацию. К ним могут относиться Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 23.11.2024) Об информации, информационных технологиях и о защите информации, Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (последняя редакция).

b) Системность в организации управления складом.

Система защиты информации представляет собой комплекс взаимосвязанных элементов, направленных на обеспечение конфиденциальности, целостности и доступности данных.

Технические средства оборудование и программное обеспечение, используемое для защиты информации (например, межсетевые экраны, системы шифрования, антивирусные программы).

Учет изменений при системности.

Системный подход также подразумевает учет изменений во времени:

Технологические изменения появление новых угроз и уязвимостей требует регулярного обновления технических средств и пересмотра политик безопасности.

c) Комплекс мероприятий по контролю в процессе осуществления системности.

Мониторинг системы регулярный контроль за функционированием автоматизированных систем (АС) и систем защиты информации.

Аудиты безопасности проведение регулярных проверок и оценок для выявления уязвимостей и недостатков в системе безопасности.

Комплексность в организации управления складом.

Эшелонированная защита при проектировании непрерывной защиты

Эшелонированная (многоуровневая) защита подразумевает использование нескольких слоев безопасности, которые работают вместе для обеспечения защиты информации. Каждый уровень должен перекрывать потенциальные уязвимости, создавая тем самым более устойчивую защиту. Примеры уровней защиты могут включать:

Физическая безопасность защита серверных помещений, контроль доступа и видеонаблюдение.

Сетевая безопасность использование межсетевых экранов, систем обнаружения и предотвращения вторжений (IDS/IPS), VPN и других технологий для защиты сети.

d) Непрерывность защиты в организации управлении складом.

Непрерывность защиты подразумевает, что безопасность не является одноразовым мероприятием, а требует постоянного внимания и действий. Это включает в себя:

Мониторинг и анализ: Постоянный мониторинг системы на предмет аномалий и угроз, а также анализ инцидентов для выявления и устранения уязвимостей.

Целеполагание в непрерывности защиты.

Целеполагание в контексте непрерывной защиты подразумевает установление четких целей и задач для обеспечения безопасности, таких как:

Снижение рисков определение допустимого уровня риска и разработка мер по его снижению.

Соответствие стандартам обеспечение соответствия требованиям законодательства, стандартам и лучшим практикам в области безопасности.

Устойчивость к инцидентам разработка планов реагирования на инциденты и обеспечение возможности восстановления после атак или сбоев

е) Своевременность в организации управлении складом.

Анализ угроз регулярная оценка потенциальных угроз и уязвимостей, связанных с информационными системами, используемыми для управления складом.

Оценка рисков определение вероятности возникновения инцидентов и их потенциальных последствий для бизнеса.

Преемственность и совершенствование в организации управлении складом.

Преемственность и совершенствование в организации управления складом действительно предполагают упреждающий характер мер для обеспечения безопасности информации.

Преемственность в управлении в организации управлении складом.

Непрерывность процессов обеспечение стабильности и последовательности в управлении складом, включая передачу знаний и опыта между сотрудниками, что способствует лучшему пониманию вопросов безопасности информации.

Документирование процессов создание и поддержание актуальных документов и инструкций по безопасности, что позволяет новым сотрудникам быстро ориентироваться в существующих мерах и процедурах.

Совершенствование мер безопасности

Анализ и адаптация регулярный анализ текущих мер безопасности и их эффективности. Это включает в себя оценку новых угроз и уязвимостей, а также адаптацию существующих политик и процедур.

Внедрение инноваций использование новых технологий и методов для повышения уровня безопасности, таких как автоматизация процессов, внедрение систем управления доступом и использование современных средств защиты данных.

f) Разумная достаточность в организации управлении складом.

ценка ценности информационных ресурсов.

Идентификация критически важных данных определение, какие информационные ресурсы являются наиболее ценными для бизнеса и требуют повышенного уровня защиты (например, данные о клиентах, финансовая информация, интеллектуальная собственность).

Классификация информации разделение информации на категории в зависимости от ее важности и чувствительности, что позволяет установить приоритеты в обеспечении безопасности.

Оценка возможного ущерба.

Анализ рисков проведение регулярного анализа рисков для определения потенциальных угроз и уязвимостей, а также оценки возможных последствий инцидентов для бизнеса.

Финансовая оценка ущерба оценка возможного финансового ущерба в случае утечки или потери информации, включая прямые и косвенные последствия например, репутационные потери, штрафы.

Оптимизация затрат на безопасность.

Сбалансированный подход установление соотношения между затратами на меры безопасности и потенциальным ущербом. Это позволяет избежать

излишних затрат на защиту менее ценных данных, при этом обеспечивая надежную защиту критически важных ресурсов.

Приоритетные инвестиции направление ресурсов на те меры безопасности, которые обеспечат максимальную защиту при минимальных затратах. Это может включать автоматизацию процессов, использование облачных решений для хранения данных и внедрение эффективных систем мониторинга.

g) Персональная ответственность в организации управлении складом.

Определение ролей и обязанностей.

Четкие должностные инструкции каждому сотруднику необходимо предоставить ясные инструкции о его обязанностях в области безопасности информации. Это включает в себя понимание того, какие данные он обрабатывает и какие меры безопасности должны быть соблюдены.

Уровни доступа установление различных уровней доступа к информации в зависимости от роли сотрудника, что помогает ограничить доступ к чувствительным данным только тем, кто действительно нуждается в них для выполнения своих функций.

Обучение и осведомленность.

Регулярное обучение: Проведение тренингов и семинаров по безопасности информации для сотрудников, чтобы они осознавали важность защиты данных и знали, как действовать в случае инцидента.

Создание культуры безопасности: Формирование у сотрудников осознания их роли в обеспечении безопасности информации, что способствует более ответственному отношению к работе с данными.

Мониторинг и оценка.

Контроль выполнения обязанностей: Регулярный мониторинг соблюдения сотрудниками установленных процедур безопасности и ответственности за обработку информации.

Оценка рисков периодическая оценка уровня риска, связанного с действиями сотрудников, и корректировка обязанностей в зависимости от выявленных уязвимостей.

Ответственность за инциденты.

Прозрачность в отчетности установление четких процедур для сообщения о нарушениях безопасности и инцидентах, что позволяет быстро реагировать на потенциальные угрозы.

Последствия за нарушения определение последствий за несоблюдение правил безопасности, что подчеркивает важность ответственности каждого сотрудника

h) Принцип минимизации полномочий в организации управлении складом.

Определение необходимых полномочий.

Анализ ролей проведение анализа ролей и обязанностей сотрудников для определения, какие права доступа необходимы каждому из них для выполнения своих задач.

Классификация данных разделение данных на категории в зависимости от их чувствительности, что помогает установить, какие данные могут быть доступны определенным пользователям.

Установление уровней доступа.

Доступ по принципу предоставление доступа к информации только тем пользователям, которые действительно нуждаются в ней для выполнения своих функций, что снижает риск несанкционированного доступа.

Регулярный пересмотр прав доступа периодическая проверка и корректировка прав доступа сотрудников в зависимости от изменений в их ролях или задачах.

i) Взаимодействие и сотрудничество в организации управлении складом.

Командная работа.

Поощрение сотрудничества создание условий для совместной работы между различными подразделениями, такими как склад, логистика и отдел продаж. Это может включать в себя совместные проекты и задачи, которые требуют взаимодействия.

Обмен опытом и знаниями организация встреч и семинаров, на которых сотрудники могут делиться своими знаниями и лучшими практиками, что способствует улучшению общего уровня компетенции.

Открытая коммуникация.

Прозрачность информации обеспечение доступа к необходимой информации для всех сотрудников, что помогает избежать недопонимания и способствует более быстрому решению проблем.

Обратная связь создание каналов для обратной связи, чтобы сотрудники могли высказывать свои мнения и предложения, что способствует формированию атмосферы доверия и уважения.

j) Гибкость системы защиты в организации управлении складом.

Модульная архитектура системы.

Компоненты защиты использование модульных решений, которые могут быть легко добавлены или удалены в зависимости от изменяющихся потребностей. Например, системы видеонаблюдения, контроля доступа и сигнализации могут быть интегрированы в единую архитектуру.

Настройка функций возможность настраивать функции системы защиты в соответствии с текущими требованиями, что позволяет быстро адаптироваться к новым угрозам или изменениям в операционной среде.

k) Открытость алгоритмов и механизмов защиты в организации управлении складом.

Проверяемость систем открытость алгоритмов позволяет независимым экспертам и аудиторам проверять и анализировать систему защиты. Это способствует повышению доверия к системе и её эффективности.

Снижение зависимости от секретности если защита основывается только на секретности, это может привести к уязвимостям. Открытые алгоритмы

могут быть протестированы на устойчивость к атакам, что повышает общую безопасность.

Устойчивость к угрозам.

Безопасность через разнообразие знание алгоритмов не должно позволять злоумышленникам легко их обойти. Это достигается путем внедрения многоуровневой защиты и использования различных методов защиты, которые работают в совокупности.

Адаптация к новым угрозам открытость позволяет сообществу безопасности быстрее реагировать на новые угрозы, разрабатывать обновления и улучшения, что делает систему более устойчивой.

Простота применения в организации управлении складом средств защиты.

Автоматизация процессов использование автоматизированных решений для мониторинга и управления безопасностью может значительно снизить нагрузку на сотрудников. Например, автоматические уведомления о подозрительной активности или автоматическое обновление систем защиты.

Интеграция с существующими системами механизмы защиты должны быть интегрированы с другими системами управления складом, чтобы избежать дублирования задач и минимизировать необходимость в дополнительных действиях со стороны пользователей.

Обучение и поддержка.

Обучение сотрудников проведение регулярных тренингов и семинаров поможет пользователям лучше понять механизмы защиты и их применение. Это также повысит их уверенность в использовании системы.

Доступ к справочным материалам предоставление доступных и понятных руководств, видеоуроков и часто задаваемых вопросов (FAQ) поможет пользователям быстро находить ответы на свои вопросы.

Обратная связь от пользователей.

Сбор отзывов регулярный сбор обратной связи от пользователей о работе механизмов защиты поможет выявить проблемы и области для

улучшения. Это может быть сделано через опросы или обсуждения на рабочих встречах.

Адаптация системы на основе полученной обратной связи система может быть адаптирована для повышения удобства и эффективности.

Научная обоснованность и техническая реализуемость в организации управлении складом.

Научная обоснованность и техническая реализуемость в организации управления складом с использованием информационных технологий, технических и программных средств, а также средств и мер защиты информации являются критически важными аспектами для обеспечения эффективной и безопасной работы. Рассмотрим ключевые элементы, которые подчеркивают эти аспекты:

Научная обоснованность.

Исследования и разработки применение современных научных исследований и разработок в области информационных технологий и защиты информации позволяет создать более эффективные и адаптированные решения для управления складом.

Методологии и стандарты следование научно обоснованным методологиям и стандартам (например, ISO/IEC 27001) обеспечивает системный подход к управлению информационной безопасностью и минимизации рисков.

Техническая реализуемость.

Современные технологии использование передовых технологий (например, IoT, облачные решения, искусственный интеллект) позволяет оптимизировать процессы управления складом и повысить уровень безопасности информации.

Интеграция систем технические решения должны быть совместимы и интегрированы с существующими системами управления, что обеспечивает комплексный подход к обработке и защите данных.

Специализация и профессионализм в организации управлении складом.

Привлечение специализированных организаций.

Опыт и экспертиза специализированные компании, обладающие опытом практической работы в области защиты информации, могут предложить эффективные решения, которые учитывают специфические риски и угрозы.

Государственная лицензия наличие лицензии на оказание услуг в области безопасности информации свидетельствует о том, что организация соответствует установленным стандартам и требованиям, что повышает доверие к ее услугам.

Разработка мер защиты информации.

Анализ угроз профессиональные специалисты могут провести комплексный анализ угроз, связанных с хранением и обработкой информации на складе, и разработать соответствующие меры защиты.

Индивидуальные решения специализированные организации могут предложить индивидуальные решения, адаптированные под конкретные нужды и специфику бизнеса.

l) Обязанность контроля в организации управлении складом.

Мониторинг и наблюдение.

Использование технологий внедрение систем видеонаблюдения и других технологий мониторинга (например, датчиков движения, контроля доступа) помогает своевременно выявлять нарушения и реагировать на них.

Регулярные проверки проведение регулярных проверок и аудитов безопасности позволяет выявлять потенциальные угрозы и недостатки в системе контроля.

Обучение и информирование сотрудников.

Обучение по безопасности сотрудники должны быть обучены правилам безопасности и процедурам контроля. Это поможет им быть более внимательными к возможным нарушениям.

Информирование о последствиях объяснение сотрудникам последствий нарушения правил безопасности может служить дополнительным стимулом для их соблюдения.

Система реагирования на инциденты.

План действий при нарушениях необходимо иметь четкий план действий на случай выявления нарушений. Это включает в себя как немедленное реагирование, так и последующее расследование инцидента.

Документирование инцидентов все случаи нарушений должны быть задокументированы для анализа и предотвращения повторения подобных ситуаций в будущем.

9. Меры, методы и средства защиты.

Система организации управления складом является важным элементом логистической цепи, обеспечивающим эффективное и безопасное хранение и обработку товаров. Оптимизация процессов, применение современных технологий и постоянный контроль за качеством позволяют значительно повысить производительность и снизить затраты. Порядок взаимодействия работников с системой. Эффективное взаимодействие работников с системой управления складом требует четкого следования установленным процессам и постоянного обучения. Это не только повышает производительность, но и обеспечивает точность учета и безопасность на складе. Обучение и профессиональное развитие. Индивидуальное обучение проведение тренингов для новых сотрудников, охватывающих основы работы с WMS, правила безопасности и эффективные методы работы. Постоянное обучение регулярные курсы повышения квалификации и обновления знаний для существующих сотрудников, чтобы они были в курсе последних функций и обновлений системы. Поддержка и техническая помощь. Служба поддержки наличие команды технической поддержки, готовой помочь работникам с любыми проблемами или вопросами по использованию WMS. Доступ к базам данным регламентируется с генеральным деректором и командой разработчиков для устранения попыток навредить системе. Модернизация оборудования регламентируется с предложениями разработчиков.

Доступ к помещениям имеет только персонал для того чтобы пройти на рабочую зону им потребуется предоставить системе уникальный ключ для доступа.

Физические средства защиты.

Контроль доступа на территорию с использованием систем видеонаблюдения, охраны и систем контроля доступа (например, магнитные карты, биометрические системы). Ограничение доступа в помещения, где расположены серверы и другие критически важные системы, с использованием замков, охраны и систем сигнализации.

Технические средства защиты.

Аппаратно-программные средства: использование межсетевых экранов систем предотвращения вторжений антивирусного ПО и программного обеспечения для шифрования данных. Криптографические средства применение алгоритмов шифрования для защиты данных при передаче и хранении, использование цифровых подписей для подтверждения подлинности документов.

Идентификация и аутентификация пользователей внедрение многофакторной аутентификации (MFA) для повышения уровня безопасности доступа к системам. Использование уникальных логинов и паролей для каждого пользователя, а также регулярное обновление паролей.

Управление системой обеспечения информационной безопасности

Главные цели системы.

Защиты информации обеспечение конфиденциальности, целостности и доступности информации, хранящейся и обрабатываемой в автоматизированных системах.

Защита от несанкционированного доступа, утечек данных и кибератак.

Снижение рисков, оценка и минимизация рисков, связанных с информационной безопасностью, включая угрозы и уязвимости.

Разработка и внедрение мер по предотвращению инцидентов безопасности.

Соответствие нормативным требованиям соответствия требованиям законодательства и стандартам в области информационной безопасности. Поддержка соответствия внутренним политикам и правилам организации.

10. Первоочередные мероприятия.

Для успешного внедрения основных положений Концепции информационной безопасности необходимо осуществить ряд первоочередных мероприятий:

1) Перед тем как полностью модернизировать систему необходимо следать резервное копирование данных и обновлять операционные системы.

2) Проводить разведку OSINIT.

3) Сбрасывать и проектировать новую сетевую инфраструктуру для запутывания от (НСД).

Вывод в результате мы смогли полностью спроектировать информационную систему и научились разрабатывать концепции защиты, автоматизированной (информационной) системы.