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 «Определения уровня защищенности ИСПДн и выбор мер по обеспечению безопасности ПДн»

Вариант 11

Практическое задание № 9

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

2025

Практическое задание № 9

Цель: Определения уровня защищенности ИСПДн и выбор мер по обеспечению безопасности ПДн

Введение: Информационная система управления складом представляет собой сложный комплекс взаимосвязанных компонентов, обеспечивающих автоматизацию процессов учета товаров, контроля запасов, планирования поставок.

Задания. На основе исходных данных, предоставленных преподавателем, провести анализ ИСПДн и подготовить отчет о практической работе, содержащий:

1. Перечень ИСПДн и их основные характеристики.

2. Перечень персональных данных, обрабатываемых в ИСПДн и подлежащих защите (для каждой ИСПДн).

3. Перечень должностей сотрудников, участвующих в обработке персональных данных.

4. Схему расположения ИСПДн относительно границ КЗ – на плане этажа (здания) отметить расположение всех технических средств ИСПДн и границы КЗ.

5. Схему локальной вычислительной сети (при наличии), иллюстрирующей связи между конечными сетевыми устройствами, входящими в состав ИСПДн, коммутаторами (концентраторами), маршрутизаторами, межсетевыми экранами и т.п.

6. Схему информационных потоков в ИСПДн.

7. Перечень программных средств, используемых в процессе обработки персональных данных.

8. Информацию о местах хранения носителей персональных данных, обрабатываемых без использования средств автоматизации.

9. Результат определения уровня защищенности ИСПДн

Ход работы:

Задание 1.

1. Системы управления складом (WMS) основные функции включают управление запасами, оптимизацию размещения товаров, поддержку различных методов обработки заказов, а также интеграцию с другими системами, такими как TMS и ERP. WMS позволяет отслеживать уровень запасов в реальном времени, что способствует повышению эффективности операций и снижению затрат.

2. Системы управления транспортом (TMS) она помогает автоматизировать выбор наилучших маршрутов для доставки, отслеживать местоположение грузов, управлять затратами на транспортировку и генерировать отчеты по транспортным операциям. Интеграция TMS с WMS и ERP обеспечивает единый поток информации, что повышает общую эффективность логистических процессов.
3. ERP-системы (Enterprise Resource Planning) они обеспечивают централизованное управление данными, автоматизацию процессов от закупок до продаж и финансов, а также поддержку отчетности и аналитики. Модульная структура ERP позволяет добавлять новые функции в зависимости от потребностей бизнеса, а интеграция с другими системами (WMS, TMS, CRM) повышает уровень координации и эффективности.
4. Системы учёта товарных запасов они хранят информацию о клиентах, автоматизируют процессы продаж, анализируют клиентские данные и поддерживают обслуживание клиентов. Интеграция CRM с ERP и другими системами позволяет создать единый поток информации, что улучшает качество обслуживания и способствует увеличению продаж.
5. Системы управления отношениями с клиентами (CRM) они интегрируются с различными источниками данных, включая WMS, TMS и ERP, и позволяют анализировать производительность, создавать отчеты о продажах, запасах и транспортировке. Возможности прогнозирования и визуализации данных помогают выявлять тренды и принимать обоснованные решения для дальнейшего развития бизнеса.
6. Системы анализа и отчетности системы анализа и отчетности предназначены для сбора, анализа и визуализации данных, что помогает в принятии управленческих решений. Они интегрируются с различными источниками данных, включая WMS, TMS и ERP, и позволяют анализировать производительность, создавать отчеты о продажах, запасах и транспортировке.
7. Безопасность и защита персональных данных: обеспечение безопасности и защиты персональных данных критически важнЫЙ аспект для всех информационных систем. Это включает в себя шифрование данных, аутентификацию и авторизацию пользователей, регулярное обновление и патчинг систем для защиты от уязвимостей, а также мониторинг активности пользователей для выявления подозрительных действий.

Задача 2.

В информационной защите управления складом информация подлежит защите строго в клиентской базе данных где содержаться данные клиентских заказов и транзакций.

Задание 3.

В складской организации и логистике существует множество должностей, связанных с обработкой персональных данных. Вот перечень основных должностей сотрудников, которые могут участвовать в этом процессе:

Менеджер по логистике: Ответственен за планирование и координацию логистических операций, включая управление данными клиентов и поставщиков.

Специалист по работе с клиентами: Обрабатывает запросы клиентов, управляет их данными и обеспечивает качественное обслуживание.

Кладовщик: Участвует в учете и обработке товаров, включая данные о поставках и клиентах.

Оператор склада: Работает с системами управления складом (WMS) и может обрабатывать данные о товарных запасах и клиентах.

Специалист по учету товарных запасов: Участвует в учете и контроле запасов, включая обработку данных о движении товаров.

IT-специалист по безопасности данных: Обеспечивает защиту персональных данных и соблюдение требований безопасности в информационных системах.

Аналитик данных: Анализирует данные о клиентах и операциях, что может включать обработку персональных данных для выявления трендов и улучшения бизнес-процессов.

Задание 4.

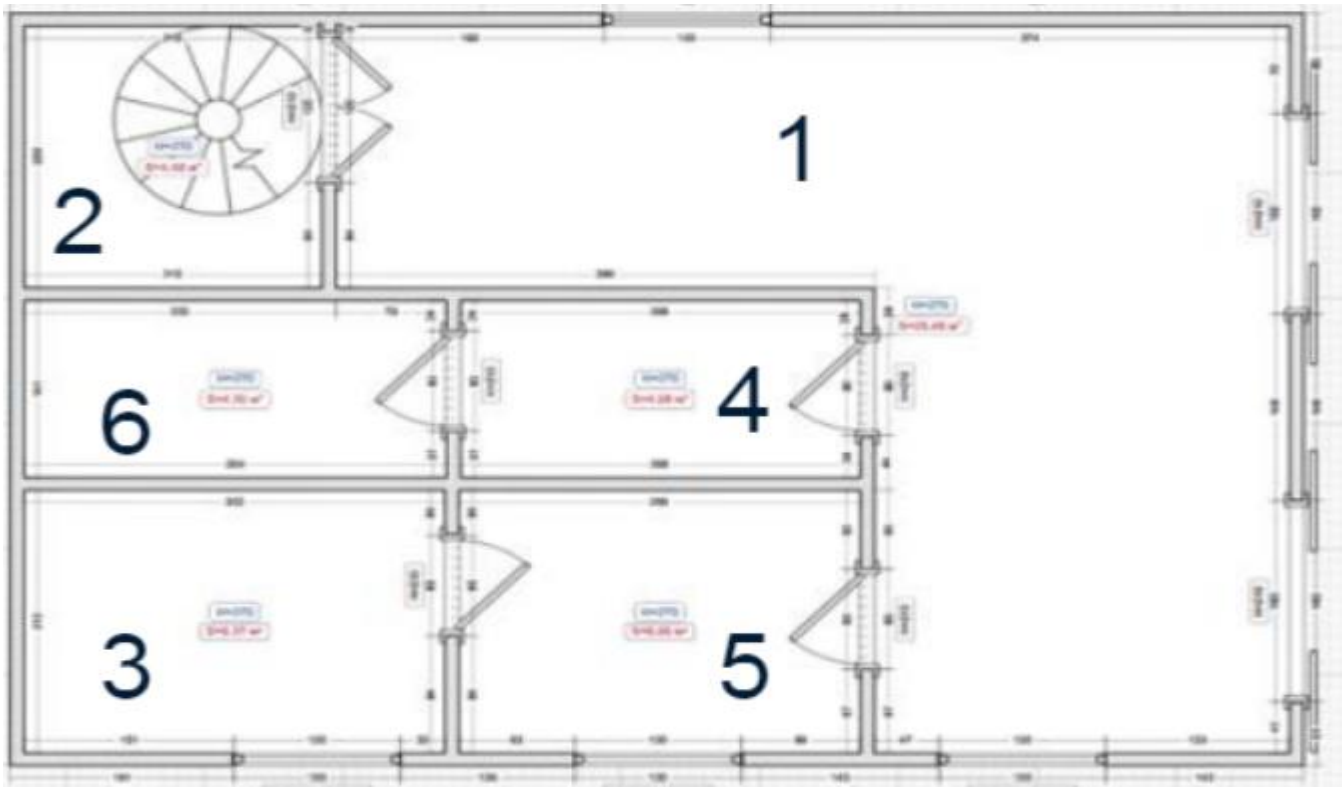


Рисунок 1 Схема здания орагнизации склада ИСПДн

В комната 3 наиболее контролируемая потому что это комната где располагается компьютер главного разработчика.

Вторая контролируемая зона — это комната 2 там, где лестница потому что там находиться коммутатор.

Задание 5.

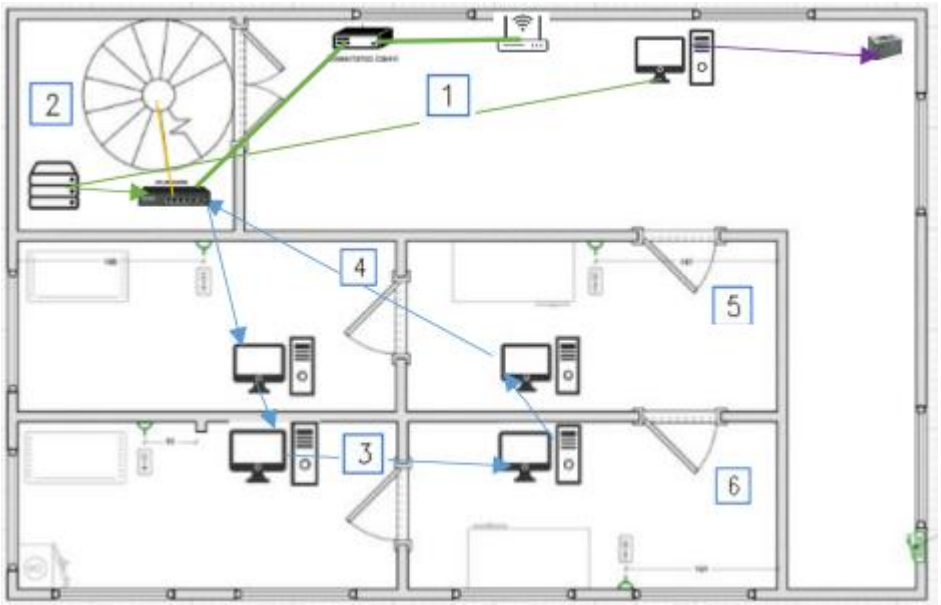


Рис. 2 Построенная локальная сеть

Схема локальной вычислительной сети демонстрируется на рис. 2 где на 1

комнате представлен роутер коммутатор и сетевой принтер. Во второй комнате имеется маршутизатор, сервер и коммутатор.

Задание 6.

Схема информационных потоков в ИСПДн

1. Поставщики

Передача данных о товарах, поставках и условиях сотрудничества.

Данные: наименование товара, количество, условия доставки, контактные данные.

2. Клиенты

Получение заказов и контактной информации.

Данные: имя, адрес, телефон, история заказов, предпочтения.

3. Системы управления складом (WMS)

Обработка данных о товарных запасах, движении товаров и отгрузках.

Данные: количество, местоположение на складе, статус запасов.

4. Системы управления транспортом (TMS)

Передача информации о маршрутах, транспортных средствах и графиках доставки.

Данные: маршруты, время доставки, информация о водителях.

5. Системы управления отношениями с клиентами (CRM)

Хранение и обработка данных о клиентах и их взаимодействиях.

Данные: история покупок, предпочтения, обратная связь.

6. Финансовые системы

Обработка платежей и финансовых данных.

Данные: счета, платежные реквизиты, история транзакций.

7. IT-отдел и службы безопасности

Обеспечение защиты и безопасности данных, контроль доступа к системам.

Данные: логины, пароли, журналы доступа.

8. Аналитические системы

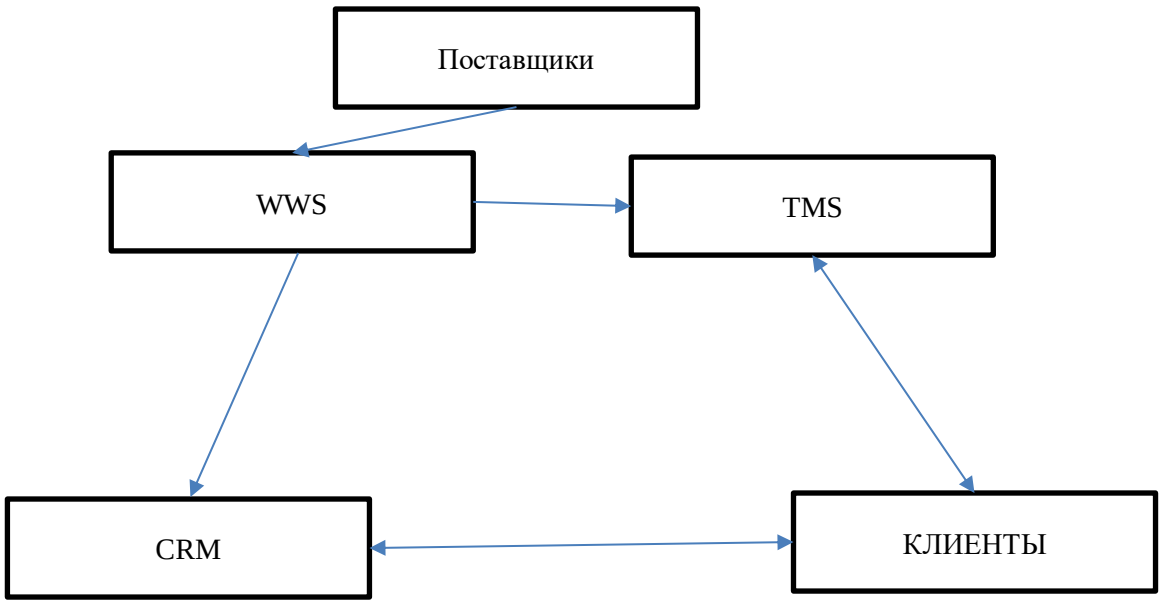
Сбор и анализ данных для принятия управленческих решений.

Данные: отчеты о продажах, анализ запасов, прогнозы.

9. Юридический отдел

Обеспечение соблюдения законодательства о защите персональных данных.

Данные: документы по комплексу, отчеты о соблюдении норм.



Потоки данных

От поставщиков к WMS: информация о поступлениях товаров.

От клиентов к CRM: данные о заказах и обратная связь.

От WMS к TMS: информация о готовности товаров к отгрузке.

От TMS к клиентам: уведомления о статусе доставки.

От WMS и CRM к аналитическим системам: данные для анализа и отчетности.

Задание 7.

Системы управления складом (WMS) SAP Extended Warehouse Management, Oracle Warehouse Management, Manhattan Associates WMS

Системы управления транспортом (TMS) SAP Transportation Management, Oracle Transportation Management, JDA Transportation Management

Системы управления отношениями с клиентами (CRM) Salesforce, Microsoft Dynamics 365, HubSpot

Финансовые системы 1С:Бухгалтерия, SAP Financials, QuickBooks

Аналитические системы Tableau, Microsoft Power BI, QlikView

Задание 8

Персональные данные часто хранятся в физических документах. Это могут быть договора с клиентами и поставщиками, накладные, отчеты о доставках и личные дела сотрудников. Эти документы обычно располагаются в офисных архивах, специализированных сейфах или шкафах, предназначенных для хранения конфиденциальной информации. Важно, чтобы доступ к таким местам был ограничен и контролировался.

Открытые данные могут храниться на электронных носителях, таких как USB-накопители, внешние жесткие диски и CD/DVD-диски. Эти носители зачастую находятся на рабочих местах сотрудников или в офисных шкафах. Для обеспечения безопасности таких устройств необходимо использовать специальные зоны для их хранения, а также следить за тем, чтобы они не находились в открытом доступе.

Задание 9.

Уровни защищенности ИСПДн в складской организации и логистике выявило ряд недостатков и уязвимостей, которые могут угрожать безопасности персональных данных. Для повышения уровня защищенности необходимо внедрять дополнительные меры, направленные на защиту информации и обучение сотрудников, что позволит минимизировать риски и обеспечить соответствие требованиям законодательства в области защиты персональных данных.

Задание построение модели угроз безопасности персональных данных

Построение модель угроз фстэк базовая модель угроз персональных данных при их обработке информации в информации в информационных системах персональных данных в складской организации.

Побочные электромагнитные излучения и наводки - электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Технический канал утечки информации носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Программное (программно-математическое) воздействие - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Методики угроз персональных данных ISO/IEC 27005, OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), FAIR (Factor Analysis of Information Risk), NIST SP 800-30, FSTEC.

1. методика основана на международном стандарте ISO/IEC 27005, который предоставляет рекомендации по управлению рисками в области информационной безопасности.

2. OCTAVE - это методика, разработанная для оценки рисков и угроз, направленная на улучшение управления безопасностью информационных систем.

3. FAIR - это методология, основанная на количественном анализе рисков, позволяющая оценить влияние угроз на бизнес.

4. Национальным институтом стандартов и технологий США (NIST), предназначена для оценки рисков в области информационных технологий.

5. ФСТЭК России, направленная на защиту персональных данных и

информации в информационных системах.

Вывод: В результате выполнения работы мы научились проектировать защиту персональных данных от несанкционированного доступа, утечек в организации склада и других угроз, что, в свою очередь, способствует повышению доверия клиентов и партнеров, а также соблюдению законодательных требований. Комплексный и системный подход к этим вопросам позволяет организациям эффективно управлять.