



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 «Построение модели угроз»**

Вариант 11

Практическое задание № 5

**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 № 5

Цель: Построение модели угроз безопасности информации в информационной системе управления складом.

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

Ход работы: Проведение анализа угроз модели в информационной системе управления складом для выявления уязвимостей в системе управления складом, для того чтобы обеспечить защиту конфиденциальной информации и предотвратить финансовые потери, связанные с утечками данных.

Задание 1. Приведите примеры каналов несанкционированного получения информации, согласно вариантам.

По виду доступа имеет удалённый характер.

По уровню доступа пользовательского уровня, административного уровня.

В информационной системе управления складом существуют такие каналы как:

1. У организации так же есть канал несанкционированного получения информации такой как параметрические (тройные программы и шпионское ПО).

2. 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-инъекции, xss-атаки.

3. Электромагнитные — копирование полей путём снятия индуктивных наводок. Информационные электромагнитные излучения, а именно размещение ОТСС с учетом $R2 < K3$ является основным каналом утечки информации.

4. Акустические — запись звука, подслушивание и прослушивание. Технические каналы несанкционированного доступа могут быть акустоэлектрические сигналы (микрофонный эффект) в него входит телефон, факс, лампы накаливания, датчики пожарной и охранной организации.

5. В информационной системе у организации есть канал утечки информации материально вещественный, а именно перехват сигналов и перехват радиосигналов.

Задание 2. Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных.

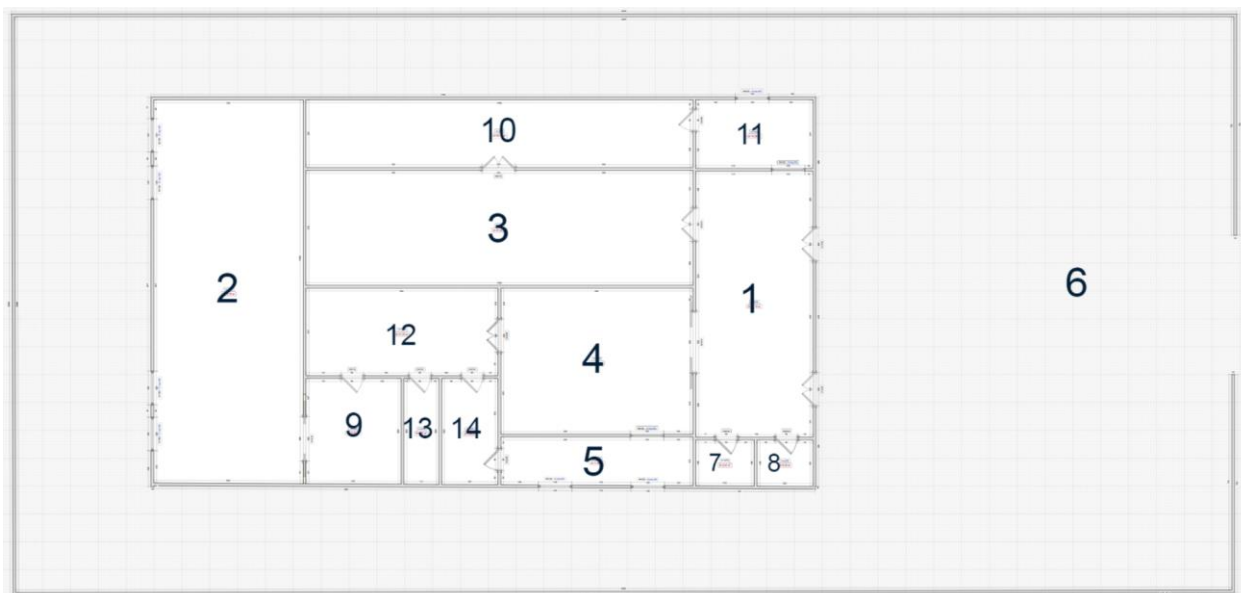


Рисунок 1 информационной системе управления складом

Таблица 1 Распределение помещений для информационной системы склада

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

Таблица 1 (Продолжение) Распределение помещений для информационной системы 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 также 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) Распределение помещений для информационной системы 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 помещении оно отличается лишь только тем что постоянно мониторится активные процессы от утечки по электромагнитному каналу утечки.

Задание 3. Проведите анализ потенциальных каналов утечки на указанном объекте. Составьте перечень каналов утечки информации на защищаемом объекте с указанием места расположения по образцу.

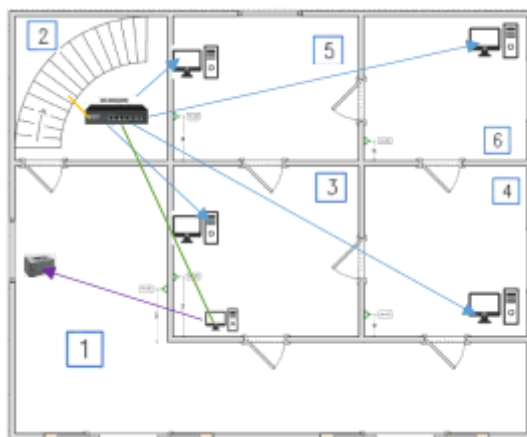


Рисунок 2 Схема здания организации Этаж 1

Таблица 2 Распределение помещений для информационной системы склада

Каналы утечки информации с объекта защиты			Место Расположения
1	Оптический канал	Окно со стороны проспекта	каб.№1
		Окно со стороны проспекта	каб.№2
		Окно со стороны проспекта	каб.№3
2	Радио электронный канал	Стоянка авто транспорта на просп.	Не имеется
		Система часофикации	Каб, 3
		Телефон	Каб. 2
		Розетки	Каб. 3, 4, 5, 6
		ПЭВМ	Каб. 3
		Воздушная линия электро передачи	Каб, 1
		Система оповещения	Каб, 1
		Система пожарной сигнализации	Расположена в каб 1, 2, 3, 4, 5, 6
3	Акустический канал	Теплопровод подземный	Расположен под каб. 1
		Водопровод подземный	Расположен под каб. 1
		Стены помещения	Гипсокартоновые
		Батареи	Каб. 1 2, 3, 4, 5, 6
		Окна контролируемого помещения	Каб. 1, 3
4	Материально-вещественный канал	Документы на бумажных носителях	Каб. 1
		Персонал предприятия	Каб. 1 3 4 6
		Производственные отходы	Расположены в каб. 1 перед входом каб. 4

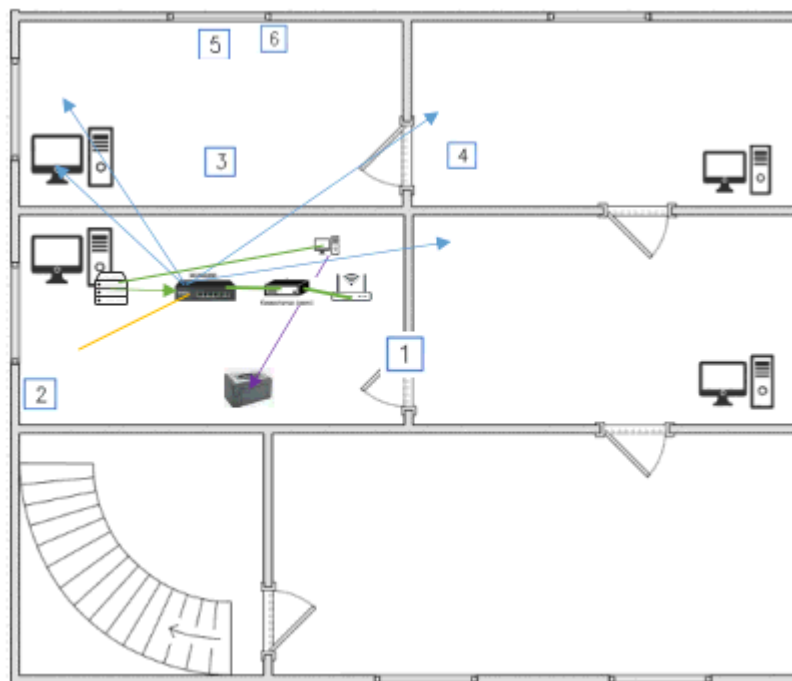


Рисунок 3 Схема здания орагнизации Этаж 2

Таблица 3 Распределение помещений для информационной системы склада

Каналы утечки информации с объекта защиты			Место Расположения
1	Оптический канал	Окно со стороны проспекта	каб.№2
		Окно со стороны проспекта	каб.№3
		Окно со стороны проспекта	каб.№4
2	Радио электронный канал	Зона 100 метров вокруг территории предприятия	
		Система часофикации	Каб. 3
		Телефон	Каб. 3
		Розетки	Располагаются во всех кабинетах кроме коридора в правых углах комнат
		ПЭВМ	Каб. 2
		Воздушная линия электро передачи	Не имеется
		Система оповещения	Каб. 1
		Система пожарной сигнализации	Расположена в коридоре, место лестницы(спуска на 1 этаж), каб 1, 2, 3, 4
3	Акустический канал	Теплопровод подземный	Расположен под коридором, который находится перед каб. 1
		Водопровод подземный	Проведён через каб. 2

Таблица 3 (продолжение) Распределение помещений для информационной системы склада

Каналы утечки информации с объекта защиты			Место Расположения
3	Акустический канал	Теплопровод подземный	Расположен под коридором, который находится перед каб. 1
		Водопровод подземный	Проведён через каб. 2
		Стены помещения	Гипсокартон
		Батареи	Расположены на выходе у каб. 1. и располагаются в каб 2, 3, 4
		Окна контролируемого помещения	Каб, 3
4	Материально-вещественный канал	Документы на бумажных носителях	Каб. 2
		Персонал предприятия	Находится в каб. 1, 2, 3, 4
		Производственные отходы	Расположены на выходе у каб. 1

Задание 4. Постройте модель угроз защищаемого объекта.

Таблица 4 модель угроз защищаемого объекта информационной системы управления складом

№ элемента	Цена информации	Путь проникновения	Оценка реальности	Величина угрозы	Ранг угрозы
1	Неценная информация	Сетевые атаки могут произойти из за нехватки персонала для быстрого среагирования на атаки	Может произойти из за нехватки профессиональных сотрудников которые могли бы поставить межсетевые экраны на 2 этаже а также провести дополнительное переобучение		

Таблица 4 (продолжение) модель угроз защищаемого объекта информационной системы управления складом

№ элемента	Цена информации	Путь проникновения	Оценка реальности	Величина угрозы	Ранг угрозы
2	Ценная информация	Социальная инженерия может быть применена злоумышленником, который будет воздействовать на сотрудника после окончания рабочего дня на эмоции с целью получения необходимой информации	Может произойти в организации в случае нарушения на предприятии распространении конфиденциальной информации из за недостатка обучения сотрудников	Ведёт за собой потерю контроля над сотрудником и риском появления шпионов или агентов с целью нарушения инф. системы	3
3	Ценная информация	Уязвимость ПО может включать в себя обнаружение каких либо сигнатур для обхода функций защиты	Из за отсуствий обфуксации или крипто на файл программа которой пользуются сотрудники могут взломать или заревёрсить программу стоит также делать различные ловушки		4

Таблица 4 (продолжение) модель угроз защищаемого объекта информационной системы управления складом

№ элемента	Цена информации	Путь проникновения	Оценка реальности	Величина угрозы	Ранг угрозы
4	Ценная информация	Утечка данных потеря контроля доступа и бесконтрольное похищение информации может быть вызвано из за слабой защиты информационной системы	Она может произойти если не настроить локальную сеть либо ужесточить контроль идентификации	В случае проявления такой угрозы будет потеряна ценная информации без возможности восстановления	5
5	Ценная информация	Фишинг С помощью спама или таргетированной рекламы злоумышленники рассылают свои поддельные сообщения большому числу людей. Они могут использовать базы данных с контактами	Злоумышленники создают поддельные электронные письма, сообщения в мессенджерах или сайты, которые выглядят как легитимные	Ведёт за собой незначительную проблему так как легко обнаруживается но может привести к затруднениям рабочей среды сотрудников по складу	3

Таблица 4 (продолжение) модель угроз защищаемого объекта информационной системы управления складом

№ элемента	Цена информации	Путь проникновения	Оценка реальности	Величина угрозы	Ранг угрозы
6	Неценная информация	Вредоносное ПО направленно на повреждение или вовсе уничтожения информации	Распространяется в случае ошибок сисадмина из за нехватки знаний	Может привести к конечному повреждение системы и форматирование данных	3

Задание 5. Теоретические вопросы.

1. Классы каналов несанкционированного получения информации.

Через человек хищение носителей информации, чтение информации с экрана или клавиатуры, чтение информации из распечатки.

Через программу перехват паролей, расшифровка зашифрованной информации, копирование информации с носителя.

Через аппаратуру подключение специально разработанных аппаратных средств, обеспечивающих доступ к информации перехват побочных электромагнитных излучений от аппаратуры, линий связи, сетей электропитания.

Также каналы утечки конфиденциальной информации можно разделить на три большие группы:

Материально-вещественные. Возникают при физическом контакте злоумышленника с носителем, например, хищение или потеря USB-накопителя, передача физических документов. 2

Визуальные и визуально-оптические. Возникают при дистанционном считывании и фиксации информации с различных носителей: фотографирование дисплеев мониторов, экранов для демонстрации презентаций, бумажных носителей, аудиозапись переговоров и пр..

Непосредственно физического контакта с носителем данных в этом случае не происходит. 2

Технические. К ним относятся, например, прослушивание сетевых интерфейсов, подключение к сети технических устройств перехвата, использование вредоносного программного обеспечения.

2. Моделирование угроз безопасности информации включает в себя:

Идентификация активов Определение всех объектов, представляющих ценность для организации, например, данные клиентов, финансовые отчёты, интеллектуальная собственность.

Анализ угроз выявление всех возможных источников угрозы, включая внешних злоумышленников, инсайдеров и технические сбои.

3. Модель нарушителя информационной безопасности.

Персонал могут появиться побуждения и у нарушителя могут быть планы, по которым они могут действовать действовать: финансовая выгода, месть, шпионаж, хулиганство.

Знания и навыки технические знания и опыт могут для проведения атаки: программирование, знание сетей, криптографии на определённые информационные системы.

Ресурсы средства, которыми располагает нарушитель финансирование, оборудование, доступ к специализированному ПО.

Вывод:

В результате выполнения работы мы подробно ознакомились с этапами и выявлениями потоков утечек информации что позволит в будущем нам миновать эти угрозы.