Правительство Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

Кафедра компьютерной безопасности

Домашняя работа по дисциплине «Основы информационной безопасности»

Работу выполнил

студент группы СКБ211 _____ Ф.С. Урусов

подпись, дата

Работу проверил _____ А. В. Сорокин

подпись, дата

Москва 2022

Оглавление

Введение

В данной домашней работе рассматриваемым объектом информатизации является шоколадная фабрика.

В ней рассмотрены следующие внутренние компоненты:

- Сервер
- Центр управления фабрикой
- Отдел логистики
- Склад
- Производственная линия

Центр управления – это центральный элемент. Центр управления через сервер управляет сборочной линией, передавая указания на АРМ сотрудникам производственной линии. Он в связан с главным офисом управляющей компании, для координации действий и получения указаний. Также центр управления связан с отделом логистики, чтобы координировать перечень необходимых продуктов, которые необходимо закупить для производства, закупочные цены и пр. Центр управления связан с сервером, на котором хранится вся актуальная информация о производственном процессе, включая весь ассортимент склада.

Сервер связан со складом, от которого он получает информацию о изменении кол-ва товаров, с центром управления, выдавая ему всю информацию о производстве, включая кол-во товаров на складе, с центром логистики, выдавая ему только информацию о кол-ве товаров на складе, и с внешними службами доставки, предоставляя им информацию о кол-ве готовых товаров, которые можно забрать для дальнейшего использования.

Отдел логистики связан с центром управления для координации закупок (например, подтверждение/отказ) и с сервером, чтобы получить актуальную информацию о кол-ве товаров на складе. Он также связан с внешними поставщиками товаров, у которых он заказывает необходимые товары.

На складе есть АРМ, в котором работники фиксируют изменение кол-ва товаров и передают эти данные на сервер.

Производственная линия оборудована АРМ, который автоматизирует процесс изготовления готовой продукции. Линия соединена с сервером по локальной сети и через него получает указания для работы от центра управления.

Шоколадная фабрика, как объект информатизации

Рисунок 1. Объект информатизации

Способы передачи данных

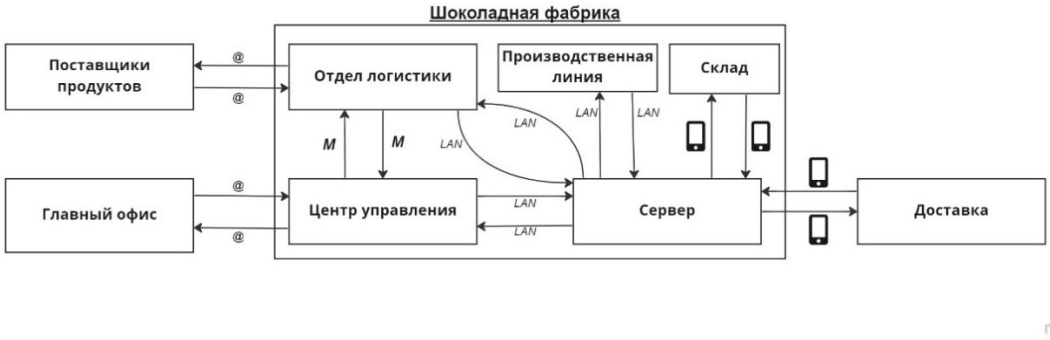

Рисунок 2. Способы передачи данных

Таблица 1

	Приложение
@	Электронная почта
LAN	Локальная сеть
M	Корпоративный мессенджер

Свойства информации, которые необходимо защищать

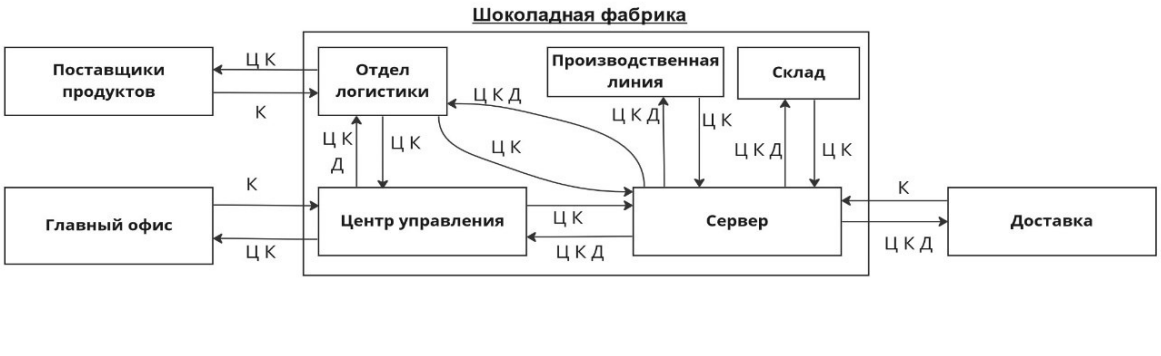

Рисунок 3. Свойства передаваемой информации

Условное обозначение	Описание
К	Конфиденциальность
Ц	Целостность
Д	Доступность

Таблица 1. Условные обозначения свойств передаваемой информации

В следующей таблице представлен подробный перечень потоков информации с объяснением определенных для них свойств, которые надо обеспечить.

ТАБЛИЦА 2 ИНФОРМАЦИОННЫЕ ПОТОКИ

№ потока	Способ передачи информации	Назначение информационных потоков	Свойства информации, которые необходимо обеспечить
1 Отдел логистики -> Сервер	Электронный файл по LAN сети	Запрос к серверу (о кол-ве продуктов на складе)	Целостность нужна, чтобы запрос на сервер пришел правильный Конфиденциальность нужна, потому что запрос может включать конфиденциальную информацию о кол-ве товаров
2 Сервер->Отдел логистики	Электронный файл по LAN сети	Ответ сервера (о кол-ве продуктов на складе)	Конфиденциальность, потому что ответ сервера может содержать конфиденциальную информацию о количестве товаров Доступность, потому что сервер должен быть доступен в любое время Целостность, потому что важно получать полную и корректную информацию от сервера
3 Сервер ->Склад	Сообщение по сети интернет (приложение)	Вернуть сотрудникам склада записанные на сервере данные о кол-ве товаров	Конфиденциальность, потому что ответ сервера может содержать конфиденциальную информацию о количестве товаров Доступность, потому что сервер должен быть доступен в любое время Целостность, потому что важно получать полную и корректную информацию от сервера
4 Склад->сервер	Сообщение по сети интернет (приложение)	Передать на сервер информацию о изменении кол-ва товаров на складе	Целостность нужна, чтобы информация на сервер пришла правильная Конфиденциальность нужна, потому что запрос включает конфиденциальную информацию о кол-ве товаров

5 Центр управления-> Сервер	Электронный файл по сети LAN	Запрос на получение всей информации, хранящийся на сервере или передача команд на АРМ производственной линии	Целостность нужна, чтобы запрос на сервер пришел правильный Конфиденциальность нужна, потому что запрос включает конфиденциальную информацию о работе предприятия
6 Сервер -> центр управления	Электронный файл по сети LAN	Передать всю информацию, хранящуюся на сервере или ответ от АРМ линии сборки	Конфиденциальность, потому что ответ сервера содержит конфиденциальную информацию о количестве товаров Доступность, потому что сервер должен быть доступен в любое время Целостность, потому что важно получать полную и корректную информацию от сервера
7 Отдел логистики -> поставщики	Электронное письмо	Запрос на покупку определенного кол-ва товара	Целостность нужна, чтобы передать именно корректную информацию о необходимых продуктах Конфиденциальность нужна, потому что запрос включает конфиденциальную информацию о кол-ве товаров
8 Поставщики -> отдел логистики	Электронное письмо	Ответ на запрос о покупке определенного кол-ва товара	конфиденциальность нужна, чтобы ответ от поставщиков, который может содержать важную информацию, был доставлен только получателю
9 Главный офис -> центр управления	Электронное письмо	Запрос на отчет по всей деятельности фабрики	Конфиденциальность нужна, потому что запрос включает конфиденциальную информацию о работе компании
10 Центр управления -> главный офис	Электронное письмо	Пересылка отчета по всей деятельности фабрики	Конфиденциальность, потому что ответ содержит конфиденциальную информацию о работе предприятия Доступность, потому что ответ руководство должен быть доступен в любое время Целостность, потому что важно получать полную и

			корректную информацию центра управления
11 Сервер -> служба доставки	Электронное сообщение по сети Интернет через приложение	Ответ о возможности забрать товар со склада, количестве	Конфиденциальность, потому что ответ сервера содержит конфиденциальную информацию о количестве товаров Доступность, потому что сервер должен быть доступен в любое время Целостность, потому что важно получать полную и корректную информацию от сервера
12 Служба доставки -> Сервер	Электронное сообщение по сети Интернет через приложение	Запрос на получение службой доставки товара со склада	Конфиденциальность, потому что ответ сервера содержит конфиденциальную информацию о количестве товаров
13 Центр управления -> Отдел логистики	Сообщение через корпоративный мессенджер	Подтверждение факта закупки и его деталей	Целостность нужна, чтобы информация центру управления пришла правильная Конфиденциальность нужна, потому что запрос включает конфиденциальную информацию о закупках
14 Отдел логистики -> центр управления	Сообщение через корпоративный мессенджер	Подтверждение факта закупки и его деталей	Конфиденциальность, потому что ответ сервера содержит конфиденциальную информацию закупках Доступность, потому что центру управления важно всегда знать, что происходит с закупками Целостность, потому что важно получать полную и корректную информацию центра логистики
15 Сервер -> Производственная линия	Электронный файл по сети LAN	Команда для управляющей системы (АРМ) линии сборки	Конфиденциальность, потому что ответ сервера содержит конфиденциальную информацию о производственном процессе Доступность, потому что производственная линия всегда должна получать

			информацию, что она должна делать Целостность, потому что важно получать полную и корректную информацию от сервера
16 Производственная линия-> Сервер	Электронный файл по сети LAN	Ответ управляющей системы (АРМ) линии сборки на команду	Целостность нужна, чтобы информация центру управления пришла правильная Конфиденциальность нужна, потому что ответ включает конфиденциальную информацию о процессе производства

Таблица 2. Перечень потоков информации

Возможные негативные последствия от реализации угроз безопасности информации

Определим возможные для рассматриваемого объекта информатизации негативные последствия от реализации угроз безопасности информации.

Таблица 3 Виды рисков (ущерба) и негативные последствия от реализации угроз безопасности информации

№	Виды риска (ущерба)	Возможные негативные последствия
У1	Ущерб физическому лицу	1. Угроза жизни или здоровью 2. Разглашение персональных данных
У2	Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью	1. Срыв запланированной сделки с партнером 2. Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств). 3. Потеря клиентов, поставщиков. 4. Потеря конкурентного преимущества. 5. Принятие неправильных решений 6. Потеря доверия 7. Нарушение деловой репутации 8. нарушение штатного режима функционирования
У3	Ущерб государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности	-

Таблица 3. Возможные негативные последствия

Объекты воздействия и виды воздействия на них

Таблица 4 Объекты воздействия и виды воздействия на них

Негативные последствия	Объекты воздействия	Виды воздействия
Угроза жизни или здоровью (У1)	АРМ производственной линии	Внедрение вредоносного ПО, выводящее из строя производственное оборудование или приводящее к неправильной работе
	Сервер	Внедрение вредоносного ПО,(скрипта) искажающего ответы сервера к производственной линии
Разглашение персональных данных (У1)	Сервер	Внедрение вредоносного ПО,(скрипта) искажающего ответы сервера в приложении и дублирующего данные клиентов (сотрудников доставки) на внешнее хранилище
Срыв запланированной сделки с партнером(У2)	АРМ производственной линии	Вывод из строя АРМ физическим воздействием
	АРМ сотрудника отдела логистики	Модификация информации, отправляемой поставщикам
Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств).(У2)	Сервер	Вывод из строя сервера физическим воздействием
	Сервер	Внедрение вредоносного ПО, искажающего данные
	АРМ производственной линии	Вывод из строя АРМ физическим воздействием
	АРМ производственной линии	Внедрение вредоносного ПО, выводящее из строя производственное оборудование или приводящее к неправильной работе
Потеря клиентов, поставщиков.(У2)	Сервер	Модификация данных отправляемых доставке
	АРМ сотрудника отдела логистики	Модификация информации, отправляемой поставщикам
Потеря конкурентного преимущества (У2)	Сервер	Вывод из строя сервера физическим воздействием
	Сервер	Внедрение вредоносного ПО, искажающего данные и

		передающие данные, составляющие коммерческую тайну
	АРМ производственной линии	Вывод из строя АРМ физическим воздействием
	АРМ производственной линии	Внедрение вредоносного ПО, выводящее из строя производственное оборудование или приводящее к неправильной работе
Принятие неправильных решений (У2)	АРМ сотрудника отдела логистики	Модификация информации, получаемой от поставщикам
	Сервер	Модификация данных, полученных от партнеров по доставке
Потеря доверия (У2)	АРМ сотрудников центра управления	Модификация данных, отправляемых в главный офис
Нарушение деловой репутации	Сервер	Модификация данных, отправляемых партнерам по доставке

Таблица 4. Объекты воздействия и виды воздействия на них

Определение источников угроз безопасности информации

Определив объекты воздействия и виды воздействия на них, рассмотрим источники угроз безопасности информации, для этого определив цели УБИ нарушителями, список актуальных нарушителей и их возможности.

Оценка целей реализации нарушителями угроз безопасности информации в зависимости от возможных негативных последствий и видов ущерба от их реализации.

Таблица 5

Виды нарушителей	Возможные цели и реализации угроз безопасности информации			Соответствие целей видам риска (ущерба) и возможным негативным последствиям
	Нанесение ущерба физическому лицу (У1)	Нанесение ущерба юридическому лицу, индивидуальному предпринимателю (У2)	Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности (У3)	
Специальные службы иностранных государств	-	-	-	-
Террористические, экстремистские группировки	-	-	-	-
Преступные группы (криминальные структуры)	+ (получение финансовой выгоды за счет продажи конфиденциальных данных)	-	-	У1 Утечка конфиденциальной информации
Отдельные физические лица (Хакеры)	+ Любопытство или желание самореализации	+ Получение финансовой или иной материальной выгоды.	-	У2 Утечка конфиденциальной информации У2

				Потеря доверия Нарушение деловой репутации
Конкуренты	-	+ Получение конкурентных преимуществ.	-	У2 (Потеря клиентов, поставщиков)
Разработчики программных, программно-аппаратных средств	-	+ Внедрение дополнительных функциональых возможностей в программные или программно-аппаратные средства на этапе разработки	-	У2 Принятие неправильных решений
Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	-	+ непреднамеренные, неосторожные или неквалифицированные действия	-	У2 Срыв запланированной сделки с партнером
Поставщики вычислительных услуг, услуг связи	-	+ Получение конкурентных преимуществ	-	У2 Срыв запланированной сделки с партнером; Потеря конкурентного преимущества
Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	-	+ неосторожные неквалифицированные действия	-	У2 Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка,

				ремонт указанных средств)
Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)	-	+ неосторожные неквалифицированные действия	-	У2 Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств)
Авторизованные пользователи систем и сетей	-	+ Любопытство или желание самореализации и (подтверждение статуса). Месть за ранее совершенные действия.	-	У2 Срыв запланированной сделки с партнером (Потеря клиентов, поставщиков)
Системные администраторы и администраторы безопасности	+ (получение финансовой выгоды за счет продажи персональных данных)	-	-	У1 Разглашение персональных данных граждан
Бывшие работники (пользователи)	+ (месть за ранее совершенные действия)	-	-	У1 Нарушение тайны переписки, телефонных переговоров, иных сообщений

Таблица 5. Цели реализации нарушителями угроз безопасности информации

Актуальные нарушители при реализации угроз безопасности информации и соответствующие им возможности

Таблица 6: Актуальная нарушители при реализации угроз безопасности информации и соответствующие им возможности

№ п/п	Виды риска (ущерба) и возможные негативные последствия	Виды актуального нарушителя	Категория нарушителя	Уровень возможностей нарушителя
1	У1: Угроза жизни или здоровью Разглашение персональных данных	Системные администраторы и администраторы безопасности	Внутренний	Н2
		Бывшие работники (пользователи)	Внешний	Н1
2	У2: 1. Срыв запланированной сделки с партнером 2. Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств). 3. Потеря клиентов, поставщиков. 4. Потеря конкурентного преимущества. 5. Принятие неправильных решений 6. Потеря доверия 7. Нарушение деловой репутации	Отдельные физические лица (хакеры)	Внешний	Н1
		Конкурирующие организации	Внешний	Н2
		Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	Н1
		Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Н2
		Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)	Внутренний	Н1
		Авторизованные пользователи систем и сетей	Внутренний	Н1
		Преступные группы (криминальные структуры)	внешние	Н2
		Разработчики программных, программно-аппаратных средств	Внутренний	Н3
		Поставщики вычислительных услуг, услуг связи	внутренние	Н2

Таблица 6. Актуальные нарушители при реализации УБИ и соответствующие им возможности

Определение способов реализации (возникновения) угроз безопасности информации

Таблица 7: Актуальные способы реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
1	Отдельные физические лица (хакеры) (H1)	Внешний	АРМ сотрудника отдела логистики	Внешний сетевой интерфейс АРМ сотрудника отдела маркетинга	Внедрение вредоносного ПО(Заражённое вирусом электронное письмо)
			Сервер	Административный сетевой интерфейс АРМ сотрудника центра управления или логистики	Внедрение вредоносного ПО (Заражённое вирусом с возможностью удалённого доступа к ПК)
2	Конкурирующие организации (H2)	Внешний	АРМ сотрудников центра управления	Внешний сетевой интерфейс АРМ сотрудника центра управления	Внедрение вредоносного ПО(Заражённое вирусом электронное письмо)
			Сервер	Административный сетевой интерфейс АРМ сотрудника центра управления или логистики	Внедрение вредоносного ПО (Заражённое вирусом с возможностью удалённого доступа АРМ производственной линии)
3	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем (H1)	Внешний	АРМ производственной линии	Съёмные носители с вирусом; Доступ к компонентам системы	Внедрение вредоносного ПО (Флешка с вирусом) Некачественное ПО для оборудования
			АРМ сотрудника отдела логистики	Съёмные носители с вирусом; Доступ к компонентам системы	Внедрение вредоносного ПО (Флешка с вирусом) Некачественное ПО для работы с ПК
4	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ (H1)	Внутренний	АРМ производственной линии	Съёмные носители с вирусом Возможность доступа к компонентам системы	Внедрение вредоносного ПО (Флешка с вирусом) Неправильная настройка оборудования
5	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)	Внутренний	Сервер	Возможность доступа к компонентам системы	Физическое воздействие (механическое повреждение)

	(H1)				
6	Авторизованные пользователи систем и сетей (H1)	Внутренний	АРМ производственной линии	Внутренний сетевой интерфейс АРМ сотрудника производственного отдела	Удаление или модификация настроек оборудования
			АРМ производственной линии	Возможность доступа к компонентам системы	Физическое воздействие
			АРМ сотрудников центра управления	Внутренний сетевой интерфейс АРМ сотрудника производственного отдела; Съёмные носители с вирусом	Флешка с вирусом Неправильная настройка или удаление необходимого ПО
			АРМ сотрудника отдела логистики	Внутренний сетевой интерфейс АРМ сотрудника производственного отдела; Съёмные носители с вирусом	Внедрение вредоносного ПО
			Сервер	Административный сетевой интерфейс сотрудника отдела логистики	Передача данных с сервера в сеть Интернет
7	Системные администраторы и администраторы безопасности (H2)	Внутренний	Сервер	Административный сетевой интерфейс сотрудника отдела логистики или центра управления	Передача данных с сервера в сеть Интернет
8	Бывшие (уволенные) работники (пользователи) (H1)	Внешний	АРМ сотрудников центра управления	Внешний сетевой интерфейс АРМ сотрудника центра управления	Заражённое вирусом электронное письмо
9	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.) (H1)	Внутренний	АРМ производственной линии	Возможность доступа к компонентам системы	Физическое воздействие
10	Разработчики программных, программно-аппаратных средств (H3)	Внутренний	Сервер	Внутренний сетевой интерфейс корпоративного мессенджера	Использование не декларированных возможностей

Таблица 7. Способы реализации УБИ

Определение угроз безопасности информации

$УБИ_1$ = [хакер-любитель (отдельные физические лица); Сервер (через АРМ сотрудников логистики); Внедрение вредоносного ПО; Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств)]

$УБИ_2$ = [хакер-любитель (отдельные физические лица); АРМ сотрудников логистики; Внедрение вредоносного ПО; Нарушение деловой репутации]

$УБИ_3$ = [Сотрудник склада (авторизованные пользователи систем и сетей); АРМ сотрудника склада; разломал свой АРМ (физическое воздействие); нарушение штатного режима функционирования]

$УБИ_4$ = [Сотрудник склада(авторизованные пользователи систем и сетей);Сервер ; SQL инъекция через приложение;(Внедрение вредоносного ПО); Недополучение прибыли]

$УБИ_5$ = [сотрудник компании конкурента (конкурирующее организации);АРМ сотрудников центра управления; заражение системы сервера вирусом (Внедрение вредоносного ПО); Потеря конкурентного преимущества]

$УБИ_6$ = [хакер-любитель(отдельные физические лица);Сервер (через АРМ сотрудников логистики); заражение системы сервера вирусом;(Внедрение вредоносного ПО); Утечка конфиденциальной информации]

$УБИ_7$= [обиженный уволенный работник (бывший сотрудник);АРМ сотрудников логистики; заражение системы сервера вирусом через электронное письмо (Внедрение вредоносного ПО); Модификация передаваемых данных]

$УБИ_8$= [член банды радикальных противников сладкого (криминальные группировки); АРМ сотрудников логистики; заражение системы сервера вирусом;(Внедрение вредоносного ПО); нарушение штатного режима функционирования]

$УБИ_9$= [Сотрудник центра управления (авторизованные пользователи систем и сетей);Сервер (АРМ сотрудников логистики); заражение системы сервера вирусом;(Внедрение вредоносного ПО); Недополучение прибыли]

$УБИ_{10}$ = [обиженный уволенный работник (бывший сотрудник); АРМ сотрудников центра управления; установка перед увольнением устройства для перехвата электронных писем центра управления (Перехват побочных излучений); Утечка конфиденциальной информации]

$УБИ_{11}$= [Сотрудник центра управления (авторизованные пользователи систем и сетей); Сервер (АРМ сотрудников центра управления); заражение системы сервера вирусом;(Внедрение вредоносного ПО); Потеря деловой репутации]

$УБИ_{12}$ = [сотрудник компании конкурента (конкурирующее организации);Сервер (через Веб приложение); SQL-инъекция, ломающая работу сервера(Внедрение вредоносного ПО); Нарушение штатного режима функционирования]

$УБИ_{13}$= [Сотрудник центра управления (авторизованные пользователи систем и сетей);АРМ сотрудников центра управления; разломал молотком АРМ (физическое воздействие); Недополучение прибыли]

$УБИ_{14}$= [Сотрудник отдела логистики (авторизованные пользователи систем и сетей); АРМ сотрудников логистики; извлек из своего АРМ видеокарту и процессор (похищение комплектующих устройства); Нарушение деловой репутации]

$УБИ_{15}$= [хакер-любитель(отдельные физические лица);Сервер (АРМ сотрудников логистики); заражение системы сервера вирусом;(Внедрение вредоносного ПО); Недополучение прибыли]

$УБИ_{16}$= [уборщик (Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)) АРМ производственной линии; вылил на АРМ чай (физическое воздействие); Нарушение штатного режима функционирования]

Определение для актуальных угроз мер защиты

Таблица 8: Меры защиты против активных угроз

Ребро	Свойство	УБИ(i)	Категория мер защиты	Подробно
1 Отдел логистики -> Сервер	Конфиденциальность	УБИ1	Организационные (Административные)	Должностные инструкции для сотрудников отвечающих за проверку антивирусных программ; Должностные инструкции для сотрудников отдела логистики по эксплуатации антивирусных средств защиты и общей ИБ
			Программно-технические	Ограничение доступа персонала к компонентам локальной системы, установка и своевременное обновление САВЗ установка локальных межсетевых экранов на сервер
2 Сервер->Отдел логистики	Конфиденциальность Целостность Доступность	УБИ2	Организационные (Административные)	Должностные инструкции для сотрудников отвечающих за проверку антивирусных программ; Должностные инструкции для сотрудников отдела логистики Должностные инструкции по эксплуатации антивирусных средств защиты
			Программно-технические	Ограничение доступа персонала к компонентам локальной системы, установка и своевременное обновление САВЗ
3 Сервер ->Склад	Конфиденциальность Целостность Доступность	УБИ3	Организационные (Административные)	Должностные инструкции для сотрудников склада Инструкция по использованию камер видеонаблюдения Регламент сотрудников охраны Регламент установки камер видеонаблюдения
			Организационные (организационно - технические)	Установка камер видеонаблюдения
4 Склад->сервер	Целостность	УБИ4	Программно-технические	Ограничение доступа персонала к компонентам локальной системы, установка и своевременное обновление САВЗ Установка локальных межсетевых экранов на сервере
			Организационные (Административные)	Должностные инструкции для сотрудников склада
5 Центр управления ->Сервер	Целостность	УБИ5	Программно-технические	Установка и своевременное обновление САВЗ Установка локальных межсетевых экранов на сервере Обеспечение резервного копирования

			Организационные (Административные)	Должностные инструкции для сотрудников центра управления по работе с сервером
6 Сервер -> центр управления	Конфиденциальность Целостность Доступность	УБИ6	Программно-технические	Установка и своевременное обновление САВЗ Установка локальных межсетевых экранов на сервере
			Организационные (Административные)	Должностные инструкции для сотрудников центра управления Должностные инструкции для сотрудников отвечающих за проверку антивирусных программ; Должностные инструкции по эксплуатации антивирусных средств защиты
7 Отдел логистики -> поставщики	Конфиденциальность	УБИ6	Программно-технические	Своевременное обновление САВЗ своевременное обновление и контроль доступа сотрудников в локальной системе Установка внешнего сетевого экрана Использование модуля DLP
			Организационные (Административные)	Должностные инструкции для сотрудников отвечающих за проверку антивирусных программ; Должностные инструкции по эксплуатации антивирусных средств защиты
			Криптографические	Добавление электронной цифровой подписи на отправляемый по email сообщение
8 Поставщики -> отдел логистики	конфиденциальность	УБИ8	Программно-технические	Своевременное обновление САВЗ своевременное обновление и контроль доступа сотрудников в локальной системе Установка внешнего сетевого экрана
			Организационные (Административные)	Должностные инструкции для сотрудников отвечающих за проверку антивирусных программ; Должностные инструкции по эксплуатации антивирусных средств защиты
9 Главный офис -> центр управления	Конфиденциальность	УБИ9	Программно-технические	Ограничение доступа персонала к компонентам локальной системы, установка и своевременное обновление САВЗ
			Организационные (Административные)	Должностные инструкции для сотрудников отвечающих за проверку антивирусных программ;

				Должностные инструкции по эксплуатации антивирусных средств защиты
			Криптографические	Добавление электронной цифровой подписи на отправляемый по email сообщение
10 Центр управления -> главный офис	Конфиденциальность Целостность	УБИ10	Программно-технические	Ограничение доступа персонала к компонентам локальной системы, установка и своевременное обновление САВЗ
			Организационные (Административные)	Должностные инструкции для сотрудников отвечающих за проверку антивирусных программ; Должностные инструкции по эксплуатации антивирусных средств защиты
			Криптографические	Добавление электронной цифровой подписи на отправляемый по email сообщение
11 Сервер -> служба доставки	Конфиденциальность Целостность Доступность	УБИ11	Программно-технические	Ограничение доступа персонала к компонентам локальной системы, установка и своевременное обновление САВЗ
			Организационные (Административные)	Должностные инструкции для сотрудников отвечающих за проверку антивирусных программ; Должностные инструкции по эксплуатации антивирусных средств защиты Двухфакторная аутентификация внешних пользователей Использование модуля DLP
12 Служба доставки -> Сервер	Конфиденциальность	УБИ12	Программно-технические	Ограничение доступа персонала к компонентам локальной системы, установка и своевременное обновление САВЗ
			Организационные (Административные)	Должностные инструкции для сотрудников отвечающих за проверку антивирусных программ; Должностные инструкции по эксплуатации антивирусных средств защиты Двухфакторная аутентификация внешних пользователей
13 Центр управления ->	Целостность	УБИ13	Организационные (организационно - технические)	Установка камер видеонаблюдения

Отдел логистики			Организационные (Административные)	Должностные инструкции для сотрудников отвечающих за проверку антивирусных программ; Должностные инструкции по эксплуатации антивирусных средств защиты Инструкция по использованию камер видеонаблюдения Регламент сотрудников охраны Регламент установки камер видеонаблюдения
14 Отдел логистики -> центр управления	Целостность	УБИ14	Организационные (организационно - технические)	Установка камер видеонаблюдения Ограничение физического доступа пользователей к компонентам системы (физическое защита)
			Организационные (Административные)	Должностные инструкции для сотрудников отвечающих за проверку антивирусных программ; Должностные инструкции по эксплуатации антивирусных средств защиты
15 Сервер -> Производственная линия	Целостность Доступность Конфиденциальность	УБИ15	Программно-технические	Ограничение доступа персонала к компонентам локальной системы, установка и своевременное обновление САВЗ Добавление локального межсетевого экрана
			Организационные (Административные)	Должностные инструкции для сотрудников отвечающих за проверку антивирусных программ; Должностные инструкции по эксплуатации антивирусных средств защиты
16 Производственная линия-> Сервер	Целостность	УБИ16	Организационные (организационно - технические)	Установка камер видеонаблюдения Ограничение физического доступа пользователей к компонентам системы (физическое защита)
			Организационные (Административные)	Должностные инструкции для сотрудников отвечающих за проверку антивирусных программ; Должностные инструкции по эксплуатации антивирусных средств защиты Должностные инструкции для лиц поддерживающих работу инфраструктуры

Таблица 9. Меры защиты информации для актуальный УБИ

Итоговый список всех мер защиты информации

Программно-технические:

- Ограничение доступа персонала к компонентам локальной системы
- Установка и своевременное обновление САВЗ
- Установка локальных межсетевых экранов на сервер
- Создание и использование DLP в локальной сети
- Обеспечение резервного копирования

Организационные (Административные):

- Назначение персонала, отвечающего за проверку и обновление САВЗ
- Должностные инструкции по эксплуатации антивирусных средств защиты
- Должностные инструкции для сотрудников отвечающих за проверку антивирусных программ
- Закупка и использование защищенных сервисов электронной почты
- Закупка и использование защищенных сервисов для мобильного приложения
- Инструкция по использованию камер видеонаблюдения
- Регламент сотрудников охраны
- Регламент установки камер видеонаблюдения
- Должностные инструкции для сотрудников отдела логистики
- Должностные инструкции для сотрудников отдела центра управления
- Должностные инструкции для сотрудников склада
- Составление графика проверки обновления САВЗ
- Обеспечить резервное питание сервера

Организационные (организационно - технические):

- Установка камер видеонаблюдения
- Ограничение физического доступа пользователей к компонентам системы (физическая защита)
- Внедрение системы аутентификации для работы с приложением

Криптографические:

- Добавление электронной цифровой подписи на отправляемый по email сообщение