Правительство Российской Федерации
Федеральное государственное автономное образовательное
учреждение высшего образования
«Национальный исследовательский университет
«Высшая школа экономики»

Московский институт электроники и математики им. А. Н. Тихонова

Департамент прикладной математики

ОТЧЕТ
по курсовой работе по дисциплине
«Основы информационной безопасности»

Выполнил студент группы СКБ192
Березин Александр Евгеньевич

Тема работы: «Построение модели угроз безопасности информации для объекта информатизации»

Москва, 2022

Введение

В качестве объекта информатизации для данной работы выбрана вымышленная Научно-производственная корпорация «Уралвагонзавод», взаимодействующая с клиентами как гражданского (РЖД), так и оборонного (Министерство Обороны) секторов, реализующая разработку и проектирование (Конструкторское бюро) продукта (с возможным последующим оформлением разработок в Патентном бюро), его создание и обслуживание (Отдел производства). Финансовая отчетность организации контролируется отделом Бухгалтерии, который взаимодействует с Банком для выполнения финансовых операций.

1. Выбор объекта информатизации и его компонент

Схема объекта информатизации представлена ниже (Рисунок 1).

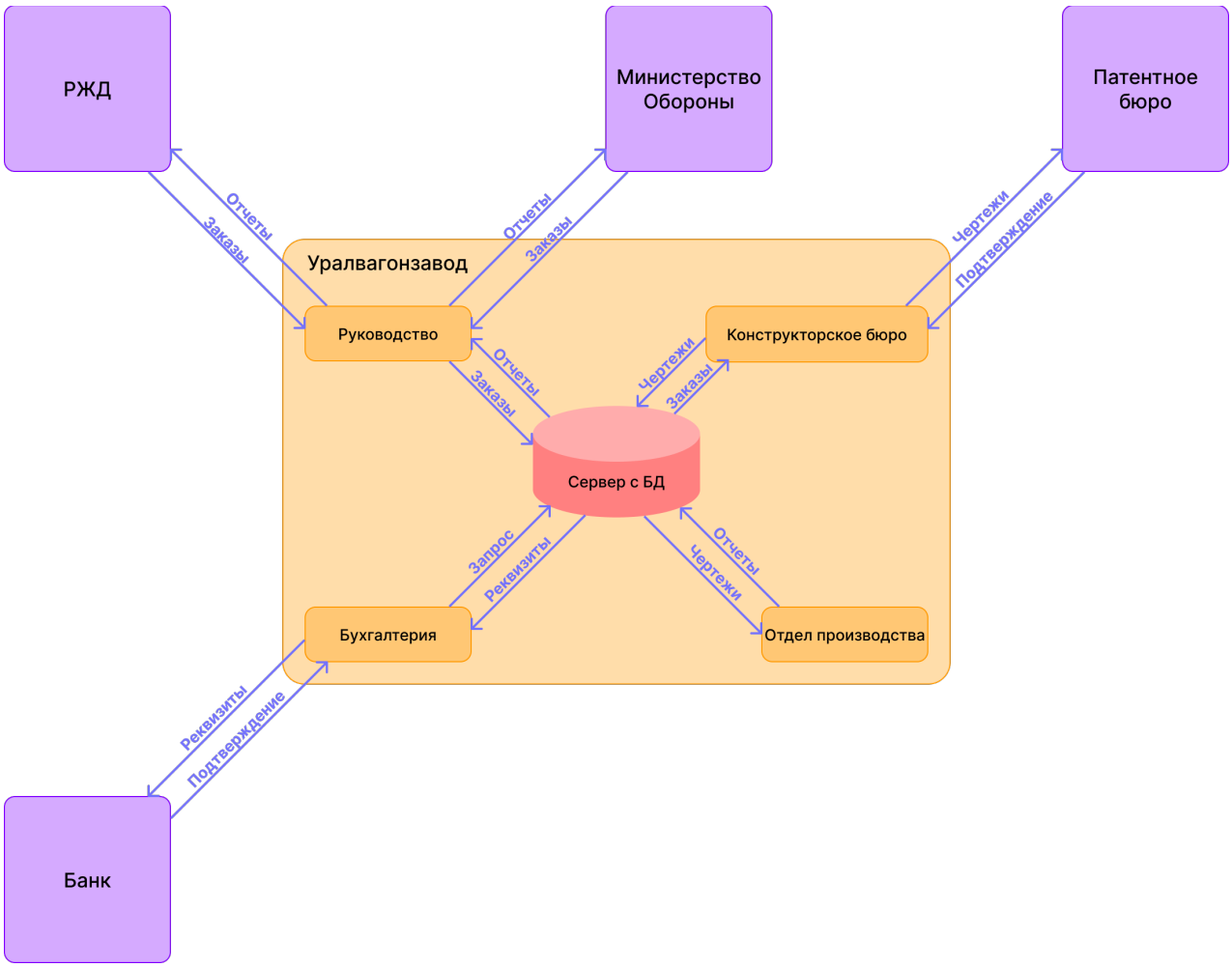

Рисунок 1. Схема объекта информатизации

2. Определение способов передачи для всех потоков информации

Способы передачи для каждого потока информации определены на схеме, с использованием следующих условных обозначений:

Условное обозначение	Описание
	Взаимодействие по внешней сети (Email)
	Взаимодействие по локальной сети (сетевой пакет)

Таблица 1. Условные обозначения способов передачи информации

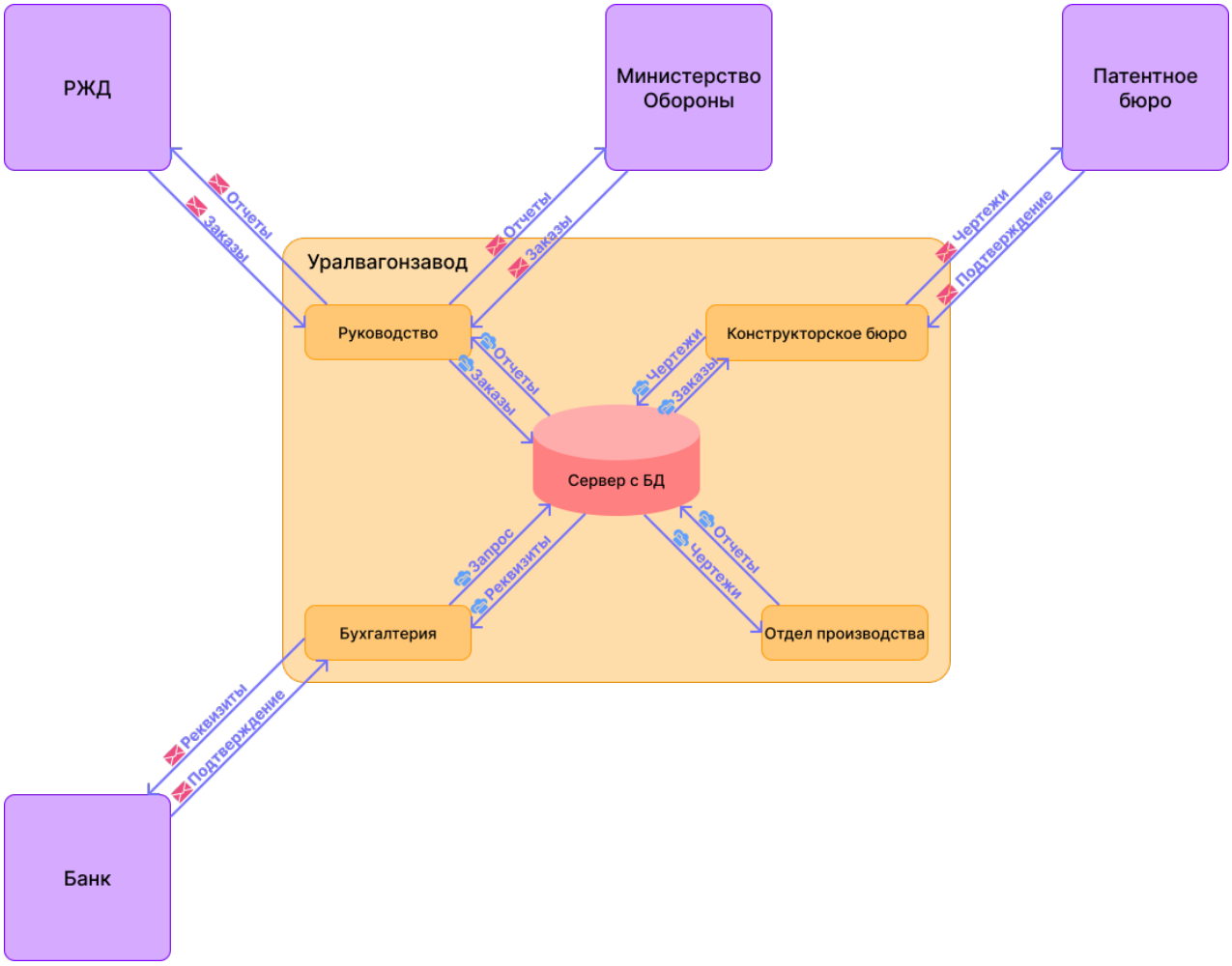

Рисунок 2. Схема объекта информатизации с указанием способов передачи

3. Определение свойств информации, которые необходимо обеспечить

Условные обозначения, применяющиеся на схеме:

- К – конфиденциальность
- Ц – целостность
- Д – доступность

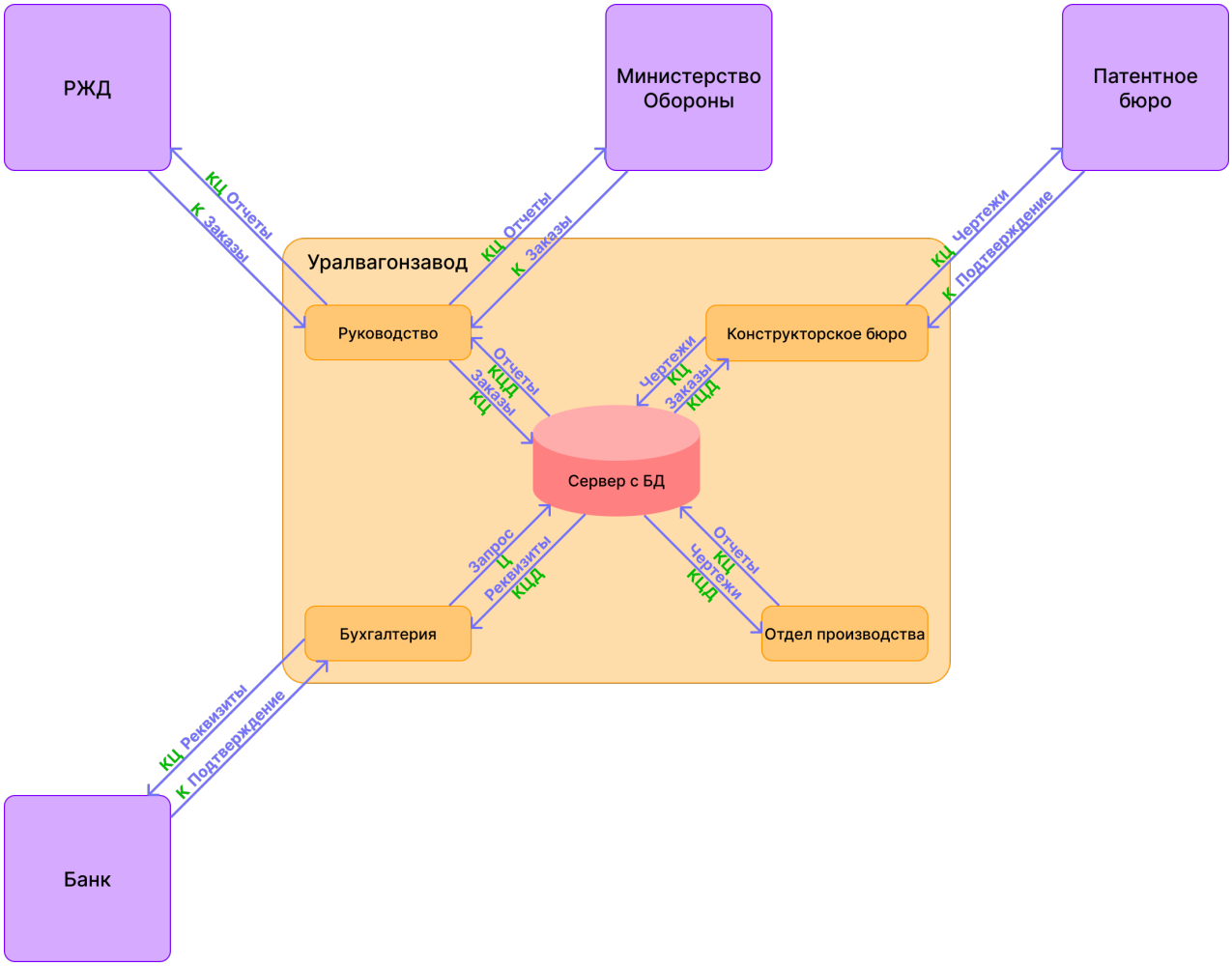

Рисунок 3. Схема объекта информатизации с указанием свойств информации

В следующей таблице представлен подробный перечень потоков информации с объяснением передаваемой по ним информации и определенных для них свойств, которые необходимо обеспечить.

Условные обозначения, применяющиеся в таблице:

- МО – Министерство Обороны
- КБ – Конструкторское бюро
- ПБ – Патентное бюро
- ОП – Отдел производства

Поток информации	Передаваемая информация	Свойство	Объяснение

РЖД – Руководство	Новые коммерческие заказы и правки по текущим коммерческим заказам	К	Для потоков информации извне объект информатизации может обеспечить лишь конфиденциальность информации. Она важна, так как передаваемая информация не должна открыто распространяться и передаваться третьим лицам
Руководство – РЖД	Отчеты о проделанной работе по текущим коммерческим заказам	КЦ	Передаваемая информация является коммерческой тайной и является отчетностью перед заказчиком, в связи с чем ее разглашение и нарушение целостности не позволительны
МО – Руководство	Новые государственные заказы и правки по текущим государственным заказам	К	Для потоков информации извне объект информатизации может обеспечить лишь конфиденциальность информации. Она важна, так как передаваемая информация не должна открыто распространяться и передаваться третьим лицам
Руководство – МО	Отчеты о проделанной работе по текущим государственным заказам	КЦ	Передаваемая информация является государственной тайной и является отчетностью перед заказчиком, в связи с чем ее разглашение и нарушение целостности не позволительны
КБ – ПБ	Заявки на регистрацию разработок (чертежей) в патентном бюро	КЦ	Передаваемая информация является коммерческой тайной и является интеллектуальной собственностью рассматриваемого объекта информатизации, в связи с чем ее

			разглашение и нарушение целостности не позволительны
ПБ – КБ	Ответ на ранее поданные заявки на регистрацию разработок (чертежей)	К	Для потоков информации извне объект информатизации может обеспечить лишь конфиденциальность информации. Она важна, так как передаваемая информация не должна открыто распространяться и передаваться третьим лицам
Бухгалтерия – Банк	Реквизиты для перевода заработных плат сотрудникам	КЦ	Передаваемая информация представляет собой персональные данные сотрудников, в случае нарушения целостности и получения адресатом неверных данных или в случае разглашения которых сотрудники организации могут понести финансовые потери
Банк – Бухгалтерия	Ответ на ранее поданные заявки на перевод денежных средств	К	Для потоков информации извне объект информатизации может обеспечить лишь конфиденциальность информации. Она важна, так как передаваемая информация не должна открыто распространяться и передаваться третьим лицам
Бухгалтерия – Сервер	Запрос на предоставление реквизитов сотрудников	Ц	Запрос на получение платежных данных от сотрудников отдела Бухгалтерии к Серверу с базой данных не должен быть искажен в процессе передачи, так как это может привести к получению в дальнейшем неверной информации в ответ на данный запрос, что

			может повлечь финансовые потери со стороны сотрудников организации. Конфиденциальность в данном случае обеспечивать не требуется, так как запрос не содержит персональных данных и иной конфиденциальной информации, а лишь является средством запроса от сервера информации об определенной группе сотрудников (по должности) либо всех вместе
Сервер – Бухгалтерия	Реквизиты сотрудников	КЦД	Передаваемая информация представляет собой персональные данные сотрудников, в случае нарушения целостности и получения адресатом неверных данных или в случае разглашения которых сотрудники организации могут понести финансовые потери. Сервер должен обеспечивать доступность информации и предоставлять ее по запросу
Руководство – Сервер	Новые заказы, для которых необходимо разработать чертежи продукта	КЦ	Передаваемая информация является коммерческой или государственной тайной, а также сведениями о количественной и качественной составляющих будущей работы компании, изменение которой влечет как финансовые, так и репутационные потери, в связи с чем ее разглашение и

			нарушение целостности не позволительны
Сервер – Руководство	Отчеты о проделанной работе, текущем состоянии (готовности) продуктов	КЦД	Передаваемая информация является коммерческой или государственной тайной и является отчетностью перед заказчиком, в связи с чем ее разглашение и нарушение целостности не позволительны. Сервер должен обеспечивать доступность информации и предоставлять ее по запросу
Сервер – КБ	Новые заказы, для которых необходимо разработать чертежи продукта	КЦД	Передаваемая информация является коммерческой или государственной тайной, в связи с чем ее разглашение и нарушение целостности не позволительны. Сервер должен обеспечивать доступность информации и предоставлять ее по запросу
КБ – Сервер	Новые (разработанные) чертежи для продуктов по текущим заказам	КЦ	Передаваемая информация является коммерческой или государственной тайной, а также интеллектуальной собственностью рассматриваемого объекта информатизации, в связи с чем ее разглашение и нарушение целостности не позволительны
Сервер – ОП	Чертежи для продуктов по текущим заказам	КЦД	Передаваемая информация является коммерческой или государственной тайной, а также интеллектуальной собственностью рассматриваемого

			объекта информатизации, в связи с чем ее разглашение и нарушение целостности не позволительны. Сервер должен обеспечивать доступность информации и предоставлять ее по запросу
ОП – Сервер	Отчеты о проделанной работе, текущем состоянии (готовности) продуктов	КЦ	Передаваемая информация является коммерческой или государственной тайной и является отчетностью перед заказчиком, в связи с чем ее разглашение и нарушение целостности не позволительны

Таблица 2. Перечень потоков информации

4. Определение возможных негативных последствий от реализации угроз безопасности информации

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

№	Виды риска (ущерба)	Возможные негативные последствия
У1	Ущерб физическому лицу	• Финансовый ущерб физическому лицу. • Разглашение персональных данных граждан. • Угроза жизни или здоровью.
У2	Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью	• Недополучение ожидаемой (прогнозируемой) прибыли. • Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций. • Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. • Потеря конкурентного преимущества. • Нарушение деловой репутации и утрата доверия.

		• Утечка конфиденциальной информации (коммерческой тайны, секретов производства).
УЗ	Ущерб государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности	• Причинение ущерба жизни и здоровью людей. • Снижение уровня дохода организации с государственным участием. • Снижение показателей государственного оборонного заказа. • Утечка информации ограниченного доступа.

Таблица 3. Возможные негативные последствия

5. Определение объектов воздействия и видов воздействия на них

После определения возможных негативных последствий рассмотрим объекты воздействия и виды воздействия на них для каждого из определенных последствий.

Негативные последствия	Объекты воздействия	Виды воздействия
У1: Финансовый ущерб физическому лицу	База данных информационной системы, содержащая конфиденциальную информацию о сотрудниках	Несанкционированные модификация / удаление платежной информации сотрудников (банковских реквизитов) в базе данных; блокирование доступа к базе данных
	Автоматизированное рабочее место (АРМ) сотрудника отдела Бухгалтерии	Несанкционированная модификация (подмена) платежной информации сотрудников (банковских реквизитов), передаваемой через АРМ сотрудника в банк
У1: Разглашение персональных данных граждан	База данных информационной системы, содержащая конфиденциальную информацию о сотрудниках	Несанкционированный доступ к базе данных с последующей утечкой идентификационной информации граждан
У1: Угроза жизни или здоровью	База данных информационной системы, содержащая список всех чертежей	Несанкционированная модификация чертежей с добавлением уязвимых (физически потенциально опасных) мест в ходе его производства
У2: Недополучение ожидаемой (прогнозируемой) прибыли	База данных информационной системы, содержащая список всех текущих заказов и отчетов	Несанкционированные модификация / удаление информации о текущих заказах и отчетов о ходе их выполнения; блокирование доступа к базе данных
	Автоматизированное рабочее место (АРМ) сотрудника отдела Руководства	Несанкционированная подмена данных получателя в электронных письмах, ложное извещение об отправлении (и отсутствие отправления) электронных писем с отчетностью о ходе выполнения текущих заказов
У2: Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций	База данных информационной системы, содержащая список всех текущих заказов и отчетов	Несанкционированные модификация / удаление информации о текущих заказах и отчетов о ходе их выполнения
	Автоматизированное рабочее место (АРМ) сотрудника отдела Руководства	Несанкционированная подмена данных получателя в электронных письмах; ложное извещение об отправлении, блокировка отправлений электронных писем; подмена файлов с заказами и отчетами о ходе их выполнения
	Автоматизированное рабочее место (АРМ) сотрудника Конструкторского бюро	Несанкционированные модификация / удаление / разглашение (утечка) разрабатываемых чертежей

	Автоматизированное рабочее место (АРМ) сотрудника Отдела производства	Несанкционированные модификация / удаление разработанных чертежей; фальсификация / модификация / удаление отчетов о ходе производства продуктов
У2: Необходимость дополнительных (незапланированных) затрат на восстановление деятельности	База данных информационной системы, содержащая список всех текущих заказов и отчетов	Несанкционированные модификация / удаление большого количества информации о текущих заказах и отчетов о ходе их выполнения; блокирование доступа к базе данных; вывод базы данных из строя путем воздействия на физические составляющие
	Автоматизированное рабочее место (АРМ) сотрудника Конструкторского бюро	Несанкционированные модификация / удаление большого количества информации о разрабатываемых чертежей
	Автоматизированное рабочее место (АРМ) сотрудника Отдела производства	Несанкционированные модификация / удаление большого количества информации о разработанных чертежах
У2: Нарушение деловой репутации и утрата доверия	База данных информационной системы, содержащая конфиденциальную информацию о сотрудниках	Несанкционированный доступ к базе данных с последующей утечкой идентификационной информации граждан
	База данных информационной системы, содержащая список всех текущих заказов, отчетов и чертежей	Несанкционированный доступ к базе данных с последующей утечкой информации о текущих заказах, отчетов о ходе их выполнения и чертежей разрабатываемых / создаваемых продуктов
	Автоматизированное рабочее место (АРМ) сотрудника Отдела производства	Несанкционированные модификация / удаление / разглашение (утечка) разработанных чертежей; фальсификация / модификация / удаление / разглашение (утечка) отчетов о ходе производства продуктов
У2: Утечка конфиденциальной информации (коммерческой тайны, секретов производства)	База данных информационной системы, содержащая список всех чертежей	Несанкционированный доступ к базе данных с последующим разглашением (утечкой) информации о разработанных чертежах, являющихся коммерческой тайной
	Автоматизированное рабочее место (АРМ) сотрудника отдела Руководства	Несанкционированный доступ к проходящему трафику информации с последующим разглашением (утечкой) информации о текущих заказах, являющихся коммерческой тайной
	Автоматизированное рабочее место (АРМ) сотрудника Конструкторского бюро	Несанкционированный доступ к базе данных с последующим разглашением (утечкой) информации о

		разрабатываемых чертежах, являющихся коммерческой тайной
	Автоматизированное рабочее место (АРМ) сотрудника Отдела производства	Несанкционированный доступ к базе данных с последующим разглашением (утечкой) разработанных чертежей, отчетов о ходе производства продуктов
У2: Потеря конкурентного преимущества	База данных информационной системы, содержащая список всех чертежей	Несанкционированные модификация / удаление / разглашение (утечка) информации о разработанных чертежах, являющихся коммерческой тайной
	Автоматизированное рабочее место (АРМ) сотрудника Конструкторского бюро	Несанкционированные модификация / удаление / разглашение (утечка) информации о разрабатываемых чертежах
У3: Причинение ущерба жизни и здоровью людей	База данных информационной системы, содержащая список всех чертежей	Несанкционированная модификация чертежей с добавлением уязвимых (физически потенциально опасных) мест в конечной реализации продукта или в ходе его производства
У3: Снижение уровня дохода организации с государственным участием	База данных информационной системы, содержащая список всех текущих заказов и отчетов	Несанкционированные модификация / удаление большого количества информации о текущих заказах и отчетов о ходе их выполнения; блокирование доступа к базе данных
	Автоматизированное рабочее место (АРМ) сотрудника Конструкторского бюро	Несанкционированные модификация / удаление разрабатываемых чертежей
	Автоматизированное рабочее место (АРМ) сотрудника Отдела производства	Несанкционированные модификация / удаление разработанных чертежей; фальсификация / модификация / удаление отчетов о ходе производства продуктов
У3: Снижение показателей государственного оборонного заказа	База данных информационной системы, содержащая список всех текущих заказов и отчетов	Несанкционированные модификация / удаление большого количества информации о текущих заказах и отчетов о ходе их выполнения; блокирование доступа к базе данных
	Автоматизированное рабочее место (АРМ) сотрудника Отдела производства	Несанкционированные фальсификация / модификация / удаление отчетов о ходе производства продуктов; блокирование работы АРМ
У3: Утечка информации ограниченного доступа	База данных информационной системы, содержащая список всех чертежей	Несанкционированный доступ к базе данных с последующим разглашением (утечкой) информации о разработанных чертежах, являющихся государственной тайной
	Автоматизированное рабочее место (АРМ) сотрудника отдела Руководства	Несанкционированный доступ к проходящему трафику информации с последующим разглашением (утечкой) информации о текущих заказах, являющихся государственной тайной

	Автоматизированное рабочее место (АРМ) сотрудника Конструкторского бюро	Несанкционированный доступ к базе данных с последующим разглашением (утечкой) информации о разрабатываемых чертежах, являющихся государственной тайной
	Автоматизированное рабочее место (АРМ) сотрудника Отдела производства	Несанкционированный доступ к базе данных с последующим разглашением (утечкой) информации о разработанных чертежах, являющихся государственной тайной

Таблица 4. Объекты воздействия и виды воздействия на них

6. Определение источников угроз безопасности информации

Определив объекты воздействия и виды воздействия на них, рассмотрим источники угроз безопасности информации, для этого определив цели реализации 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

Виды нарушителей	Возможные цели реализации угроз безопасности информации			Негативные последствия
	У1	У2	У3	
Специальные службы иностранных государств	-	-	+ (Нанесение ущерба государству в области обеспечения обороны, безопасности и правопорядка, дискредитация или дестабилизация деятельности отдельных органов государственной власти, получение конкурентных преимуществ на уровне государства	У3: Причинение ущерба жизни и здоровью людей. Снижение уровня дохода организации с государственным участием. Снижение показателей государственного оборонного заказа. Утечка информации ограниченного доступа.
Террористические, экстремистские группировки	+ (Угроза жизни граждан)	-	+ (Угроза жизни граждан, нанесение ущерба отдельным сферам	У1: Угроза жизни или здоровью. У3: Причинение ущерба жизни и

			деятельности или секторам экономики государства; дестабилизация деятельности органов государственной власти)	здоровью людей. Снижение уровня дохода организации с государственным участием. Снижение показателей государственного оборонного заказа. Утечка информации ограниченного доступа.
Преступные группы (криминальные структуры)	+ (Получение финансовой выгоды за счет продажи украденных персональных данных)	+ (Получение финансовой или иной материальной выгоды; желание самореализации (подтверждение статуса))	+ (Получение финансовой или иной материальной выгоды; желание самореализации (подтверждение статуса))	У1: Разглашение персональных данных граждан. У2: Недополучение ожидаемой (прогнозируемой) прибыли. Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. Нарушение деловой репутации и утрата доверия. Утечка конфиденциальной информации (коммерческой тайны, секретов производства). У3: Снижение уровня дохода организации с государственным участием. Утечка информации ограниченного доступа.
Отдельные физические лица (хакеры)	+ (Получение финансовой	+ (Получение финансовой или	+ (Получение финансовой или	У1:

	выгоды за счет продажи украденных персональных данных)	иной материальной выгоды; любопытство, желание самореализации (подтверждение статуса))	иной материальной выгоды; любопытство, желание самореализации (подтверждение статуса))	Разглашение персональных данных граждан. У2: Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. Нарушение деловой репутации и утрата доверия. Утечка конфиденциальной информации (коммерческой тайны, секретов производства). У3: Снижение уровня дохода организации с государственным участием. Утечка информации ограниченного доступа.
Конкурирующие организации	-	+ (Получение конкурентных преимуществ; получение финансовой или иной материальной выгоды)	+ (Получение конкурентных преимуществ)	У2: Недополучение ожидаемой (прогнозируемой) прибыли. Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций. Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. Потеря конкурентного преимущества. Нарушение деловой

				репутации и утрата доверия. Утечка конфиденциальной информации (коммерческой тайны, секретов производства). У3: Утечка информации ограниченного доступа.
Разработчики программных, программно-аппаратных средств	-	-	-	-
Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	+ (Получение финансовой выгоды за счет продажи украденных персональных данных)	+ (Получение финансовой выгоды за счет продажи украденных данных, представляющих коммерческую тайну или нанесения финансовых потерь; получение конкурентных преимуществ)	+ (Получение финансовой выгоды за счет продажи украденных данных, представляющих государственную тайну)	У1: Разглашение персональных данных граждан. У2: Потеря конкурентного преимущества. Нарушение деловой репутации и утрата доверия. Утечка конфиденциальной информации (коммерческой тайны, секретов производства). У3: Утечка информации ограниченного доступа.
Поставщики вычислительных услуг, услуг связи	-	-	-	-
Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	+ (Получение финансовой выгоды за счет продажи украденных персональных данных)	+ (Получение финансовой выгоды за счет продажи украденных данных, представляющих коммерческую	+ (Получение финансовой выгоды за счет продажи украденных данных, представляющих	У1: Разглашение персональных данных граждан. У2: Потеря конкурентного преимущества.

		тайну или нанесения финансовых потерь; получение конкурентных преимуществ)	государственную тайну)	Нарушение деловой репутации и утрата доверия. Утечка конфиденциальной информации (коммерческой тайны, секретов производства). У3: Утечка информации ограниченного доступа.
Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.)	+ (Получение финансовой выгоды за счет продажи украденных персональных данных; непреднамеренные, неосторожные или неквалифицированные действия)	+ (Получение финансовой выгоды за счет продажи украденных данных, представляющих коммерческую тайну или нанесения финансовых потерь; непреднамеренные, неосторожные или неквалифицированные действия)	+ (Получение финансовой выгоды за счет продажи украденных данных, представляющих государственную тайну; неосторожные или неквалифицированные действия)	У1: Разглашение персональных данных граждан. Угроза жизни или здоровью. У2: Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций. Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. Утечка конфиденциальной информации (коммерческой тайны, секретов производства). У3: Причинение ущерба жизни и здоровью людей. Утечка информации ограниченного доступа.
Авторизованные пользователи систем и сетей	+ (Получение финансовой	+ (Получение финансовой	+ (Получение финансовой	У1:

	выгоды за счет продажи украденных персональных данных; непреднамеренные, неосторожные или неквалифицированные действия)	выгоды за счет продажи украденных данных, представляющих коммерческую тайну или за счет снижения деловой репутации; любопытство или желание самореализации (подтверждение статуса); непреднамеренные, неосторожные или неквалифицированные действия)	выгоды за счет продажи украденных данных, представляющих государственную тайну)	Разглашение персональных данных граждан. Угроза жизни или здоровью. У2: Нарушение деловой репутации и утрата доверия. Потеря конкурентного преимущества. Утечка конфиденциальной информации (коммерческой тайны, секретов производства). У3: Утечка информации ограниченного доступа.
Системные администраторы и администраторы безопасности	+ (Получение финансовой выгоды за счет продажи украденных персональных данных; месть за ранее совершённые действия; непреднамеренные, неосторожные или неквалифицированные действия)	+ (Получение финансовой выгоды за счет продажи украденных данных, представляющих коммерческую тайну или за счет снижения деловой репутации; любопытство или желание самореализации (подтверждение статуса); непреднамеренные, неосторожные или неквалифицированные действия)	+ (Получение финансовой выгоды за счет продажи украденных данных, представляющих государственную тайну)	У1: Финансовый ущерб физическому лицу. Разглашение персональных данных граждан. Угроза жизни или здоровью. У2: Нарушение деловой репутации и утрата доверия. Потеря конкурентного преимущества. Утечка конфиденциальной информации (коммерческой тайны, секретов производства). У3: Утечка информации ограниченного доступа.

Бывшие работники (пользователи)	+ (Получение финансовой выгоды за счет продажи украденных персональных данных, месть за ранее совершённые действия)	+ (Получение финансовой выгоды за счет продажи украденных данных, представляющих коммерческую тайну или за счет снижения деловой репутации, месть за ранее совершённые действия)	+ (Получение финансовой выгоды за счет продажи украденных данных, представляющих государственную тайну, месть за ранее совершённые действия)	У1: Финансовый ущерб физическому лицу. Разглашение персональных данных граждан. У2: Недополучение ожидаемой (прогнозируемой) прибыли. Нарушение деловой репутации и утрата доверия. Утечка конфиденциальной информации (коммерческой тайны, секретов производства). У3: Снижение уровня дохода организации с государственным участием. Утечка информации ограниченного доступа.

Таблица 5. Цели реализации нарушителями угроз безопасности информации

Актуальные 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: Финансовый ущерб физическому лицу	Бывшие работники (пользователи)	Внешний	Н1
		Системные администраторы и администраторы безопасности	Внутренний	Н2
2	У1: Разглашение персональных данных граждан	Бывшие работники (пользователи)	Внешний	Н1
		Системные администраторы и администраторы безопасности	Внутренний	Н2

		Авторизованные пользователи систем и сетей	Внутренний	H1
		Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.)	Внутренний	H1
		Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	H2
		Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	H1
		Отдельные физические лица (хакеры)	Внешний	H1
		Преступные группы (криминальные структуры)	Внешний	H2
3	У1: Угроза жизни или здоровью	Системные администраторы и администраторы безопасности	Внутренний	H2
		Авторизованные пользователи систем и сетей	Внутренний	H1
		Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.)	Внутренний	H1

		Террористические, экстремистские группировки	Внешний	Н3
4	У2: Недополучение ожидаемой (прогнозируемой) прибыли	Бывшие работники (пользователи)	Внешний	Н1
		Конкурирующие организации		
		Преступные группы (криминальные структуры)	Внешний	Н2
5	У2: Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций	Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.)	Внутренний	Н1
		Конкурирующие организации	Внешний	Н2
6	У2: Необходимость дополнительных (незапланированных) затрат на восстановление деятельности	Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.)	Внутренний	Н1
		Конкурирующие организации	Внешний	Н2
		Отдельные физические лица (хакеры)	Внешний	Н1
		Преступные группы (криминальные структуры)	Внешний	Н2
7	У2: Нарушение деловой репутации и утрата доверия	Бывшие работники (пользователи)	Внешний	Н1
		Системные администраторы и администраторы безопасности	Внутренний	Н2
		Авторизованные пользователи систем и сетей	Внутренний	Н1
		Лица, привлекаемые для установки, настройки,	Внутренний	Н2

		испытаний, пусконаладочных и иных видов работ		
		Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	H1
		Конкурирующие организации	Внешний	H2
		Отдельные физические лица (хакеры)	Внешний	H1
		Преступные группы (криминальные структуры)	Внешний	H2
8	У2: Утечка конфиденциальной информации (коммерческой тайны, секретов производства)	Бывшие работники (пользователи)	Внешний	H1
		Системные администраторы и администраторы безопасности	Внутренний	H2
		Авторизованные пользователи систем и сетей	Внутренний	H1
		Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.)	Внутренний	H1
		Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	H2
		Лица, обеспечивающие поставку программных, программно-аппаратных средств,	Внешний	H1

		обеспечивающих систем		
		Конкурирующие организации	Внешний	Н2
		Отдельные физические лица (хакеры)	Внешний	Н1
		Преступные группы (криминальные структуры)	Внешний	Н2
9	У2: Потеря конкурентного преимущества	Системные администраторы и администраторы безопасности	Внутренний	Н2
		Авторизованные пользователи систем и сетей	Внутренний	Н1
		Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Н2
		Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	Н1
		Конкурирующие организации	Внешний	Н2
10	У3: Причинение ущерба жизни и здоровью людей	Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.)	Внутренний	Н1
		Террористические, экстремистские группировки	Внешний	Н3
		Специальные службы иностранных государств	Внешний	Н4

11	УЗ: Снижение уровня дохода организации с государственным участием	Бывшие работники (пользователи)	Внешний	Н1
		Отдельные физические лица (хакеры)	Внешний	Н1
		Преступные группы (криминальные структуры)	Внешний	Н2
		Террористические, экстремистские группировки	Внешний	Н3
		Специальные службы иностранных государств	Внешний	Н4
12	УЗ: Снижение показателей государственного оборонного заказа	Террористические, экстремистские группировки	Внешний	Н3
		Специальные службы иностранных государств	Внешний	Н4
13	УЗ: Утечка информации ограниченного доступа	Бывшие работники (пользователи)	Внешний	Н1
		Системные администраторы и администраторы безопасности	Внутренний	Н2
		Авторизованные пользователи систем и сетей	Внутренний	Н1
		Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.)	Внутренний	Н1
		Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Н2
		Лица, обеспечивающие поставку программных, программно-	Внешний	Н1

		аппаратных средств, обеспечивающих систем		
		Конкурирующие организации	Внешний	H2
		Отдельные физические лица (хакеры)	Внешний	H1
		Преступные группы (криминальные структуры)	Внешний	H2
		Террористические, экстремистские группировки	Внешний	H3
		Специальные службы иностранных государств	Внешний	H4

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

7. Определение способов реализации (возникновения) угроз безопасности информации

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
1	Специальные службы иностранных государств (H4)	Внешний	База данных информационной системы, содержащая список всех чертежей, текущих заказов и отчетов: Несанкционированный доступ к защищаемой информации, нарушение целостности (модификация), доступности (удаление), конфиденциальности (утечка); блокирование доступа к базе данных	Пользовательский интерфейс доступа к базе данных информационной системы	Получение доступа к базе данных через АРМ пользователя путем внедрения вредоносного программного обеспечения

			Автоматизированное рабочее место (АРМ) сотрудника отдела Руководства: Нарушение конфиденциальности (утечка) и целостности (модификация) информации, содержащейся на АРМ пользователя	Съемные машинные носители информации, подключаемые к АРМ пользователя	Внедрение вредоносного программного обеспечения
				Доступ через локальную вычислительную сеть организации	Внедрение вредоносного программного обеспечения
				Доступ через внешнюю сеть (Интернет)	Использование уязвимостей конфигурации доступа к внешней сети Внедрение вредоносного программного обеспечения в потоки обмена информацией (email)
			Автоматизированное рабочее место (АРМ) сотрудника Конструкторского бюро: Нарушение конфиденциальности (утечка) и целостности (модификация) информации, содержащейся на АРМ пользователя	Съемные машинные носители информации, подключаемые к АРМ пользователя	Внедрение вредоносного программного обеспечения
				Доступ через локальную вычислительную сеть организации	Внедрение вредоносного программного обеспечения
				Доступ через внешнюю сеть (Интернет)	Использование уязвимостей конфигурации доступа к внешней сети
			Автоматизированное рабочее место (АРМ) сотрудника Отдела производства: Нарушение конфиденциальности (утечка) и целостности (модификация)	Съемные машинные носители информации, подключаемые к АРМ пользователя	Внедрение вредоносного программного обеспечения
				Доступ через локальную вычислительную	Внедрение вредоносного программного обеспечения

			информации, содержащейся на АРМ пользователя	сеть организации	
2	Террористические, экстремистские группировки (Н3)	Внешний	База данных информационной системы, содержащая список всех чертежей, текущих заказов и отчетов: Несанкционированный доступ к защищаемой информации, нарушение целостности (модификация), доступности (удаление), конфиденциальности (утечка); блокирование доступа к базе данных	Пользовательский интерфейс доступа к базе данных информационной системы	Получение доступа к базе данных через АРМ пользователя путем внедрения вредоносного программного обеспечения
			Автоматизированное рабочее место (АРМ) сотрудника отдела Руководства: Нарушение конфиденциальности (утечка) и целостности (модификация) информации, содержащейся на АРМ пользователя	Съемные машинные носители информации, подключаемые к АРМ пользователя	Внедрение вредоносного программного обеспечения
				Доступ через локальную вычислительную сеть организации	Внедрение вредоносного программного обеспечения
				Доступ через внешнюю сеть (Интернет)	Использование уязвимостей конфигурации доступа к внешней сети Внедрение вредоносного программного обеспечения в потоки обмена информацией (email)
			Автоматизированное рабочее место (АРМ) сотрудника	Съемные машинные носители	Внедрение вредоносного

			Конструкторского бюро: Нарушение конфиденциальности (утечка) и целостности (модификация) информации, содержащейся на АРМ пользователя	информации, подключаемые к АРМ пользователя	программного обеспечения
				Доступ через локальную вычислительную сеть организации	Внедрение вредоносного программного обеспечения
				Доступ через внешнюю сеть (Интернет)	Использование уязвимостей конфигурации доступа к внешней сети
			Автоматизированное рабочее место (АРМ) сотрудника Отдела производства: Нарушение конфиденциальности (утечка) и целостности (модификация) информации, содержащейся на АРМ пользователя	Съемные машинные носители информации, подключаемые к АРМ пользователя	Внедрение вредоносного программного обеспечения
				Доступ через локальную вычислительную сеть организации	Внедрение вредоносного программного обеспечения
3	Преступные группы (криминальные структуры) (Н2)	Внешний	База данных информационной системы, содержащая конфиденциальную информацию о сотрудниках, список всех чертежей, текущих заказов и отчетов: Несанкционированный доступ к защищаемой информации, нарушение целостности (модификация), доступности (удаление), конфиденциальности (утечка); блокирование доступа к базе данных	Пользовательский интерфейс доступа к базе данных информационной системы	Получение доступа к базе данных через АРМ пользователя путем внедрения вредоносного программного обеспечения

			Автоматизированное рабочее место (АРМ) сотрудника отдела Руководства: Нарушение конфиденциальности (утечка) и целостности (модификация) информации, содержащейся на АРМ пользователя	Съемные машинные носители информации, подключаемые к АРМ пользователя	Внедрение вредоносного программного обеспечения
				Доступ через локальную вычислительную сеть организации	Внедрение вредоносного программного обеспечения
				Доступ через внешнюю сеть (Интернет)	Использование уязвимостей конфигурации доступа к внешней сети Внедрение вредоносного программного обеспечения в потоки обмена информацией (email)
			Автоматизированное рабочее место (АРМ) сотрудника Конструкторского бюро: Нарушение конфиденциальности (утечка) и целостности (модификация) информации, содержащейся на АРМ пользователя	Съемные машинные носители информации, подключаемые к АРМ пользователя	Внедрение вредоносного программного обеспечения
				Доступ через локальную вычислительную сеть организации	Внедрение вредоносного программного обеспечения
				Доступ через внешнюю сеть (Интернет)	Использование уязвимостей конфигурации доступа к внешней сети
			Автоматизированное рабочее место (АРМ) сотрудника Отдела производства: Нарушение конфиденциальности (утечка) и целостности (модификация)	Съемные машинные носители информации, подключаемые к АРМ пользователя	Внедрение вредоносного программного обеспечения
				Доступ через локальную вычислительную	Внедрение вредоносного программного обеспечения

			информации, содержащейся на АРМ пользователя	сеть организации	
4	Отдельные физические лица (хакеры) (H1)	Внешний	База данных информационной системы, содержащая конфиденциальную информацию о сотрудниках, список всех чертежей, текущих заказов и отчетов: Несанкционированный доступ к защищаемой информации, нарушение целостности (модификация), доступности (удаление), конфиденциальности (утечка); блокирование доступа к базе данных	Пользовательский интерфейс доступа к базе данных информационной системы	Получение доступа к базе данных через АРМ пользователя путем внедрения вредоносного программного обеспечения
			Автоматизированное рабочее место (АРМ) сотрудника отдела Руководства: Нарушение конфиденциальности (утечка) и целостности (модификация) информации, содержащейся на АРМ пользователя	Съемные машинные носители информации, подключаемые к АРМ пользователя	Внедрение вредоносного программного обеспечения
				Доступ через локальную вычислительную сеть организации	Внедрение вредоносного программного обеспечения
				Доступ через внешнюю сеть (Интернет)	Использование уязвимостей конфигурации доступа к внешней сети Внедрение вредоносного программного обеспечения в потоки обмена информацией (email)

			Автоматизированное рабочее место (АРМ) сотрудника Конструкторского бюро: Нарушение конфиденциальности (утечка) и целостности (модификация) информации, содержащейся на АРМ пользователя	Съемные машинные носители информации, подключаемые к АРМ пользователя	Внедрение вредоносного программного обеспечения
				Доступ через локальную вычислительную сеть организации	Внедрение вредоносного программного обеспечения
				Доступ через внешнюю сеть (Интернет)	Использование уязвимостей конфигурации доступа к внешней сети
			Автоматизированное рабочее место (АРМ) сотрудника Отдела производства: Нарушение конфиденциальности (утечка) и целостности (модификация) информации, содержащейся на АРМ пользователя	Съемные машинные носители информации, подключаемые к АРМ пользователя	Внедрение вредоносного программного обеспечения
				Доступ через локальную вычислительную сеть организации	Внедрение вредоносного программного обеспечения
5	Конкурирующие организации (Н2)	Внешний	База данных информационной системы, содержащая конфиденциальную информацию о сотрудниках, список всех чертежей, текущих заказов и отчетов: Несанкционированный доступ к защищаемой информации, нарушение целостности (модификация), доступности (удаление), конфиденциальности (утечка); блокирование	Пользовательский интерфейс доступа к базе данных информационной системы	Получение доступа к базе данных через АРМ пользователя путем внедрения вредоносного программного обеспечения

			доступа к базе данных		
			Автоматизированное рабочее место (АРМ) сотрудника отдела Руководства: Нарушение конфиденциальности (утечка) и целостности (модификация) информации, содержащейся на АРМ пользователя	Съемные машинные носители информации, подключаемые к АРМ пользователя	Внедрение вредоносного программного обеспечения
				Доступ через локальную вычислительную сеть организации	Внедрение вредоносного программного обеспечения
				Доступ через внешнюю сеть (Интернет)	Использование уязвимостей конфигурации доступа к внешней сети Внедрение вредоносного программного обеспечения в потоки обмена информацией (email)
			Автоматизированное рабочее место (АРМ) сотрудника Конструкторского бюро: Нарушение конфиденциальности (утечка) и целостности (модификация) информации, содержащейся на АРМ пользователя	Съемные машинные носители информации, подключаемые к АРМ пользователя	Внедрение вредоносного программного обеспечения
				Доступ через локальную вычислительную сеть организации	Внедрение вредоносного программного обеспечения
				Доступ через внешнюю сеть (Интернет)	Использование уязвимостей конфигурации доступа к внешней сети
			Автоматизированное рабочее место (АРМ) сотрудника Отдела производства: Нарушение конфиденциальности (утечка) и	Съемные машинные носители информации, подключаемые к АРМ пользователя	Внедрение вредоносного программного обеспечения
				Доступ через локальную	Внедрение вредоносного

			целостности (модификация) информации, содержащейся на АРМ пользователя	вычислительную сеть организации	программного обеспечения
6	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем (Н1)	Внешний	База данных информационной системы, содержащая конфиденциальную информацию о сотрудниках, список всех чертежей, текущих заказов и отчетов: Несанкционированный доступ к защищаемой информации, нарушение целостности (модификация), доступности (удаление), конфиденциальности (утечка); блокирование доступа к базе данных	Пользовательский интерфейс доступа к базе данных информационной системы	Получение доступа к базе данных через АРМ пользователя путем внедрения вредоносного программного обеспечения
				Программные/программно-аппаратные средства обеспечивающих систем	Использование уязвимостей поставляемых средств
			Автоматизированное рабочее место (АРМ) сотрудника отдела Руководства: Нарушение конфиденциальности (утечка) и целостности (модификация) информации, содержащейся на АРМ пользователя	Программные/программно-аппаратные средства обеспечивающих систем	Использование уязвимостей поставляемых средств
			Автоматизированное рабочее место (АРМ) сотрудника Конструкторского бюро: Нарушение конфиденциальности (утечка) и целостности (модификация)	Программные/программно-аппаратные средства обеспечивающих систем	Использование уязвимостей поставляемых средств

			информации, содержащейся на АРМ пользователя		
			Автоматизированное рабочее место (АРМ) сотрудника Отдела производства: Нарушение конфиденциальности и (утечка) и целостности (модификация) информации, содержащейся на АРМ пользователя	Программные/программно-аппаратные средства обеспечивающих систем	Использование уязвимостей поставляемых средств
7	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ (Н2)	Внутренний	База данных информационной системы, содержащая конфиденциальную информацию о сотрудниках, список всех чертежей, текущих заказов и отчетов: Несанкционированный доступ к защищаемой информации, нарушение целостности (модификация), доступности (удаление), конфиденциальности и (утечка); блокирование доступа к базе данных	Пользовательский интерфейс доступа к базе данных информационной системы	Получение непосредственного доступа к базе данных через АРМ пользователя в ходе проведения производимых работ
				Локальная вычислительная сеть организации	Ошибочные действия в ходе проведения работ над сервером с базой данных
			Автоматизированное рабочее место (АРМ) сотрудника отдела Руководства: Непреднамеренные /преднамеренные действия, повлекшие нарушение конфиденциальности и (утечка) и	Локальная вычислительная сеть организации	Ошибочные действия в ходе проведения работ над АРМ сотрудника отдела Руководства
				Съемные машинные носители информации,	Внедрение вредоносного программного обеспечения

			целостности (модификация) информации, содержащейся на АРМ пользователя	подключаемые к АРМ пользователя	
			Автоматизированное рабочее место (АРМ) сотрудника Конструкторского бюро: Непреднамеренные /преднамеренные действия, повлекшие нарушение конфиденциальности (утечка) и целостности (модификация) информации, содержащейся на АРМ пользователя	Локальная вычислительная сеть организации	Ошибочные действия в ходе проведения работ над АРМ сотрудника Конструкторского бюро
				Съемные машинные носители информации, подключаемые к АРМ пользователя	Внедрение вредоносного программного обеспечения
			Автоматизированное рабочее место (АРМ) сотрудника Отдела производства: Непреднамеренные /преднамеренные действия, повлекшие нарушение конфиденциальности (утечка) и целостности (модификация) информации, содержащейся на АРМ пользователя	Локальная вычислительная сеть организации	Ошибочные действия в ходе проведения работ над АРМ сотрудника Отдела производства
				Съемные машинные носители информации, подключаемые к АРМ пользователя	Внедрение вредоносного программного обеспечения
8	Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.) (Н1)	Внутренний	База данных информационной системы, содержащая конфиденциальную информацию о сотрудниках, список всех чертежей, текущих заказов и отчетов: Несанкционированный доступ к	Локальная вычислительная сеть организации	Проникновение в помещение с сервером с базой данных и причинение физического ущерба

			защищаемой информации, нарушение целостности (модификация), доступности (удаление), конфиденциальности (утечка); блокирование доступа к базе данных		
			Автоматизированное рабочее место (АРМ) сотрудника отдела Руководства: Нарушение конфиденциальности (утечка) и целостности (модификация) информации, содержащейся на АРМ пользователя; Нарушение функционирования (работоспособности) средств обработки и хранения информации	Съемные машинные носители информации, подключаемые к АРМ пользователя	Внедрение вредоносного программного обеспечения
				Локальная вычислительная сеть организации	Проникновение в помещение с АРМ пользователя и причинение физического ущерба
			Автоматизированное рабочее место (АРМ) сотрудника Конструкторского бюро: Нарушение конфиденциальности (утечка) и целостности (модификация) информации, содержащейся на АРМ пользователя; Нарушение функционирования (работоспособности) средств обработки и хранения информации	Съемные машинные носители информации, подключаемые к АРМ пользователя	Внедрение вредоносного программного обеспечения
				Локальная вычислительная сеть организации	Проникновение в помещение с АРМ пользователя и причинение физического ущерба
			Автоматизированное рабочее место (АРМ) сотрудника	Съемные машинные носители	Внедрение вредоносного

			Отдела производства: Нарушение конфиденциальности (утечка) и целостности (модификация) информации, содержащейся на АРМ пользователя; Нарушение функционирования (работоспособности) средств обработки и хранения информации	информации, подключаемые к АРМ пользователя	программного обеспечения
				Локальная вычислительная сеть организации	Проникновение в помещение с АРМ пользователя и причинение физического ущерба
9	Авторизованные пользователи систем и сетей (Н1)	Внутренний	База данных информационной системы, содержащая конфиденциальную информацию о сотрудниках, список всех чертежей, текущих заказов и отчетов: Несанкционированный доступ к защищаемой информации, нарушение целостности (модификация), доступности (удаление), конфиденциальности (утечка); блокирование доступа к базе данных	Пользовательский интерфейс доступа к базе данных информационной системы	Использование уязвимостей конфигурации системы управления базой данных Внедрение вредоносного программного обеспечения
			Автоматизированное рабочее место (АРМ) сотрудника отдела Руководства: Непреднамеренные действия, повлекшие нарушение конфиденциальности (утечка) и целостности	Локальная вычислительная сеть организации	Ошибочные действия в ходе работы с собственным АРМ (для сотрудников отдела Руководства)

			(модификация) информации, содержащейся на АРМ пользователя		
			Автоматизированное рабочее место (АРМ) сотрудника Конструкторского бюро: Непреднамеренные действия, повлекшие нарушение конфиденциальности (утечка) и целостности (модификация) информации, содержащейся на АРМ пользователя	Локальная вычислительная сеть организации	Ошибочные действия в ходе работы с собственным АРМ (для сотрудников Конструкторского бюро)
			Автоматизированное рабочее место (АРМ) сотрудника Отдела производства: Непреднамеренные действия, повлекшие нарушение конфиденциальности (утечка) и целостности (модификация) информации, содержащейся на АРМ пользователя	Локальная вычислительная сеть организации	Ошибочные действия в ходе работы с собственным АРМ (для сотрудников Отдела производства)
10	Системные администраторы и администраторы безопасности (H2)	Внутренний	База данных информационной системы, содержащая конфиденциальную информацию о сотрудниках, список всех чертежей, текущих заказов и отчетов: Несанкционированный доступ к защищаемой информации, нарушение	Пользовательский интерфейс доступа к базе данных информационной системы	Использование уязвимостей конфигурации системы управления базой данных Внедрение вредоносного программного обеспечения

			целостности (модификация), доступности (удаление), конфиденциальности (утечка); блокирование доступа к базе данных		
			Автоматизированное рабочее место (АРМ) сотрудника отдела Руководства: Непреднамеренные /преднамеренные действия, повлекшие нарушение конфиденциальности (утечка) и целостности (модификация) информации, содержащейся на АРМ пользователя	Локальная вычислительная сеть организации	Ошибочные действия в ходе настройки локальной сети Внедрение и использование уязвимостей конфигурации локальной сети
			Автоматизированное рабочее место (АРМ) сотрудника отдела Бухгалтерии: Непреднамеренные /преднамеренные действия, повлекшие нарушение конфиденциальности (утечка) и целостности (модификация) информации, содержащейся на АРМ пользователя	Локальная вычислительная сеть организации	Ошибочные действия в ходе настройки локальной сети Внедрение и использование уязвимостей конфигурации локальной сети
			Автоматизированное рабочее место (АРМ) сотрудника Конструкторского бюро: Непреднамеренные /преднамеренные действия, повлекшие нарушение	Локальная вычислительная сеть организации	Ошибочные действия в ходе настройки локальной сети Внедрение и использование уязвимостей конфигурации локальной сети

			конфиденциальности (утечка) и целостности (модификация) информации, содержащейся на АРМ пользователя		
			Автоматизированное рабочее место (АРМ) сотрудника Отдела производства: Непреднамеренные /преднамеренные действия, повлекшие нарушение конфиденциальности (утечка) и целостности (модификация) информации, содержащейся на АРМ пользователя	Локальная вычислительная сеть организации	Ошибочные действия в ходе настройки локальной сети Внедрение и использование уязвимостей конфигурации локальной сети
11	Бывшие работники (пользователи) (Н1)	Внешний	База данных информационной системы, содержащая конфиденциальную информацию о сотрудниках, список всех чертежей, текущих заказов и отчетов: Несанкционированный доступ к защищаемой информации, нарушение целостности (модификация), доступности (удаление), конфиденциальности (утечка); блокирование доступа к базе данных	Пользовательский интерфейс доступа к базе данных информационной системы	Получение доступа к базе данных через АРМ пользователя путем внедрения вредоносного программного обеспечения
			Автоматизированное рабочее место (АРМ) сотрудника отдела Руководства:	Съемные машинные носители информации,	Внедрение вредоносного программного обеспечения

			Нарушение конфиденциальности (утечка) и целостности (модификация) информации, содержащейся на АРМ пользователя	подключаемые к АРМ пользователя	
				Доступ через локальную вычислительную сеть организации	Внедрение вредоносного программного обеспечения
				Доступ через внешнюю сеть (Интернет)	Использование уязвимостей конфигурации доступа к внешней сети Внедрение вредоносного программного обеспечения в потоки обмена информацией (email)
			Автоматизированное рабочее место (АРМ) сотрудника отдела Бухгалтерии: Нарушение конфиденциальности (утечка) и целостности (модификация) информации, содержащейся на АРМ пользователя	Съемные машинные носители информации, подключаемые к АРМ пользователя	Внедрение вредоносного программного обеспечения
				Доступ через локальную вычислительную сеть организации	Внедрение вредоносного программного обеспечения
				Доступ через внешнюю сеть (Интернет)	Использование уязвимостей конфигурации доступа к внешней сети
			Автоматизированное рабочее место (АРМ) сотрудника Конструкторского бюро: Нарушение конфиденциальности (утечка) и целостности (модификация) информации, содержащейся на АРМ пользователя	Съемные машинные носители информации, подключаемые к АРМ пользователя	Внедрение вредоносного программного обеспечения
				Доступ через локальную вычислительную сеть организации	Внедрение вредоносного программного обеспечения
				Доступ через внешнюю сеть (Интернет)	Использование уязвимостей конфигурации

					доступа к внешней сети
			Автоматизированное рабочее место (АРМ) сотрудника Отдела производства: Нарушение конфиденциальности (утечка) и целостности (модификация) информации, содержащейся на АРМ пользователя	Съемные машинные носители информации, подключаемые к АРМ пользователя	Внедрение вредоносного программного обеспечения
				Доступ через локальную вычислительную сеть организации	Внедрение вредоносного программного обеспечения

Таблица 7. Способы реализации УБИ

8. Определение угроз безопасности информации

$УБИ_1$ = [Бывший сотрудник отдела разработки (Бывшие работники (пользователи) (Н1)); АРМ сотрудника отдела Бухгалтерии; Использование уязвимостей конфигурации доступа к внешней сети; Разглашение платежных данных сотрудников (Разглашение персональных данных граждан);]

$УБИ_2$ = [Системный администратор (Системные администраторы и администраторы безопасности (Н2)); АРМ сотрудника отдела Бухгалтерии; Ошибочные действия в ходе настройки локальной сети; Нарушение автозаполнения платежных реквизитов сотрудников (Финансовый ущерб физическому лицу);]

$УБИ_3$ = [Конкурирующая организация (Конкурирующие организации (Н2)); АРМ сотрудника Отдела производства; Внедрение вредоносного программного обеспечения через внешний носитель информации сотрудника; Кража чертежей и отчетов;]

$УБИ_4$ = [Неквалифицированный сотрудник Отдела производства (Авторизованные пользователи систем и сетей (Н1)); АРМ сотрудника Отдела производства; Ошибочные действия в ходе работы с собственным АРМ (для сотрудников Отдела производства); Потеря части данных в отчетах;]

$УБИ_5$ = [Уборщица (Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.) (Н1)); АРМ сотрудника Конструкторского бюро; Внедрение вредоносного программного обеспечения через внешний носитель информации сотрудника; Разглашение информации, проходящей через АРМ пользователя (Утечка конфиденциальной информации);]

$УБИ_6$ = [Студент IT специальности (Отдельные физические лица (хакеры) (Н1)); АРМ сотрудника Конструкторского бюро; Использование уязвимостей конфигурации доступа к внешней сети, несанкционированный доступ к информации, проходящей через АРМ пользователя; Модификация элементов конструкций в чертежах;]

$УБИ_7$ = [Преступная группа (Преступные группы (криминальные структуры) (Н2)); АРМ сотрудника отдела Руководства; Внедрение вредоносного программного обеспечения через внешние потоки

обмена информацией (email); Публикация в открытом доступе сведений о текущих заказах и отчетов о ходе их выполнения;]

$УБИ_8$ = [Мастер-наладчик программного обеспечения (Лицо, привлекаемое для установки, настройки, испытаний (H2)); АРМ сотрудника отдела Руководства; Внедрение вредоносного программного обеспечения - шифровальщика; Шифрование (модификация) информации, исходящей из АРМ пользователя;]

$УБИ_9$ = [Специальные службы иностранных государств (H4); Сервер с базой данных информационной системы; Получение доступа к базе данных через АРМ пользователя путем внедрения вредоносного программного обеспечения; Копирование (кража) с последующим удалением всей информации из базы данных;]

$УБИ_{10}$ = [Электрик (Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.) (H1)); Сервер с базой данных информационной системы; Проникновение в серверную и обесточивание оборудования; Блокирование доступа к базе данных;]

$УБИ_{11}$ = [Террористическая организация (Террористические, экстремистские группировки (H3)); Сервер с базой данных информационной системы; Получение доступа к базе данных через АРМ пользователя путем внедрения вредоносного программного обеспечения; Модификация всей хранящейся информации;]

9. Определение перечня актуальных угроз

$УБИ_1$ = [Бывший сотрудник отдела разработки (Бывшие работники (пользователи) (H1)); АРМ сотрудника отдела Бухгалтерии; Использование уязвимостей конфигурации доступа к внешней сети; Разглашение платежных данных сотрудников (Разглашение персональных данных граждан);]

Сценарий реализации:

→ T1: Сбор информации о системах и сетях:

T1.1. Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций

T1.2. Сбор информации о подключенных к публичным системам и сетям устройствах и их службах при помощи поисковых систем, включая сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений.

→ T2: Получение первоначального доступа к компонентам систем и сетей:

T2.3. Эксплуатация уязвимостей сетевого оборудования и средств защиты вычислительных сетей для получения доступа к компонентам систем и сетей при удаленной атаке.

T2.4. Использование ошибок конфигурации сетевого оборудования и средств защиты, в том числе слабых паролей и паролей по умолчанию, для получения доступа к компонентам систем и сетей при удаленной атаке

T2.10. Несанкционированный доступ путем подбора учетных данных сотрудника или легитимного пользователя (методами прямого перебора, словарных атак, паролей

производителей по умолчанию, использования одинаковых паролей для разных учетных записей, применения «радужных» таблиц или другими)

→ Т10: Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям:

Т10.1. Несанкционированный доступ к информации в памяти системы, файловой системе, базах данных, репозиториях, в программных модулях и прошивках

→ $УБИ_1$ актуальна

$УБИ_2$ = [Системный администратор (Системные администраторы и администраторы безопасности (Н2)); АРМ сотрудника отдела Бухгалтерии; Ошибочные действия в ходе настройки локальной сети; Нарушение автозаполнения платежных реквизитов сотрудников (Финансовый ущерб физическому лицу);]

Сценарий реализации:

→ Т10: Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям:

Т10.3. Несанкционированное воздействие на программные модули прикладного программного обеспечения

Т10.7. Подмена информации (например, платежных реквизитов) в памяти или информации, хранимой в виде файлов, информации в базах данных и репозиториях, информации на неразмеченных областях дисков и сменных носителей

→ $УБИ_2$ актуальна

$УБИ_3$ = [Конкурирующая организация (Конкурирующие организации (Н2)); АРМ сотрудника Отдела производства; Внедрение вредоносного программного обеспечения через внешний носитель информации сотрудника; Кража чертежей и отчетов;]

Сценарий реализации:

→ Т1: Сбор информации о системах и сетях:

Т1.1. Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций

Т1.11. Сбор информации о пользователях, устройствах, приложениях, внутренней информации о компонентах систем и сетей путем применения социальной инженерии, в том числе фишинга

→ Т2: Получение первоначального доступа к компонентам систем и сетей:

Т2.7. Использование в системе внешних носителей информации, которые могли подключаться к другим системам и быть заражены вредоносным программным обеспечением.

В том числе дарение, подмена или подлог носителей информации и внешних устройств, содержащих вредоносное программное обеспечение или предназначенных для реализации вредоносных функций.

→ Т3: Внедрение и исполнение вредоносного программного обеспечения в системах и сетях:

Т3.6. Автоматическое создание вредоносных скриптов при помощи доступного инструментария от имени пользователя в системе с использованием его учетных данных

Т3.10. Подмена дистрибутивов (установочных комплектов) программ на носителях информации или общих сетевых ресурсах

→ Т4: Закрепление (сохранение доступа) в системе или сети:

Т4.3. Скрытая установка и запуск средств удаленного доступа и управления операционной системы.

Внесение изменений в конфигурацию и состав программных и программно-аппаратных средств атакуемой системы или сети, вследствие чего становится возможен многократный запуск вредоносного кода

→ Т5: Управление вредоносным программным обеспечением и (или) компонентами, к которым ранее был получен доступ:

Т5.3. Коммуникация с внешними серверами управления через хорошо известные порты на этих серверах, разрешенные на межсетевом экране (SMTP/25, HTTP/80, HTTPS/443 и др.)

Т5.4. Коммуникация с внешними серверами управления через нестандартные порты на этих серверах, что в некоторых случаях позволяет эксплуатировать уязвимости средств сетевой фильтрации для обхода этих средств

$УБИ_3$ неактуальна, *так как АРМ сотрудника Отдела производства не имеет доступа к внешней сети (Интернет), а значит использование средств удаленного доступа и управления операционной системы АРМ невозможно.*

$УБИ_4$ = [Неквалифицированный сотрудник Отдела производства (Авторизованные пользователи систем и сетей (Н1)); АРМ сотрудника Отдела производства; Ошибочные действия в ходе работы с собственным АРМ (для сотрудников Отдела производства); Потеря части данных в отчетах;]

Сценарий реализации:

→ Т10: Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям:

Т10.8. Уничтожение информации, включая информацию, хранимую в виде файлов, информацию в базах данных и репозиториях, информацию на неразмеченных областях дисков и сменных носителей

→ $УБИ_4$ актуальна

$УБИ_5$ = [Уборщица (Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.) (Н1)); АРМ сотрудника Конструкторского бюро; Внедрение вредоносного программного обеспечения через внешний

носитель информации сотрудника; Разглашение информации, проходящей через АРМ пользователя (Утечка конфиденциальной информации);]

Сценарий реализации:

→ T1: Сбор информации о системах и сетях:

T1.1. Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций

T1.11. Сбор информации о пользователях, устройствах, приложениях, внутренней информации о компонентах систем и сетей путем применения социальной инженерии, в том числе фишинга

→ T2: Получение первоначального доступа к компонентам систем и сетей:

T2.7. Использование в системе внешних носителей информации, которые могли подключаться к другим системам и быть заражены вредоносным программным обеспечением.

В том числе дарение, подмена или подлог носителей информации и внешних устройств, содержащих вредоносное программное обеспечение или предназначенных для реализации вредоносных функций.

T2.8. Использование методов социальной инженерии, в том числе фишинга, для получения прав доступа к компонентам системы

T2.10. Несанкционированный доступ путем подбора учетных данных сотрудника или легитимного пользователя (методами прямого перебора, словарных атак, паролей производителей по умолчанию, использования одинаковых паролей для разных учетных записей, применения «радужных» таблиц или другими)

T2.11. Несанкционированный доступ путем компрометации учетных данных сотрудника организации, в том числе через компрометацию многократно используемого в различных системах пароля (для личных или служебных нужд)

→ T3: Внедрение и исполнение вредоносного программного обеспечения в системах и сетях:

T3.1. Автоматический запуск скриптов и исполняемых файлов в системе с использованием пользовательских или системных учетных данных, в том числе с использованием методов социальной инженерии

T3.7. Подмена файлов легитимных программ и библиотек непосредственно в системе.

→ T5: Управление вредоносным программным обеспечением и (или) компонентами, к которым ранее был получен доступ

T5.5. Управление через съемные носители, в частности, передача команд управления между скомпрометированными изолированной системой и подключенной к Интернет системой через носители информации, используемые на обеих системах

T5.A. Управление с использованием полученных ранее прав доступа непосредственно в системе

→ T10: Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям:

Т10.1. Несанкционированный доступ к информации в памяти системы, файловой системе, базах данных, репозиториях, в программных модулях и прошивках

$УБИ_5$ актуальна

$УБИ_6$ = [Студент IT специальности (Отдельные физические лица (хакеры) (H1)); АРМ сотрудника Конструкторского бюро; Использование уязвимостей конфигурации доступа к внешней сети, несанкционированный доступ к информации, проходящей через АРМ пользователя; Модификация элементов конструкций в чертежах;]

Сценарий реализации:

→ Т1: Сбор информации о системах и сетях:

Т1.1. Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций

Т1.2. Сбор информации о подключенных к публичным системам и сетям устройствах и их службах при помощи поисковых систем, включая сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений.

→ Т2: Получение первоначального доступа к компонентам систем и сетей:

Т2.3. Эксплуатация уязвимостей сетевого оборудования и средств защиты вычислительных сетей для получения доступа к компонентам систем и сетей при удаленной атаке.

Т2.4. Использование ошибок конфигурации сетевого оборудования и средств защиты, в том числе слабых паролей и паролей по умолчанию, для получения доступа к компонентам систем и сетей при удаленной атаке

Т2.10. Несанкционированный доступ путем подбора учетных данных сотрудника или легитимного пользователя (методами прямого перебора, словарных атак, паролей производителей по умолчанию, использования одинаковых паролей для разных учетных записей, применения «радужных» таблиц или другими)

→ Т10: Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям:

Т10.1. Несанкционированный доступ к информации в памяти системы, файловой системе, базах данных, репозиториях, в программных модулях и прошивках

Т10.7. Подмена информации в памяти или информации, хранимой в виде файлов, информации в базах данных и репозиториях, информации на неразмеченных областях дисков и сменных носителей

Т10.9. Добавление информации

→ $УБИ_6$ актуальна

$УБИ_7$ = [Преступная группа (Преступные группы (криминальные структуры) (H2)); АРМ сотрудника отдела Руководства; Внедрение вредоносного программного обеспечения через внешние потоки обмена информацией (email); Публикация в открытом доступе сведений о текущих заказах и отчетов о ходе их выполнения;]

Сценарий реализации:

→ T1: Сбор информации о системах и сетях:

T1.1. Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций

T1.8. Сбор информации о пользователе при посещении им веб-сайта, в том числе с использованием уязвимостей программы браузера и надстраиваемых модулей браузера

T1.11. Сбор информации о пользователях, устройствах, приложениях, внутренней информации о компонентах систем и сетей путем применения социальной инженерии, в том числе фишинга

→ T2: Получение первоначального доступа к компонентам систем и сетей:

T2.8. Использование методов социальной инженерии, в том числе фишинга, для получения прав доступа к компонентам системы

T2.11. Несанкционированный доступ путем компрометации учетных данных сотрудника организации, в том числе через компрометацию многократно используемого в различных системах пароля (для личных или служебных нужд)

→ T3: Внедрение и исполнение вредоносного программного обеспечения в системах и сетях:

T3.1. Автоматический запуск скриптов и исполняемых файлов в системе с использованием пользовательских или системных учетных данных, в том числе с использованием методов социальной инженерии

T3.3. Автоматическая загрузка вредоносного кода с удаленного сайта или ресурса с последующим запуском на выполнение

→ T4: Закрепление (сохранение доступа) в системе или сети:

T4.3. Скрытая установка и запуск средств удаленного доступа и управления операционной системы.

Внесение изменений в конфигурацию и состав программных и программно-аппаратных средств атакуемой системы или сети, вследствие чего становится возможен многократный запуск вредоносного кода

→ T5: Управление вредоносным программным обеспечением и (или) компонентами, к которым ранее был получен доступ:

T5.2. Использование штатных средств удаленного доступа и управления операционной системы

T5.3. Коммуникация с внешними серверами управления через хорошо известные порты на этих серверах, разрешенные на межсетевом экране (SMTP/25, HTTP/80, HTTPS/443 и др.)

T5.7. Туннелирование трафика управления через VPN

→ T7: Сокрытие действий и применяемых при этом средств от обнаружения:

T7.2. Очистка/затирание истории команд и журналов регистрации, перенаправление записей в журналы регистрации, переполнение истории команд и журналов регистрации, затруднение доступа к журналам регистрации для авторизованных пользователей

→ Т9: Сбор и вывод из системы или сети информации, необходимой для дальнейших действий при реализации угроз безопасности информации или реализации новых угроз:

Т9.2. Доступ к системе для сбора информации и вывод информации через использование штатных средств удаленного доступа и управления операционной системы

Т9.3. Вывод информации на хорошо известные порты на внешних серверах, разрешенные на межсетевом экране (SMTP/25, HTTP/80, HTTPS/443 и др.)

Т9.8. Туннелирование трафика передачи данных через VPN

→ Т10: Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям:

Т10.1. Несанкционированный доступ к информации в памяти системы, файловой системе, базах данных, репозиториях, в программных модулях и прошивках

$УБИ_7$ актуальна

$УБИ_8$ = [Мастер-наладчик программного обеспечения (Лицо, привлекаемое для установки, настройки, испытаний (Н2)); АРМ сотрудника отдела Руководства; Внедрение вредоносного программного обеспечения - шифровальщика; Шифрование (модификация) информации, исходящей из АРМ пользователя;]

Сценарий реализации:

→ Т1: Сбор информации о системах и сетях:

Т1.1. Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций

Т1.4. Направленное сканирование при помощи специализированного программного обеспечения подключенных к сети устройств с целью идентификации сетевых сервисов, типов и версий программного обеспечения этих сервисов, а также с целью получения конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений.

Т1.11. Сбор информации о пользователях, устройствах, приложениях, внутренней информации о компонентах систем и сетей путем применения социальной инженерии, в том числе фишинга

→ Т2: Получение первоначального доступа к компонентам систем и сетей:

Т2.7. Использование в системе внешних носителей информации, которые могли подключаться к другим системам и быть заражены вредоносным программным обеспечением.

В том числе дарение, подмена или подлог носителей информации и внешних устройств, содержащих вредоносное программное обеспечение или предназначенных для реализации вредоносных функций.

Т2.8. Использование методов социальной инженерии, в том числе фишинга, для получения прав доступа к компонентам системы

Т2.10. Несанкционированный доступ путем подбора учетных данных сотрудника или легитимного пользователя (методами прямого перебора, словарных атак, паролей производителей по умолчанию, использования одинаковых паролей для разных учетных записей, применения «радужных» таблиц или другими)

Т2.11. Несанкционированный доступ путем компрометации учетных данных сотрудника организации, в том числе через компрометацию многократно используемого в различных системах пароля (для личных или служебных нужд)

→ Т3: Внедрение и исполнение вредоносного программного обеспечения в системах и сетях:

Т3.1. Автоматический запуск скриптов и исполняемых файлов в системе с использованием пользовательских или системных учетных данных, в том числе с использованием методов социальной инженерии

Т3.15. Планирование запуска вредоносных программ через планировщиков задач в операционной системе, а также с использованием механизмов планирования выполнения в удаленной системе через удаленный вызов процедур.

→ Т7: Сокрытие действий и применяемых при этом средств от обнаружения:

Т7.4. Отключение средств защиты от угроз информационной безопасности, в том числе средств антивирусной защиты, механизмов аудита, консолей оператора мониторинга и средств защиты других типов

→ Т10: Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям:

Т10.7. Подмена информации в памяти или информации, хранимой в виде файлов, информации в базах данных и репозиториях, информации на неразмеченных областях дисков и сменных носителей

$УБИ_8$ актуальна

$УБИ_9$ = [Специальные службы иностранных государств (Н4); Сервер с базой данных информационной системы; Получение доступа к базе данных через АРМ пользователя путем внедрения вредоносного программного обеспечения; Копирование (кража) с последующим удалением всей информации из базы данных;]

Сценарий реализации:

→ Т1: Сбор информации о системах и сетях:

Т1.1. Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций

Т1.4. Направленное сканирование при помощи специализированного программного обеспечения подключенных к сети устройств с целью идентификации сетевых сервисов, типов и версий программного обеспечения этих сервисов, а также с целью получения конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений.

T1.11. Сбор информации о пользователях, устройствах, приложениях, внутренней информации о компонентах систем и сетей путем применения социальной инженерии, в том числе фишинга

T1.12. Сбор личной идентификационной информации (идентификаторы пользователей, устройств, информация об идентификации пользователей сервисами, приложениями, средствами удаленного доступа), в том числе сбор украденных личных данных сотрудников и подрядчиков на случай, если сотрудники/подрядчики используют одни и те же пароли на работе и за ее пределами

T1.15. Поиск и покупка баз данных идентификационной информации, скомпрометированых паролей и ключей на специализированных нелегальных площадках

→ T2: Получение первоначального доступа к компонентам систем и сетей:

T2.3. Эксплуатация уязвимостей сетевого оборудования и средств защиты вычислительных сетей для получения доступа к компонентам систем и сетей при удаленной атаке.

T2.4. Использование ошибок конфигурации сетевого оборудования и средств защиты, в том числе слабых паролей и паролей по умолчанию, для получения доступа к компонентам систем и сетей при удаленной атаке

T2.7. Использование в системе внешних носителей информации, которые могли подключаться к другим системам и быть заражены вредоносным программным обеспечением.

В том числе дарение, подмена или подлог носителей информации и внешних устройств, содержащих вредоносное программное обеспечение или предназначенных для реализации вредоносных функций.

T2.8. Использование методов социальной инженерии, в том числе фишинга, для получения прав доступа к компонентам системы

T2.10. Несанкционированный доступ путем подбора учетных данных сотрудника или легитимного пользователя (методами прямого перебора, словарных атак, паролей производителей по умолчанию, использования одинаковых паролей для разных учетных записей, применения «радужных» таблиц или другими)

T2.11. Несанкционированный доступ путем компрометации учетных данных сотрудника организации, в том числе через компрометацию многократно используемого в различных системах пароля (для личных или служебных нужд)

→ T3: Внедрение и исполнение вредоносного программного обеспечения в системах и сетях:

T3.2. Активация и выполнение вредоносного кода, внедренного в виде закладок в легитимное программное и программное-аппаратное обеспечение систем и сетей

T3.16. Запуск вредоносных программ при помощи легитимных, подписанных цифровой подписью утилит установки приложений и средств запуска скриптов (т.н. техника проксирования запуска), а также через средства запуска кода элементов управления ActiveX, компонентов фильтров (кодеков) и компонентов библиотек DLL.

→ T4: Закрепление (сохранение доступа) в системе или сети:

T4.1. Несанкционированное создание учетных записей или кража существующих учетных данных

Т4.3. Скрытая установка и запуск средств удаленного доступа и управления операционной системы.

Внесение изменений в конфигурацию и состав программных и программно-аппаратных средств атакуемой системы или сети, вследствие чего становится возможен многократный запуск вредоносного кода

Т4.7. Резервное копирование вредоносного кода в областях, редко подвергаемых проверке, в том числе заражение резервных копий данных, сохранение образов в неразмеченных областях жестких дисков и сменных носителей

→ Т5: Управление вредоносным программным обеспечением и (или) компонентами, к которым ранее был получен доступ:

Т5.7. Туннелирование трафика управления через VPN

Т5.10. Использование средств обфускации, шифрования, стеганографии для сокрытия трафика управления

→ Т7: Сокрытие действий и применяемых при этом средств от обнаружения:

Т7.2. Очистка/затирание истории команд и журналов регистрации, перенаправление записей в журналы регистрации, переполнение истории команд и журналов регистрации, затруднение доступа к журналам регистрации для авторизованных пользователей

Т7.4. Отключение средств защиты от угроз информационной безопасности, в том числе средств антивирусной защиты, механизмов аудита, консолей оператора мониторинга и средств защиты других типов

Т7.6. Подделка данных вывода средств защиты от угроз информационной безопасности

→ Т8: Получение доступа (распространение доступа) к другим компонентам систем и сетей или смежным системам и сетям:

Т8.2. Использование средств и интерфейсов удаленного управления для получения доступа к смежным системам и сетям

→ Т9: Сбор и вывод из системы или сети информации, необходимой для дальнейших действий при реализации угроз безопасности информации или реализации новых угроз:

Т9.6. Отправка данных по собственным протоколам

Т9.8. Туннелирование трафика передачи данных через VPN

Т9.12. Шифрование выводимой информации, использование стеганографии для сокрытия факта вывода информации

→ Т10: Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям:

Т10.1. Несанкционированный доступ к информации в памяти системы, файловой системе, базах данных, репозиториях, в программных модулях и прошивках

Т10.8. Уничтожение информации, включая информацию, хранимую в виде файлов, информацию в базах данных и репозиториях, информацию на неразмеченных областях дисков и сменных носителей

УБИ$_9$ актуальна

$УБИ_{10}$ = [Электрик (Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.) (H1)); Сервер с базой данных информационной системы; Проникновение в серверную и обесточивание оборудования; Блокирование доступа к базе данных;]

Сценарий реализации:

→ T10: Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям:

T10.10. Организация отказа в обслуживании одной или нескольких систем, компонентов системы или сети

$УБИ_{10}$ актуальна

$УБИ_{11}$ = [Террористическая организация (Террористические, экстремистские группировки (H3)); Сервер с базой данных информационной системы; Получение доступа к базе данных через АРМ пользователя путем внедрения вредоносного программного обеспечения; Модификация всей хранящейся информации;]

Сценарий реализации:

→ T1: Сбор информации о системах и сетях:

T1.1. Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций

T1.4. Направленное сканирование при помощи специализированного программного обеспечения подключенных к сети устройств с целью идентификации сетевых сервисов, типов и версий программного обеспечения этих сервисов, а также с целью получения конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений.

T1.11. Сбор информации о пользователях, устройствах, приложениях, внутренней информации о компонентах систем и сетей путем применения социальной инженерии, в том числе фишинга

T1.12. Сбор личной идентификационной информации (идентификаторы пользователей, устройств, информация об идентификации пользователей сервисами, приложениями, средствами удаленного доступа), в том числе сбор украденных личных данных сотрудников и подрядчиков на случай, если сотрудники/подрядчики используют одни и те же пароли на работе и за ее пределами

T1.15. Поиск и покупка баз данных идентификационной информации, скомпрометированых паролей и ключей на специализированных нелегальных площадках

→ T2: Получение первоначального доступа к компонентам систем и сетей:

T2.3. Эксплуатация уязвимостей сетевого оборудования и средств защиты вычислительных сетей для получения доступа к компонентам систем и сетей при удаленной атаке.

T2.4. Использование ошибок конфигурации сетевого оборудования и средств защиты, в том числе слабых паролей и паролей по умолчанию, для получения доступа к компонентам систем и сетей при удаленной атаке

T2.7. Использование в системе внешних носителей информации, которые могли подключаться к другим системам и быть заражены вредоносным программным обеспечением.

В том числе дарение, подмена или подлог носителей информации и внешних устройств, содержащих вредоносное программное обеспечение или предназначенных для реализации вредоносных функций.

T2.8. Использование методов социальной инженерии, в том числе фишинга, для получения прав доступа к компонентам системы

T2.10. Несанкционированный доступ путем подбора учетных данных сотрудника или легитимного пользователя (методами прямого перебора, словарных атак, паролей производителей по умолчанию, использования одинаковых паролей для разных учетных записей, применения «радужных» таблиц или другими)

T2.11. Несанкционированный доступ путем компрометации учетных данных сотрудника организации, в том числе через компрометацию многократно используемого в различных системах пароля (для личных или служебных нужд)

→ T3: Внедрение и исполнение вредоносного программного обеспечения в системах и сетях:

T3.16. Запуск вредоносных программ при помощи легитимных, подписанных цифровой подписью утилит установки приложений и средств запуска скриптов (т.н. техника проксирования запуска), а также через средства запуска кода элементов управления ActiveX, компонентов фильтров (кодеков) и компонентов библиотек DLL.

→ T4: Закрепление (сохранение доступа) в системе или сети:

T4.1. Несанкционированное создание учетных записей или кража существующих учетных данных

T4.3. Скрытая установка и запуск средств удаленного доступа и управления операционной системы.

Внесение изменений в конфигурацию и состав программных и программно-аппаратных средств атакуемой системы или сети, вследствие чего становится возможен многократный запуск вредоносного кода

T4.7. Резервное копирование вредоносного кода в областях, редко подвергаемых проверке, в том числе заражение резервных копий данных, сохранение образов в неразмеченных областях жестких дисков и сменных носителей

→ T5: Управление вредоносным программным обеспечением и (или) компонентами, к которым ранее был получен доступ:

T5.7. Туннелирование трафика управления через VPN

T5.10. Использование средств обфускации, шифрования, стеганографии для сокрытия трафика управления

→ T7: Сокрытие действий и применяемых при этом средств от обнаружения:

Т7.2. Очистка/затирание истории команд и журналов регистрации, перенаправление записей в журналы регистрации, переполнение истории команд и журналов регистрации, затруднение доступа к журналам регистрации для авторизованных пользователей

Т7.4. Отключение средств защиты от угроз информационной безопасности, в том числе средств антивирусной защиты, механизмов аудита, консолей оператора мониторинга и средств защиты других типов

Т7.6. Подделка данных вывода средств защиты от угроз информационной безопасности

→ Т8: Получение доступа (распространение доступа) к другим компонентам систем и сетей или смежным системам и сетям:

Т8.2. Использование средств и интерфейсов удаленного управления для получения доступа к смежным системам и сетям

→ Т9: Сбор и вывод из системы или сети информации, необходимой для дальнейших действий при реализации угроз безопасности информации или реализации новых угроз:

Т9.6. Отправка данных по собственным протоколам

Т9.8. Туннелирование трафика передачи данных через VPN

Т9.12. Шифрование выводимой информации, использование стеганографии для сокрытия факта вывода информации

→ Т10: Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям:

Т10.7. Подмена информации в памяти или информации, хранимой в виде файлов, информации в базах данных и репозиториях, информации на неразмеченных областях дисков и сменных носителей

Т10.9. Добавление информации

$УБИ_{11}$ актуальна

10. Определение для актуальных угроз мер защиты информации

$УБИ_i$	Организационные: Административные	Организационно-технические	Программно-технические
1	Информирование сотрудников об обязательных использовании разных сложных паролей и своевременном их обновлении; Плановое проведение аудита безопасности сети	-	Межсетевое экранирование; Использование генераторов сложных паролей и проверок на простоту паролей; Использование систем двухфакторной аутентификации

2	Разработка правил для сотрудников с последовательностью действий при настройке и работе с АРМ пользователей и локальной сетью и информирование сотрудников об обязательности следования им	-	-
4	Разработка правил для сотрудников с последовательностью действий при настройке и работе с АРМ пользователей и локальной сетью и информирование сотрудников об обязательности следования им	-	-
5	Разработка должностных инструкций для обслуживающего и приглашенного персонала; Проведение инструктажей по защите от воздействия методами социальной инженерии; Разграничение доступа сотрудников на территорию и в отдельные помещения объекта информатизации, а также к информационным ресурсам информационной системы	Установка камер видеонаблюдения для видеофиксации всех действий сотрудников; Установка металлодетекторов и досмотр сотрудников для пресечения фактов проноса и выноса любых внешних носителей информации	Удаление/блокировка портов для подключения внешних носителей информации; Установка и своевременное обновление антивирусных средств на всех АРМ сотрудников; Разграничение прав доступа сотрудников к определенным сегментам памяти, программам и действиям (ролевая модель разграничения доступа)
6	Информирование сотрудников об обязательных использовании разных сложных паролей и своевременном их обновлении; Плановое проведение аудита безопасности сети	-	Межсетевое экранирование; Использование генераторов сложных паролей и проверок на простоту паролей; Использование систем двухфакторной аутентификации
7	Информирование сотрудников об обязательных использовании разных сложных паролей и своевременном их обновлении;	-	Межсетевое экранирование; Использование генераторов сложных паролей и проверок на простоту паролей;

	Проведение инструктажей по защите от воздействия методами социальной инженерии; Мониторинг сетевой активности		Использование систем двухфакторной аутентификации; Установка и своевременное обновление антивирусных средств на всех АРМ сотрудников; Разграничение прав доступа сотрудников к определенным сегментам памяти, программам и действиям (ролевая модель разграничения доступа)
8	Разработка должностных инструкций для обслуживающего и приглашенного персонала; Проведение инструктажей по защите от воздействия методами социальной инженерии	Установка камер видеонаблюдения для видеофиксации всех действий сотрудников; Установка металлодетекторов и досмотр сотрудников для пресечения фактов проноса и выноса любых внешних носителей информации	Удаление/блокировка портов для подключения внешних носителей информации; Установка и своевременное обновление антивирусных средств на всех АРМ сотрудников; Разграничение прав доступа сотрудников к определенным сегментам памяти, программам и действиям (ролевая модель разграничения доступа)
9	Информирование сотрудников об обязательных использовании разных сложных паролей и своевременном их обновлении; Проведение инструктажей по защите от воздействия методами социальной инженерии; Плановое проведение аудита безопасности сети; Мониторинг сетевой активности	Установка металлодетекторов и досмотр сотрудников для пресечения фактов проноса и выноса любых внешних носителей информации	Межсетевое экранирование; Использование генераторов сложных паролей и проверок на простоту паролей; Использование систем двухфакторной аутентификации; Удаление/блокировка портов для подключения внешних носителей информации; Установка и своевременное обновление антивирусных средств на всех АРМ сотрудников; Разграничение прав доступа сотрудников к определенным сегментам памяти, программам и действиям

			(ролевая модель разграничения доступа)
10	Разработка должностных инструкций для обслуживающего и приглашенного персонала; Разграничение доступа сотрудников на территорию и в отдельные помещения объекта информатизации, а также к информационным ресурсам информационной системы	Установка камер видеонаблюдения для видеофиксации всех действий сотрудников; Обеспечение круглосуточной охраны важных технических помещений (серверных); Обеспечение резервного питания важных технических объектов (в т. ч. серверов)	-
11	Информирование сотрудников об обязательных использовании разных сложных паролей и своевременном их обновлении; Проведение инструктажей по защите от воздействия методами социальной инженерии; Плановое проведение аудита безопасности сети; Мониторинг сетевой активности	Установка металлодетекторов и досмотр сотрудников для пресечения фактов проноса и выноса любых внешних носителей информации	Межсетевое экранирование; Использование генераторов сложных паролей и проверок на простоту паролей; Использование систем двухфакторной аутентификации; Удаление/блокировка портов для подключения внешних носителей информации; Установка и своевременное обновление антивирусных средств на всех АРМ сотрудников; Разграничение прав доступа сотрудников к определенным сегментам памяти, программам и действиям (ролевая модель разграничения доступа)

Таблица 8. Меры защиты информации для актуальных УБИ

11. Итоговый список всех необходимых мер защиты информации

- Организационные: Административные:
  - Информирование сотрудников об обязательных использовании разных сложных паролей и своевременном их обновлении
  - Разработка правил для сотрудников с последовательностью действий при настройке и работе с АРМ пользователей и локальной сетью и информирование сотрудников об обязательности следования им

    - Разработка должностных инструкций для обслуживающего и приглашенного персонала
    - Проведение инструктажей по защите от воздействия методами социальной инженерии
    - Разграничение доступа сотрудников на территорию и в отдельные помещения объекта информатизации, а также к информационным ресурсам информационной системы
    - Плановое проведение аудита безопасности сети
    - Мониторинг сетевой активности
- Организационно-технические:
    - Установка камер видеонаблюдения для видеофиксации всех действий сотрудников
    - Установка металлодетекторов и досмотр сотрудников для пресечения фактов проноса и выноса любых внешних носителей информации
    - Обеспечение круглосуточной охраны важных технических помещений (серверных)
    - Обеспечение резервного питания важных технических объектов (в т. ч. серверов)
- Программно-технические:
    - Межсетевое экранирование
    - Использование генераторов сложных паролей и проверок на простоту паролей
    - Использование систем двухфакторной аутентификации
    - Удаление/блокировка портов для подключения внешних носителей информации;
    - Установка и своевременное обновление антивирусных средств на всех АРМ сотрудников;
    - Разграничение прав доступа сотрудников к определенным сегментам памяти, программам и действиям (ролевая модель разграничения доступа)