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»

Введе	ние
1.	Выбор объекта информатизации и его компонент
2.	Определение способов передачи для всех потоков информации
3.	Определение свойств информации, которые необходимо обеспечить5
4.	Определение возможных негативных последствий от реализации угроз безопасности
инфор	мации
5.	Определение объектов воздействия и видов воздействия на них
6.	Определение источников угроз безопасности информации
7.	Определение способов реализации (возникновения) угроз безопасности информации 27
8.	Определение угроз безопасности информации
9.	Определение перечня актуальных угроз
10.	Определение для актуальных угроз мер защиты информации
11.	Итоговый список всех необходимых мер защиты информации

Введение

В качестве объекта информатизации для данной работы выбрана вымышленная Научнопроизводственная 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).

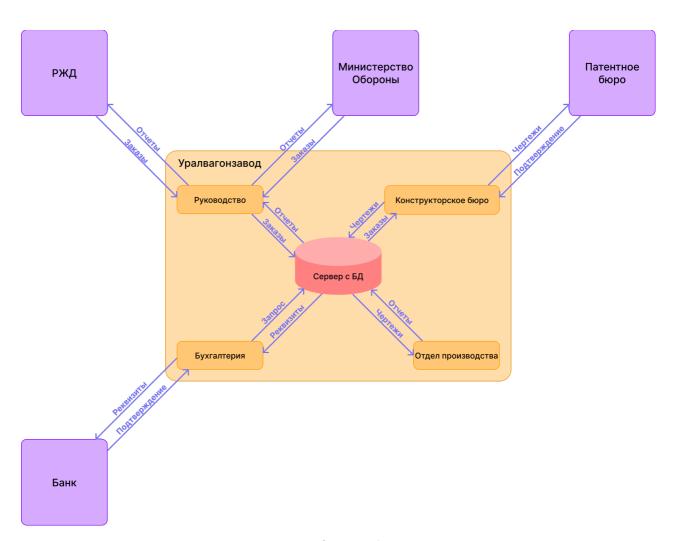


Рисунок 1. Схема объекта информатизации

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
\sim	Взаимодействие по внешней сети (Email)
	Взаимодействие по локальной сети (сетевой пакет)

Таблица 1. Условные обозначения способов передачи информации

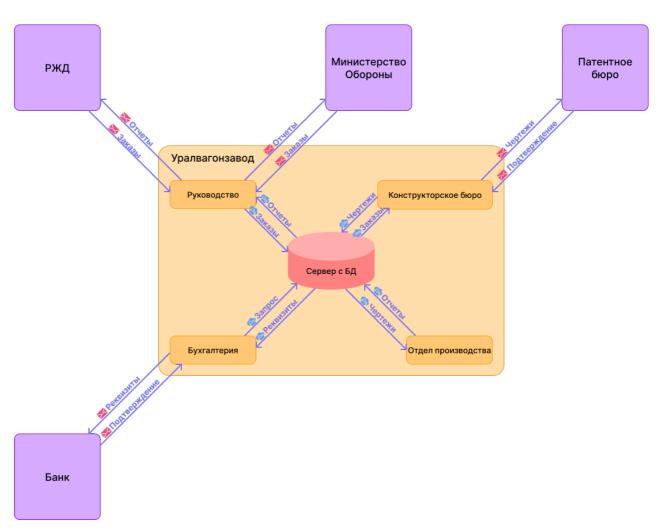


Рисунок 2. Схема объекта информатизации с указанием способов передачи

3. Определение свойств информации, которые необходимо обеспечить

Условные обозначения, применяющиеся на схеме:

- К конфиденциальность
- Ц целостность
- Д доступность

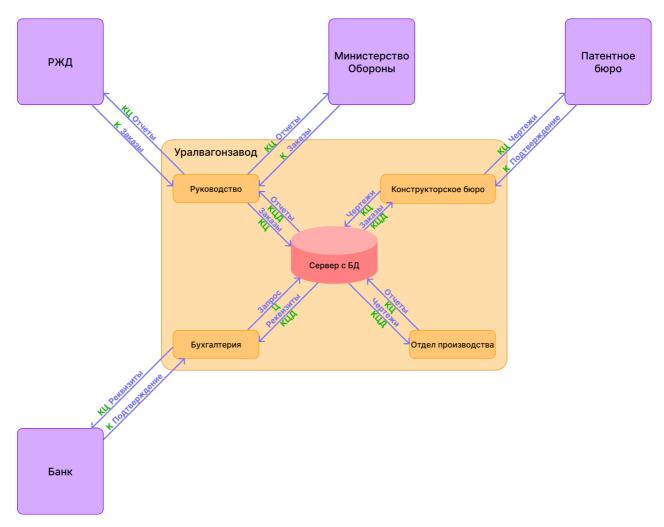


Рисунок 3. Схема объекта информатизации с указанием свойств информации

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

|--|

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	К	Для потоков
I IID – ND	на регистрацию разработок	IN.	информации извне
	(чертежей)		объект информатизации
	(чертежей)		может обеспечить лишь
			конфиденциальность
			информации. Она
			важна, так как
			передаваемая информация не должна
			открыто
			распространяться и
			передаваться третьим
F	P	1/11	лицам
Бухгалтерия – Банк	Реквизиты для перевода	КЦ	Передаваемая
	заработных плат сотрудникам		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	К	Для потоков
	на перевод денежных средств		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	Ц	Запрос на получение
	реквизитов сотрудников		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
		1	

			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
Сервер – Бухгалтерия	Реквизиты сотрудников	кцд	вместе 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.

Nº	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 (APM) сотрудника отдела Бухгалтерии	Несанкционированная модификация (подмена) платежной информации сотрудников (банковских реквизитов), передаваемой через APM 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 Автоматизированное рабочее место (APM) сотрудника отдела Руководства	Несанкционированные модификация / удаление информации о текущих заказах и отчетов о ходе их выполнения; блокирование доступа к базе данных 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 Автоматизированное рабочее место (APM) сотрудника отдела Руководства	Несанкционированные модификация / удаление информации о текущих заказах и отчетов о ходе их выполнения Несанкционированная подмена данных получателя в электронных письмах; ложное извещение об отправлении, блокировка отправлений электронных писем; подмена файлов с заказами и
	Автоматизированное рабочее место (АРМ) сотрудника Конструкторского бюро	отчетами о ходе их выполнения Несанкционированные модификация / удаление / разглашение (утечка) разрабатываемых чертежей

		T
	Автоматизированное	Несанкционированные модификация /
	рабочее место (АРМ)	удаление разработанных чертежей;
	сотрудника Отдела	фальсификация / модификация /
	производства	удаление отчетов о ходе производства
		продуктов
У2: Необходимость	База данных	Несанкционированные модификация /
дополнительных	информационной системы,	удаление большого количества
(незапланированных)	содержащая список всех	информации о текущих заказах и
затрат на	текущих заказов и отчетов	отчетов о ходе их выполнения;
восстановление	, .	блокирование доступа к базе данных;
деятельности		вывод базы данных из строя путем
Harris and the same of the sam		воздействия на физические
		составляющие
	Автоматизированное	Несанкционированные модификация /
	рабочее место (АРМ)	удаление большого количества
		информации о разрабатываемых
	сотрудника	
	Конструкторского бюро	чертежей
	Автоматизированное	Несанкционированные модификация /
	рабочее место (АРМ)	удаление большого количества
	сотрудника Отдела	информации о разработанных чертежах
	производства	
У2: Нарушение деловой	База данных	Несанкционированный доступ к базе
репутации и утрата	информационной системы,	данных с последующей утечкой
доверия	содержащая	идентификационной информации
	конфиденциальную	граждан
	информацию о сотрудниках	
	База данных	Несанкционированный доступ к базе
	информационной системы,	данных с последующей утечкой
	содержащая список всех	информации о текущих заказах, отчетов
	текущих заказов, отчетов и	о ходе их выполнения и чертежей
	чертежей	разрабатываемых / создаваемых
		продуктов
	Автоматизированное	Несанкционированные модификация /
	рабочее место (АРМ)	удаление / разглашение (утечка)
	сотрудника Отдела	разработанных чертежей;
	производства	фальсификация / модификация /
	производетва	удаление / разглашение (утечка)
		, , ,
V2: Vzauva	Бэээ дэгин гу	отчетов о ходе производства продуктов
У2: Утечка	База данных	Несанкционированный доступ к базе
конфиденциальной	информационной системы,	данных с последующим разглашением
информации	содержащая список всех	(утечкой) информации о разработанных
(коммерческой тайны,	чертежей	чертежах, являющихся коммерческой
секретов производства)		тайной
	Автоматизированное	Несанкционированный доступ к
	рабочее место (АРМ)	проходящему трафику информации с
	сотрудника отдела	последующим разглашением (утечкой)
	Руководства	информации о текущих заказах,
		являющихся коммерческой тайной
	Автоматизированное	Несанкционированный доступ к базе
	рабочее место (АРМ)	данных с последующим разглашением
	сотрудника	(утечкой) информации о
	Конструкторского бюро	
	Конструкторского бюро	

	T	1
		разрабатываемых чертежах,
		являющихся коммерческой тайной
	Автоматизированное	Несанкционированный доступ к базе
	рабочее место (АРМ)	данных с последующим разглашением
	сотрудника Отдела	(утечкой) разработанных чертежей,
	производства	отчетов о ходе производства продуктов
У2: Потеря	База данных	Несанкционированные модификация /
конкурентного	информационной системы,	удаление / разглашение (утечка)
преимущества	содержащая список всех	информации о разработанных чертежах,
	чертежей	являющихся коммерческой тайной
	Автоматизированное	Несанкционированные модификация /
	рабочее место (АРМ)	удаление / разглашение (утечка)
	сотрудника	информации о разрабатываемых
	Конструкторского бюро	чертежах
У3: Причинение ущерба	База данных	Несанкционированная модификация
жизни и здоровью	информационной системы,	чертежей с добавлением уязвимых
людей	содержащая список всех	(физически потенциально опасных) мест
людеи	чертежей	в конечной реализации продукта или в
	чертежей	
V2- C	F	ходе его производства
У3: Снижение уровня	База данных	Несанкционированные модификация /
дохода организации с	информационной системы,	удаление большого количества
государственным	содержащая список всех	информации о текущих заказах и
участием	текущих заказов и отчетов	отчетов о ходе их выполнения;
		блокирование доступа к базе данных
	Автоматизированное	Несанкционированные модификация /
	рабочее место (АРМ)	удаление разрабатываемых чертежей
	сотрудника	
	Конструкторского бюро	
	Автоматизированное	Несанкционированные модификация /
	рабочее место (АРМ)	удаление разработанных чертежей;
	сотрудника Отдела	фальсификация / модификация /
	производства	удаление отчетов о ходе производства
		продуктов
У3: Снижение	База данных	Несанкционированные модификация /
показателей	информационной системы,	удаление большого количества
государственного	содержащая список всех	информации о текущих заказах и
оборонного заказа	текущих заказов и отчетов	отчетов о ходе их выполнения;
ocoponiioro sakasa	Tery mux sarasob vi ot acrob	блокирование доступа к базе данных
	Astonostucianoscillos	
	Автоматизированное	Несанкционированные фальсификация /
	рабочее место (АРМ)	модификация / удаление отчетов о ходе
	сотрудника Отдела	производства продуктов; блокирование
	производства	работы АРМ
У3: Утечка информации	База данных	Несанкционированный доступ к базе
ограниченного доступа	информационной системы,	данных с последующим разглашением
	содержащая список всех	(утечкой) информации о разработанных
	чертежей	чертежах, являющихся государственной
		тайной
	Автоматизированное	Несанкционированный доступ к
	рабочее место (АРМ)	проходящему трафику информации с
	сотрудника отдела	последующим разглашением (утечкой)
	Руководства	информации о текущих заказах,
	, 11-	являющихся государственной тайной

	Автоматизированное рабочее место (APM)	Несанкционированный доступ к базе данных с последующим разглашением
	сотрудника	(утечкой) информации о
	Конструкторского бюро	разрабатываемых чертежах,
		являющихся государственной тайной
	Автоматизированное	Несанкционированный доступ к базе
	рабочее место (АРМ)	данных с последующим разглашением
	сотрудника Отдела	(утечкой) информации о разработанных
1	производства	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	-	-	+	У3:
службы			(Нанесение	Причинение
иностранных			ущерба	ущерба жизни и
государств			государству в	здоровью
			области	людей.
			обеспечения	Снижение
			обороны,	уровня дохода
			безопасности и	организации с
			правопорядка,	государственны
			дискредитация	м участием.
			или	Снижение
			дестабилизация	показателей
			деятельности	государственног
			отдельных	о оборонного
			органов	заказа.
			государственной	Утечка
			власти, получение	информации
			конкурентных	ограниченного
			преимуществ на	доступа.
			уровне	
			государства	
Террористичес	+	-	+	У1:
кие,	(Угроза жизни		(Угроза жизни	Угроза жизни
экстремистские	граждан)		граждан,	или здоровью.
группировки			нанесение ущерба	У3:
			отдельным	Причинение
			сферам	ущерба жизни и

Преступные группы (криминальны е структуры)	+ (Получение финансовой выгоды за счет продажи украденных персональных данных)	+ (Получение финансовой или иной материальной выгоды; желание самореализации (подтверждение статуса))	деятельности или секторам экономики государства; дестабилизация деятельности органов государственной власти) + (Получение финансовой или иной материальной выгоды; желание самореализации (подтверждение статуса))	здоровью людей. Снижение уровня дохода организации с государственны м участием. Снижение показателей государственного о оборонного заказа. Утечка информации ограниченного доступа. У1: Разглашение персональных данных граждан. У2: Недополучение ожидаемой (прогнозируемой) прибыли. Необходимость дополнительных (незапланирован ных) затрат на восстановление деятельности. Нарушение деловой репутации и утрата доверия. Утечка конфиденциальн ой информации (коммерческой тайны, секретов производства). У3: Снижение уровня дохода организации с государственны м участием. Утечка
				Утечка информации
				ограниченного
0-5				доступа.
Отдельные	+	+	+	У1:
физические	(Получение	(Получение	(Получение	
лица (хакеры)	финансовой	финансовой или	финансовой или	

	T	U		1.5
	выгоды за счет	иной	иной	Разглашение
	продажи	материальной	материальной	персональных
	украденных	выгоды;	выгоды;	данных граждан.
	персональных	любопытство,	любопытство,	У2:
	данных)	желание	желание	Необходимость
		самореализации	самореализации	дополнительных
		(подтверждение	(подтверждение	(незапланирован
		статуса))	статуса))	ных) затрат на
				восстановление
				деятельности.
				Нарушение
				деловой
				репутации и
				утрата доверия.
				Утечка
				конфиденциальн
				ой информации
				(коммерческой
				тайны, секретов
				производства).
				У3:
				Снижение
				уровня дохода
				организации с
				государственны
				м участием.
				Утечка
				информации
				ограниченного
				доступа.
Конкурирующи	-	+	+	У2:
е организации		(Получение	(Получение	Недополучение
		конкурентных	конкурентных	ожидаемой
		преимуществ;	преимуществ)	(прогнозируемой
		получение) прибыли.
		финансовой или		Необходимость
		иной		дополнительных
		материальной		(незапланирован
		выгоды)		ных) затрат на
				выплаты
				штрафов
				(неустоек) или
				компенсаций.
				Необходимость
				дополнительных
				(незапланирован
				ных) затрат на
				восстановление
				деятельности.
				Потеря
				конкурентного
				преимущества.
				Нарушение
				деловой
<u> </u>	I .	<u> </u>	I	Heyioson

				репутации и
				утрата доверия.
				Утечка
				конфиденциальн
				ой информации
				(коммерческой
				тайны, секретов
				производства).
				У3:
				Утечка
				информации
				ограниченного
Разработиции				доступа.
Разработчики	-	-	-	-
программных, программно-				
аппаратных				
средств				
Лица,	+	+	+	У1:
обеспечивающ	(Получение	(Получение	(Получение	Разглашение
ие поставку	финансовой	финансовой	финансовой	персональных
программных,	выгоды за счет	выгоды за счет	выгоды за счет	данных граждан.
программно-	продажи	продажи	продажи	У2:
аппаратных	украденных	украденных	украденных	Потеря
средств,	персональных	данных,	данных,	конкурентного
обеспечивающ	данных)	представляющих	представляющих	преимущества.
их систем		коммерческую	государственную	Нарушение
		тайну или	тайну)	деловой
		нанесения финансовых		репутации и утрата доверия.
		потерь; получение		утрата доверия. Утечка
		конкурентных		конфиденциальн
		преимуществ)		ой информации
		, = ===,		(коммерческой
				тайны, секретов
				производства).
				У3:
				Утечка
				информации
				ограниченного
				доступа.
Поставщики	-	-	-	-
вычислительны				
х услуг, услуг				
связи Лица,	+	+	+	У1:
привлекаемые	т (Получение	+ (Получение	+ (Получение	ут. Разглашение
pribrichacimbic			•	персональных
для установки	•	финансовой	Финансовои	
для установки, настройки,	финансовой	финансовой выгоды за счет	финансовой выгоды за счет	· ·
для установки, настройки, испытаний,	•	финансовой выгоды за счет продажи	финансовои выгоды за счет продажи	данных граждан. У2:
настройки,	финансовой выгоды за счет	выгоды за счет	выгоды за счет	данных граждан.
настройки, испытаний,	финансовой выгоды за счет продажи	выгоды за счет продажи	выгоды за счет продажи	данных граждан. У2:
настройки, испытаний, пусконаладочн	финансовой выгоды за счет продажи украденных	выгоды за счет продажи украденных	выгоды за счет продажи украденных	данных граждан. У2: Потеря

	Утечка информации
Лица, обеспечивающ ие функциониров ание систем и сетей или обеспечивающ их систем оператора (администраци я, охрана, уборщики и др.) Авторизованны + + + + + + + + + + + + + + + + + +	пение совой выгоды за счет ажи продажи украденных данных, данных, представляющих государственную тайну; неосторожные и ицирова йствия) и ицирова йствия) промяные и ицирова йствия) прожные и ицирова иные действия) прожные и информации (коммерческой тайны, секретов производства). УЗ: причинение ущерба жизни и здоровью людей. Утечка информации ограниченного доступа. н у1:
е пользователи (Получение (Получение финансовой финан	The state of the s

выгоды за счет продажи продажи украденных украденн данных данных представлян непреднамеренн ые, неосторожные тайну или снижени	и продажи персональных данных граждан. украденных данных граждан. Угроза жизни ющих представляющих или здоровью.
неквалифицирова деловой репутаци любопытстви желании самореализ (подтвержд статуса) непреднаме ые, неосторо или неквалифици нные дейст	тайну) Нарушение деловой репутации и утрата доверия. Потеря конкурентного преимущества. Утечка конфиденциальн ой информации (коммерческой тайны, секретов производства). Уз: Утечка
	информации
	ограниченного
Системные + +	доступа. + У1:
администратор (Получение (Получен	
ы и финансовой финансов	
администратор выгоды за счет выгоды за	
ы продажи продажи	
безопасности украденных украденн	ых украденных Разглашение
персональных данных	
данных; месть за представлян	
ранее коммерчес	
совершённые тайну или за действия; снижени	
непреднамеренн деловой	
ые, неосторожные репутаци	
или любопытств	о или репутации и
1	/ · · · · ·
неквалифицирова желани	
неквалифицирова желанис нные действия) самореализ	
неквалифицирова желани нные действия) самореализ (подтвержд	ение конкурентного
неквалифицирова желанио нные действия) самореализ (подтвержд статуса)	цение конкурентного преимущества.
неквалифицирова желанию нные действия) самореализ (подтвержд статуса) непреднаме	конкурентного преимущества. Утечка
неквалифицирова желанио нные действия) самореализ (подтвержд статуса)	конкурентного преимущества. Утечка
неквалифицирова желанио нные действия) самореализ (подтвержд статуса) непреднаме ые, неосторо	конкурентного преимущества. Утечка южные конфиденциальн ой информации
неквалифицирова желанию нные действия) самореализ (подтвержд статуса) непреднаме ые, неосторо	конкурентного преимущества. Утечка конфиденциальн ой информации (коммерческой
неквалифицирова желания нные действия) самореализ (подтвержд статуса) непреднаме ые, неосторо или неквалифиці	конкурентного преимущества. Утечка конфиденциальн ой информации (коммерческой тайны, секретов производства).
неквалифицирова желания нные действия) самореализ (подтвержд статуса) непреднаме ые, неосторо или неквалифиці	конкурентного преимущества. Утечка конфиденциальн ой информации (коммерческой тайны, секретов производства). У3:
неквалифицирова желания нные действия) самореализ (подтвержд статуса) непреднаме ые, неосторо или неквалифиці	конкурентного преимущества. Утечка конфиденциальн ой информации (коммерческой тайны, секретов производства). У3: Утечка
неквалифицирова желания нные действия) самореализ (подтвержд статуса) непреднаме ые, неосторо или неквалифиці	конкурентного преимущества. Утечка конфиденциальн ой информации (коммерческой тайны, секретов производства). У3:

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

Таблица 5. Цели реализации нарушителями угроз безопасности информации

Актуальные нарушители при реализации угроз безопасности информации и соответствующие им возможности

Nº	Виды риска (ущерба) и	Виды актуального	Категория	Уровень
п/п	возможные негативные	нарушителя	нарушителя	возможностей
	последствия			нарушителя
1	У1: Финансовый ущерб	Бывшие работники	Внешний	H1
	физическому лицу	(пользователи)		
		Системные	Внутренний	H2
		администраторы и		
		администраторы		
		безопасности		
2	У1: Разглашение	Бывшие работники	Внешний	H1
	персональных данных	(пользователи)		
	граждан	Системные	Внутренний	H2
		администраторы и		
		администраторы		
		безопасности		

		Λητοριμαοραν	Внутренний	H1
		Авторизованные пользователи	внутреннии	LIT
		систем и сетей	D	H1
		Лица,	Внутренний	LIT.
		обеспечивающие		
		функционирование		
		систем и сетей или		
		обеспечивающих		
		систем оператора		
		(администрация,		
		охрана, уборщики		
		и др.)		
		Лица,	Внутренний	H2
		привлекаемые для		
		установки,		
		настройки,		
		испытаний,		
		пусконаладочных и		
		иных видов работ		
		Лица,	Внешний	H1
		обеспечивающие		
		поставку		
		программных,		
		программно-		
		аппаратных		
		средств,		
		обеспечивающих		
		систем		
		Отдельные	Внешний	H1
		физические лица		
		(хакеры)		
		Преступные	Внешний	H2
		группы		
		(криминальные		
		структуры)		
3	У1: Угроза жизни или	Системные	Внутренний	H2
	здоровью	администраторы и	=,.,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	
		администраторы		
		безопасности		
		Авторизованные	Внутренний	H1
		пользователи	2,.,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	
		систем и сетей		
		Лица,	Внутренний	H1
		обеспечивающие	Биугренний	112
		функционирование		
		систем и сетей или		
		обеспечивающих		
		систем оператора		
		(администрация,		
		охрана, уборщики		
		и др.)		
		1 HP-1	1	

		Toppopus	Внешний	Н3
		Террористические,	внешнии	H3
		экстремистские		
		группировки		1
4	У2: Недополучение	Бывшие работники	Внешний	H1
	ожидаемой	(пользователи)		
	(прогнозируемой) прибыли	Конкурирующие		
		организации		
		Преступные	Внешний	H2
		группы		
		(криминальные		
		структуры)		
5	У2: Необходимость	Лица,	Внутренний	H1
	дополнительных	обеспечивающие		
	(незапланированных) затрат	функционирование		
	на выплаты штрафов	систем и сетей или		
	(неустоек) или компенсаций	обеспечивающих		
		систем оператора		
		(администрация,		
		охрана, уборщики		
		и др.)		
			Внешний	H2
		Конкурирующие	рнешнии	П
	V2: 115	организации	D~~	114
6	У2: Необходимость	Лица,	Внутренний	H1
	дополнительных	обеспечивающие		
	(незапланированных) затрат	функционирование		
	на восстановление	систем и сетей или		
	деятельности	обеспечивающих		
		систем оператора		
		(администрация,		
		охрана, уборщики		
		и др.)		
		Конкурирующие	Внешний	H2
		организации		
		Отдельные	Внешний	H1
		физические лица		
		(хакеры)		
		Преступные	Внешний	H2
		группы		
		(криминальные		
		структуры)		
7	У2: Нарушение деловой	Бывшие работники	Внешний	H1
,	репутации и утрата доверия	(пользователи)	51100117171	112
	penyiadani nyipata dosepha	Системные	Внутренний	H2
			ытутреппии	112
		администраторы и		
		администраторы		
		безопасности	D	114
		Авторизованные	Внутренний	H1
		пользователи		
		систем и сетей		
		Лица,	Внутренний	H2
		привлекаемые для		
		установки,		
		, , , , , , ,		

		испытаний,		
		пусконаладочных и		
		иных видов работ		
		Лица,	Внешний	H1
		обеспечивающие		
		поставку		
		программных,		
		программно-		
		аппаратных		
		средств,		
		обеспечивающих		
		систем		
		Конкурирующие	Внешний	H2
		организации		
		Отдельные	Внешний	H1
		физические лица	Бисшии	112
		(хакеры)		
			Внешний	H2
		Преступные	рнешнии	П
		группы		
		(криминальные		
		структуры)		
8	У2: Утечка	Бывшие работники	Внешний	H1
	конфиденциальной	(пользователи)		
	информации (коммерческой	Системные	Внутренний	H2
	тайны, секретов	администраторы и		
	производства)	администраторы		
		безопасности		
		Авторизованные	Внутренний	H1
		пользователи		
		систем и сетей		
		Лица,	Внутренний	H1
		обеспечивающие		
		функционирование		
		систем и сетей или		
		обеспечивающих		
		систем оператора		
		(администрация,		
		охрана, уборщики		
		и др.)		
		Лица,	Внутренний	H2
		привлекаемые для	, ,	
		установки,		
		настройки,		
		испытаний,		
		пусконаладочных и		
		иных видов работ		
		Лица,	Внешний	H1
		обеспечивающие	Эпсшии	''-
		-		
		поставку		
		программных,		
		программно-		
		аппаратных		
		средств,		

		обеспечивающих		
		систем		
		Конкурирующие	Внешний	H2
		организации	Бисшии	112
		Отдельные	Внешний	H1
		физические лица	Бисшии	111
		(хакеры)		
		Преступные	Внешний	H2
		группы	Б НЕШНИИ	П
		(криминальные		
9	V2: Потора концирации	структуры) Системные	Внутренний	H2
9	У2: Потеря конкурентного		Бнутреннии	П
	преимущества	администраторы и		
		администраторы безопасности		
			Внутренний	H1
		Авторизованные	внутреннии	LIT
		пользователи		
		систем и сетей	D×	112
		Лица,	Внутренний	H2
		привлекаемые для		
		установки,		
		настройки,		
		испытаний,		
		пусконаладочных и		
		иных видов работ	D	111
		Лица,	Внешний	H1
		обеспечивающие		
		поставку		
		программных,		
		программно-		
		аппаратных		
		средств,		
		обеспечивающих		
		систем	D	112
		Конкурирующие	Внешний	H2
10	V2 F	организации	D v	114
10	У3: Причинение ущерба	Лица,	Внутренний	H1
	жизни и здоровью людей	обеспечивающие		
		функционирование		
		систем и сетей или		
		обеспечивающих		
		систем оператора		
		(администрация,		
		охрана, уборщики		
		и др.)	D	112
		Террористические,	Внешний	H3
		экстремистские		
		группировки	D v	114
		Специальные	Внешний	H4
		службы		
		иностранных		
		государств		

11	У3: Снижение уровня дохода	Бывшие работники	Внешний	H1
	организации с	(пользователи)		
	государственным участием	Отдельные	Внешний	H1
		физические лица		
		(хакеры)		
		Преступные	Внешний	H2
		группы		
		(криминальные		
		структуры)		
		Террористические,	Внешний	H3
		экстремистские		
		группировки		
		Специальные	Внешний	H4
		службы		
		иностранных		
		государств		
12	У3: Снижение показателей	Террористические,	Внешний	Н3
	государственного	экстремистские		
	оборонного заказа	группировки		
		Специальные	Внешний	H4
		службы		
		иностранных		
12	\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \	государств		114
13	У3: Утечка информации	Бывшие работники	Внешний	H1
	ограниченного доступа	(пользователи)		112
		Системные	Внутренний	H2
		администраторы и		
		администраторы		
		безопасности	D	H1
		Авторизованные	Внутренний	HI
		пользователи систем и сетей		
		Лица,	Внутренний	H1
		лица, обеспечивающие	Бнутреннии	ПТ
		функционирование		
		систем и сетей или		
		обеспечивающих		
		систем оператора		
		(администрация,		
		охрана, уборщики		
		и др.)		
		Лица,	Внутренний	H2
		привлекаемые для	.,,,,,	
		установки,		
		настройки,		
		испытаний,		
		пусконаладочных и		
		иных видов работ		
		Лица,	Внешний	H1
		обеспечивающие		
		поставку		
		программных,		
L		программно-		
I			1	1

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

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

7. Определение способов реализации (возникновения) угроз безопасности информации

Nº	Вид нарушителя	Категория	Объект воздействия	Доступные	Способы
п/п		нарушителя		интерфейсы	реализации
1	Специальные	Внешний	База данных	Пользовательски	Получение
	службы		информационной	й интерфейс	доступа к базе
	иностранных		системы,	доступа к базе	данных через
	государств (Н4)		содержащая список	данных	APM
			всех чертежей,	информационно	пользователя
			текущих заказов и	й системы	путем
			отчетов:		внедрения
					вредоносного
			Несанкционированн		программного
			ый доступ к		обеспечения
			защищаемой		
			информации,		
			нарушение		
			целостности		
			(модификация),		
			доступности		
			(удаление),		
			конфиденциальност		
			и (утечка);		
			блокирование		
			доступа к базе		
			данных		

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

			информации,	сеть	
			содержащейся на	организации	
			АРМ пользователя	_ p. aoa = 1717	
2	Террористические,	Внешний	База данных	Пользовательски	Получение
	экстремистские		информационной	й интерфейс	доступа к базе
	группировки (Н3)		системы,	доступа к базе	данных через
			содержащая список	данных	APM
			всех чертежей,	информационно	пользователя
			текущих заказов и	й системы	путем
			отчетов:		внедрения
					вредоносного
			Несанкционированн		программного
			ый доступ к		обеспечения
			защищаемой		
			информации,		
			нарушение целостности		
			(модификация),		
			доступности		
			(удаление),		
			конфиденциальност		
			и (утечка);		
			блокирование		
			доступа к базе		
			данных		
			Автоматизированно	Съемные	Внедрение
			е рабочее место	машинные	вредоносного
			(APM) сотрудника отдела Руководства:	носители информации,	программного обеспечения
			Готдела гуководства.	подключаемые к	обеспечения
			Нарушение	APM	
			конфиденциальност	пользователя	
			и (утечка) и	Доступ через	Внедрение
			целостности	локальную	вредоносного
			(модификация)	вычислительную	программного
			информации,	сеть	обеспечения
			содержащейся на	организации	
			АРМ пользователя	Доступ через	Использование
				внешнюю сеть	уязвимостей
				(Интернет)	конфигурации
					доступа к внешней сети
					впешней сети
					Внедрение
					вредоносного
					программного
					обеспечения в
					потоки обмена
					информацией
					(email)
			Автоматизированно	Съемные	Внедрение
			е рабочее место	машинные	вредоносного
			(АРМ) сотрудника	носители	

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

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

			информации,	сеть	
			содержащейся на	организации	
			АРМ пользователя		
4	Отдельные физические лица (хакеры) (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), конфиденциальност и (утечка); блокирование доступа к базе данных	Пользовательски й интерфейс доступа к базе данных информационно й системы	Получение доступа к базе данных через APM пользователя путем внедрения вредоносного программного обеспечения
			Автоматизированно е рабочее место (АРМ) сотрудника отдела Руководства: Нарушение конфиденциальност	Съемные машинные носители информации, подключаемые к APM пользователя	Внедрение вредоносного программного обеспечения
			и (утечка) и целостности (модификация) информации, содержащейся на	Доступ через локальную вычислительную сеть организации	Внедрение вредоносного программного обеспечения
			АРМ пользователя	Доступ через внешнюю сеть (Интернет)	Использование уязвимостей конфигурации доступа к внешней сети
					Внедрение вредоносного программного обеспечения в потоки обмена информацией (email)

			Автоматизированно е рабочее место (АРМ) сотрудника Конструкторского бюро: Нарушение конфиденциальност и (утечка) и целостности (модификация) информации, содержащейся на АРМ пользователя	Съемные машинные носители информации, подключаемые к АРМ пользователя Доступ через локальную вычислительную сеть организации Доступ через внешнюю сеть (Интернет)	Внедрение вредоносного программного обеспечения Внедрение вредоносного программного обеспечения Использование уязвимостей конфигурации доступа к
			Автоматизированно е рабочее место (АРМ) сотрудника Отдела производства: Нарушение конфиденциальност и (утечка) и целостности (модификация) информации, содержащейся на АРМ пользователя	Съемные машинные носители информации, подключаемые к АРМ пользователя Доступ через локальную вычислительную сеть организации	внешней сети Внедрение вредоносного программного обеспечения 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), конфиденциальност и (утечка); блокирование	Пользовательски й интерфейс доступа к базе данных информационно й системы	Получение доступа к базе данных через АРМ пользователя путем внедрения вредоносного программного обеспечения

T			<u> </u>
	доступа к базе		
	данных		
	Автоматизированно	Съемные	Внедрение
	е рабочее место	машинные	вредоносного
	(АРМ) сотрудника	носители	программного
	отдела Руководства:	информации,	обеспечения
		подключаемые к	
	Нарушение	APM	
	конфиденциальност	пользователя	
	и (утечка) и	Доступ через	Внедрение
	целостности	локальную	вредоносного
	(модификация)	вычислительную	программного
	информации,	сеть	обеспечения
	содержащейся на	организации	
	АРМ пользователя	Доступ через	Использование
		внешнюю сеть	уязвимостей
		(Интернет)	конфигурации
			доступа к
			внешней сети
			Внедрение
			вредоносного
			программного
			обеспечения в
			потоки обмена
			информацией
			(email)
	Автоматизированно	Съемные	Внедрение
	е рабочее место	машинные	вредоносного
	(APM) сотрудника	носители	программного
	Конструкторского	информации,	обеспечения
	бюро:	подключаемые к	
		APM	
	Нарушение	пользователя	
	конфиденциальност	Доступ через	Внедрение
	и (утечка) и	локальную	вредоносного
	целостности	вычислительную	программного
	(модификация)	сеть	обеспечения
	информации,	организации	обсенс-тепии
	содержащейся на	Доступ через	Использование
	АРМ пользователя		
	/ W W HOJIDSOBATEJIA	внешнюю сеть (Интернет)	уязвимостей конфигурации
		(интернет)	
			доступа к
	Apro14671101111 = =====	C- 0	внешней сети
	Автоматизированно	Съемные	Внедрение
	е рабочее место	машинные	вредоносного
	(АРМ) сотрудника	носители	программного
	* *		ореспечения
	производства:	подключаемые к АРМ	
	Нарушение	пользователя	
	конфиденциальност		Внедрение
	и (утечка) и		вредоносного
	конфиденциальност		обеспечения Внедрение

			целостности (модификация)	вычислительную сеть	программного обеспечения
			информации, содержащейся на APM пользователя	организации	
6	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем (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), конфиденциальност и (утечка); блокирование доступа к базе данных	Пользовательски й интерфейс доступа к базе данных информационно й системы Программно-аппаратные средства обеспечивающи х систем	Получение доступа к базе данных через АРМ пользователя путем внедрения вредоносного программного обеспечения Использование уязвимостей поставляемых средств
			Автоматизированно е рабочее место (АРМ) сотрудника отдела Руководства: Нарушение конфиденциальност и (утечка) и целостности (модификация) информации,	Программные/п рограммно- аппаратные средства обеспечивающи х систем	Использование уязвимостей поставляемых средств
			содержащейся на АРМ пользователя Автоматизированно е рабочее место (АРМ) сотрудника Конструкторского бюро:	Программные/п рограммно- аппаратные средства обеспечивающи х систем	Использование уязвимостей поставляемых средств
			Нарушение конфиденциальност и (утечка) и целостности (модификация)		

			информации, содержащейся на АРМ пользователя Автоматизированно е рабочее место (АРМ) сотрудника Отдела производства:	Программные/п рограммно-аппаратные средства обеспечивающи х систем	Использование уязвимостей поставляемых средств
			конфиденциальност и (утечка) и целостности (модификация) информации, содержащейся на АРМ пользователя		
7	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ (H2)	Внутренний	База данных информационной системы, содержащая конфиденциальную информацию о сотрудниках, список всех чертежей, текущих заказов и отчетов:	Пользовательский интерфейс доступа к базе данных информационной системы	Получение непосредствен ного доступа к базе данных через АРМ пользователя в ходе проведения производимых работ
			Несанкционированн ый доступ к защищаемой информации, нарушение целостности (модификация), доступности (удаление), конфиденциальност и (утечка); блокирование доступа к базе данных	Локальная вычислительная сеть организации	Ошибочные действия в ходе проведения работ над сервером с базой данных
			Автоматизированно е рабочее место (АРМ) сотрудника отдела Руководства: Непреднамеренные /преднамеренные действия, повлекшие нарушение конфиденциальност и (утечка) и	Локальная вычислительная сеть организации Съемные машинные носители информации,	Ошибочные действия в ходе проведения работ над APM сотрудника отдела Руководства Внедрение вредоносного программного обеспечения

			целостности (модификация) информации, содержащейся на АРМ пользователя Автоматизированно е рабочее место (АРМ) сотрудника Конструкторского бюро: Непреднамеренные действия, повлекшие нарушение конфиденциальност и (утечка) и целостности (модификация) информации, содержащейся на АРМ пользователя Автоматизированно е рабочее место (АРМ) сотрудника Отдела производства: Непреднамеренные /преднамеренные действия,	подключаемые к АРМ пользователя Локальная вычислительная сеть организации Съемные машинные носители информации, подключаемые к АРМ пользователя Локальная вычислительная сеть организации	Ошибочные действия в ходе проведения работ над АРМ сотрудника Конструкторско го бюро Внедрение вредоносного программного обеспечения Ошибочные действия в ходе проведения работ над АРМ сотрудника Отдела производства
			повлекшие нарушение конфиденциальност и (утечка) и целостности (модификация) информации, содержащейся на АРМ пользователя	машинные носители информации, подключаемые к APM пользователя	Внедрение вредоносного программного обеспечения
8	Лица, обеспечивающие функционировани е 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	Проникновени е в помещение с сервером с базой данных и причинение физического ущерба

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

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

	T	T		Γ	1
			(модификация) информации, содержащейся на APM пользователя		
					06
			Автоматизированно	Локальная	Ошибочные
			е рабочее место	вычислительная	действия в
			(АРМ) сотрудника	сеть	ходе работы с
			Конструкторского	организации	собственным
			бюро:		АРМ (для
			Homo muchanou un in		сотрудников
			Непреднамеренные действия,		Конструкторско го бюро)
			повлекшие		το οιόμο)
			нарушение		
			конфиденциальност		
			и (утечка) и		
			целостности		
			(модификация)		
			информации,		
			содержащейся на		
			АРМ пользователя		
			Автоматизированно	Локальная	Ошибочные
			е рабочее место	вычислительная	действия в
			(АРМ) сотрудника	сеть	ходе работы с
			Отдела	организации	собственным
			производства:		АРМ (для
					сотрудников
			Непреднамеренные		Отдела
			действия,		производства)
			повлекшие		
			нарушение конфиденциальност		
			и (утечка) и		
			целостности		
			(модификация)		
			информации,		
			содержащейся на		
			АРМ пользователя		
10	Системные	Внутренний	База данных	Пользовательски	Использование
	администраторы и		информационной	й интерфейс	уязвимостей
	администраторы		системы,	доступа к базе	конфигурации
	безопасности (Н2)		содержащая	данных	системы
			конфиденциальную	информационно	управления
			информацию о	й системы	базой данных
			сотрудниках, список всех чертежей,		Внедрение
			текущих заказов и		вредоносного
			отчетов:		программного
					обеспечения
			Несанкционированн		
			ый доступ к		
			защищаемой		
			информации,		
			нарушение		

		целостности		
	((модификация),		
	4	доступности		
		(удаление),		
		конфиденциальност		
		и (утечка);		
		блокирование		
		доступа к базе		
		данных		
		Автоматизированно	Локальная	Ошибочные
		е рабочее место	вычислительная	действия в
		(АРМ) сотрудника	сеть	ходе настройки
		отдела Руководства:	организации	локальной сети
		. , , , , , , , , , , , , , , , , , , ,		
		Непреднамеренные		Внедрение и
		/преднамеренные		использование
		действия,		уязвимостей
	_ ·	повлекшие		конфигурации
		нарушение		локальной сети
		конфиденциальност		
		и (утечка) и		
		целостности		
		(модификация)		
		информации,		
		содержащейся на		
		АРМ пользователя		
	<u> </u>	Автоматизированно	Локальная	Ошибочные
		е рабочее место	локальная вычислительная	действия в
		е раоочее место (APM) сотрудника	сеть	ходе настройки
		отдела Бухгалтерии:	организации	локальной сети
		отдела вухгалтерии.	оргапизации	локальной сети
		Непреднамеренные		Внедрение и
		лепреднамеренные /преднамеренные		использование
	-	действия, повлекшие		уязвимостей конфигурации
				конфигурации локальной сети
		нарушение		локальной сети
		конфиденциальност		
		и (утечка) и		
		целостности		
		(модификация)		
		информации,		
		содержащейся на		
		АРМ пользователя	n	0 6
		Автоматизированно	Локальная	Ошибочные
		е рабочее место	вычислительная	действия в
		(АРМ) сотрудника	сеть	ходе настройки
1		Конструкторского	организации	локальной сети
1	(бюро:		_
				Внедрение и
				эодроо
		Непреднамеренные		использование
	,	/преднамеренные		использование уязвимостей
	,			использование уязвимостей конфигурации
	, , , , , , , , , , , , , , , , , , ,	/преднамеренные		использование уязвимостей
	, ,	/преднамеренные действия,		использование уязвимостей конфигурации

		1	1		T I
			конфиденциальност		
			и (утечка) и		
			целостности		
			(модификация)		
			информации,		
			содержащейся на		
			АРМ пользователя		
			Автоматизированно	Локальная	Ошибочные
			е рабочее место	вычислительная	действия в
			(APM) сотрудника	сеть	ходе настройки
			Отдела	организации	локальной сети
			производства:	, ,	
					Внедрение и
			Непреднамеренные		использование
			/преднамеренные		уязвимостей
			действия,		конфигурации
			деиствия, повлекшие		локальной сети
					локальной сети
			нарушение		
			конфиденциальност		
			и (утечка) и		
			целостности		
			(модификация)		
			информации,		
			содержащейся на		
			АРМ пользователя		
11	Бывшие	Внешний	База данных	Пользовательски	Получение
	работники		информационной	й интерфейс	доступа к базе
	(пользователи)		системы,	доступа к базе	данных через
	(пользователи) (H1)		системы, содержащая	доступа к базе данных	данных через АРМ
	·		•		
	·		содержащая	данных	APM
	·		содержащая конфиденциальную	данных информационно	АРМ пользователя
	·		содержащая конфиденциальную информацию о сотрудниках, список	данных информационно	АРМ пользователя путем внедрения
	·		содержащая конфиденциальную информацию о сотрудниках, список всех чертежей,	данных информационно	АРМ пользователя путем внедрения вредоносного
	·		содержащая конфиденциальную информацию о сотрудниках, список	данных информационно	АРМ пользователя путем внедрения вредоносного программного
	·		содержащая конфиденциальную информацию о сотрудниках, список всех чертежей, текущих заказов и	данных информационно	АРМ пользователя путем внедрения вредоносного
	·		содержащая конфиденциальную информацию о сотрудниках, список всех чертежей, текущих заказов и отчетов:	данных информационно	АРМ пользователя путем внедрения вредоносного программного
	·		содержащая конфиденциальную информацию о сотрудниках, список всех чертежей, текущих заказов и отчетов:	данных информационно	АРМ пользователя путем внедрения вредоносного программного
	·		содержащая конфиденциальную информацию о сотрудниках, список всех чертежей, текущих заказов и отчетов: Несанкционированный доступ к	данных информационно	АРМ пользователя путем внедрения вредоносного программного
	·		содержащая конфиденциальную информацию о сотрудниках, список всех чертежей, текущих заказов и отчетов: Несанкционированный доступ к защищаемой	данных информационно	АРМ пользователя путем внедрения вредоносного программного
	·		содержащая конфиденциальную информацию о сотрудниках, список всех чертежей, текущих заказов и отчетов: Несанкционированный доступ к защищаемой информации,	данных информационно	АРМ пользователя путем внедрения вредоносного программного
	·		содержащая конфиденциальную информацию о сотрудниках, список всех чертежей, текущих заказов и отчетов: Несанкционированный доступ к защищаемой информации, нарушение	данных информационно	АРМ пользователя путем внедрения вредоносного программного
	·		содержащая конфиденциальную информацию о сотрудниках, список всех чертежей, текущих заказов и отчетов: Несанкционированный доступ к защищаемой информации, нарушение целостности	данных информационно	АРМ пользователя путем внедрения вредоносного программного
	·		содержащая конфиденциальную информацию о сотрудниках, список всех чертежей, текущих заказов и отчетов: Несанкционированный доступ к защищаемой информации, нарушение целостности (модификация),	данных информационно	АРМ пользователя путем внедрения вредоносного программного
	·		содержащая конфиденциальную информацию о сотрудниках, список всех чертежей, текущих заказов и отчетов: Несанкционированный доступ к защищаемой информации, нарушение целостности (модификация), доступности	данных информационно	АРМ пользователя путем внедрения вредоносного программного
	·		содержащая конфиденциальную информацию о сотрудниках, список всех чертежей, текущих заказов и отчетов: Несанкционированный доступ к защищаемой информации, нарушение целостности (модификация), доступности (удаление),	данных информационно	АРМ пользователя путем внедрения вредоносного программного
	·		содержащая конфиденциальную информацию о сотрудниках, список всех чертежей, текущих заказов и отчетов: Несанкционированный доступ к защищаемой информации, нарушение целостности (модификация), доступности (удаление), конфиденциальност	данных информационно	АРМ пользователя путем внедрения вредоносного программного
	·		содержащая конфиденциальную информацию о сотрудниках, список всех чертежей, текущих заказов и отчетов: Несанкционированный доступ к защищаемой информации, нарушение целостности (модификация), доступности (удаление), конфиденциальност и (утечка);	данных информационно	АРМ пользователя путем внедрения вредоносного программного
	·		содержащая конфиденциальную информацию о сотрудниках, список всех чертежей, текущих заказов и отчетов: Несанкционированный доступ к защищаемой информации, нарушение целостности (модификация), доступности (удаление), конфиденциальност и (утечка); блокирование	данных информационно	АРМ пользователя путем внедрения вредоносного программного
	·		содержащая конфиденциальную информацию о сотрудниках, список всех чертежей, текущих заказов и отчетов: Несанкционированный доступ к защищаемой информации, нарушение целостности (модификация), доступности (удаление), конфиденциальност и (утечка); блокирование доступа к базе	данных информационно	АРМ пользователя путем внедрения вредоносного программного
	·		содержащая конфиденциальную информацию о сотрудниках, список всех чертежей, текущих заказов и отчетов: Несанкционированный доступ к защищаемой информации, нарушение целостности (модификация), доступности (удаление), конфиденциальност и (утечка); блокирование	данных информационно	АРМ пользователя путем внедрения вредоносного программного
	·		содержащая конфиденциальную информацию о сотрудниках, список всех чертежей, текущих заказов и отчетов: Несанкционированный доступ к защищаемой информации, нарушение целостности (модификация), доступности (удаление), конфиденциальност и (утечка); блокирование доступа к базе	данных информационно	АРМ пользователя путем внедрения вредоносного программного
	·		содержащая конфиденциальную информацию о сотрудниках, список всех чертежей, текущих заказов и отчетов: Несанкционированный доступ к защищаемой информации, нарушение целостности (модификация), доступности (удаление), конфиденциальност и (утечка); блокирование доступа к базе данных	данных информационно й системы	АРМ пользователя путем внедрения вредоносного программного обеспечения
	·		содержащая конфиденциальную информацию о сотрудниках, список всех чертежей, текущих заказов и отчетов: Несанкционированный доступ к защищаемой информации, нарушение целостности (модификация), доступности (удаление), конфиденциальност и (утечка); блокирование доступа к базе данных Автоматизированно	данных информационно й системы	АРМ пользователя путем внедрения вредоносного программного обеспечения
	·		содержащая конфиденциальную информацию о сотрудниках, список всех чертежей, текущих заказов и отчетов: Несанкционированный доступ к защищаемой информации, нарушение целостности (модификация), доступности (удаление), конфиденциальност и (утечка); блокирование доступа к базе данных Автоматизированно е рабочее место	данных информационно й системы Съемные машинные	АРМ пользователя путем внедрения вредоносного обеспечения внедрения вредоносного обеспечения

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

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

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);]

 $VБИ_2$ = [Системный администратор (Системные администраторы и администраторы безопасности (H2)); APM сотрудника отдела Бухгалтерии; Ошибочные действия в ходе настройки локальной сети; Нарушение автозаполнения платежных реквизитов сотрудников (Финансовый ущерб физическому лицу);]

УБИ₃ = [Конкурирующая организация (Конкурирующие организации (H2)); АРМ сотрудника Отдела производства; Внедрение вредоносного программного обеспечения через внешний носитель информации сотрудника; Кража чертежей и отчетов;]

УБИ₄ = [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;]

УБИ₅ = [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);]

УБИ₆ = [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) (H2)); APM 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;]

УБИ₈ = [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;]

УБИ₉ = [Специальные службы иностранных государств (Н4); Сервер с базой данных информационной системы; Получение доступа к базе данных через APM 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.) (Н1)); Сервер с базой данных информационной системы; Проникновение в серверную и обесточивание оборудования; Блокирование доступа к базе данных;]

УБИ $_{11}$ = [Террористическая организация (Террористические, экстремистские группировки (Н3)); 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

УБИ₁ = [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);]

- → Т1: 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
 - 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.
 - 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
 - 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)

- → 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

\rightarrow УБИ₁ актуальна

УБИ $_2$ = [Системный администратор (Системные администраторы и администраторы безопасности (H2)); APM сотрудника отдела Бухгалтерии; Ошибочные действия в ходе настройки локальной сети; Нарушение автозаполнения платежных реквизитов сотрудников (Финансовый ущерб физическому лицу);]

Сценарий реализации:

- → T10: 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
 - T10.7. 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

\rightarrow УБИ₂ актуальна

 $УБИ_3$ = [Конкурирующая организация (Конкурирующие организации (H2)); APM сотрудника Отдела производства; Внедрение вредоносного программного обеспечения через внешний носитель информации сотрудника; Кража чертежей и отчетов;]

- → Т1: 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
- → Т2: 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.

- \rightarrow T3: 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

- \rightarrow T5: Управление вредоносным программным обеспечением и (или) компонентами, к которым ранее был получен доступ:
 - 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.)
 - T5.4. 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

УБИ₃ <u>неактуальна</u>, так как APM сотрудника Отдела производства не имеет доступа к внешней сети (Интернет), а значит использование средств удаленного доступа и управления операционной системы APM невозможно.

УБИ₄ = [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:

- \rightarrow T10: Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям:
 - T10.8. Уничтожение информации, включая информацию, хранимую в виде файлов, информацию в базах данных и репозиториях, информацию на неразмеченных областях дисков и сменных носителей
- → УБИ4 актуальна

УБИ₅ = [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
- → Т2: 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)
- → ТЗ: Внедрение и исполнение вредоносного программного обеспечения в системах и сетях:
 - ТЗ.1. Автоматический запуск скриптов и исполняемых файлов в системе с использованием пользовательских или системных учетных данных, в том числе с использованием методов социальной инженерии
 - Т3.7. Подмена файлов легитимных программ и библиотек непосредственно в системе.
- ightarrow 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
 - Т5.А. Управление с использованием полученных ранее прав доступа непосредственно в системе
- \rightarrow 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

УБИ₅ актуальна

УБИ₆ = [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;]

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
 - 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.
 - 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)
- \rightarrow 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
 - T10.7. 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

\rightarrow УБИ₆ 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
- → Т2: Получение первоначального доступа к компонентам систем и сетей:
 - Т2.8. 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)
- \rightarrow T3: Внедрение и исполнение вредоносного программного обеспечения в системах и сетях:
 - ТЗ.1. Автоматический запуск скриптов и исполняемых файлов в системе с использованием пользовательских или системных учетных данных, в том числе с использованием методов социальной инженерии
 - ТЗ.З. Автоматическая загрузка вредоносного кода с удаленного сайта или ресурса с последующим запуском на выполнение
- → 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

- \rightarrow T5: Управление вредоносным программным обеспечением и (или) компонентами, к которым ранее был получен доступ:
 - Т5.2. 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
- → Т7: 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
- → 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

УБИ₇ актуальна

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;]

Сценарий реализации:

- → Т1: 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
 - 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
- → Т2: 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)
- \rightarrow T3: Внедрение и исполнение вредоносного программного обеспечения в системах и сетях:
 - ТЗ.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:
 - T7.4. Отключение средств защиты от угроз информационной безопасности, в том числе средств антивирусной защиты, механизмов аудита, консолей оператора мониторинга и средств защиты других типов
- → T10: Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям:
 - T10.7. Подмена информации в памяти или информации, хранимой в виде файлов, информации в базах данных и репозиториях, информации на неразмеченных областях дисков и сменных носителей

УБИ₈ актуальна

УБИ₉ = [Специальные службы иностранных государств (Н4); Сервер с базой данных информационной системы; Получение доступа к базе данных через APM пользователя путем внедрения вредоносного программного обеспечения; Копирование (кража) с последующим удалением всей информации из базы данных;]

- → 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
 - 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
- Т1.12. 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
- Т1.15. Поиск и покупка баз данных идентификационной информации, скомпрометированых паролей и ключей на специализированных нелегальных площадках
- → 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.
 - 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)
- \rightarrow T3: Внедрение и исполнение вредоносного программного обеспечения в системах и сетях:
 - Т3.2. Активация и выполнение вредоносного кода, внедренного в виде закладок в легитимное программное и программное-аппаратное обеспечение систем и сетей
 - Т3.16. 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.
- → Т4: Закрепление (сохранение доступа) в системе или сети:
 - Т4.1. 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
- \rightarrow T5: Управление вредоносным программным обеспечением и (или) компонентами, к которым ранее был получен доступ:
 - T5.7. 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:
 - 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
 - T7.4. 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
- \rightarrow T8: 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
- → 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
 - T10.8. Уничтожение информации, включая информацию, хранимую в виде файлов, информацию в базах данных и репозиториях, информацию на неразмеченных областях дисков и сменных носителей

УБИ $_{10}$ = [Электрик (Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.) (Н1)); 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:
 - Т10.10. Организация отказа в обслуживании одной или нескольких систем, компонентов системы или сети

УБИ₁₀ актуальна

УБИ $_{11}$ = [Террористическая организация (Террористические, экстремистские группировки (Н3)); Сервер с базой данных информационной системы; Получение доступа к базе данных через АРМ пользователя путем внедрения вредоносного программного обеспечения; Модификация всей хранящейся информации;]

- → Т1: 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
 - 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
 - Т1.12. 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
 - Т1.15. Поиск и покупка баз данных идентификационной информации, скомпрометированых паролей и ключей на специализированных нелегальных площадках
- → 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.

- 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)
- \rightarrow T3: Внедрение и исполнение вредоносного программного обеспечения в системах и сетях:
 - Т3.16. 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.
- → Т4: Закрепление (сохранение доступа) в системе или сети:
 - Т4.1. 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

- 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
- \rightarrow T5: Управление вредоносным программным обеспечением и (или) компонентами, к которым ранее был получен доступ:
 - T5.7. 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:

- 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
- T7.4. 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
- \rightarrow T10: Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям:
 - T10.7. 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

УБИ₁₁ актуальна

10. Определение для актуальных угроз мер защиты информации

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

		Г	T
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	Установка камер	Удаление/блокировка портов
	инструкций для	видеонаблюдения для	для подключения внешних
	обслуживающего и	видеофиксации всех	носителей информации;
	приглашенного персонала;	действий сотрудников;	
		, , , ,	Установка и своевременное
	Проведение инструктажей	Установка	обновление антивирусных
	по защите от воздействия	металлодетекторов и	средств на всех АРМ
	методами социальной	досмотр сотрудников для	сотрудников;
	инженерии;	пресечения фактов проноса	
		и выноса любых внешних	Разграничение прав доступа
	Разграничение доступа	носителей информации	сотрудников к определенным
	сотрудников на территорию	постелен тформации	сегментам памяти,
	и в отдельные помещения		программам и действиям
	объекта информатизации, а		(ролевая модель
	также к информационным		разграничения доступа)
			разграничения доступа)
	ресурсам информационной		
	СИСТЕМЫ		Maycotopas augasus account
6	Информирование	-	Межсетевое экранирование;
	сотрудников об		Mana ni aona ilia aona na mana
	обязательных		Использование генераторов
	использовании разных		сложных паролей и проверок
	сложных паролей и		на простоту паролей;
	своевременном их		и
	обновлении;		Использование систем
			двухфакторной
	Плановое проведение		аутентификации
	аудита безопасности сети		
7	Информирование	-	Межсетевое экранирование;
	сотрудников об		
	обязательных		Использование генераторов
	использовании разных		сложных паролей и проверок
	сложных паролей и		на простоту паролей;
	своевременном их		
	обновлении;		

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

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

- Разработка должностных инструкций для обслуживающего и приглашенного персонала
- о 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
- о Плановое проведение аудита безопасности сети
- о Мониторинг сетевой активности

• Организационно-технические:

- о Установка камер видеонаблюдения для видеофиксации всех действий сотрудников
- Установка металлодетекторов и досмотр сотрудников для пресечения фактов проноса и выноса любых внешних носителей информации
- о Обеспечение круглосуточной охраны важных технических помещений (серверных)
- о Обеспечение резервного питания важных технических объектов (в т. ч. серверов)

• Программно-технические:

- о Межсетевое экранирование
- о Использование генераторов сложных паролей и проверок на простоту паролей
- о Использование систем двухфакторной аутентификации
- о 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)