

ТОИБ: Лабораторная работа 2:

Таблица 1.

Предмет регулирования	обоснование
конституционные	Конституционные права действуют на всей территории государства, в том числе и на территории предприятия
административные	Взаимодействие органов власти и предприятия: например, лицензирование, контроль за безопасностью и т.д.
финансовые	Вопросы с финансами – это одни из базовых вопросов для коммерческих организаций: покупка сырья, продажа продукции, взятие кредитов и т.д.
земельные	Использование земельных участков, на которых расположено наше предприятие, их покупка и/или аренда
таможенные	Взаимодействие с таможней при покупке и продаже за границей
налоговые	Оплата налогов за прибыль, полученную после реализации продукции
гражданско-процессуальные	Так как периодически между гражданами (например, бывшими работниками) и предприятием возникают гражданско-правовые отношения, решаемые через суд, то предприятие периодически вступает в гражданско-процессуальные отношения
информационные	Правила публикации открытой информации. Правила работы с конфиденциальной и закрытой информацией. Правила работы с персональными данными и т.п
гражданско-правовые	Предприятие и граждане (например, работники) являются субъектами гражданского права, между которыми осуществляется взаимодействие по тем или иным вопросам

экологические	Регулирование воздействия на экологию со стороны предприятия
трудовые	Трудовые отношения между предприятием и работниками

Таблица 2. Текущее задание: 2

1. Почему информация должна являться объектом права?	
Секретная информация (С, СС, ОВ)	Секретная информация содержит сведения, для получения которых у гражданина должен быть соответствующий доступ. Если доступ к такой информации получает гражданин без этой формы допуска, то это нарушение прав доступа к информации. Если же гражданин разглашает подобную информацию, то это неправомочное разглашение секретной информации. Если же гражданин передает ее другой стране (или другой компании), то это уже шпионаж.
Конфиденциальная информация	Конфиденциальная информация содержит сведения, для получения которых у гражданина должно быть разрешение от лица, владеющего этой конфиденциальной информацией. Если у гражданина такого разрешения нет, и он использует эту информацию для своей выгоды или разглашает ее, то у такого гражданина наступает ответ
Персональные данные	Персональные данные содержит сведения, позволяющие установить личность того или иного гражданина. Доступ к этим данным можно получить только с разрешения этого гражданина. В противном случае это будет нарушение его прав.
Информация ДСП	Существует проект постановления Правительства РФ от 01.12.2021 г. "Об утверждении Положения о порядке обращения с документами для служебного пользования" – т.е. обращение с ДСП информацией также регламентирована с точки зрения закона.
Общедоступная информация	Пользователь может использовать открытые данные свободно, бесплатно, бессрочно, безвозмездно и без ограничения территории использования. Однако он обязан использовать их: только в законных целях, не искажать, сохранять ссылку на источник информации. Т.е. у пользователя есть не только права, но и обязанности.
2. Какой социальный эффект достигается?	
Секретная информация (С, СС, ОВ)	Общество знает, что секретная информация надежно защищена, что ведет к надежной защите интересов государства.

Конфиденциальная информация	Общество и каждый гражданин знают, что конфиденциальная информация (например, медицинские данные) не попадет не в те руки и не будет использована с преступным умыслом против отдельного гражданина, всего общества или государства.
Персональные данные	Каждый гражданин может быть уверен (в идеальном мире), что его персональные данные без его ведома не попадут в чьи-либо руки и не будут использованы для преступных целей.
Информация ДСП	Персонал, использующий информацию с грифом ДСП знает, что его деятельность с такой информацией четко регламентирована.
Общедоступная информация	Общество и граждане знают, что общедоступная информация, которую они могут как предоставлять, так и получать не искажена и используется только в законных целях.
3. Какие нормы и правила?	
Секретная информация (С, СС, ОВ)	Федеральный закон «О государственной тайне»
Конфиденциальная информация	Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) "Об утверждении Перечня сведений конфиденциального характера"
Персональные данные	Федеральный закон «О персональных данных» и т.д.
Информация ДСП	Проект постановления Правительства РФ от 01.12.2021 г. "Об утверждении Положения о порядке обращения с документами для служебного пользования" (01/01/12-21/00123026)
Общедоступная информация	Федеральный закон "Об информации, информационных технологиях и о защите информации"
4. Что применяется: запреты и обязывания, льготы и дозволения	
Секретная информация (С, СС, ОВ)	Получение разрешения для работы с секретными данными от соответствующих органов. Соглашение о неразглашении секретной информации. Статьи УК
Конфиденциальная информация	Получение разрешения для работы с конфиденциальной информацией от ее владельца. Соглашение о неразглашении конфиденциальных данных. Статьи УПК
Персональные данные	Получение от гражданина разрешения на сбор и обработку его персональных данных.

Информация ДСП	Внутренние регламенты по работе с ДСП документами
Общедоступная информация	Обязательство использования открытой информации только в законных целях, без искажения, с сохранением ссылки на источник информации.

Таблица 3. Текущее задание: 3

Вид информации	ТИП конфиденциальности	Релевантные (относящиеся) законы РФ
Бумажные		
1. Бумажные чертежи и документация военной продукции	С, СС, ОВ, ДСП (в некоторых случаях)	Федеральный закон «О государственной тайне» Проект постановления Правительства РФ от 01.12.2021 г. "Об утверждении Положения о порядке обращения с документами для служебного пользования" (01/01/12-21/00123026)
2. Бумажные чертежи и документация гражданской продукции	С, ДСП, коммерческая тайна	Федеральный закон «О государственной тайне» Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) "Об утверждении Перечня сведений конфиденциального характера" Проект постановления Правительства РФ от 01.12.2021 г. "Об утверждении Положения о порядке обращения с документами для служебного пользования" (01/01/12-21/00123026)
3. Бумажная документация на автоматизированную линию сборки	ДСП, коммерческая тайна	Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) "Об утверждении

		<p>"Перечня сведений конфиденциального характера"</p> <p>Проект постановления Правительства РФ от 01.12.2021 г. "Об утверждении Положения о порядке обращения с документами для служебного пользования" (01/01/12-21/00123026)</p>
4. Бумажная справочная литература	ДСП, коммерческая тайна, без ограничений	<p>Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ</p> <p>Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) "Об утверждении Положения о порядке обращения с документами для служебного пользования" (01/01/12-21/00123026)</p>
Электронные		
1. Информация о работниках	Персональные данные	<p>Федеральный закон «О персональных данных»</p> <p>«Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 февраля 2008 года[12];</p> <p>«Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» утв. ФСТЭК РФ 14 февраля 2008 года[12];</p> <p>«Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» приказ ФСТЭК России от</p>

		<p>18.02.2013 № 21 (Зарегистрировано в Минюсте России 14.05.2013 № 28375).</p> <p>«Об утверждении требований и методов по обезличиванию персональных данных» приказ Роскомнадзора от 05.09.2013 № 996 (Зарегистрировано в Минюсте России 10.09.2013 N 29935);</p> <p>"Методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» утв. Роскомнадзором 13.12.2013;</p>
2. Электронные чертежи и документация военной продукции	С, СС, ОВ, ДСП (в некоторых случаях)	<p>Федеральный закон «О государственной тайне»</p> <p>Проект постановления Правительства РФ от 01.12.2021 г. "Об утверждении Положения о порядке обращения с документами для служебного пользования" (01/01/12-21/00123026)</p>
3. Электронные чертежи и документация гражданской продукции	С, ДСП, коммерческая тайна	<p>Федеральный закон «О государственной тайне»</p> <p>Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ</p> <p>Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) "Об утверждении Перечня сведений конфиденциального характера"</p> <p>Проект постановления Правительства РФ от 01.12.2021 г. "Об утверждении Положения о порядке обращения с документами для служебного пользования" (01/01/12-21/00123026)</p>
4. Настройки и конфигурация автоматизированной линии сборки	ДСП, коммерческая тайна	<p>Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ</p> <p>Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) "Об утверждении</p>

		<p>"Перечня сведений конфиденциального характера"</p> <p>Проект постановления Правительства РФ от 01.12.2021 г. "Об утверждении Положения о порядке обращения с документами для служебного пользования" (01/01/12-21/00123026)</p>
5. Настройка и конфигурация системы безопасности	ДСП, Конфиденциальные данные	<p>Проект постановления Правительства РФ от 01.12.2021 г. "Об утверждении Положения о порядке обращения с документами для служебного пользования" (01/01/12-21/00123026)</p> <p>Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) "Об утверждении Перечня сведений конфиденциального характера"</p>
6. Электронная схема сетей и коммуникаций	ДСП, Конфиденциальные данные	<p>Проект постановления Правительства РФ от 01.12.2021 г. "Об утверждении Положения о порядке обращения с документами для служебного пользования" (01/01/12-21/00123026)</p> <p>Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) "Об утверждении Перечня сведений конфиденциального характера"</p>
7. Электронные данные о закупках оборудования и материалов для военной продукции	С, ДСП	<p>Федеральный закон «О государственной тайне»</p> <p>Проект постановления Правительства РФ от 01.12.2021 г. "Об утверждении Положения о порядке обращения с документами для служебного пользования" (01/01/12-21/00123026)</p>
8. Электронные данные о закупках оборудования и материалов для гражданской продукции	ДСП, Конфиденциальные данные	<p>Проект постановления Правительства РФ от 01.12.2021 г. "Об утверждении Положения о порядке обращения с документами для служебного пользования" (01/01/12-21/00123026)</p>

		Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) "Об утверждении Перечня сведений конфиденциального характера"
--	--	--

Таблица 4.1. Текущее задание 4

	ТИП конфиденциальности	Модель нарушителя	Способ использования и ущерб	Правовые меры по защите
Данные на сервере по персональным данным	Персональные данные	конкуренты	Размещение в соц сетях. Дискредитация	Соглашение о неразглашении
Бумажные				
1. Бумажные чертежи и документация военной продукции	С, СС, ОВ, ДСП (в некоторых случаях)	Спецслужбы других государств, конкуренты, недобросовестные сотрудники	Способ использования: получение знаний о секретных особенностях современной военной техники для выработки способов противодействия, либо для создания своих аналогов (или даже прямого копирования). Ущерб: снижение обороноспособности государства, потеря в конкурентной гонке на рынке	Законы о государственной тайне Соглашение о неразглашении секретной информации Статьи УК Внутренние регламенты по работе с ДСП документами Регистрация патентов

			вооружений, денежные потери, дискредитация предприятия и государства	
2. Бумажные чертежи и документация гражданской продукции	С, ДСП, коммерческая тайна	Конкуренты, недобросовестные сотрудники	<p>Способ использования: получение знаний о внутреннем устройстве и способах функционирования, которые невозможно получить из открытых источников, создание своих аналогов (или даже прямого копирования).</p> <p>Ущерб: получение конкурентного преимущества на рынке, денежные потери, дискредитация предприятия.</p>	<p>Законы о государственной тайне</p> <p>Законы о коммерческой тайне</p> <p>Соглашение о неразглашении секретной информации</p> <p>Соглашение о неразглашении коммерческой тайны</p> <p>Статьи УПК</p> <p>Регистрация патентов</p> <p>Внутренние регламенты по работе с ДСП документами</p>
3. Бумажная документация на автоматизированную линию сборки	ДСП, коммерческая тайна	Конкуренты, недобросовестные сотрудники	<p>Способ использования: получение знаний о технологиях сборки/обработки изделий.</p> <p>Ущерб: получение</p>	<p>Законы о коммерческой тайне</p> <p>Соглашение о неразглашении коммерческой тайны</p> <p>Статьи УПК</p>

			конкурентного преимущества на рынке, денежные потери, дискредитация предприятия.	Внутренние регламенты по работе с ДСП документами
4. Бумажная справочная литература	ДСП, коммерческая тайна, без ограничений	Конкуренты, недобросовестные сотрудники	Способ использования: получение знаний, которые невозможно получить из открытых источников. Ущерб: получение конкурентного преимущества на рынке.	Законы о коммерческой тайне Соглашение о неразглашении коммерческой тайны Статьи УПК Внутренние регламенты по работе с ДСП документами
Электронные				
1. Информация о работниках	Персональные данные	Хакеры, преступные группировки, недобросовестные сотрудники	Способ использования: продажа данных преступным группировкам, использование в преступных целях, размещение в соц.сетях. Ущерб: фишинг, спам, разглашение информации о работе тот или	Законодательство о персональных данных Внутренние регламенты по обработке персональных данных

			иного гражданина на данном предприятии, денежные и репутационные потери	
2. Электронные чертежи и документация военной продукции	С, СС, ОВ, ДСП (в некоторых случаях)	Спецслужбы других государств, хакеры, недобросовестные сотрудники	<p>Способ использования: получение знаний о секретных особенностях современной военной техники для выработки способов противодействия, либо для создания своих аналогов (или даже прямого копирования).</p> <p>Ущерб: снижение обороноспособности государства, потеря в конкурентной гонке на рынке вооружений, денежные потери, дискредитация предприятия и государства</p>	<p>Законы о государственной тайне</p> <p>Соглашение о неразглашении секретной информации</p> <p>Статьи УК</p> <p>Внутренние регламенты по работе с ДСП данными</p> <p>Регистрация патентов</p>
3. Электронные чертежи и документация	С, ДСП, коммерческая тайна	Конкуренты, хакеры,	Способ использования: получение	Законы о государственной тайне

гражданской продукции		недобросовестные сотрудники	<p>заний о внутреннем устройстве и способах функционирования, которые невозможно получить из открытых источников, создание своих аналогов (или даже прямого копирования).</p> <p>Ущерб: получение конкурентного преимущества на рынке, денежные потери, дискредитация предприятия.</p>	<p>Законы о коммерческой тайне</p> <p>Соглашение о неразглашении секретной информации</p> <p>Соглашение о неразглашении коммерческой тайны</p> <p>Статьи УПК</p> <p>Регистрация патентов</p> <p>Внутренние регламенты по работе с ДСП данными</p>
4. Настройки и конфигурация автоматизированной линии сборки	ДСП, коммерческая тайна	Конкуренты, хакеры, недобросовестные сотрудники	<p>Способ использования: получение знаний о технологиях сборки/обработки изделий, внесение таких изменений, которые могут как ухудшить работу оборудования, так и сломать его.</p> <p>Ущерб: получение конкурентного</p>	<p>Законы о коммерческой тайне</p> <p>Соглашение о неразглашении коммерческой тайны</p> <p>Статьи УПК</p> <p>Внутренние регламенты по работе с ДСП данными</p>

			преимущества на рынке, денежные потери, дискредитация предприятия.	
5. Настройка и конфигурация системы безопасности	ДСП, Конфиденциальные данные	Конкуренты, хакеры, недобросовестные сотрудники	Способ использования: поиск уязвимостей в защите, продажа хакерским группировкам или конкурентам Ущерб: осуществление атак с целью получения секретных и конфиденциальных данных, либо с целью нарушения нормального функционирования системы безопасности и самого предприятия	Законы о конфиденциальных данных Соглашение о неразглашении конфиденциальных данных Статьи УПК Внутренние регламенты по работе с ДСП данными
6. Электронная схема сетей и коммуникаций	ДСП, Конфиденциальные данные	Спецслужбы других государств, преступные группировки, хакеры, недобросовестные сотрудники	Способ использования: поиск уязвимостей для физического проникновения, либо для размещения устройств, считывающих	Законы о конфиденциальных данных Соглашение о неразглашении конфиденциальных данных Статьи УПК

			<p>информацию (видео, аудио, через поля), продажа заинтересованным в проникновении лицам, создание аварийных ситуаций</p> <p>Ущерб: незаконное физическое проникновение, размещения устройств, считывающих информацию, денежные потери, загрязнение экологии (из-за техногенной аварии), дискредитация предприятия.</p>	Внутренние регламенты по работе с ДСП данными
7. Электронные данные о закупках оборудования и материалов для военной продукции	С, ДСП	Спецслужбы других государств, хакеры, недобросовестные сотрудники	<p>Способ использования: получение информации о закупаемых материалах и оборудования, получение информации о поставщиках, продажа этой информации заинтересованным лицам.</p> <p>Ущерб: получение</p>	<p>Законы о государственной тайне</p> <p>Соглашение о неразглашении секретной информации</p> <p>Статьи УПК</p> <p>Внутренние регламенты по работе с ДСП данными</p>

			некоторой информации о секретных военных изделиях, получение конкурентного преимущества на рынке, денежные потери, дискредитация предприятия и государства.	
8. Электронные данные о закупках оборудования и материалов для гражданской продукции	ДСП, Конфиденциальные данные	Конкуренты, хакеры, недобросовестные сотрудники	Способ использования: получение информации о закупаемых материалах и оборудования, получение информации о поставщиках, продажа этой информации заинтересованным лицам. Ущерб: получение конкурентного преимущества на рынке, денежные потери, дискредитация предприятия.	Законы о конфиденциальных данных Соглашение о неразглашении конфиденциальных данных Статьи УПК Внутренние регламенты по работе с ДСП данными

Таблица 4.2. Текущее задание 4

1. идентификация и аутентификация

2. разграничение доступа (и изоляция)
3. регистрация событий и аудит
4. контроль целостности
5. шифрование данных и ЭП
6. резервирование и резервное затирание остаточной информации
7. обнаружение и обезвреживание вирусов
8. фильтрация трафика и трансляция адресов
9. выявление и устранение уязвимостей
10. обнаружение вторжений (атак)
11. маскировка и создание ложных объектов

ВАШИ ВИДЫ ИНФОРМАЦИИ	1	2	3	4	5	6	7	8	9	10	11
Бумажные											
1. Бумажные чертежи и документация военной продукции	1	1	1	0	0	0	0	0	0	0	0
2. Бумажные чертежи и документация гражданской продукции	1	1	1	0	0	0	0	0	0	0	0
3. Бумажная документация на автоматизированную линию сборки	1	1	1	0	0	0	0	0	0	0	0
4. Бумажная справочная литература	1/0	1/0	0/1	0	0	0	0	0	0	0	0
Электронные											
1. Информация о работниках	1	1	1	1	1	1	1	0	0	0	0
2. Электронные чертежи и документация военной продукции	1	1	1	1	1	1	1	0	0	0	0
3. Электронные чертежи и документация гражданской продукции	1	1	1	1	1	1	1	0	0	0	0

3. Файловые хранилища	1	1	1	1	1	1	1	1	1	1	1
4. ПО на рабочих станциях	1	1	1	1	1	1	1	1	1	1	1
5. ПО на оборудовании линии сборки	1	1	1	1	1	1	1	1	1	1	1
6. Общедоступная информация для чтения в сети Интернет	0	0	1	1	0	1	1	1	1	1	1

* Примечание:

1 – применяется или целесообразно применить.

0 – не применимо или нецелесообразно

Бумажная справочная литература частично открытая, частично является коммерческой тайной или имеет допуск ДСП. Для открытой бумажной справочной литературы, мы считаем, что никакие меры применять не нужно.

Таблица 5.

1 Возможность физической защиты

2 Возможность воздействий:

2.1 Природных

2.2. Технических

2.3 Преднамеренных

3 Необходимость физической защиты

4. Внутренние меры:

4.1 Маркировка (идентификация)

4.2 Разграничение доступа в помещение, кодовые замки

4.3 Охранная сигнализация помещений, контроль вскрытие компьютеров

4.4 Охрана помещений

4.5 Физическая изоляция портов

4.6 Подавление излучений (видео, аудио, ЭМИ)

4.7 Биометрическая идентификация при аутентификации и в помещения

4.8 Другие (ваш вариант)

5 Внешние:

5.1 Нейтрализация излучений за пределами периметра

5.2 Охрана территории

5.3 Контроль выноса

5.4 Внешнее легендирование зданий и территории

ВАШИ ВИДЫ ИНФОРМАЦИИ ДЛЯ ВАШЕГО ВАРИАНТА	1	2	3	4	5
Бумажные					
1. Бумажные чертежи и документация военной продукции	1	2.1-2.3	3	4.1-4.4	5.2-5.3
2. Бумажные чертежи и документация гражданской продукции	1	2.1-2.3	3	4.1-4.4	5.2-5.3
3. Бумажная документация на автоматизированную линию сборки	1	2.1-2.3	3	4.1-4.4	5.2-5.3
4. Бумажная справочная литература	1	2.1-2.3	3	4.1-4.4	5.2-5.3
Электронные					
1. Информация о работниках	1	2.1-2.3	3	4.1-4.4	5.2-5.3
2. Электронные чертежи и документация военной продукции	1	2.1-2.3	3	4.1-4.4	5.2-5.3
3. Электронные чертежи и документация гражданской продукции	1	2.1-2.3	3	4.1-4.4	5.2-5.3
4. Настройки и конфигурация автоматизированной линии сборки	1	2.1-2.3	3	4.1-4.4	5.2-5.3
5. Настройка и конфигурация системы безопасности	1	2.1-2.3	3	4.1-4.4	5.2-5.3
6. Электронная схема сетей и коммуникаций	1	2.1-2.3	3	4.1-4.4	5.2-5.3
7. Электронные данные о закупках оборудования и материалов для военной продукции	1	2.1-2.3	3	4.1-4.4	5.2-5.3
8. Электронные данные о закупках оборудования и материалов для гражданской продукции	1	2.1-2.3	3	4.1-4.4	5.2-5.3
Поля					
1. Совещания, с использованием видео и аудио связи	1	2.1-2.3	3	4.1-4.4, 4.6	5.1-5.3
Технологические линии					
1. Линии сборки	1	2.1-2.3	3	4.1-4.4, 4.6, 4.7	5.1-5.4

Образцы					
1. Прототипы изделий	1	2.1-2.3	3	4.1-4.4, 4.6, 4.7	5.1-5.4
По типам оборудования					
1. Сервера	1	2.1-2.3	3	4.1-4.7	5.1-5.3
2. Сетевое оборудование	1	2.1-2.3	3	4.1-4.7	5.1-5.3
3. Беспроводное оборудование	1	2.1-2.3	3	4.1-4.7	5.1-5.3
4. Оборудование систем безопасности	1	2.1-2.3	3	4.1-4.7	5.1-5.3
5. Оборудование для энергоснабжения	1	2.1-2.3	3	4.1-4.7	5.1-5.3
По типам ПО					
1. ОС	1	2.1-2.3	3	4.1-4.7	5.2-5.3
2. БД	1	2.1-2.3	3	4.1-4.7	5.2-5.3
3. Файловые хранилища	1	2.1-2.3	3	4.1-4.7	5.2-5.3
4. ПО на рабочих станциях	1	2.1-2.3	3	4.1-4.7	5.2-5.3
5. ПО на оборудовании линии сборки	1	2.1-2.3	3	4.1-4.7	5.2-5.3
6. Общедоступная информация для чтения в сети Интернет	1	2.1-2.3	3	4.1-4.5	5.2-5.3

Таблица 6.

Должности ПО ВАШЕМУ ВАРИАНТУ	Уровень знаний	Способ воздействия	Меры защиты
Администратор ИБ, менеджеры банка	Пароли	Ночной звонок для выведывания пароля	Сокрытие перс. данных каналов связи вне работы, обучение
Оператор банка	Номера карт	Запрос по почте от имени босса	Сокрытие перс. данных, каналов связи, обучение
администратор	Доступ практически во все	Использование методов	Использование многофакторной

	подсистемы, доступ к бекапам, пароли, архитектура/схема построения системы ИБ	социальной инженерии, фишинг, угрозы, подкуп	аутентификации, регистрация всех действий, метод минимальных привилегий (администратору БД не нужен полный доступ, например, к AD), работа СБ
сотрудник отдела кадров	Доступ к персональным данным пользователей	Использование методов социальной инженерии, фишинг, угрозы, подкуп	Использование многофакторной аутентификации, регистрация всех действий, метод минимальных привилегий, защита на уровне оборудования (физическое блокирование портов, работа без выхода во внешнюю сеть), работа СБ
рабочий	Доступ к линии сборке, к собираемым изделиям, к части чертежей	Угрозы, подкуп	Запрет использования на территории предприятия мобильных телефонов, фотоаппаратов и т.д. Контроль работников на вынос чертежей, документации, изделий и их частей. Работа СБ. Использование системы видеонаблюдения
сотрудник охраны	Доступ во многие помещения и к линии сборки.	Угрозы, подкуп	Запрет использования на территории предприятия мобильных телефонов, фотоаппаратов и т.д. Контроль работников на вынос изделий и их частей. Работа СБ. Использование системы видеонаблюдения. Запрет обхода территории по одному
инженер	Доступ к линии сборке, к собираемым	Использование методов социальной инженерии,	Запрет использования на территории предприятия мобильных телефонов, фотоаппаратов и т.д. Контроль работников на

	изделиям, к чертежам	фишинг, угрозы, подкуп	вынос чертежей, документации, изделий и их частей. Использование многофакторной аутентификации, регистрация всех действий, защита на уровне оборудования (физическое блокирование портов, работа без выхода во внешнюю сеть), работа СБ. Использование системы видеонаблюдения.
руководство	Доступ к большинству секретной информации	Использование методов социальной инженерии, фишинг, угрозы, подкуп	Использование многофакторной аутентификации, регистрация всех действий, защита на уровне оборудования (физическое блокирование портов, работа без выхода во внешнюю сеть), работа СБ. Использование системы видеонаблюдения.

Таблица 7.

Техника	Что могут выведать у сотрудников вашего предприятия	Методы противодействия
1. Фишинг	Данные аутентификации Доступ ко внутренним системам и сетям Закрытую или конфиденциальную информацию и документацию.	Многофакторная аутентификация Обучение сотрудников распознаванию фишинговых сообщений. Проведение регулярных проверок. Регистрация всех действий. IDS/IPS системы

2. Вишинг	Данные аутентификации Закрытую или конфиденциальную информацию	Создание протокола идентификации звонящего. Обучение персонала
3. Претекстинг	Данные аутентификации Доступ ко внутренним системам и сетям Закрытую или конфиденциальную информацию и документацию.	Создание протоколов обмена чувствительной и секретной информацией. Обучение персонала. Регистрация всех действий. IDS/IPS системы
4. Квид про кво (Quid pro quo)	Данные аутентификации Закрытую или конфиденциальную информацию и документацию.	Создание протоколов обмена чувствительной и секретной информацией. Обучение персонала. Регистрация всех действий.
5. Дорожное яблоко (Baiting)	Доступ ко внутренним системам и сетям Закрытую или конфиденциальную информацию и документацию.	Физическое блокирование портов. Обучение сотрудников не использовать неизвестные устройства. Регулярные проверки. Регистрация всех действий. IDS/IPS системы
6. Сбор информации из открытых источников (OSINT)	Информация о том, кто является сотрудником, подробности работы: должность, обязанности и т.д.	Регулярные проверки открытых источников и социальных сетей работников. Обучение персонала
7. Плечевой серфинг (Shoulder surfing)	Данные аутентификации Закрытую или конфиденциальную информацию	Запрет на выход с рабочими УЗ за пределами предприятия. Работа с секретными данными в специально отведенных для этого местах

8. Обратная социальная инженерия	Данные аутентификации Закрытую или конфиденциальную информацию	Создание протоколов взаимодействия с другими подразделениями. Обучение персонала. Регистрация всех действий.
----------------------------------	---	---