Индивидуальный предприниматель Котин Александр Сергеевич
ИНН 662314246941, ОГРНИП 318665800034671,
620076, Свердловская обл., город Екатеринбург, ул. Щербакова, д. 20, кв. 337

Котин Александр Сергеевич

Подписано цифровой подписью: Котин Александр Сергеевич
DN: 1.2.643.100.5=120F3331383636353830303033363731, 1.2.643.100.3=120B303237343703134333337, 1.2.643.3.131.1.1=120C3636323331343234363934 31, email=akotin@bk.ru, c=RU, cn=Котин Александр Сергеевич, givenName=Александр Сергеевич, sn=Котин
Дата: 2025.04.29 14:37:02 +05'00'
Версия Adobe Acrobat Reader: 2024.005.20320

УТВЕРЖДАЮ
Индивидуальный предприниматель
Котин Александр Сергеевич

МП подпись
18 марта 2025 г.

МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

Настоящая Модель угроз безопасности персональных данных (далее – Модель угроз), в информационной системе персональных данных Индивидуального предпринимателя Котина Александра Сергеевича (ИНН 662314246941, ОГРНИП 318665800034671) (далее – ИСПДн), разработана на основании следующих документов:

– Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

– Методика оценки угроз безопасности информации (утв. ФСТЭК России 05 февраля 2021 г.);

– Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСТЭК России 15 февраля 2008 г.);

– Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Модель угроз используется при разработке системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса ИСПДн.

Ответственным за обеспечение защиты персональных данных Индивидуального предпринимателя Котина Александра Сергеевича (далее - ИП) является Ответственный за безопасность персональных данных, который назначается приказом ИП.

2. Основные понятия

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (далее – ПДн);

Персональные данные, разрешенные субъектом персональных данных для распространения – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном настоящим Федеральным законом;

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (далее – ИСПДн);

Автоматизированная система – это система, состоящая из персонала и комплекса средств автоматизации его деятельности и реализует информационную технологию выполнения установленных функций (далее – АС);

Автоматизированная информационная система – это совокупность программных и аппаратных средств, предназначенных для хранения и (или) управления данными и информацией, а также для производства вычислений (далее – АИС);

Информационная безопасность – это сохранение и защита информации, а также ее важнейших элементов, в том числе системы и оборудование, предназначенные для использования, сбережения и передачи этой информации (далее – ИБ);

НСД – несанкционированный доступ;

ПСЗИ – программная система защиты информации;

СВТ – средство вычислительной техники;

СФ СЗПДн – среда функционирования системы защиты персональных данных;

Система защиты персональных данных – это комплекс мер и мероприятий организационного и технического характера, направленных на противодействие несанкционированному доступу к закрытой информации с учетом актуального типа угроз безопасности (далее – СЗПДн).

3. Состав и структура персональных данных

3.1. В ИСПДн ИП обрабатываются следующие персональные данные: **фамилия, имя, отчество субъекта, дата рождения, адрес местожительства или регистрации, семейное положение, данные паспорта.**

3.2. В соответствии с пп. 6 и 7 «Требований к защите персональных данных при их обработке в информационных системах персональных данных», утверждённых постановлением Правительства от 1 ноября 2012 г. № 1119 и Актом оценки потенциального вреда субъектам персональных данных ИП для информационной системы Оператора актуальны угрозы безопасности персональных данных 3-го типа. С учётом того, что информационная система Оператора обрабатывает персональные данные менее чем 100 000 субъектов персональных

данных, необходимо обеспечение 4-го уровня защищённости персональных данных при их обработке в информационной системе Оператора.

4. Общее описание информационно-технологической структуры

4.1. Персональные данные обрабатываются ИП в следующих целях: обеспечение соблюдения законодательных и иных нормативных правовых актов РФ, локальных нормативных актов Оператора; исполнения обязанностей, возложенных законодательством РФ на Оператора, в том числе связанных с представлением персональных данных в налоговые органы, Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования, а также в иные государственные органы; регулирования трудовых отношений с работниками Оператора (трудоустройство, контроль количества и качества выполняемой работы, обеспечение сохранности имущества); исполнения судебных актов, актов других государственных органов или должностных лиц; реализации прав и законных интересов Оператора в рамках ведения видов деятельности, предусмотренных локальными нормативными актами Оператора, или третьих лиц либо достижения общественно значимых целей.

4.2. ИП имеет собственную локальную вычислительную сеть, к которой подключены базы данных информации, содержащие персональные данные граждан РФ по следующему адресу: 620076, Свердловская обл., город Екатеринбург, ул. Щербакова, д. 20, кв. 337.

4.3. Доступ в офис ИП осуществляется одним из следующих способов:

– вход при помощи механического средства защиты от взлома.

4.4. Средства защиты в виде антивирусной программы установлены на рабочих местах и на серверах ИП.

4.5. Доступ в системы осуществляется по индивидуальному логину и паролю.

4.6. Каждому работнику осуществляется рассылка информационных материалов и нормативных документов в области информационной безопасности.

5. Возможные негативные последствия от реализации (возникновения) угроз безопасности персональных данных

5.1. Виды рисков, которые могут наступить от нарушения или прекращения основных процессов:

– ущерб физическому лицу;

– риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью

– ущерб государству в области обеспечения безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности и другие;

5.2. Возможные негативные последствия, наступление которых может привести к возникновению риска, представлены в Таблице ниже:

№	Виды риска (ущерба)	Возможные типовые негативные последствия
У1	Ущерб физическому лицу	Угроза жизни или здоровью. Унижение достоинства личности. Нарушение свободы, личной неприкосновенности. Нарушение неприкосновенности частной жизни. Нарушение личной, семейной тайны, утрата чести и доброго имени. Нарушение тайны переписки, телефонных переговоров, иных сообщений. Нарушение иных прав и свобод гражданина, закреплённых в Конституции Российской Федерации и федеральных законах. Финансовый, иной материальный ущерб физическому лицу. Нарушение конфиденциальности (утечка) персональных данных. "Травля" гражданина в сети "Интернет". Разглашение персональных данных граждан.
У2	Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью	Нарушение законодательства Российской Федерации. Потеря (хищение) денежных средств. Недополучение ожидаемой (прогнозируемой) прибыли. Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций. Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств). Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса. Срыв запланированной сделки с партнёром. Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. Потеря клиентов, поставщиков. Потеря конкурентного преимущества. Невозможность заключения договоров, соглашений.

		Нарушение деловой репутации. Снижение престижа. Дискредитация работников. Утрата доверия. Причинение имущественного ущерба. Неспособность выполнения договорных обязательств. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций). Необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций). Принятие неправильных решений. Простой информационной системы или сети. Публикация недостоверной информации на веб-ресурсах организации. Использование веб-ресурсов для распространения и управления вредоносным программным обеспечением. Рассылка информационных сообщений с использованием вычислительных мощностей оператора и (или) от его имени. Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.)
У3	Ущерб государству в области обеспечения безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности	Причинение ущерба жизни и здоровью людей. Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения. Прекращение или нарушение функционирования сети связи. Прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций в системно значимой кредитной организации, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем, системно значимой инфраструктурной организацией финансового рынка. Вредные воздействия на окружающую среду. Прекращение или нарушение функционирования пункта управления (ситуационного центра). Нарушение законодательства Российской Федерации. Публикация недостоверной социально значимой информации на веб-ресурсах, которая может привести к социальной напряженности, панике среди населения и др. Нарушение штатного режима функционирования автоматизированной системы управления и

		управляемого объекта и/или процесса, если это ведет к выводу из строя технологических объектов, их компонентов. Нарушение общественного правопорядка, возможность потери или снижения уровня контроля за общественным правопорядком. Нарушение выборного процесса. Отсутствие возможности оперативного оповещения населения о чрезвычайной ситуации. Организация пикетов, забастовок, митингов и других акций. Массовые увольнения. Появление негативных публикаций в общедоступных источниках. Доступ к системам и сетям с целью незаконного использования вычислительных мощностей. Утечка информации ограниченного доступа.

6. Возможные объекты воздействия угроз безопасности персональных данных

6.1. Примеры возможных объектов воздействия определим для следующих видов негативных последствий: разглашение персональных данных граждан; хищение денежных средств со счета организации; срыв запланированной сделки с партнером.

Негативные последствия	Объекты воздействия	Виды воздействия
Разглашение персональных данных граждан (У1)	База данных информационной системы, содержащая идентификационную информацию граждан	Утечка идентификационной информации граждан из базы данных
	Удаленное автоматизированное рабочее место (АРМ) пользователя	Утечка идентификационной информации граждан с АРМ пользователя
	Линия связи между сервером основного центра обработки данных и сервером резервного центра обработки данных	Перехват информации, содержащей идентификационную информацию граждан, передаваемой по линиям связи
	Веб-приложение информационной системы, обрабатывающей идентификационную информацию граждан	Несанкционированный доступ к идентификационной информации граждан, содержащейся в веб-приложении

		информационной системы
Хищение денежных средств со счета организации (У2)	Банк-клиент	Несанкционированная подмена данных, содержащихся в реквизитах платежного поручения
	АРМ финансового директора	Несанкционированная модификация информации в платежных распоряжениях и отправка недостоверных распоряжений от имени финансового директора
	Электронный почтовый ящик финансового директора	Модификация информации в платежных распоряжениях и отправка недостоверных распоряжений от имени финансового директора
	АРМ главного бухгалтера	Подмена данных, содержащих реквизиты платежных поручений и другой платежной информации на АРМ главного бухгалтера
Срыв запланированной сделки с партнером (У2)	АРМ руководителя организации	Модификация информации и отправка электронных писем с недостоверной информацией от имени руководителя организации
	Электронный почтовый ящик руководителя организации	Модификация информации и отправка электронных писем с недостоверной информацией от имени руководителя организации

7. Классификация нарушителей

7.1. По признаку принадлежности к ИСПДн все нарушители делятся на две группы:

- внешние нарушители - физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн;
- внутренние нарушители - физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн.

7.2. В качестве внешнего нарушителя информационной безопасности, рассматривается нарушитель, который не имеет непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны. Предполагается, что внешний нарушитель не может воздействовать на защищаемую информацию по техническим каналам утечки, так как объем информации, хранимой и обрабатываемой в ИСПДн, является недостаточным для возможной мотивации внешнего нарушителя к осуществлению действий, направленных утечку информации по техническим каналам утечки. Предполагается, что внешний нарушитель может воздействовать на защищаемую информацию только во время ее передачи по каналам связи.

7.3. Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированного доступа. Система разграничения доступа ИСПДн обеспечивает разграничение прав пользователей на доступ к информационным, программным, аппаратным и другим ресурсам ИСПДн в соответствии с принятой политикой информационной безопасности (правилами).

К внутренним нарушителям могут относиться:

- системный администратор (категория I);
- программист (категория II);
- пользователи ИСПДн (категория III);
- пользователи, являющиеся внешними по отношению к конкретной АС (категория IV);
- лица, обладающие возможностью доступа к системе передачи данных (категория V);
- сотрудники ИП, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются элементы ИСПДн, но не имеющие права доступа к ним (категория VI);
- обслуживающий персонал (работники инженерно-технических служб и т.д.) (категория VII);
- уполномоченный персонал разработчиков ИСПДн, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИСПДн (категория VIII).

На лиц категорий I и II возложены задачи по администрированию программно-аппаратных средств и баз данных ИСПДн для интеграции и обеспечения взаимодействия различных подсистем, входящих в состав ИСПДн. Администраторы потенциально могут реализовывать угрозы ИБ, используя возможности по непосредственному доступу к защищаемой

информации, обрабатываемой и хранимой в ИСПДн, а также к техническим и программным средствам ИСПДн, включая средства защиты, используемые в конкретных АС, в соответствии с установленными для них административными полномочиями. Эти лица хорошо знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и ИСПДн в целом, а также с применяемыми принципами и концепциями безопасности. Предполагается, что они могли бы использовать стандартное оборудование либо для идентификации уязвимостей, либо для реализации угроз ИБ. Данное оборудование может быть, как частью штатных средств, так и может относиться к легко получаемому (например, программное обеспечение, полученное из общедоступных внешних источников). Кроме того, предполагается, что эти лица могли бы располагать специализированным оборудованием.

К лицам категорий I и II ввиду их исключительной роли в ИСПДн должен применяться комплекс особых организационно-режимных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей. Предполагается, что в число лиц категорий I и II будут включаться только доверенные лица и поэтому указанные лица исключаются из числа вероятных нарушителей. Предполагается, что лица категорий III-VIII относятся к вероятным нарушителям. Предполагается, что возможность сговора внутренних нарушителей маловероятна ввиду принятых организационных и контролирующих мер.

7.4. В качестве основных уровней знаний нарушителей об АС можно выделить следующие:

- общая информация - информации о назначениях и общих характеристиках ИСПДн;
- эксплуатационная информация – информация, полученная из эксплуатационной документации;
- чувствительная информация - информация, дополняющая эксплуатационную информацию об ИСПДн (например, сведения из проектной документации ИСПДн).

В частности, нарушитель может иметь:

- данные об организации работы, структуре и используемых технических, программных и программно-технических средствах ИСПДн;
- сведения об информационных ресурсах ИСПДн:
- порядок и правила создания, хранения и передачи информации, структура и свойства информационных потоков;
- данные об уязвимостях, включая данные о недокументированных (недекларированных) возможностях технических, программных и программно-технических средств ИСПДн;
- данные о реализованных в ПСЗИ принципах и алгоритмах;
- исходные тексты программного обеспечения ИСПДн;

- сведения о возможных каналах реализации угроз;
- информацию о способах реализации угроз.

Предполагается, что лица категории III и категории IV владеют только эксплуатационной информацией, что обеспечивается организационными мерами. При этом лица категории IV не владеют парольной, аутентифицирующей и ключевой информацией, используемой в АИС, к которым они не имеют санкционированного доступа. Предполагается, что лица категории V владеют в той или иной части чувствительной и эксплуатационной информацией о системе передачи информации и общей информацией об АИС, использующих эту систему передачи информации, что обеспечивается организационными мерами. При этом лица категории V не владеют парольной и аутентифицирующей информацией, используемой в АИС.

Предполагается, что лица категории VI и лица категории VII по уровню знаний не превосходят лица категории V. Предполагается, что лица категории VIII обладают чувствительной информацией об ИСПДн и функционально ориентированных АИС, включая информацию об уязвимостях технических и программных средств ИСПДн. Организационными мерами предполагается исключить доступ лиц категории VIII к техническим и программным средствам ИСПДн в момент обработки с использованием этих средств защищаемой информации.

Таким образом, наиболее информированными об АИС являются лица категории III и лица категории VIII. Степень информированности нарушителя зависит от многих факторов, включая реализованные конкретные организационные меры и компетенцию нарушителей. Поэтому объективно оценить объем знаний вероятного нарушителя в общем случае практически невозможно.

В связи с изложенным, с целью создания определенного запаса прочности предполагается, что вероятные нарушители обладают всей информацией, необходимой для подготовки и реализации угроз, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты информации. К такой информации, например, относится парольная, аутентифицирующая и ключевая информация.

7.5. Предполагается, что нарушитель имеет:
- аппаратные компоненты СЗПДн и СФ СЗПДн;
- доступные в свободной продаже технические средства и программное обеспечение;специально разработанные технические средства и программное обеспечение.

Внутренний нарушитель может использовать штатные средства. Состав имеющихся у нарушителя средств, которые он может использовать для реализации угроз ИБ, а также возможности по их применению зависят от многих факторов, включая реализованные на

объектах ИП предпринимает конкретные организационные меры, финансовые возможности и компетенцию нарушителей. Поэтому объективно оценить состав имеющихся у нарушителя средств реализации угроз в общем случае практически невозможно.

Поэтому, для создания устойчивой СЗПДн предполагается, что вероятный нарушитель имеет все необходимые для реализации угроз средства, возможности которых не превосходят возможности аналогичных средств реализации угроз на информацию, содержащую сведения, составляющие государственную тайну, и технические и программные средства, обрабатывающие эту информацию. Вместе с тем предполагается, что нарушитель не имеет:

- средств перехвата в технических каналах утечки;
- средств воздействия через сигнальные цепи (информационные и управляющие интерфейсы СВТ);
- средств воздействия на источники и через цепи питания;
- средств воздействия через цепи заземления;
- средств активного воздействия на технические средства (средств облучения).

Предполагается, что наиболее совершенными средствами реализации угроз обладают лица категории III и лица категории VIII.

8. Способы реализации (возникновения) угроз безопасности персональных данных

8.1. Нарушители могут использовать различные способы реализации угроз безопасности персональных данных, например, к ним относятся: использование не декларированных возможностей программного обеспечения телекоммуникационного оборудования; использование уязвимостей конфигурации системы управления базами данных; установка программных закладок в телекоммуникационное оборудование; извлечение аутентификационной информации из постоянной памяти носителя (инвазивный метод); внедрение вредоносного программного обеспечения; использование уязвимостей конфигурации системы управления доступом к АРМ пользователя; использование уязвимостей кода программного обеспечения веб-сервера; внедрение вредоносного кода в веб-приложение; ошибочные действия в ходе настройки АРМ главного бухгалтера и другие.

8.2. Перечень основных тактик и соответствующих им типовых техник, используемых для построения сценариев реализации угроз безопасности персональных данных приведен в Таблице ниже:

№	Тактика	Основные техники
Т1	Сбор информации о системах и сетях Тактическая задача:	Т1.1. Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков, материалы конференций

	нарушитель стремится получить любую техническую информацию, которая может оказаться полезной в ходе реализации угроз безопасности информации	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.
		Т1.3. Пассивный сбор (прослушивание) информации о подключенных к сети устройствах с целью идентификации сетевых служб, типов и версий ПО этих служб и в некоторых случаях - идентификационной информации пользователей
		Т1.4. Направленное сканирование при помощи специализированного программного обеспечения подключенных к сети устройств с целью идентификации сетевых сервисов, типов и версий программного обеспечения этих сервисов, а также с целью получения конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений.
		Т1.5. Сбор информации о пользователях, устройствах, приложениях, а также сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений путем поиска и эксплуатации уязвимостей подключенных к сети устройств.
		Т1.6. Сбор информации о пользователях, устройствах, приложениях, авторизуемых сервисами вычислительной сети, путем перебора. Пример: сбор информации о почтовых адресах при помощи directoryharvestattack на почтовые сервера.
		Т1.7. Сбор информации, предоставляемой DNS сервисами, включая DNS Hijacking.
		Т1.8. Сбор информации о пользователе при посещении им веб-сайта, в том числе с использованием уязвимостей программы браузера и надстраиваемых модулей браузера.
		Т1.9. Сбор информации о пользователях, устройствах, приложениях путем поиска информации в памяти, файлах, каталогах, базах данных, прошивках устройств, репозиториях исходных кодов ПО, включая поиск паролей в исходном и хэшированном виде, криптографических ключей. Пример: получение хэшей паролей из /etc/passwd или получение паролей по умолчанию путем обратного инжиниринга прошивки устройства.
		Т1.10. Кража цифровых сертификатов, включая кражу физических токенов, либо неавторизованное выписывание новых сертификатов (возможно после компрометации инфраструктуры доменного регистратора или аккаунта администратора зоны на стороне жертвы)
		Т1.11. Сбор информации о пользователях, устройствах, приложениях, внутренней информации о компонентах

		систем и сетей путем применения социальной инженерии, в том числе фишинга.
		T1.12. Сбор личной идентификационной информации (идентификаторы пользователей, устройств, информация об идентификации пользователей сервисами, приложениями, средствами удаленного доступа), в том числе сбор украденных личных данных сотрудников и подрядчиков на случай, если сотрудники/подрядчики используют одни и те же пароли на работе и за ее пределами.
		T1.13. Сбор информации через получение доступа к системам физической безопасности и видеонаблюдения.
		T1.14. Сбор информации через получение контроля над личными устройствами сотрудников (смартфонами, планшетами, ноутбуками) для скрытой прослушки и видеофиксации.
		T1.15. Поиск и покупка баз данных идентификационной информации, скомпрометированных паролей и ключей на специализированных нелегальных площадках.
		T1.16. Сбор информации через получение доступа к базам данных результатов проведенных инвентаризаций, реестрам установленного оборудования и ПО, данным проведенных аудитов безопасности, в том числе через получение доступа к таким данным через компрометацию подрядчиков и партнеров.
		T1.17. Пассивный сбор и анализ данных телеметрии для получения информации о технологическом процессе, технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах.
		T1.18. Сбор и анализ данных о прошивках устройств, количестве и подключении этих устройств, используемых промышленных протоколах для получения информации о технологическом процессе, технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах.
		T1.19. Сбор и анализ специфических для отрасли или типа предприятия характеристик технологического процесса для получения информации о технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах.
		T1.20. Техники конкурентной разведки и промышленного шпионажа для сбора информации о технологическом процессе, технологических установках, системах и ПО на предприятиях в автоматизированных

		системах управления производственными и технологическими процессами, в том числе на критически важных объектах.
		Примечание 1: Сбор информации может выполняться с использованием одной или более из перечисленных выше техник, пока нарушитель не получит достаточно информации для реализации другой тактики в продолжении атаки.
T2	Получение первоначального доступа к компонентам систем и сетей Тактическая задача: нарушитель, находясь вне инфраструктуры сети или системы, стремится получить доступ к любому узлу в инфраструктуре и использовать его как плацдарм для дальнейших действий.	T2.1. Использование внешних сервисов организации в сетях публичного доступа (Интернет) Примеры: 1) доступ к веб-серверу, расположенному в сети организации; 2) доступ к интерфейсу электронной почты OutlookWebAccess (OWA) почтового сервера организации.
		T2.2. Использование устройств, датчиков, систем, расположенных на периметре или вне периметра физической защиты объекта, для получения первичного доступа к системам и компонентам внутри этого периметра. Примеры 1) доступ к датчикам автономной системы дистанционного контроля давления газа участка газопровода; 2) доступ к умному счетчику, расположенному на частном объекте, как к части инфраструктуры поставщика электроэнергии; 3) доступ к интерфейсу управления камеры видеонаблюдения через сети ближнего действия.
		T2.3. Эксплуатация уязвимостей сетевого оборудования и средств защиты вычислительных сетей для получения доступа к компонентам систем и сетей при удаленной атаке. Пример: обход межсетевого экрана путем эксплуатации уязвимостей реализации правил фильтрации.
		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.
		T2.5. Эксплуатация уязвимостей компонентов систем и сетей при удалённой или локальной атаке. Примеры: 1) эксплуатация уязвимостей веб-сервера с целью выполнения произвольного кода в контексте этого сервера; 2) эксплуатация уязвимостей операционной системы устройства человеко-машинного интерфейса автоматизированной системы управления с целью внедрения средств получения вводимых на этом устройстве паролей доступа; 3) эксплуатация уязвимостей браузера вредоносными скриптами при посещении пользователем вредоносного или скомпрометированного веб-сайта.
		T2.6. Использование недокументированных возможностей программного обеспечения сервисов, приложений, оборудования, включая использование

		отладочных интерфейсов, программных, программно-аппаратных закладок.
		Т2.7. Использование в системе внешних носителей информации, которые могли подключаться к другим системам и быть заражены вредоносным программным обеспечением. В том числе дарение, подмена или подлог носителей информации и внешних устройств, содержащих вредоносное программное обеспечение или предназначенных для реализации вредоносных функций. Примеры: 1) передача флеш-носителя в комплекте материалов выездного мероприятия; 2) подмена USB-адаптера беспроводной клавиатуры схожим внешне, но реализующим функции сбора и передачи данных устройством.
		Т2.8. Использование методов социальной инженерии, в том числе фишинга, для получения прав доступа к компонентам системы.
		Т2.9. Несанкционированное подключение внешних устройств. Пример: несанкционированное подключение точки доступа Wi-Fi.
		Т2.10. Несанкционированный доступ путем подбора учетных данных сотрудника или легитимного пользователя (методами прямого перебора, словарных атак, паролей производителей по умолчанию, использования одинаковых паролей для разных учетных записей, применения "радужных" таблиц или другими).
		Т2.11. Несанкционированный доступ путем компрометации учетных данных сотрудника организации, в том числе через компрометацию многократно используемого в различных системах пароля (для личных или служебных нужд).
		Т2.12. Использование доступа к системам и сетям, предоставленного сторонним организациям, в том числе через взлом инфраструктуры этих организаций, компрометацию личного оборудования сотрудников сторонних организаций, используемого для доступа. Пример: использование доступа третьей доверенной стороны (поставщики ИТ-услуг, поставщики услуг безопасности).
		Т2.13. Реализация атаки типа "человек посередине" для осуществления доступа, например, NTLM/SMB Relaying атаки.
		Т2.14. Доступ путем эксплуатации недостатков систем биометрической аутентификации. Пример: демонстрация фотографии для аутентификации через функцию распознавания лиц.
		Примечание 2: Получение доступа может выполняться в несколько шагов с использованием одной или более из перечисленных выше техник, пока нарушитель не достигнет целевой системы или не будет вынужден прибегнуть к другой тактике для продолжения атаки.

Т3	Внедрение и исполнение вредоносного программного обеспечения в системах и сетях Тактическая задача: получив доступ к узлу сети или системы, нарушитель стремится внедрить в его программную среду инструментальные средства, необходимые ему для дальнейших действий.	Т3.1. Автоматический запуск скриптов и исполняемых файлов в системе с использованием пользовательских или системных учетных данных, в том числе с использованием методов социальной инженерии.
		Т3.2. Активация и выполнение вредоносного кода, внедренного в виде закладок в легитимное программное и программное-аппаратное обеспечение систем и сетей.
		Т3.3. Автоматическая загрузка вредоносного кода с удаленного сайта или ресурса с последующим запуском на выполнение.
		Т3.4. Копирование и запуск скриптов и исполняемых файлов через средства удаленного управления операционной системой и сервисами.
		Т3.5. Эксплуатация уязвимостей типа удаленное исполнение программного кода (RCE, Remotecodeexecution).
		Т3.6. Автоматическое создание вредоносных скриптов при помощи доступного инструментария от имени пользователя в системе с использованием его учетных данных.
		Т3.7. Подмена файлов легитимных программ и библиотек непосредственно в системе. Примечание 3: В том числе может сочетаться с техникой компрометации сертификата, используемого для цифровой подписи образа ПО.
		Т3.8. Подмена легитимных программ и библиотек, а также легитимных обновлений программного обеспечения, поставляемых производителем удаленно через сети связи, в репозиториях поставщика или при передаче через сети связи. Примечание 4: В том числе может сочетаться с техникой компрометации сертификата, используемого для цифровой подписи образа программного обеспечения.
		Т3.9. Подмена ссылок на легитимные программы и библиотеки, а также на легитимные обновления программного обеспечения, поставляемые производителем удаленно через сети связи, подмена информации о таких обновлениях, включая атаки на инфраструктурные сервисы поставщика (такие как DNS hijacking), атаки на третьесторонние ресурсы, атаки на электронную почту и другие средства обмена сообщениями. Примечание 5: В том числе может сочетаться с техникой компрометации сертификата, используемого для цифровой подписи образа программного обеспечения.
		Т3.10. Подмена дистрибутивов (установочных комплектов) программ на носителях информации или общих сетевых ресурсах Примечание 6: В том числе может сочетаться с техникой компрометации сертификата, используемого для цифровой подписи образа программного обеспечения.
		Т3.11. Компрометация сертификата, используемого для

		цифровой подписи образа ПО, включая кражу этого сертификата у производителя ПО или покупку краденого сертификата на нелегальных площадках в сетях связи (т.н. "даркнет") и подделку сертификата с помощью эксплуатации уязвимостей ПО, реализующего функции генерирования криптографических ключей, хранения и управления цифровыми сертификатами.
		Т3.12. Компрометация средств создания программного кода приложений в инфраструктуре разработчика этих приложений (компиляторов, линковщиков, средств управления разработкой) для последующего автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы.
		Т3.13. Компрометация средств сборки, конфигурирования и разворачивания программного кода, а также средств создания узкоспециализированного кода (к примеру, кода промышленных контроллеров) в инфраструктуре целевой системы для автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы.
		Т3.14. Планирование запуска вредоносных программ при старте операционной системы путем эксплуатации стандартных механизмов, в том числе путем правки ключей реестра, отвечающих за автоматический запуск программ, запуска вредоносных программ как сервисов и т.п.
		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. Выполнение в контексте планировщика в ряде случаев позволяет авторизовать вредоносное программное обеспечение и повысить доступные ему привилегии.
		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. Примеры: 1) запуск MSI-файлов в операционной системе Windows при помощи утилиты msiexec; 2) использование утилит Regsvr32.exe (MicrosoftWindowsRegisterServer) и odbcconf.exe для проксирования исполнения кода библиотек dll в операционной системе Windows посредством внесения изменений в реестр операционных систем.
		Примечание 7: Внедрение и исполнение вредоносного программного обеспечения в системах и сетях может

		выполняться в несколько шагов с использованием одной или более из перечисленных выше техник, пока нарушитель не достигнет целевой системы или не будет вынужден прибегнуть к другой тактике для продолжения атаки.
Т4	Закрепление (сохранение доступа) в системе или сети Тактическая задача: получив доступ к узлу сети с помощью некоторой последовательности действий, нарушитель стремится упростить себе повторное получение доступа к этому узлу, если он ему впоследствии понадобится (например, устанавливает средства удаленного управления узлом, изменяет настройки средств защиты и другие действия)	Т4.1. Несанкционированное создание учетных записей или кража существующих учетных данных.
		Т4.2. Использование штатных средств удаленного доступа и управления операционной системы.
		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.
		Т4.4. Маскирование подключенных устройств под легитимные (например, нанесение корпоративного логотипа, инвентарного номера, телефона службы поддержки).
		Т4.5. Внесение соответствующих записей в реестр, автозагрузку, планировщики заданий, обеспечивающих запуск вредоносного программного обеспечения при перезагрузке системы или сети.
		Т4.6. Компрометация прошивок устройств с использованием уязвимостей или программно-аппаратных закладок, к примеру, внедрение новых функций в BIOS (UEFI), компрометация прошивок жестких дисков.
		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.
		Примечание 8: Закрепление (сохранение доступа в системе) может производиться с использованием одной или более из перечисленных выше техник.
Т5	Управление вредоносным программным обеспечением и (или) компонентами, к которым ранее был получен доступ Тактическая задача: внедрив вредоносное программное обеспечение или обеспечивпостоянное присутствие на узле	Т5.1. Удаленное управление через стандартные протоколы (например, RDP, SSH), а также использование инфраструктуры провайдеров средств удаленного администрирования. Пример: использование средств удаленного управления RMS/teamviewer для создания канала связи и управления скомпрометированной системой со стороны злоумышленников.
		Т5.2. Использование штатных средств удаленного доступа и управления операционной системы.
		Т5.3. Коммуникация с внешними серверами управления через хорошо известные порты на этих серверах, разрешенные на межсетевом экране (SMTP/25, HTTP/80, HTTPS/443 и др.).

	сети, нарушитель стремится автоматизировать управление внедренными инструментальными средствами, организовав взаимодействия скомпрометированным узлом и сервером управления, который может быть размещен в сети Интернет или в инфраструктуре организации	Т5.4. Коммуникация с внешними серверами управления через нестандартные порты на этих серверах, что в некоторых случаях позволяет эксплуатировать уязвимости средств сетевой фильтрации для обхода этих средств.
		Т5.5. 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.
		Т5.6. Проксирование трафика управления для маскировки подозрительной сетевой активности, обхода правил на межсетевом экране и сокрытия адресов инфраструктуры нарушителей, дублирование каналов связи, обфускация и разделение трафика управления во избежание обнаружения. Примеры: 1) использование скомпрометированных систем в той же сети, для которых правилами МЭ разрешен доступ в Интернет, в качестве прокси серверов; 2) использование инфраструктуры сети TOR для проксирования запросов к серверам управления; 3) использование одного коммуникационного протокола для запроса, и другого - для ответа на запрос.
		Т5.7. Туннелирование трафика управления через VPN.
		Т5.8. Туннелирование трафика управления в поля заполнения и данных служебных протоколов, к примеру, туннелирование трафика управления в поля данных и заполнения протоколов DNS, ICMP или другие.
		Т5.9. Управление через подключённые устройства, реализующие дополнительный канал связи с внешними системами или между скомпрометированными системами в сети.
		Т5.10. Использование средств обфускации, шифрования, стеганографии для сокрытия трафика управления.
		Т5.11. Передача команд управления через нестандартно интерпретируемые типовые операции, к примеру, путем выполнения копирования файла по разрешенному протоколу (FTP или подобному), путем управления разделяемыми сетевыми ресурсами по протоколу SMB и т.п.
		Т5.12. Передача команд управления через публикацию на внешнем легитимном сервисе, таком как веб-сайт, облачный ресурс, ресурс в социальной сети и т.п.
		Т5.13. Динамическое изменение адресов серверов управления, идентификаторов внешних сервисов, на которых публикуются команды управления, и т.п. по известному алгоритму во избежание обнаружения.
		Примечание 9: Управление вредоносным программным обеспечением и (или) компонентами, к которым ранее был получен доступ, может производиться нарушителем с использованием одной или более из перечисленных

		выше техник для управления труднодоступными компонентами или для реализации резервных каналов управления.
T6	Повышение привилегий по доступу к компонентам систем и сетей Тактическая задача: получив первоначальный доступ к узлу с привилегиями, недостаточными для совершения нужных ему действий, нарушитель стремится повысить полученные привилегии и получить контроль над узлом	T6.1. Получение данных для аутентификации и авторизации от имени привилегированной учетной записи путем поиска этих данных в папках и файлах, поиска в памяти или перехвата в сетевом трафике. Данные для авторизации включают пароли, хэш-суммы паролей, токены, идентификаторы сессии, криптографические ключи, но не ограничиваются ими.
		T6.2. Подбор пароля или другой информации для аутентификации от имени привилегированной учетной записи.
		T6.3 Эксплуатация уязвимостей ПО к повышению привилегий. Пример: эксплуатация уязвимости драйвера службы печати, позволяющей выполнить код с привилегиями системной учетной записи, через доступ к этому драйверу из приложения, запущенного от имени непривилегированного пользователя.
		T6.4. Эксплуатация уязвимостей механизма имперсонации (запуска операций в системе от имени другой учетной записи). Пример: эксплуатация уязвимости штатного механизма имперсонации, реализуемого операционной системой.
		T6.5. Манипуляции с идентификатором сессии, токеном доступа или иным параметром, определяющим права и полномочия пользователя в системе таким образом, что новый или измененный идентификатор/токен/параметр дает возможность выполнения ранее недоступных пользователю операций. Пример: кража и подделка cookie сессии для получения авторизованного доступа к вебинтерфейсу управления сетевого устройства.
		T6.6. Обход политики ограничения пользовательских учетных записей в выполнении групп операций, требующих привилегированного режима. Пример: обход UserAccountControl в операционной системе Windows.
		T6.7. Использование уязвимостей конфигурации системы, служб и приложений, в том числе предварительно сконфигурированных профилей привилегированных пользователей, автоматически запускаемых от имени привилегированных пользователей скриптов,приложений и экземпляров окружения, позволяющих вредоносному ПО выполняться с повышенными привилегиями. Примеры: 1) использование профилей PowerShell для закрепления вредоносного ПО в системе и выполнения этого ПО с повышенными привилегиями; 2) конфигурация команды перехода в привилегированный режим sudo, при которой успешный результат

		выполнения этой команды на некоторое время кэшируется, что при определенных обстоятельствах может быть использовано вредоносным кодом для выполнения привилегированных операций в течение этого времени; 3) параметры исполнения файлов (ImageFileExecutionOptions, IFEO), позволяющие переключать исполнение файлов в режим отладки, выполняя вредоносные приложения под видом отладчиков и средств мониторинга, что позволяет им отключать системные приложения и средства защиты.
		Т6.8. Эксплуатация уязвимостей, связанных с отдельным, и вероятно менее строгим контролем доступа к некоторым ресурсам (например, к файловой системе) для непривилегированных учетных записей. Пример: подмена на диске бинарных файлов или скриптов, предназначенных для исполнения в привилегированном контексте, приложением, исполняющимся в непривилегированном контексте.
		Т6.9. Эксплуатация уязвимостей средств ограничения среды исполнения (виртуальные машины, песочницы и т.п.) для исполнения кода вне этой среды. Пример: эксплуатация уязвимости обработки буфера данных в рамках песочницы, реализуемой браузером для ограничения работы мобильного кода (Javascript), с последующим выполнением кода в контексте процесса браузера.
		Примечание 10: Повышение привилегий по доступу к компонентам систем и сетей может производиться с использованием одной или более из перечисленных выше техник, пока нарушитель не получит достаточно привилегий для реализации другой тактики в продолжении атаки.
Т7	Сокрытие действий и применяемых при этом средств от обнаружения Тактическая задача: нарушитель стремится затруднить применение мер защиты информации, которые способны помешать его действиям или обнаружить их	Т7.1. Использование нарушителем или вредоносной платформой штатных инструментов администрирования, утилит и сервисов операционной системы, сторонних утилит, в том числе двойного назначения.
		Т7.2. Очистка/затирание истории команд и журналов регистрации, перенаправление записей в журналы регистрации, переполнение истории команд и журналов регистрации, затруднение доступа к журналам регистрации для авторизованных пользователей.
		Т7.3. Удаление файлов, переписывание файлов произвольными данными, форматирование съемных носителей.
		Т7.4. Отключение средств защиты от угроз информационной безопасности, в том числе средств антивирусной защиты, механизмов аудита, консолей оператора мониторинга и средств защиты других типов.
		Т7.5. Отключение систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности автоматизированной системы управления

		технологическими процессами и управляемого (контролируемого) объекта и (или) процесса.
		Т7.6. Подделка данных вывода средств защиты от угроз информационной безопасности.
		Т7.7. Подделка данных телеметрии, данных вывода автоматизированных систем управления, данных систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности автоматизированной системы управления технологическими процессами и управляемого (контролируемого) объекта и (или) процесса, данных видеонаблюдения и других визуально или автоматически интерпретируемых данных.
		Т7.8. Выполнение атаки отказа в обслуживании на основные и резервные каналы связи, которые могут использоваться для доставки сообщений о неработоспособности систем или их компонентов или о других признаках атаки.
		Т7.9. Подписание кода, включая использование скомпрометированных сертификатов авторитетных производителей ПО для подписания вредоносных программных модулей. Примечание 11: Сочетается с техникой компрометации сертификата, используемого для цифровой подписи образа ПО.
		Т7.10. Внедрение вредоносного кода в доверенные процессы операционной системы и другие объекты, которые не подвергаются анализу на наличие такого кода, для предотвращения обнаружения.
		Т7.11. Модификация модулей и конфигурации вредоносного программного обеспечения для затруднения его обнаружения в системе. Пример: внесение изменений в модули и конфигурацию вредоносного ПО для удаления индикаторов компрометации этим ВПО после обнаружения его в других системах.
		Т7.12. Манипуляции именами и параметрами запуска процессов и приложений для обеспечения скрытности. Примеры: 1) сокрытие окна приложения через параметры запуска процесса в ОС Windows; 2) выбор для вредоносного приложения имени файла (процесса), похожего на имя известного и/или системного приложения или совпадающего с ним.
		Т7.13. Создание скрытых файлов, скрытых учетных записей.
		Т7.14. Установление ложных доверенных отношений, в том числе установка корневых сертификатов для успешной валидации вредоносных программных модулей и авторизации внешних сервисов.
		Т7.15. Внедрение вредоносного кода выборочным/целевым образом на наиболее важные

		системы или системы, удовлетворяющие определенным критериям, во избежание преждевременной компрометации информации об используемых при атаке уязвимостях и обнаружения факта атаки.
		Т7.16. Искусственное временное ограничение распространения или активации вредоносного кода внутри сети, во избежание преждевременного обнаружения факта атаки. Пример: распространение вредоносного ПО единовременно по всем интересующим злоумышленникам системам и единовременный запуск его на выполнение по команде, вплоть до выполнения которой компрометацию системы обнаружить сложно.
		Т7.17. Обфускация, шифрование, упаковка с защитой паролем или сокрытие стеганографическими методами программного кода вредоносного ПО, данных и команд управляющего трафика, в том числе при хранении этого кода и данных в атакуемой системе, при хранении на сетевом ресурсе или при передаче по сети.
		Т7.18. Использование средств виртуализации для сокрытия вредоносного кода или вредоносной активности от средств обнаружения в операционной системе.
		Т7.19. Туннелирование трафика управления через VPN.
		Т7.20. Туннелирование трафика управления в поля заполнения и данных служебных протоколов, к примеру, туннелирование трафика управления в поля данных и заполнения протоколов DNS, ICMP или другие.
		Т7.21. Изменение конфигурации сети, включая изменение конфигурации сетевых устройств, организацию прокси-соединений, изменение таблиц маршрутизации, сброс и модификацию паролей доступа к интерфейсам управления сетевыми устройствами.
		Т7.22. Подмена и компрометация прошивок, в том числе прошивок BIOS, жестких дисков.
		Т7.23. Подмена файлов легитимных программ и библиотек непосредственно в системе. Примечание 12: В том числе может сочетаться с техникой компрометации сертификата, используемого для цифровой подписи образа ПО.
		Т7.24. Подмена легитимных программ и библиотек, а также легитимных обновлений программного обеспечения, поставляемых производителем удаленно через сети связи, в репозиториях поставщика или при передаче через сети связи. Примечание 13: В том числе может сочетаться с техникой компрометации сертификата, используемого для цифровой подписи образа ПО.
		Т7.25. Подмена ссылок на легитимные программы и библиотеки, а также на легитимные обновления программного обеспечения, поставляемые производителем удаленно через сети связи, информации

		о таких обновлениях, включая атаки на инфраструктурные сервисы поставщика (такие как DNS hijacking), атаки на третьесторонние ресурсы, атаки на электронную почту и другие средства обмена сообщениями. Примечание 14: в том числе может сочетаться с техникой компрометации сертификата, используемого для цифровой подписи образа ПО.
		Т7.26. Подмена дистрибутивов (установочных комплектов) программ на носителях информации или общих сетевых ресурсах. Примечание 15: в том числе может сочетаться с техникой компрометации сертификата, используемого для цифровой подписи образа ПО.
		Т7.27. Компрометация сертификата, используемого для цифровой подписи образа ПО, включая кражу этого сертификата у производителя ПО или покупку краденого сертификата на нелегальных площадках в сетях связи (т.н. "дарквеб") и подделку сертификата с помощью эксплуатации уязвимостей ПО, реализующего функции генерирования криптографических ключей, хранения и управления цифровыми сертификатами.
		Т7.28. Компрометация средств создания программного кода приложений в инфраструктуре разработчика этих приложений (компиляторов, линковщиков, средств управления разработкой) для последующего автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы.
		Т7.29. Компрометация средств сборки, конфигурирования и разворачивания программного кода, а также средств создания узкоспециализированного кода (к примеру, кода промышленных контроллеров), в инфраструктуре целевой системы, для автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы.
		Примечание 16: Сокрытие действий и применяемых при этом средств от обнаружения может производиться с использованием одной или более из перечисленных выше техник для сокрытия разных свидетельств компрометации системы или для более эффективного сокрытия.
Т8	Получение доступа (распространение доступа) к другим компонентам систем и сетей или смежным системам и сетям	Т8.1. Эксплуатация уязвимостей для повышения привилегий в системе или сети для удаленного выполнения программного кода для распространения доступа.
		Т8.2. Использование средств и интерфейсов удаленного управления для получения доступа к смежным системам и сетям.

	Тактическая задача: получив доступ к некоторым узлам инфраструктуры, нарушитель стремится получить доступ к другим узлам. Подобное распространение доступа может быть нецеленаправленным: так, еще не зная, к каким именно компонентам инфраструктуры требуется получить доступ для того, чтобы вызвать нужные ему негативные последствия, нарушитель может стремиться получить контроль над как можно большей частью инфраструктуры систем и сетей	Т8.3. Использование механизмов дистанционной установки программного обеспечения и конфигурирования. Пример: распространение вредоносного кода групповыми политиками ActiveDirectory, обычно используемыми для автоматического управления легитимным программным обеспечением.
		Т8.4. Удаленное копирование файлов, включая модули вредоносного программного обеспечения и легитимные программные средства, которые позволяют злоумышленнику получать доступ к смежным системам и сетям.
		Т8.5. Изменение конфигурации сети, включая изменение конфигурации сетевых устройств, организацию прокси-соединений, изменение таблиц маршрутизации, сброс и модификацию паролей доступа к интерфейсам управления сетевыми устройствами.
		Т8.6. Копирование вредоносного кода на съемные носители.
		Т8.7. Размещение вредоносных программных модулей на разделяемых сетевых ресурсах в сети.
		Т8.8. Использование доверенных отношений скомпрометированной системы и пользователей этой системы с другими системами и пользователями для распространения вредоносного программного обеспечения или для доступа к системам и информации в других системах и сетях. Пример: отсылка сообщений корпоративной электронной почты от имени коллег и прочих доверенных лиц.
		Примечание 17: Получение доступа (распространение доступа) к другим компонентам систем и сетей или смежным системам и сетям может выполняться в несколько шагов с использованием одной или более из перечисленных выше техник, пока нарушитель не достигнет целевой системы или не будет вынужден прибегнуть к другой тактике для продолжения атаки.
Т9	Сбор и вывод из системы или сети информации, необходимой для дальнейших действий при реализации угроз безопасности информации или реализации новых угроз Тактическая задача: в ходе реализации угроз безопасности	Т9.1. Доступ к системе для сбора информации и вывод информации через стандартные протоколы управления (например, RDP, SSH), а также использование инфраструктуры провайдеров средств удаленного администрирования. Пример: использование средств удаленного управления RMS/teamviewer для создания канала связи и управления скомпрометированной системой со стороны злоумышленников.
		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

	информации, нарушителю может потребоваться получить и вывести за пределы инфраструктуры большие объемы информации, избежав при этом обнаружения или противодействия	внешних серверах, разрешенные на межсетевом экране (SMTP/25, HTTP/80, HTTPS/443 и др.).
		T9.4. Вывод информации на нестандартные порты на внешних серверах, что в некоторых случаях позволяет эксплуатировать уязвимости средств сетевой фильтрации для обхода этих средств.
		T9.5. Отправка данных по известным протоколам управления и передачи данных.
		T9.6. Отправка данных по собственным протоколам.
		T9.7. Проксирование трафика передачи данных для маскировки подозрительной сетевой активности, обхода правил на межсетевом экране и сокрытия адресов инфраструктуры нарушителей, дублирование каналов связи, обфускация и разделение трафика передачи данных во избежание обнаружения. Примеры: 1) использование скомпрометированных систем в той же сети, для которых правилами МЭ разрешен доступ в Интернет в качестве прокси серверов; 2) использование инфраструктуры сети TOR для проксирования запросов к серверам управления; 3) использование одного коммуникационного протокола для запроса, и другого - для ответа на запрос.
		T9.8. Туннелирование трафика передачи данных через VPN.
		T9.9. Туннелирование трафика управления в поля заполнения и данных служебных протоколов, к примеру, туннелирование трафика управления в поля данных и заполнения протоколов DNS, ICMP или другие.
		T9.10. Вывод информации через съемные носители, в частности, передача данных между скомпрометированными изолированной системой и подключенной к Интернет системой через носители информации, используемые на обеих системах.
		T9.11. Отправка данных через альтернативную среду передачи данных. Пример: вывод конфиденциальной информации через субтитры видеоряда, демонстрируемого на веб-сайте.
		T9.12. Шифрование выводимой информации, использование стеганографии для сокрытия факта вывода информации.
		T9.13. Вывод информации через предоставление доступа к файловым хранилищам и базам данных в инфраструктуре скомпрометированной системы или сети, в том числе путем создания новых учетных записей или передачи данных для аутентификации и авторизации имеющихся учетных записей.
		T9.14. Вывод информации путем размещения сообщений или файлов на публичных ресурсах, доступных для анонимного нарушителя (форумы, файлообменные сервисы, фотобанки, облачные сервисы, социальные сети).

		Примечание 18: Сбор и вывод из системы или сети информации, необходимой для дальнейших действий при реализации угроз безопасности информации или реализации новых угроз может выполняться с использованием одной или более из перечисленных выше техник для реализации резервных каналов вывода информации.
T10	Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям Тактическая задача: достижение нарушителем конечной цели, приводящее к реализации моделируемой угрозы и причинению недопустимых негативных последствий	T10.1. Несанкционированный доступ к информации в памяти системы, файловой системе, базах данных, репозиториях, в программных модулях и прошивках.
		T10.2. Несанкционированное воздействие на системное программное обеспечение, его конфигурацию и параметры доступа.
		T10.3. Несанкционированное воздействие на программные модули прикладного программного обеспечения.
		T10.4. Несанкционированное воздействие на программный код, конфигурацию и параметры доступа прикладного программного обеспечения.
		T10.5. Несанкционированное воздействие на программный код, конфигурацию и параметры доступа системного программного обеспечения.
		T10.6. Несанкционированное воздействие на программный код, конфигурацию и параметры доступа прошивки устройства.
		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.
		T10.8. Уничтожение информации, включая информацию, хранимую в виде файлов, информацию в базах данных и репозиториях, информацию на неразмеченных областях дисков и сменных носителей.
		T10.9. Добавление информации (например, дефейсинг корпоративного портала, публикация ложной новости).
		T10.10. Организация отказа в обслуживании одной или нескольких систем, компонентов системы или сети.
		T10.11. Нецелевое использование ресурсов системы. Примеры: 1) организация майнинговой платформы; 2) организация платформы для осуществления атак отказа в обслуживании на смежные системы и сети.
		T10.12. Несанкционированное воздействие на автоматизированные системы управления с целью вызова отказа или нарушения функций управления, в том числе на АСУ критически важных объектов, потенциально опасных объектов, объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов. Примеры: 1) воздействие на автоматизированные системы управления объектов транспорта; 2) удаленное

		воздействие на цифровые системы и первичное оборудование объектов электроэнергетики; 3) воздействие на системы управления технологическим процессом нефтехимического объекта.
		Т10.13. Несанкционированное воздействие на автоматизированные системы управления с целью вызова отказа или поломки оборудования, в том числе АСУ критически важных объектов, потенциально опасных объектов, объектов, представляющих повышенную.
		Т10.14. Отключение систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности, в том числе критически важных объектов, потенциально опасных объектов, объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов.
		Т10.15. Воздействие на информационные ресурсы через системы распознавания визуальных, звуковых образов, системы геопозиционирования и ориентации, датчики вибрации, прочие датчики и системы преобразования сигналов физического мира в цифровое представление с целью полного или частичного вывода системы из строя или несанкционированного управления системой. Примеры: 1) нанесение нелегитимной разметки дорожного полотна с целью вызова сбоя системы автоматического управления автомобилем; 2) использование специальных символов в идентификационном знаке физического объекта, распознаваемом камерами видеонаблюдения.
		Примечание 19: Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящее к негативным последствиям при реализации угроз безопасности информации или реализации новых угроз, может выполняться с использованием одной или более из перечисленных выше техник для повышения эффективности воздействия с точки зрения нарушителя или для реализации нескольких типов воздействия на атакуемую систему.

9. Определение актуальных угроз безопасности персональных данных в ИСПДн

Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для ПДн.

Актуальность угрозы определяется следующими параметрами:

- уровень исходной защищенности ИСПДн;
- частота (вероятность) реализации рассматриваемой угрозы.

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн.

Показатели исходной защищенности ИСПДн

№	Параметр	Значение	Уровень защищенности
1.	Территориальное размещение	Корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации	высокий
2.	Наличие соединений с сетями общего пользования	ИСПДн, имеющая одноточечный выход в сеть общего пользования	высокий
3.	Встроенные (легальные) операции с записями баз персональных данных	Запись, сортировка, удаление	средний
4.	Разграничение доступа к персональным данным	ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект ПДн	средний
5.	Наличие соединений с другими базами ПДн иных ИСПДн	ИСПДн, в которой используется одна база ПДн, принадлежащая организации - владельцу данной ИСПДн	высокий
6.	Уровень обобщения (обезличивания) ПДн	ИСПДн, в которой предоставляемые пользователю данные не являются безличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	средний
7.	Объем ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	ИСПДн, не предоставляющие никакой информации	высокий

Значению уровня защищенности «Высокий» соответствуют 4 характеристики, значению уровня «Средний» - 3 характеристики. Таким образом, числовой коэффициент исходной защищенности ИСПДн Y1 соответствует значению 5 - средняя степень исходной защищенности.

В таблице ниже приведены данные об оценке актуальности угроз. Для каждой угрозы определяется вероятность реализации угрозы Y2 и соответствующий коэффициент:

0 - для маловероятной угрозы;

2 - для низкой вероятности угрозы;

5 - для средней вероятности угрозы;

10 - для высокой вероятности угрозы.

С учетом этого реализуемость каждой угрозы Y рассчитывается по формуле:

Y = (Yl+Y2)/20.

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

если 0<7<0,3, то возможность реализации угрозы признается низкой;

если 0,3<7 <0,6, то возможность реализации угрозы признается средней;

если 0,6<Г <0,8, то возможность реализации угрозы признается высокой;

если Y <0,8, то возможность реализации угрозы признается очень высокой.

Далее оценивается опасность каждой угрозы. При оценке опасности на основе опроса экспертов определяется вербальный показатель опасности для рассматриваемой ИСПДн.

Этот показатель имеет три значения:

низкая опасность - если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

средняя опасность - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

высокая опасность - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Затем осуществляется выбор из общего (предварительного) перечня угроз безопасности тех, которые относятся к актуальным для данной ИСПДн, в соответствии с правилами, приведёнными в таблице ниже.

Возможность реализации угрозы	**Показатель опасности угрозы**		
	Низкая	**Средняя**	**Высокая**
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Состав угроз определён следующим образом. На основе «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных» установлена типовая модель угроз безопасности, актуальная для ИП: Типовая модель угроз безопасности персональных данных, обрабатываемых в распределенных информационных системах персональных данных, имеющих подключение к сетям связи общего пользования и(или) сетям международного информационного обмена. Для данной типовой модели возможна реализация следующих угроз безопасности ПДн:

Таблица угроз и их характеристики

Наименование угрозы	Вероятность Y2	РеализуемостьY	Опасность	Актуальность

Угрозы утечки информации по техническим каналам				
Угрозы утечки акустической (речевой) информации	маловероятно (0)	низкая (0,25)	низкая	неактуальная
Угрозы утечки видовой информации	маловероятно (0)	низкая (0,25)	низкая	неактуальная
Угрозы утечки информации по каналу ПЭМИН	маловероятно (0)	низкая (0,25)	низкая	неактуальная
Угрозы НСД к ПДн непосредственно в ИСПДн				
Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой	маловероятно (0)	низкая (0,25)	средняя	неактуальная
Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование и т.п.) операционной системы или какой-либо прикладной программы, с применением специально созданных для выполнения НСД программ	маловероятно (0)	низкая (0,25)	средняя	неактуальная
Угрозы внедрения вредоносных программ	средняя вероятность (5)	средняя (0,5)	низкая	неактуальная
Сетевые угрозы				
Угрозы "Анализа сетевого трафика" с перехватом передаваемой по сети информации	низкая вероятность (2)	средняя (0,35)	средняя	актуальная

Угрозы выявления паролей	низкая вероятность (2)	средняя (0,35)	средняя	актуальная
Угрозы удаленного запуска приложений	низкая вероятность (2)	средняя (0,35)	средняя	актуальная
Угрозы внедрения по сети вредоносных программ	низкая вероятность (2)	средняя (0,35)	низкая	неактуальная
Угрозы из внешних сетей				
Угрозы "Анализа сетевого трафика" с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации	низкая вероятность (2)	средняя (0,35)	средняя	актуальная
Угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.	маловероятно (0)	низкая (0,25)	низкая	неактуальная
Угрозы выявления паролей	низкая вероятность (2)	средняя (0,35)	средняя	актуальная
Угрозы получения НСД путем подмены доверенного объекта	маловероятно (0)	низкая (0,25)	низкая	неактуальная
Угрозы типа "Отказ в обслуживании"	низкая вероятность (2)	средняя (0,35)	средняя	актуальная
Угрозы удаленного запуска приложений	маловероятно (0)	низкая (0,25)	низкая	неактуальная
Угрозы внедрения по сети вредоносных программ	средняя вероятность (5)	средняя (0,5)	средняя	актуальная

10. Мероприятия по предотвращению угроз безопасности ПДн

№	Актуальные угрозы	Мероприятия по предотвращению угроз
1.	Сетевые угрозы: Угрозы "Анализа сетевого трафика" с перехватом передаваемой по сети информации; Угрозы выявления паролей; Угрозы удаленного запуска приложений; Угрозы из внешних сетей: Угрозы "Анализа сетевого трафика" с перехватом передаваемой во внешние сети и принимаемой из внешних сетей	Реализация системы с установленными для передачи информации ограниченного доступа сертифицированными механизмами защиты, например, ViPNet и других, отвечающих требованиям безопасности информации в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

	информации; Угрозы выявления паролей; Угрозы типа "Отказ в обслуживании"; Угрозы внедрения по сети вредоносных программ.	
2.	Угрозы безопасности ПДн при обмене ПДн с внешними организациями и подразделениями компании через информационные системы.	Организация доступа работников ИП к системам, рекомендованным для передачи в электронном виде информации, содержащие персональные данные. Временные мероприятия: 1. Передача документов, содержащих ПДн, через ЕАСД с обязательной пометкой «Ограниченный доступ». 2. Передача ПДн на съемных машинных носителях информации с соблюдением требований нормативных документов ИП по информационной безопасности и делопроизводству.
3.	Угроза отсутствия блокировки учетной записи при покидании рабочего места работником	1. Установить периодичность смены пароля учетной записи. 2. Провести обучение работников о необходимости блокировки учетной записи при покидании рабочего места более чем на 5 минут или при отсутствии зрительного контроля доступа постороннего лица к учетной записи. 3. Провести обучение руководителей о необходимости контроля блокировки учетной записи работниками при покидании рабочего места.

Лист ознакомления с Моделью угроз безопасности персональных данных в информационной системе персональных данных

№ п/п	ФИО работника	Дата ознакомления	Подпись работника