УТВЕРЖДАЮ
Генеральный директор

И.И. Иванов

«___» 2009 г.

М.П.

Модель угроз информационной системы персональных данных "АВТОКАДРЫ"

2009 г.

СПИСОК СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

АВС	- антивирусные средства
АРМ	- автоматизированное рабочее место
АС	- автоматизированная система
АСЗИ	- автоматизированная система в защищенном исполнении
ИСПДн	- информационная система персональных данных
КОИ	- криптографически опасная информация
ЛВС	- локальная вычислительная сеть
МЭ	- межсетевой экран
ОС	- операционная система
ПДн	- персональные данные
ПМВ	- программно-математическое воздействие
ПО	- программное обеспечение
ПЭМИН	- побочные электромагнитные излучения и наводки
САЗ	- система анализа защищенности
СЗИ	- средства защиты информации
СЗПДн	- система (подсистема) защиты персональных данных
СКЗИ	- средства криптографической защиты информации
СОВ	- система обнаружения вторжений
ТС	- техническое средство
УБПДн	- угрозы безопасности персональных данных

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Автоматизированная система в защищенном исполнении (АСЗИ) – автоматизированная система, реализующая информационную технологию выполнения установленных функций в соответствии с требованиями стандартов и (или) иных нормативных документов по защите информации.

Адекватность – свойство соответствия преднамеренному поведению и результатам.

Атака – целенаправленные действия нарушителя с использованием технических и (или) программных средств с целью нарушения заданных характеристик безопасности защищаемой криптосредством информации или с целью создания условий для этого.

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

Безопасность объекта – состояние защищенности объекта от внешних и внутренних угроз.

Безопасность персональных данных – состояние защищенности персональных данных характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Встраивание криптосредства – процесс подключения криптосредства к техническим и программным средствам, совместно с которыми предполагается его штатное функционирование, за исключением процесса инсталляции.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

Документированные (декларированные) возможности ПО (ТС) – функциональные возможности ПО (ТС), описанные в документации на ПО (ТС).

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Жизненно важные интересы – совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Инсталляция – установка программного продукта на компьютер. Инсталляция обычно выполняется под управлением инсталлятора – программы, которая приводит состав и структуру устанавливаемого программного изделия в соответствии с конфигурацией компьютера, а также настраивает программные параметры согласно типу имеющейся операционной системы, классам решаемых задач и режимам работы. Таким образом, инсталляция делает программный продукт пригодным для использования в данной вычислительной системе и готовым решать определенный класс задач в определенном режиме работы.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационная система персональных данных – это информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таки средств.

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Информационно-телекоммуникационная сеть общего пользования – информационно-телекоммуникационная сеть, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано.

Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Канал атаки – среда переноса от субъекта к объекту атаки (а, возможно, и от объекта к субъекту атаки) действий, осуществляемых при проведении атаки.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Контролируемая зона - это пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Криптографически опасная информация (КОИ) – информация о состояниях криптосредства, знание которой нарушителем позволит ему строить алгоритмы определения ключевой информации (или ее части) или алгоритмы бесключевого чтения.

Криптосредство – шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну. В частности, к криптосредствам относятся средства криптографической защиты информации (СКЗИ) - шифровальные (криптографические) средства защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Модель нарушителя – предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

Модель угроз – перечень возможных угроз.

Нарушитель (субъект атаки) – лицо (или инициируемый им процесс), проводящее (проводящий) атаку.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Негативные функциональные возможности – документированные и недокументированных возможности программных и аппаратных компонентов криптосредства и среды функционирования криптосредства, позволяющие:

- модифицировать или искажать алгоритм работы криптосредств в процессе их использования;
- модифицировать или искажать информационные или управляющие потоки и процессы, связанные с функционированием криптосредства;

получать доступ нарушителям к хранящимся в открытом виде ключевой, идентификационной и (или) аутентифицирующей информации, а также к защищаемой информации.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носители сведений, составляющих государственную тайну, – материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов.

Примечание

Так как по своей природе сведения, составляющие государственную тайну, не отличаются от всех остальных сведений, то приведенное определение можно корректно использовать для любых сведений.

Учитывая определение понятия «информация», термин «носитель информации» можно использовать в качестве синонима термину «носитель сведений».

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Обработка персональных данных – действия (операции) с персональными данными включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Объект информатизации – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Опубликованные возможности ПО или ТС – возможности, сведения о которых содержатся в общедоступных открытых источниках (технические и любые другие материалы разработчика ПО или ТС, монографии, публикации в СМИ, материалы конференций и других форумов, информация из сети Internet и т.д.).

Перехват (информации) - неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Пользователь – лицо, участвующее в эксплуатации криптосредства или использующее результаты его функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и(или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Ресурс информационной системы - именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Специальная защита – комплекс организационных и технических мероприятий, обеспечивающих защиту информации от утечки по каналам побочных излучений и наводок.

Среда функционирования криптосредства (СФК) – совокупность технических и программных средств, совместно с которыми предполагается штатное функционирование криптосредства и которые способны повлиять на выполнение предъявляемых к криптосредству требований.

Средства имитозащиты - аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации.

Средства кодирования - средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций.

Средства криптографической защиты информации - средства шифрования, средства имитозащиты, средства кодирования, средства электронной цифровой подписи, средства изготовления ключевых документов (независимо от вида носителя ключевой информации), ключевые документы (независимо от вида носителя ключевой информации).

Средства шифрования - аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении.

Средства электронной цифровой подписи - аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи

подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи.

Средства вычислительной техники - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технические средства информационной системы персональных данных – технические средства, осуществляющие обработку ПДн (средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации).

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Трансграничная передача персональных данных - передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Угроза безопасности – совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства.

Угроза безопасности объекта – возможное нарушение характеристики безопасности объекта.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которого невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Уровень криптографической защиты информации – совокупность требований, предъявляемых к криптосредству.

Успешная атака – атака, достигшая своей цели.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уполномоченное оператором лицо – лицо, которому на основании договора оператор поручает обработку персональных данных.

Учетность – свойство, обеспечивающее однозначное отслеживание собственных действий любого логического объекта.

Уязвимость - некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации.

Характеристика безопасности объекта – требование к объекту, или к условиям его создания и существования, или к информации об объекте и условиях его создания и

существования, выполнение которого необходимо для обеспечения защищенности жизненно важных интересов личности, общества или государства.

Целостность информации - способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

НОРМАТИВНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Настоящий документ составлен в соответствии со следующими действующими нормативно-методическими документами по защите персональных данных:

[1] - Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

[2] - Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

[3] - Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденное постановления Правительства Российской Федерации от 17 ноября 2007 года № 781;

[4] - Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденное приказом ФСБ России от 9 февраля 2005 года № 66 (зарегистрирован Минюстом России 3 марта 2005 года, регистрационный № 6382);

[5] - Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (ФСБ России, № 149/6/6-622, 2008);

[6] - Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (ФСБ России, № 149/5-144, 2008).

ОБЩИЕ ПОЛОЖЕНИЯ

Настоящий документ разработан на основе нормативно-методических документов ФСБ России ([5], [6]), регламентирующих порядок обеспечения безопасности ПДн.

Настоящая «Модель угроз информационной системы персональных данных "АВТОКАДРЫ"» (далее – Модель угроз) содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационной системе персональных данных (ИСПДн). Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц, действиями зарубежных спецслужб или организаций (в том числе террористических), а также криминальных группировок, создающими условия (предпосылки) для нарушения безопасности персональных данных, которые ведут к ущербу жизненно важным интересам личности, общества и государства.

Модель угроз содержит данные по угрозам безопасности персональных данных, обрабатываемых в ИСПДн, связанным:

с использованием средств криптографической защиты информации;

с перехватом (съемом) ПДн по техническим каналам с целью их копирования или неправомерного распространения;

с несанкционированным, в том числе случайным, доступом в ИСПДн с целью изменения, копирования, неправомерного распространения ПДн или деструктивных воздействий на элементы ИСПДн и обрабатываемых в них ПДн с использованием программных и программно-аппаратных средств с целью уничтожения или блокирования ПДн.

Модель угроз является методическим документом и предназначена для должностных и ответственных лиц оператора персональных данных, администраторов ИСПДн, разработчиков ИСПДн и их подсистем.

Модель угроз разработана на основе [5] и [6] для конкретной ИСПДн "АВТОКАДРЫ" с учетом ее назначения, условий и особенностей функционирования.

Модель угроз предназначена для решения следующих задач:

- анализ защищенности ИСПДн от угроз безопасности ПДн в ходе организации и выполнения работ по обеспечению безопасности ПДн;
- разработка системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса ИСПДн;
- проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
- недопущение воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование;
- контроль за обеспечением уровня защищенности персональных данных.

В Модели угроз дано обобщённое описание ИСПДн как объекта защиты, возможных источников УБПДн, основных классов уязвимостей ИСПДн, возможных видов неправомерных действий и деструктивных воздействий на ПДн, а также основных способов их реализации.

Угрозы безопасности ПДн, обрабатываемых в ИСПДн, содержащиеся в настоящей Модели угроз, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств реализации УБПДн в ИСПДн. Кроме того, Модель угроз может быть пересмотрена по решению оператора (Общество с ограниченной ответственностью "ФИРМА") на основе периодически проводимых им анализа и оценки угроз безопасности ПДн с учетом особенностей и (или) изменений ИСПДн, а также по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности ПДн при их обработке в информационной системе.

ОПИСАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Наименование ИСПДн

Наименование ИСПДн - "АВТОКАДРЫ". ИСПДн является собственностью общества с ограниченной ответственностью "ФИРМА".

Местонахождение ИСПДн

ИСПДн располагается по адресу: 624600, Свердловская область, город Екатеринбург, ул. Ленина, 15, ИСПДн занимает: №123, №456.

Охрана помещений

Охраной помещений организации занимается предприятие "Охрана", также данное предприятие занимается обслуживанием установленной пожарно-охранной сигнализации.

Состав ТС ИСПДн

В таблице указан перечень используемых ТС:

№ п/п	Наименование ТС	Обозначение
1	Кластер из терминальных серверов (HP DL380 G5)	ТС1
2	Сервер БД (HP Proliant DL580 G4)	ТС2
3	Резервный сервер БД (HP Proliant DL380G5)	ТС3
4	Сервер управления резервным копированием (Kraftway)	ТС4
5	Ленточная библиотека для хранения резервных копий (MSL-6060)	ТС5
6	Система хранения данных (EMC Clariion)	ТС6
7	Коммутатор системы хранения (Brocade 24FC ports)	ТС7
8	Управляющие сетевые интерфейсы (iLO, iLO, ECM CX3-80 SPA, ECM CX3-80 SPB, DS-5000B-x, MSL-6060 ICx)	ТС8
9	Коммутатор сетевой (Cisco Catalyst 3750)	ТС9
10	Рабочие станции пользователей КИС	ТС10
11	Рабочие станции пользователей КИС, обрабатывающие ПДн	ТС11
12	Удаленные рабочие станции пользователей КИС	ТС12
13	Удаленные рабочие станции пользователей КИС, обрабатывающие ПДн	ТС13
14	Прочие рабочие станции и сервера, подключенные к КСПД	ТС14
15	Сервер обновлений	ТС15
16	Сетевые кабели с открытой защищаемой информации на серверной площадке КИС	ТС16
17	Сетевые кабели, соединяющие серверную площадку КИС с рабочими станциями, обрабатывющими ПДн	ТС17
18	Сетевые кабели, соединяющие серверную площадку КИС с рабочими станциями	ТС18
19	Сетевое оборудование участвующее в передаче ПДн по КСПД	ТС19
20	Кабели питания серверов и рабочих станций, обрабатывающих ПДн	ТС20
21	Линии вспомогательных средств и систем, размещенных в помещениях с техническими средствами, обрабатывающими ПДн	ТС21
22	Принтеры (локальные и сетевые) и прочие печатающие устройства	ТС22
23	Сервер системы Device Lock	ТС23
24	Сервер контроллер домена	ТС24
25	Съемные носители информации (учтенные)	ТС25
26	Система резервного питания (ИБП, генераторы)	ТС26
27	Съемные носители информации (неучтенные)	ТС27

Состав ПО ИСПДн

В таблице указан перечень используемого ПО:

№ п/п	Наименование	Обозначение
1	ОС Microsoft Windows 2003 Server x86 Enterprise Edition	ПО1
2	ОС Microsoft Windows 2003 Server x64 Enterprise Edition	ПО2
3	ПО резервного копирования Veritas NetBackup server ENTERPRISE SERVER 6.5	ПО3
4	ПО резервного копирования Veritas NetBackup client ENTERPRISE client 6.5	ПО4
5	ПО резервного копирования Veritas NetBackup CLIENT APPLICATION AND DATABASE PACK 6.5	ПО5
6	ПО резервного копирования Veritas NETBACKUP STANDARD CLIENT 6.5 XPLAT	ПО6
7	Антивирус Касперского 6.0 для серверов	ПО7
8	Антивирус Symantec 10.1.7 для рабочих станций	ПО8
9	ОС Microsoft Windows XP 32bit	ПО9
10	Microsoft Office 2003/2007	ПО10
11	КИС (серверная часть)	ПО11
12	КИС (клиентская часть)	ПО12
13	Крипто-Про CSP	ПО13
14	СУБД Oracle	ПО14
15	Клиент СУБД Oracle	ПО15

Взаимодействие с другими ИСПДн

Взаимодействие ИСПДн "АВТОКАДРЫ" с другими информационными системами не предполагается.

ПРИНЦИПЫ МОДЕЛИ УГРОЗ

Согласно [6] в основе Модели угроз в аспектах, касающихся использования криптосредств, лежат следующие общие принципы:

1) Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных (п. 2.2 документа [6]).

2) При формировании модели угроз необходимо учитывать как угрозы, осуществление которых нарушает безопасность персональных данных (далее – прямая угроза), так и угрозы, создающие условия для появления прямых угроз (далее – косвенные угрозы) или косвенных угроз.

3) Персональные данные обрабатываются и хранятся в информационной системе с использованием определенных информационных технологий и технических средств, порождающих объекты защиты различного уровня, атаки на которые создают прямые или косвенные угрозы защищаемой информации.

4) Криптосредство штатно функционирует совместно с техническими и программными средствами, которые способны повлиять на выполнение предъявляемых к криптосредству требований и которые образуют среду функционирования криптосредства (СФК).

5) Система защиты персональных данных не может обеспечить защиту информации от действий, выполняемых в рамках предоставленных субъекту действий полномочий (например, криптосредство не может обеспечить защиту информации от раскрытия лицами, которым предоставлено право на доступ к этой информации).

6) Нарушитель может действовать на различных этапах жизненного цикла криптосредства и СФК (под этими этапами в настоящем документе понимаются разработка, производство, хранение, транспортировка, ввод в эксплуатацию, эксплуатация программных и технических средств криптосредства и СФК).

7) Для обеспечения безопасности персональных данных при их обработке в информационных системах должны использоваться сертифицированные в системе сертификации ФСБ России (имеющие положительное заключение экспертной организации о соответствии требованиям нормативных документов по безопасности информации) криптосредства.

МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ВЕРХНЕГО УРОВНЯ

Данный раздел определяет характеристики безопасности защищаемых ПДн и других объектов защиты.

Используемые в ИСПДн информационные технологии создания и использования ПДн

Используемые для создания и обработки ПДн ТС и ПО указаны в разделе «Описание информационной системы персональных данных» настоящей Модели угроз.

Используются нижеуказанные информационные технологии:

Необходимо вручную дать описание используемых в ИСПДн информационных технологий.

В качестве дополнительных объектов угроз рассматриваются программное обеспечение и технические средства ИСПДн.

Формы представления ПДн в информационной системе "АВТОКАДРЫ"

ПДн имеют в ИСПДн ряд форм фиксации. Данные формы представлены в таблице.

№ п/п	Формы фиксации	Обозначение
1	Резервные копии ПДн на съемном носители	ФФ2
2	ПДн в записях на ленте библиотеки для хранения резервных копий	ФФ3
3	ПДн в виде сигналов в оперативной памяти технических средств	ФФ4
4	ПДн в областях (страницах) оперативной памяти	ФФ5
5	ПДн в виде сигналов передающихся через интерфейсы технических средств в открытом виде	ФФ6
6	ПДн в виде файлов (данных) на жестких магнитных дисках	ФФ7
7	ПДн в виде данных в незашифрованных сетевых пакетах	ФФ8
8	ПДн в виде данных в зашифрованных сетевых пакетах	ФФ9
9	ПДн в виде побочных электромагнитных излучений и наводок	ФФ10
10	ПДн в виде изображений на экране монитора	ФФ11
11	ПДн в виде твердой бумажной копии, распечатываемые на принтере	ФФ12
12	ПДн в виде записей БД КИС	ФФ13

Информация, сопутствующая процессам создания и использования ПДн

В процессе обработки ПДн используется и появляется сопутствующая информация. Типы данной информации применительно к ИСПДн приведены в таблице.

№ п/п	Сопутствующая информация	Обозначение
1	Ключевая, аутентифицирующая и парольная информация криптосредства	СИ1
2	Криптографически опасная информация (КОИ)	СИ2
3	Конфигурационная информация	СИ3
4	Управляющая информация	СИ4
5	Информация в электронных журналах регистрации	СИ5
6	Побочные сигналы, которые возникают в процессе функционирования технических средств и в которых полностью или частично отражаются персональные данные или другая защищаемая информация	СИ6
7	Резервные копии файлов с защищаемой информацией, которые могут создаваться в процессе обработки этих фалов	СИ7
8	Остаточная информация на носителях информации	СИ8

Характеристики безопасности объектов угроз

В данном подразделе устанавливаются характеристики безопасности объектов угроз.

Список характеристик безопасности:

№ п/п	Значение	Обозначение
1	Кофиденциальность	ХАР1
2	Целостность	ХАР2
3	Доступность	ХАР3

а) Характеристики безопасности программного обеспечения ИСПДн:

№ п/п	ПО\Характеристика	ХАР1	ХАР2	ХАР3
1	ПО1	-	+	+
2	ПО2	-	+	+
3	ПО3	-	+	-
4	ПО4	-	+	-
5	ПО5	-	+	-
6	ПО6	-	+	-
7	ПО7	-	+	-
8	ПО8	-	+	-
9	ПО9	-	+	-
10	ПО10	-	+	-
11	ПО11	-	+	+
12	ПО12	-	+	-
13	ПО13	-	+	-
14	ПО14	-	+	+
15	ПО15	-	+	-

б) Характеристики безопасности технических средств ИСПДн:

№ п/п	ТС\Характеристика	ХАР1	ХАР2	ХАР3
1	ТС1	-	-	+
2	ТС2	-	-	+
3	ТС3	-	-	+
4	ТС4	-	-	+
5	ТС5	+	+	+
6	ТС6	+	+	+
7	ТС7	-	-	+
8	ТС8	-	-	+
9	ТС9	-	-	+
10	ТС10	-	+	-
11	ТС11	-	-	+
12	ТС12	-	+	-
13	ТС13	-	-	+
14	ТС14	-	-	-
15	ТС15	-	+	-
16	ТС16	+	+	+
17	ТС17	+	-	-
18	ТС18	-	+	-
19	ТС19	+	-	+
20	ТС20	-	-	+
21	ТС21	+	-	-
22	ТС22	+	-	-
23	ТС23	-	+	-
24	ТС24	-	+	+
25	ТС25	+	+	+
26	ТС26	-	-	+
27	ТС27	-	-	-

в) Характеристики безопасности защищаемой информации (персональных данных и сопутствующей информации):

№ п/п	Объект\Характеристика	ХАР1	ХАР2	ХАР3
1	ФФ2	+	+	+
2	ФФ3	+	+	+
3	ФФ4	+	-	-
4	ФФ5	+	+	-
5	ФФ6	+	+	-
6	ФФ7	+	+	+
7	ФФ8	+	+	+
8	ФФ9	+	+	+
9	ФФ10	+	-	-
10	ФФ11	+	-	-
11	ФФ12	+	-	-
12	ФФ13	+	+	+
13	СИ1	+	-	+
14	СИ2	+	-	-
15	СИ3	-	+	+
16	СИ4	-	+	+
17	СИ5	-	+	+
18	СИ6	+	-	-
19	СИ7	+	-	-
20	СИ8	+	-	-

ФАКТОРЫ УГРОЗ, НЕ ЯВЛЯЮЩИХСЯ АТАКАМИ

Все рассматриваемые угрозы в данном разделе могут повлечь в какой-то мере случайное нарушение характеристик безопасности объектов. Предполагается, что отсутствует заинтересованный нарушитель. Поэтому, если воздействие фактора непосредственно не приводит к нарушению характеристики, то считается, что угрозы нет.

Рассматриваются следующие факторы угроз, не являющихся атаками:

№ п/п	Фактор	Обозначение
1	разрушения от ветра, попадания молнии в объекты инфраструктуры, обрывы проводов могут привести к нарушению электропитания ИСПДн, обрыву связи с сетями общего пользования	ФР1
2	негативные социальные явления могут создать предпосылки для невозможности работы ИСПДн – отключения электроэнергии, нарушение работы каналов связи	ФР2
3	непредумышленное искажение или удаление программных компонентов АСЗИ	ФР3
4	внедрение и использование неучтенных программ	ФР4
5	нарушение правил хранения информации ограниченного доступа, используемой при эксплуатации средств защиты информации (в частности, ключевой, парольной и аутентифицирующей информации)	ФР5
6	предоставление посторонним лицам возможности доступа к средствам защиты информации, а также к техническим и программным средствам, способным повлиять на выполнение предъявляемых к средствам защиты информации требований	ФР6
7	настройка и конфигурирование средств защиты информации, а также технических и программных средств, способных повлиять на выполнение предъявляемых к средствам защиты информации требований, в нарушение нормативных и технических документов	ФР7
8	несообщение о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа	ФР8
9	техногенные аварии (отключение электропитания, системы заземления, разрушение инженерных сооружений и т.д.)	ФР9
10	неисправности, сбои аппаратных средств, нестабильность параметров системы электропитания, заземления и т.д	ФР10
11	помехи и наводки, приводящие к сбоям в работе аппаратных средств	ФР11

Данные факторы могут воздействовать на объекты угроз, с нарушением характеристик безопасности.

Списки угроз, не являющихся атаками, приведены в разделе «Список угроз по модели нарушителя».

Защита от угроз, не являющихся атаками, в основном регламентируется инструкциями и распорядительными документами, разработанными с учетом особенностей эксплуатации ИСПДн и действующей нормативной базы. При этом по возможности также используются инженерно-технические меры.

МОДЕЛЬ НАРУШИТЕЛЯ

В настоящем разделе определяется совокупность условий и факторов, создающих опасность нарушения характеристик безопасности возможных объектов угроз.

В данном разделе под угрозами будут пониматься атаки.

Объекты атак

В качестве объектов атак рассматриваются защищаемые персональные данные, сопутствующая информация, программное обеспечение ИСПДн, технические средства ИСПДн, помещения, в которых расположены технические средства.

Субъекты атак

В качестве субъектов атак рассматриваются физические лица, имеющие доступ к техническим и программным средства информационной системы:

№ п/п	Субъект	Категория	Внутренний	Внешний	Условное обозначение
1	Администраторы БД	2	+	+	CA9
2	Администраторы домена и сотрудники отдела информационных технологий и телекомуникаций	2	+	+	CA10
3	Внешний нарушитель	1	-	+	CA18
4	Легальные пользователи информационной системы, имеющие доступ к ПДн	2	+	+	CA3
5	Легальные пользователи информационной системы, не имеющие доступа к ПДн	2	+	+	CA4
6	Разработчики программного обеспечения, используемого в КИС	1	-	+	CA13
7	Сотрудники сторонних организаций, производящие обслуживание вспомогательных технических средств	2	+	+	CA14
8	Сотрудники, производящие обслуживание помещений и вспомогательных технических средств	2	+	+	CA15
9	Удаленные легальные пользователи КИС, имеющие доступ к ПДн	1	-	+	CA5
10	Удаленные легальные пользователи сторонних информационных систем	1	-	+	CA8

Пояснения:

категория 1 - лица не имеющие права доступа в контролируемую зону информационной систем;

категория 2 – лица, имеющие право постоянного или разового доступа в контролируемую зону информационной системы;

внешние нарушители - нарушители, осуществляющие атаки из-за пределов контролируемой зоны информационной системы;

внутренние нарушители – нарушители, осуществляющие атаки, находясь в пределах контролируемой зоны информационной системы.

Привилегированные пользователи информационной системы, которые назначаются из числа особо доверенных лиц и осуществляют техническое обслуживание технических и программных средств криптосредства и СФК, включая их настройку, конфигурирование и распределение ключевой документации между непривилегированными пользователями:

№ п/п	Субъект
1	СА9
2	СА10

Субъекты, исключаемые из числа потенциальных нарушителей:

№ п/п	Субъект	Обоснование
1	СА9	Администраторы заинтересованы в соблюдении характеристик безопасности объектов информационной системы и защищаемой информации.
2	СА10	Администраторы сети не являются потенциальными нарушителями, так как являются доверенными лицами, заинтересованными в соблюдении характеристик безопасности защищаемых объектов.

Возможность сговора субъектов атак представлена в виде таблицы:

№ п/п	Субъект	СА3	СА4	СА5	СА8	СА9	СА10	СА13	СА14	СА15	СА18
1	СА3	-	+	-	-	-	-	-	-	+	-
2	СА4	+	-	-	-	-	-	-	-	-	-
3	СА5	-	-	-	+	-	-	-	-	-	-
4	СА8	-	-	+	-	-	-	-	-	-	-
5	СА9	-	-	-	-	-	-	-	-	-	-
6	СА10	-	-	-	-	-	-	-	-	-	-
7	СА13	-	-	-	-	-	-	-	-	-	-
8	СА14	-	-	-	-	-	-	-	-	+	-
9	СА15	+	-	-	-	-	-	-	+	-	-
10	СА18	-	-	-	-	-	-	-	-	-	-

Пояснения:

“-” – сговор между субъектами атаки невозможен: субъекты не могут иметь общих интересов; субъекты не встречаются в реальном мире; сферы деятельности субъектов не позволяют им действовать сообща; крайне низкая вероятность сговора; ЛИБО у субъектов атаки имеется возможность организовать сговор, но сговор не позволяет им объединить знания и (или) возможности для проведения совместной атаки, либо сговор не дает новых знаний и (или) возможностей для проведения атаки;

“+” – сговор между субъектами атаки возможен.

Таким образом, получаются следующие возможности для сговора:

№ п/п	Значение	Условное обозначение
1	Внешний нарушитель	СА18
2	Легальные пользователи информационной системы, имеющие доступ к ПДн	СА3
3	Легальные пользователи информационной системы, не имеющие доступа к ПДн	СА4
4	Разработчики программного обеспечения, используемого в КИС	СА13
5	Сговор(<Легальные пользователи информационной системы, имеющие доступ к ПДн>, <Легальные пользователи информационной системы, не имеющие доступа к ПДн>, <Сотрудники сторонних организаций, производящие обслуживание вспомогательных технических средств>, <Сотрудники,	СА1088

№ п/п	Значение	Условное обозначение
	производящие обслуживание помещений и вспомогательных технических средств>)	
6	Сговор(<Легальные пользователи информационной системы, имеющие доступ к ПДн>, <Легальные пользователи информационной системы, не имеющие доступа к ПДн>, <Сотрудники, производящие обслуживание помещений и вспомогательных технических средств>)	CA1086
7	Сговор(<Легальные пользователи информационной системы, имеющие доступ к ПДн>, <Сотрудники сторонних организаций, производящие обслуживание вспомогательных технических средств>, <Сотрудники, производящие обслуживание помещений и вспомогательных технических средств>)	CA1087
8	Сговор(<Легальные пользователи информационной системы, имеющие доступ к ПДн>, <Сотрудники, производящие обслуживание помещений и вспомогательных технических средств>)	CA1083
9	Сговор(<Легальные пользователи информационной системы, не имеющие доступа к ПДн>, <Легальные пользователи информационной системы, имеющие доступ к ПДн>)	CA1082
10	Сговор(<Сотрудники сторонних организаций, производящие обслуживание вспомогательных технических средств>, <Сотрудники, производящие обслуживание помещений и вспомогательных технических средств>)	CA1084
11	Сговор(<Удаленные легальные пользователи КИС, имеющие доступ к ПДн>, <Удаленные легальные пользователи сторонних информационных систем>)	CA1085
12	Сотрудники сторонних организаций, производящие обслуживание вспомогательных технических средств	CA14
13	Сотрудники, производящие обслуживание помещений и вспомогательных технических средств	CA15
14	Удаленные легальные пользователи КИС, имеющие доступ к ПДн	CA5
15	Удаленные легальные пользователи сторонних информационных систем	CA8

Возможности доступа:

№ п/п	Субъект\Форма	ФФ2	ФФ3	ФФ4	ФФ5	ФФ6	ФФ7	ФФ8	ФФ9	ФФ10	ФФ11	ФФ12	ФФ13	СИ1	СИ2	СИ3	СИ4	СИ5	СИ6	СИ7	СИ8
1	CA1082	-	-	+	+	+	-	+	-	-	+	+	+	-	-	-	-	-	-	-	-
2	CA1083	-	-	+	+	+	-	+	-	-	+	+	+	-	-	-	-	-	-	-	-
3	CA1084	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
4	CA1085	-	-	+	+	+	-	+	-	-	+	+	+	-	-	-	-	-	-	-	-
5	CA1086	-	-	+	+	+	-	+	-	-	+	+	+	-	-	-	-	-	-	-	-
6	CA1087	-	-	+	+	+	-	+	-	-	+	+	+	-	-	-	-	-	-	-	-
7	CA1088	-	-	+	+	+	-	+	-	-	+	+	+	-	-	-	-	-	-	-	-

Внешний нарушитель может принимать участие в любом из сговоров с целью получения дополнительных возможностей для проведения атаки, становиться связующим звеном для любого из сговоров.

Наибольшие возможности нарушители получают при множественном сговоре. Соответственно наиболее опасны именно такие сговоры, хотя их вероятность ниже двусторонних сговоров.

Предположения об имеющейся у нарушителя информации об объектах атак

Нарушители обладают полной информацией, необходимой для подготовки и проведения атак, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты.

Список имеющейся у нарушителя информации:

№ п/п	Информация	Обозначение	Обоснование
1	Содержание технической документации на технические и программные компоненты СФК	ОИ1	-
2	Долговременные ключи криптосредства	ОИ2	-
3	Все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от несанкционированного доступа (НСД) к информации организационно-техническими мерами (фазовые пуски, синхропосылки, незашифрованные адреса, команды управления и т.п.	ОИ3	-
4	Сведения о линиях связи, по которым передается защищаемая информация	ОИ4	-
5	Все сети связи, работающие на едином ключе	ОИ5	-
6	Все проявляющиеся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, нарушения правил эксплуатации криптосредства и СФК	ОИ6	-
7	Все проявляющиеся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, неисправности и сбои технических средств криптосредства и СФК	ОИ7	-
8	Сведения, получаемые в результате анализа любых сигналов от технических средств криптосредства и СФК, которые может перехватить нарушитель	ОИ8	-

Ограничения на имеющуюся у нарушителя информацию об объектах атак удобно представить в виде таблицы:

№ п/п	Субъект	ОИ1	ОИ2	ОИ3	ОИ4	ОИ5	ОИ6	ОИ7	ОИ8
1	СА18	+	-	+	+	-	-	-	+
2	СА3	-	-	-	-	-	-	-	-
3	СА4	-	-	-	-	-	-	-	-
4	СА13	+	-	-	-	-	-	-	-
5	СА1088	+	-	-	+	-	-	-	-
6	СА1086	+	-	-	+	-	-	-	-
7	СА1087	+	-	-	+	-	-	-	-
8	СА1083	+	-	-	+	-	-	-	-
9	СА1082	-	-	-	-	-	-	-	-
10	СА1084	+	-	-	+	-	-	-	-
11	СА1085	-	-	-	-	-	-	-	-
12	СА14	-	-	-	-	-	-	-	-
13	СА15	+	-	-	+	-	-	-	-
14	СА5	-	-	-	-	-	-	-	-
15	СА8	-	-	-	-	-	-	-	-

где:

“+” – нарушитель располагает информацией;

“-” – нарушитель не располагает информацией.

Обоснования ограничений:

№ п/п	Субъект	Информация	Обоснование

№ п/п	Субъект	Информация	Обоснование
1	СА10	ОИ8	Администраторы не имеют соответствующего оборудования и навыков для получения и анализа сигналов от технических средст.
2	СА18	ОИ2	Постороннему нарушителю информация о долговременных ключах криптосредства недоступна.
3	СА18	ОИ5	Постороннему нарушителю информация о сетях связи, работающих на едином ключе недоступна.
4	СА18	ОИ6	Постороннему внешнему нарушителю информация о нарушениях правил эксплуатации недоступна.
5	СА18	ОИ7	Постороннему внешнему нарушителю информация о всех возможных неисправностях и сбоях недоступна, так как нарушителю неизвестен состав всех используемых технических средств криптосредства и СФК.
6	СА3	ОИ1	Легальные пользователи не обладают данными знаниями (см. легальных пользователей, не имеющих доступ к ПДн).
7	СА3	ОИ2	Пользователям не известны долговременные ключи криптосредств.
8	СА3	ОИ3	Легальные пользователи не обладают данными знаниями (см. легальных пользователей, не имеющих доступ к ПДн).
9	СА3	ОИ4	Легальные пользователи не обладают данными знаниями (см. легальных пользователей, не имеющих доступ к ПДн).
10	СА3	ОИ5	Легальные пользователи не обладают данными знаниями (см. легальных пользователей, не имеющих доступ к ПДн).
11	СА3	ОИ6	Легальные пользователи не обладают данными знаниями (см. легальных пользователей, не имеющих доступ к ПДн).
12	СА3	ОИ7	Легальные пользователи не обладают данными знаниями (см. легальных пользователей, не имеющих доступ к ПДн).
13	СА3	ОИ8	Легальные пользователи не обладают данными знаниями (см. легальных пользователей, не имеющих доступ к ПДн).
14	СА4	ОИ1	Техническая документация пользователям недоступна.
15	СА4	ОИ2	Пользователям не известны долговременные ключи крпитосредства.
16	СА4	ОИ3	Пользователи не обладают необходимыми знаниями для анализа передаваемых в открытом виде данных.
17	СА4	ОИ4	Пользователи не обладают информацией о линиях связи, по которым передается защищаемая информация.
18	СА4	ОИ5	Пользователи не обладают информацией о всех сетях связи, работающих на едином ключе.
19	СА4	ОИ6	Пользователи не обладают необходимыми знаниями для использования проявляющихся в каналах связи, не защищенных от НСД к информации, нарушений правил эксплуатации криптосредств и СФК.
20	СА4	ОИ7	Пользователи не обладают необходимыми знаниями для использования проявляющихся в каналах связи, не защищенных от НСД к информации, неисправностей и сбоев технических средств криптосредств и СФК.
21	СА4	ОИ8	Пользователи не могут получать и анализировать сигналы от технических средств криптосредства и СФК, так как не обладают необходимым оборудованием и навыками.
22	СА13	ОИ2	Разработчикам КИС известно только лишь содержание документации и возможности, заложенные в программное и техническое обеспечение.
23	СА13	ОИ3	Разработчикам КИС известно только лишь содержание документации и возможности, заложенные в программное и техническое обеспечение.
24	СА13	ОИ4	Разработчикам КИС известно только лишь содержание документации и возможности, заложенные в программное и техническое обеспечение.
25	СА13	ОИ5	Разработчикам КИС известно только лишь содержание документации и возможности, заложенные в программное и техническое обеспечение.

№ п/п	Субъект	Информация	Обоснование
26	СА13	ОИ6	Разработчикам КИС известно только лишь содержание документации и возможности, заложенные в программное и техническое обеспечение.
27	СА13	ОИ7	Разработчикам КИС известно только лишь содержание документации и возможности, заложенные в программное и техническое обеспечение.
28	СА13	ОИ8	Разработчикам КИС известно только лишь содержание документации и возможности, заложенные в программное и техническое обеспечение.
29	СА14	ОИ1	Сотрудники сторонних организаций, обслуживающие вспомогательное оборудование, не могут обладать знаниями об особенностях функционирования информационной системы.
30	СА14	ОИ2	Сотрудники сторонних организаций, обслуживающие вспомогательное оборудование, не могут обладать знаниями об особенностях функционирования информационной системы.
31	СА14	ОИ3	Сотрудники сторонних организаций, обслуживающие вспомогательное оборудование, не могут обладать знаниями об особенностях функционирования информационной системы.
32	СА14	ОИ4	Сотрудники сторонних организаций, обслуживающие вспомогательное оборудование, не могут обладать знаниями об особенностях функционирования информационной системы.
33	СА14	ОИ5	Сотрудники сторонних организаций, обслуживающие вспомогательное оборудование, не могут обладать знаниями об особенностях функционирования информационной системы.
34	СА14	ОИ6	Сотрудники сторонних организаций, обслуживающие вспомогательное оборудование, не могут обладать знаниями об особенностях функционирования информационной системы.
35	СА14	ОИ7	Сотрудники сторонних организаций, обслуживающие вспомогательное оборудование, не могут обладать знаниями об особенностях функционирования информационной системы.
36	СА14	ОИ8	Сотрудники сторонних организаций, обслуживающие вспомогательное оборудование, не могут обладать знаниями об особенностях функционирования информационной системы.
37	СА15	ОИ2	Обслуживающему персоналу ТФЭС неизвестны сведения об организации защиты информации.
38	СА15	ОИ3	Обслуживающему персоналу ТФЭС неизвестна информация о нарушениях пользователей.
39	СА15	ОИ5	Обслуживающему персоналу ТФЭС неизвестны сведения об организации защиты информации.
40	СА15	ОИ6	Обслуживающему персоналу ТФЭС неизвестна информация о нарушениях пользователей.
41	СА15	ОИ7	Обслуживающему персоналу ТФЭС неизвестна информация о всех возможных сбоях и неисправностях технических средств.
42	СА15	ОИ8	Обслуживающему персоналу ТФЭС неизвестны сведения об организации защиты информации.
43	СА5	ОИ1	Удаленные пользователи не имеют доступа в контролируемую зону и к штатным средствам информационной системы, к аппаратным компонентам, расположенным в контролируемой зоне.
44	СА5	ОИ2	Пользователям не известны долговременные ключи криптосредства.
45	СА5	ОИ3	Удаленные пользователи не имеют доступа в контролируемую зону и к штатным средствам информационной системы, к аппаратным компонентам, расположенным в контролируемой зоне.
46	СА5	ОИ4	Удаленные пользователи не имеют доступа в контролируемую зону и к штатным средствам информационной системы, к аппаратным компонентам, расположенным в контролируемой зоне.
47	СА5	ОИ5	Удаленные пользователи не имеют доступа в контролируемую зону и к штатным средствам информационной системы, к

№ п/п	Субъект	Информация	Обоснование
			аппаратным компонентам, расположенным в контролируемой зоне.
48	СА5	ОИ6	Удаленные пользователи не имеют доступа в контролируемую зону и к штатным средствам информационной системы, к аппаратным компонентам, расположенным в контролируемой зоне.
49	СА5	ОИ7	Удаленные пользователи не имеют доступа в контролируемую зону и к штатным средствам информационной системы, к аппаратным компонентам, расположенным в контролируемой зоне.
50	СА5	ОИ8	Удаленные пользователи не имеют доступа в контролируемую зону и к штатным средствам информационной системы, к аппаратным компонентам, расположенным в контролируемой зоне.
51	СА8	ОИ1	Легальные пользователи не обладают данными знаниями (см. легальных пользователей, не имеющих доступ к ПДн).
52	СА8	ОИ2	Легальные пользователи не обладают данными знаниями (см. легальных пользователей, не имеющих доступ к ПДн).
53	СА8	ОИ3	Легальные пользователи не обладают данными знаниями (см. легальных пользователей, не имеющих доступ к ПДн).
54	СА8	ОИ4	Легальные пользователи не обладают данными знаниями (см. легальных пользователей, не имеющих доступ к ПДн).
55	СА8	ОИ5	Легальные пользователи не обладают данными знаниями (см. легальных пользователей, не имеющих доступ к ПДн).
56	СА8	ОИ6	Легальные пользователи не обладают данными знаниями (см. легальных пользователей, не имеющих доступ к ПДн).
57	СА8	ОИ7	Легальные пользователи не обладают данными знаниями (см. легальных пользователей, не имеющих доступ к ПДн).
58	СА8	ОИ8	Легальные пользователи не обладают данными знаниями (см. легальных пользователей, не имеющих доступ к ПДн).

Предположения об имеющихся у нарушителя средствах атак

Нарушители имеют все необходимые для проведения атак по доступным им каналам атак средства, возможности которых не превосходят возможности аналогичных средств атак на информацию, содержащую сведения, составляющие государственную тайну.

Список имеющихся у нарушителя средств атак:

№ п/п	Информация	Обозначение	Обоснование
1	Аппаратные компоненты криптосредства и СФК	СПА9	-
2	Доступные в свободной продаже технические средства и программное обеспечение	СПА10	-
3	Специально разработанные технические средства и программное обеспечение	СПА11	-
4	Штатные средства	СПА12	-

При этом имеются следующие ограничения на имеющиеся у нарушителей средства атак:

№ п/п	Субъект\Средство	СПА9	СПА10	СПА11	СПА12
1	СА18	-	+	+	-
2	СА3	+	+	-	+
3	СА4	+	+	-	+
4	СА13	-	+	+	-
5	СА1088	+	+	+	+
6	СА1086	+	+	+	+
7	СА1087	+	+	+	+
8	СА1083	+	+	+	+

№ п/п	Субъект\Средство	СПА9	СПА10	СПА11	СПА12
9	СА1082	+	+	-	+
10	СА1084	+	+	+	+
11	СА1085	-	+	-	+
12	СА14	-	+	+	-
13	СА15	+	+	+	+
14	СА5	-	+	-	+
15	СА8	-	+	-	-

где:
“+” – нарушитель располагает средством атаки;
“-” – нарушитель не располагает средством атаки.
Обоснования ограничений:

№ п/п	Субъект	Информация	Обоснование
1	СА10	СПА11	Администраторы домена не имеют возможности самостоятельно разработать специальные технические средства и программное обеспечение, а также не иметют ресурсов для приобретения.
2	СА18	СПА9	Нарушитель не имеет физического доступа к используемым криптосредствам и СФК.
3	СА18	СПА12	Нарушитель не имеет физического доступа к используемым штатным средствам операционной системы.
4	СА3	СПА11	Пользователи систем не обладают навыками по созданию и использованию специальных технических средств и программного обеспечения.
5	СА4	СПА11	Пользователи не имеют необходимых навыков для самостоятельной разработки и(или) использования специального программного обеспечения и технических средств.
6	СА13	СПА9	Разработчики программного обеспечения не имеют доступа к аппаратным средствам, штатным средствам доступа.
7	СА13	СПА12	Разработчики программного обеспечения не имеют доступа к аппаратным средствам, штатным средствам доступа.
8	СА14	СПА9	Сотрудники сторонних организаций не имеют непосредственного доступа к средствам информационной системы в качестве средств проведения атак.
9	СА14	СПА12	Сотрудники сторонних организаций не имеют непосредственного доступа к средствам информационной системы в качестве средств проведения атак.
10	СА5	СПА9	Удаленные пользователи не имеют доступа в контролируемую зону, к аппаратным компонентам, расположенным в контролируемой зоне, не обладают знаниями для приобретения и применения специальных технических средств и программного обеспечения.
11	СА5	СПА11	Удаленные пользователи не имеют доступа в контролируемую зону, к аппаратным компонентам, расположенным в контролируемой зоне, не обладают знаниями для приобретения и применения специальных технических средств и программного обеспечения.
12	СА8	СПА9	Удаленные пользователи не имеют доступа в контролируемую зону и к штатным средствам информационной системы, к аппаратным компонентам, расположенным в контролируемой зоне.
13	СА8	СПА11	Удаленные пользователи не имеют доступа в контролируемую зону и к штатным средствам информационной системы, к аппаратным компонентам, расположенным в контролируемой зоне.
14	СА8	СПА12	Удаленные пользователи не имеют доступа в контролируемую зону и к штатным средствам информационной системы, к аппаратным компонентам, расположенным в контролируемой

№ п/п	Субъект	Информация	Обоснование
			зоне.

Каналы атак

Описание каналов атак.

№ п/п	Канал атаки	Обозначение	Обоснование
1	Каналы связи (как внутри, так и вне контролируемой зоны), не защищенные от НСД к информации организационно-техническими мерами	КА13	-
2	Штатные средства	КА14	-
3	Каналы непостредственного доступа к объекту атаки (акустический, визуальные, физический)	КА15	-
4	Машинные носители информации	КА16	-
5	Носители информации, выведенные из употребления	КА17	-
6	Технические каналы утечки	КА18	-
7	Сигнальные цепи	КА19	-
8	Цепи электропитания	КА20	-
9	Цепи заземления	КА21	-
10	Канал утечки за счет электронных устройств негласного получения информации	КА22	-
11	Информационные и управляющие интерфейсы СВТ	КА23	-

Ограничения на доступ к каналам атаки.

В силу действующих правил доступ и должностных обязанностей таблица доступа к каналам атаки выглядит следующим образом:

№ п/п	Субъект\Канал	КА13	КА14	КА15	КА16	КА17	КА18	КА19	КА20	КА21	КА22	КА23
1	СА18	+	-	-	-	-	+	-	+	+	+	-
2	СА3	+	+	+	+	+	+	+	+	+	+	+
3	СА4	+	+	+	+	+	+	+	+	+	+	+
4	СА13	+	-	-	-	-	-	-	-	-	-	-
5	СА1088	+	+	+	+	+	+	+	+	+	+	+
6	СА1086	+	+	+	+	+	+	+	+	+	+	+
7	СА1087	+	+	+	+	+	+	+	+	+	+	+
8	СА1083	+	+	+	+	+	+	+	+	+	+	+
9	СА1082	+	+	+	+	+	+	+	+	+	+	+
10	СА1084	+	-	+	-	-	+	+	+	+	+	-
11	СА1085	+	+	+	-	-	-	-	-	-	-	-
12	СА14	-	-	+	-	-	+	+	+	+	+	-
13	СА15	+	-	+	-	-	+	+	+	+	+	-
14	СА5	+	+	+	-	-	-	-	-	-	-	-
15	СА8	+	-	-	-	-	-	-	-	-	-	-

где:

“+” – нарушитель имеет возможность воспользоваться каналом атаки;

“-” – нарушитель не имеет возможности воспользоваться каналом атаки атаки.

Тип нарушителя

Исходя из возможностей, устанавливаются следующие типы нарушителей:

№ п/п	Субъект атаки	Категория	Внутренний	Внешний	Тип нарушителя
1	СА18	1	-	+	Н1
2	СА3	2	+	+	Н2
3	СА4	2	+	+	Н2
4	СА13	1	-	+	Н1

№ п/п	Субъект атаки	Категория	Внутренний	Внешний	Тип нарушителя
5	CA1088	2	+	+	H2
6	CA1086	2	+	+	H2
7	CA1087	2	+	+	H2
8	CA1083	2	+	+	H2
9	CA1082	2	+	+	H2
10	CA1084	2	+	+	H2
11	CA1085	1	-	+	H1
12	CA14	2	+	+	H2
13	CA15	2	+	+	H2
14	CA5	1	-	+	H1
15	CA8	1	-	+	H1

Угрозы, возникающие на этапах разработки, производства, хранения, транспортировки, ввода в эксплуатацию технических и программных средств криптосредства и СФК, приведены в разделе «Список угроз по модели нарушителя».

Угрозы, связанные с моделью нарушителя и возникающие на этапе эксплуатации, приведены в разделе «Список угроз по модели нарушителя».

СПИСОК УГРОЗ ПО МОДЕЛИ НАРУШИТЕЛЯ

Разные факторы случайных воздействий могут приводить к реализации схожих угроз. В результате анализа характеристик факторов случайных воздействий и особенностей функционирования ИСПДн, факторы случайных воздействий сгруппированы в списки, которые представлены в таблице.

№ п/п	Название списка	Элементы списка
1	Список "Факторы 1"	ФР1, ФР2
2	Список "Факторы 2"	ФР1, ФР2, ФР3, ФР4, ФР9, ФР10, ФР11
3	Список "Факторы 3"	ФР1, ФР2, ФР9, ФР10, ФР11
4	Список "Факторы 4"	ФР2, ФР9, ФР10, ФР11
5	Список "Факторы 5"	ФР3
6	Список "Факторы 6"	ФР3, ФР4, ФР6, ФР7, ФР8
7	Список "Факторы 7"	ФР5
8	Список "Факторы 8"	ФР5, ФР6
9	Список "Факторы 9"	ФР5, ФР6, ФР7, ФР8
10	Список "Факторы 10"	ФР6
11	Список "Факторы 11"	ФР6, ФР7
12	Список "Факторы 12"	ФР6, ФР8
13	Список "Факторы 13"	ФР6, ФР9, ФР10
14	Список "Факторы 14"	ФР7
15	Список "Факторы 15"	ФР9
16	Список "Факторы 16"	ФР9, ФР10
17	Список "Факторы 17"	ФР10, ФР11
18	Список "Факторы 18"	ФР11

На разные объекты атак могут быть направлены схожие угрозы. В результате анализа характеристик объектов атак и особенностей функционирования ИСПДн, объекты атак сгруппированы в списки, которые представлены в таблице.

№ п/п	Название списка	Элементы списка
1	Список "Объекты доступа 1"	ТС1, ПО1, ТС2, ПО2, ФФ2, ТС3, ФФ3, ТС4, ФФ4, ТС5, ФФ5, ТС6, ТС7, ФФ7, ТС8, ФФ8, ТС9, ТС11, ПО11, ТС13, ФФ13, ПО14, ТС16, ТС20, ТС24, ТС25, ТС26
2	Список "Объекты доступа 2"	ТС1, ТС2, ТС3, ТС4, ТС5, ТС6, ТС7, ТС8, ТС9, ТС11, ТС19
3	Список "Объекты доступа 3"	ПО1, ПО2, ФФ2, ПО3, ФФ3, ПО4, ФФ4, ТС5, ПО5, ФФ5, ТС6, ПО6, ПО7, ФФ7, ПО8, ФФ8, ПО9, ТС10, ПО10, ПО11, ТС12, ПО12, ПО13, ФФ13, ПО14, ТС15, ПО15, ТС16, ТС18, ТС23, ТС24, ТС25
4	Список "Объекты доступа 4"	ПО1, ПО2, ПО3, СИ3, ПО4, СИ4, ПО5, ПО6, ПО7, ПО8, ПО9, ПО10, ПО11, ПО12, ПО13, ФФ13, ПО14, ТС15, ПО15, ТС16, ТС18, ТС23, ТС24
5	Список "Объекты доступа 5"	ПО1, ПО2, ПО3, СИ3, ПО4, СИ4, ПО5, ПО6, ПО7, ПО8, ПО9, ПО10, ПО11, ПО12, ПО13, ПО14, ПО15, ТС23, ТС24
6	Список "Объекты доступа 6"	ПО1, ПО2, ПО11, ПО14
7	Список "Объекты доступа 7"	ПО1, ФФ3, ФФ4, ФФ5, ПО7, ПО8, ФФ8, ПО9, ТС10, ПО10, ТС12, ПО13, ФФ13, ТС15, ТС24
8	Список "Объекты доступа 8"	ПО1, ФФ3, ФФ4, ФФ5, ФФ8, ТС9, ТС11, ТС13, ФФ13, ТС24
9	Список "Объекты доступа 9"	СИ1
10	Список "Объекты доступа 10"	СИ1, ФФ2, СИ2, ФФ3, ФФ7, СИ7, СИ8, ФФ9
11	Список "Объекты доступа 11"	СИ1, СИ2, ФФ3, ФФ8, СИ8, ФФ11, ФФ12, ФФ13
12	Список "Объекты доступа 12"	ФФ2, ФФ3, ФФ4, ТС5, ТС6, ФФ7, ФФ8, ФФ11, ФФ12, ФФ13, ТС16, ТС17, ТС21, ТС22, ТС25
13	Список "Объекты доступа 13"	ФФ2, ФФ3, ТС25

№ п/п	Название списка	Элементы списка
14	Список "Объекты доступа 14"	СИ3, СИ4
15	Список "Объекты доступа 15"	СИ3, СИ4, ФФ13
16	Список "Объекты доступа 16"	ФФ4, ФФ5, ФФ6, ФФ8, ФФ11, ФФ12, ФФ13, ТС17, ТС21, ТС22
17	Список "Объекты доступа 17"	ФФ4, ФФ8, ФФ11, ФФ13, ТС21, ТС22
18	Список "Объекты доступа 18"	ФФ4, ФФ11, ФФ12, ТС17, ТС21, ТС22
19	Список "Объекты доступа 19"	ФФ4, ФФ11, ФФ12, ТС17, ТС22
20	Список "Объекты доступа 20"	ФФ4, ФФ12, ТС21, ТС22
21	Список "Объекты доступа 21"	ТС5, ТС6
22	Список "Объекты доступа 22"	ФФ5, ФФ6
23	Список "Объекты доступа 23"	ФФ5, ФФ6, ФФ7
24	Список "Объекты доступа 24"	ФФ5, ФФ6, ПО8, ФФ8, ПО9, ТС10, ПО10, ПО12, ПО13, ФФ13, ТС18, ТС23
25	Список "Объекты доступа 25"	ФФ5, ФФ6, ПО8, ФФ8, ПО9, ПО10, ПО12, ПО13, ФФ13
26	Список "Объекты доступа 26"	ФФ5, ФФ6, ПО8, ФФ8, ПО9, ПО10, ПО12, ПО13, ФФ13, ТС23
27	Список "Объекты доступа 27"	ФФ5, ФФ6, ФФ8, ФФ13
28	Список "Объекты доступа 28"	ФФ5, ФФ6, ТС19
29	Список "Объекты доступа 29"	ФФ7
30	Список "Объекты доступа 30"	ПО8, ПО9, ТС10, ПО10, ПО12, ПО13, ТС18
31	Список "Объекты доступа 31"	ПО8, ПО9, ПО10, ПО12, ПО13
32	Список "Объекты доступа 32"	ФФ8, ФФ9
33	Список "Объекты доступа 33"	ФФ8, ТС11, ФФ13, ТС20
34	Список "Объекты доступа 34"	ФФ8, ТС11, ФФ13, ТС20, ТС26
35	Список "Объекты доступа 35"	ФФ8, ФФ13
36	Список "Объекты доступа 36"	ТС10, ТС12
37	Список "Объекты доступа 37"	ТС11, ТС20
38	Список "Объекты доступа 38"	ТС13
39	Список "Объекты доступа 39"	ТС15
40	Список "Объекты доступа 40"	ТС16
41	Список "Объекты доступа 41"	ТС16, ТС17
42	Список "Объекты доступа 42"	ТС18
43	Список "Объекты доступа 43"	ТС18, ТС23

№ п/п	Название списка	Элементы списка
44	Список "Объекты доступа 44"	ТС19
45	Список "Объекты доступа 45"	ТС20
46	Список "Объекты доступа 46"	ТС20, ТС26
47	Список "Объекты доступа 47"	ТС21
48	Список "Объекты доступа 48"	ТС21, ТС22
49	Список "Объекты доступа 49"	ТС22
50	Список "Объекты доступа 50"	ТС23
51	Список "Объекты доступа 51"	ТС24
52	Список "Объекты доступа 52"	ТС26

Для разных объектов атак могут быть установлены схожие характеристики безопасности. В результате анализа характеристик безопасности и особенностей функционирования ИСПДн, характеристики безопасности сгруппированы в списки, которые представлены в таблице.

№ п/п	Название списка	Элементы списка
1	Список "Характеристики безопасности 1"	ХАР1
2	Список "Характеристики безопасности 2"	ХАР1, ХАР2
3	Список "Характеристики безопасности 3"	ХАР2
4	Список "Характеристики безопасности 4"	ХАР2, ХАР3
5	Список "Характеристики безопасности 5"	ХАР3

Разные субъекты могут пытаться осуществить схожие атаки и обладать схожими возможностями и навыками. В результате анализа характеристик субъектов атак и особенностей функционирования ИСПДн, субъекты атак сгруппированы в списки, которые представлены в таблице.

№ п/п	Название списка	Элементы списка
1	Список "Субъекты доступа 1"	СА0
2	Список "Субъекты доступа 2"	СА3
3	Список "Субъекты доступа 3"	СА3, СА4
4	Список "Субъекты доступа 4"	СА4
5	Список "Субъекты доступа 5"	СА5
6	Список "Субъекты доступа 6"	СА5, СА1085
7	Список "Субъекты доступа 7"	СА8
8	Список "Субъекты доступа 8"	СА13
9	Список "Субъекты доступа 9"	СА14
10	Список "Субъекты доступа 10"	СА15
11	Список "Субъекты доступа 11"	СА18
12	Список "Субъекты доступа 12"	СА1082
13	Список "Субъекты доступа 13"	СА1083
14	Список "Субъекты доступа 14"	СА1085
15	Список "Субъекты доступа 15"	СА1086
16	Список "Субъекты доступа 16"	СА1086, СА1088
17	Список "Субъекты доступа 17"	СА1087
18	Список "Субъекты доступа 18"	СА1088

Одна и та же информация может быть известна разным субъектам атак. В результате анализа информации, известной субъектам атак, и особенностей функционирования ИСПДн, сведения сгруппированы в списки, которые представлены в таблице.

№ п/п	Название списка	Элементы списка
1	Список "Информация 1"	ОИ0
2	Список "Информация 2"	ОИ1
3	Список "Информация 3"	ОИ1, ОИ3, ОИ4, ОИ8
4	Список "Информация 4"	ОИ1, ОИ4

Одни и те же средства проведения атак могут быть известны быть использованы разными субъектами атак. В результате анализа средств проведения атак, доступных субъектам атак, и особенностей функционирования ИСПДн, средства проведения атак сгруппированы в списки, которые представлены в таблице.

№ п/п	Название списка	Элементы списка
1	Список "Средства атаки 1"	СПА0
2	Список "Средства атаки 2"	СПА9, СПА10, СПА11, СПА12
3	Список "Средства атаки 3"	СПА9, СПА10, СПА12
4	Список "Средства атаки 4"	СПА10
5	Список "Средства атаки 5"	СПА10, СПА11
6	Список "Средства атаки 6"	СПА10, СПА12

Одни и те же каналы проведения атак могут быть использованы разными субъектами атак. В результате анализа каналов проведения атак, доступных субъектам атак, и особенностей функционирования ИСПДн, каналы проведения атак сгруппированы в списки, которые представлены в таблице.

№ п/п	Название списка	Элементы списка
1	Список "Каналы атак 1"	КА0
2	Список "Каналы атак 2"	КА13
3	Список "Каналы атак 3"	КА13, КА14, КА15
4	Список "Каналы атак 4"	КА13, КА14, КА15, КА16, КА17, КА18, КА19, КА20, КА21, КА22, КА23
5	Список "Каналы атак 5"	КА13, КА15, КА18, КА19, КА20, КА21, КА22
6	Список "Каналы атак 6"	КА13, КА18, КА20, КА21, КА22
7	Список "Каналы атак 7"	КА15, КА18, КА19, КА20, КА21, КА22

Списки угроз, возникающих под воздействием посторонних факторов:

№ п/п	Идентификатор	Фактор угрозы	Объект угрозы	Нарушаемая характеристика
1	ПФ 1	Факторы 3	Объекты доступа 2	Характеристики безопасности 5
2	ПФ 2	Факторы 8	Объекты доступа 21	Характеристики безопасности 2
3	ПФ 3	Факторы 6	Объекты доступа 36	Характеристики безопасности 3
4	ПФ 4	Факторы 2	Объекты доступа 38	Характеристики безопасности 5
5	ПФ 5	Факторы 10	Объекты доступа 4	Характеристики безопасности 3
6	ПФ 6	Факторы 9	Объекты доступа 41	Характеристики безопасности 1
7	ПФ 7	Факторы 13	Объекты доступа 40	Характеристики безопасности 5
8	ПФ 8	Факторы 12	Объекты доступа 44	Характеристики безопасности 1
9	ПФ 9	Факторы 16	Объекты доступа 46	Характеристики безопасности 5
10	ПФ 10	Факторы 18	Объекты доступа 47	Характеристики безопасности 1
11	ПФ 11	Факторы 8	Объекты доступа 49	Характеристики безопасности 1

№ п/п	Идентификатор	Фактор угрозы	Объект угрозы	Нарушаемая характеристика
12	ПФ 12	Факторы 14	Объекты доступа 5	Характеристики безопасности 3
13	ПФ 13	Факторы 4	Объекты доступа 51	Характеристики безопасности 5
14	ПФ 14	Факторы 15	Объекты доступа 13	Характеристики безопасности 4
15	ПФ 15	Факторы 11	Объекты доступа 6	Характеристики безопасности 5
16	ПФ 16	Факторы 7	Объекты доступа 10	Характеристики безопасности 1
17	ПФ 17	Факторы 10	Объекты доступа 11	Характеристики безопасности 1
18	ПФ 18	Факторы 17	Объекты доступа 23	Характеристики безопасности 3
19	ПФ 19	Факторы 17	Объекты доступа 29	Характеристики безопасности 5
20	ПФ 20	Факторы 1	Объекты доступа 32	Характеристики безопасности 4
21	ПФ 21	Факторы 10	Объекты доступа 15	Характеристики безопасности 5
22	ПФ 22	Факторы 7	Объекты доступа 9	Характеристики безопасности 5
23	ПФ 23	Факторы 5	Объекты доступа 14	Характеристики безопасности 4
24	ПФ 24	Факторы 14	Объекты доступа 14	Характеристики безопасности 5

Списки угроз, возникающих по вине нарушителя (атаки):

№ п/п	Идентификатор	Субъект	Объект	Информация	Канал	Средство	Нарушаемая характеристика
1	Атака 1	Субъекты доступа 1	Объекты доступа 16	Информация 1	Каналы атак 1	Средства атаки 1	Характеристики безопасности 1
2	Атака 2	Субъекты доступа 1	Объекты доступа 24	Информация 1	Каналы атак 1	Средства атаки 1	Характеристики безопасности 3
3	Атака 3	Субъекты доступа 1	Объекты доступа 34	Информация 1	Каналы атак 1	Средства атаки 1	Характеристики безопасности 5
4	Атака 4	Субъекты доступа 7	Объекты доступа 16	Информация 1	Каналы атак 2	Средства атаки 4	Характеристики безопасности 1
5	Атака 5	Субъекты доступа 7	Объекты доступа 24	Информация 1	Каналы атак 2	Средства атаки 4	Характеристики безопасности 3
6	Атака 6	Субъекты доступа 7	Объекты доступа 34	Информация 1	Каналы атак 2	Средства атаки 4	Характеристики безопасности 5
7	Атака 7	Субъекты доступа 6	Объекты доступа 27	Информация 1	Каналы атак 3	Средства атаки 6	Характеристики безопасности 2
8	Атака 8	Субъекты доступа 6	Объекты доступа 35	Информация 1	Каналы атак 3	Средства атаки 6	Характеристики безопасности 5
9	Атака 9	Субъекты доступа 5	Объекты доступа 19	Информация 1	Каналы атак 3	Средства атаки 6	Характеристики безопасности 1
10	Атака 10	Субъекты доступа 5	Объекты доступа 31	Информация 1	Каналы атак 3	Средства атаки 6	Характеристики безопасности 3
11	Атака 11	Субъекты доступа 5	Объекты доступа 38	Информация 1	Каналы атак 3	Средства атаки 6	Характеристики безопасности 5
12	Атака 12	Субъекты доступа 10	Объекты доступа 48	Информация 4	Каналы атак 5	Средства атаки 2	Характеристики безопасности 1
13	Атака 13	Субъекты доступа 10	Объекты доступа 43	Информация 4	Каналы атак 5	Средства атаки 2	Характеристики безопасности 3
14	Атака 14	Субъекты доступа	Объекты доступа	Информация 4	Каналы атак 5	Средства атаки 2	Характеристики безопасности 5

№ п/п	Идентификатор	Субъект	Объект	Информация	Канал	Средство	Нарушаемая характеристика
		10	46				
15	Атака 15	Субъекты доступа 9	Объекты доступа 16	Информация 1	Каналы атак 7	Средства атаки 5	Характеристики безопасности 1
16	Атака 16	Субъекты доступа 9	Объекты доступа 26	Информация 1	Каналы атак 7	Средства атаки 5	Характеристики безопасности 3
17	Атака 17	Субъекты доступа 9	Объекты доступа 34	Информация 1	Каналы атак 7	Средства атаки 5	Характеристики безопасности 5
18	Атака 18	Субъекты доступа 14	Объекты доступа 18	Информация 1	Каналы атак 3	Средства атаки 6	Характеристики безопасности 1
19	Атака 19	Субъекты доступа 14	Объекты доступа 30	Информация 1	Каналы атак 3	Средства атаки 6	Характеристики безопасности 3
20	Атака 20	Субъекты доступа 14	Объекты доступа 37	Информация 1	Каналы атак 3	Средства атаки 6	Характеристики безопасности 5
21	Атака 21	Субъекты доступа 12	Объекты доступа 48	Информация 1	Каналы атак 4	Средства атаки 3	Характеристики безопасности 1
22	Атака 22	Субъекты доступа 12	Объекты доступа 50	Информация 1	Каналы атак 4	Средства атаки 3	Характеристики безопасности 3
23	Атака 23	Субъекты доступа 12	Объекты доступа 52	Информация 1	Каналы атак 4	Средства атаки 3	Характеристики безопасности 5
24	Атака 24	Субъекты доступа 13	Объекты доступа 48	Информация 4	Каналы атак 4	Средства атаки 2	Характеристики безопасности 1
25	Атака 25	Субъекты доступа 13	Объекты доступа 42	Информация 4	Каналы атак 4	Средства атаки 2	Характеристики безопасности 3
26	Атака 26	Субъекты доступа 13	Объекты доступа 45	Информация 4	Каналы атак 4	Средства атаки 2	Характеристики безопасности 5
27	Атака 27	Субъекты доступа 17	Объекты доступа 39	Информация 4	Каналы атак 4	Средства атаки 2	Характеристики безопасности 3
28	Атака 28	Субъекты доступа 15	Объекты доступа 17	Информация 4	Каналы атак 4	Средства атаки 2	Характеристики безопасности 1
29	Атака 29	Субъекты доступа 15	Объекты доступа 7	Информация 4	Каналы атак 4	Средства атаки 2	Характеристики безопасности 3
30	Атака 30	Субъекты доступа 15	Объекты доступа 8	Информация 4	Каналы атак 4	Средства атаки 2	Характеристики безопасности 5
31	Атака 31	Субъекты доступа 16	Объекты доступа 28	Информация 4	Каналы атак 4	Средства атаки 2	Характеристики безопасности 1
32	Атака 32	Субъекты доступа 16	Объекты доступа 22	Информация 4	Каналы атак 4	Средства атаки 2	Характеристики безопасности 3
33	Атака 33	Субъекты доступа 16	Объекты доступа 44	Информация 4	Каналы атак 4	Средства атаки 2	Характеристики безопасности 5
34	Атака 34	Субъекты доступа	Объекты доступа	Информация 4	Каналы атак 4	Средства атаки 2	Характеристики безопасности 1

№ п/п	Идентификатор	Субъект	Объект	Информация	Канал	Средство	Нарушаемая характеристика
		18	12				
35	Атака 35	Субъекты доступа 18	Объекты доступа 3	Информация 4	Каналы атак 4	Средства атаки 2	Характеристики безопасности 3
36	Атака 36	Субъекты доступа 18	Объекты доступа 1	Информация 4	Каналы атак 4	Средства атаки 2	Характеристики безопасности 5
37	Атака 37	Субъекты доступа 8	Объекты доступа 49	Информация 2	Каналы атак 2	Средства атаки 5	Характеристики безопасности 1
38	Атака 38	Субъекты доступа 3	Объекты доступа 27	Информация 1	Каналы атак 4	Средства атаки 3	Характеристики безопасности 2
39	Атака 39	Субъекты доступа 3	Объекты доступа 35	Информация 1	Каналы атак 4	Средства атаки 3	Характеристики безопасности 5
40	Атака 40	Субъекты доступа 4	Объекты доступа 19	Информация 1	Каналы атак 4	Средства атаки 3	Характеристики безопасности 1
41	Атака 41	Субъекты доступа 4	Объекты доступа 31	Информация 1	Каналы атак 4	Средства атаки 3	Характеристики безопасности 3
42	Атака 42	Субъекты доступа 4	Объекты доступа 38	Информация 1	Каналы атак 4	Средства атаки 3	Характеристики безопасности 5
43	Атака 43	Субъекты доступа 2	Объекты доступа 20	Информация 1	Каналы атак 4	Средства атаки 3	Характеристики безопасности 1
44	Атака 44	Субъекты доступа 2	Объекты доступа 30	Информация 1	Каналы атак 4	Средства атаки 3	Характеристики безопасности 3
45	Атака 45	Субъекты доступа 11	Объекты доступа 16	Информация 3	Каналы атак 6	Средства атаки 5	Характеристики безопасности 1
46	Атака 46	Субъекты доступа 11	Объекты доступа 25	Информация 3	Каналы атак 6	Средства атаки 5	Характеристики безопасности 3
47	Атака 47	Субъекты доступа 11	Объекты доступа 33	Информация 3	Каналы атак 6	Средства атаки 5	Характеристики безопасности 5